

COMMITTEE DRAFT		Reference document: SC 27 N19510	
ISO/IEC 3 rd CD 18045 (revision)			
Date: 2019-08-13		Supersedes document N18808	
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.			
ISO/IEC JTC 1/SC 27 Information security – cybersecurity and privacy protection Secretariat: Germany	Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: 2019-10-08 Please submit your comments via the online balloting application by the due date indicated.		
ISO/IEC 3 rd CD 18045 (revision)			
Title: IT security techniques — Evaluation criteria for IT security — Methodology for IT security evaluation			
Project: 1.27.36 (ISO/IEC 18045, revision)			
Explanatory Report			
Status	SC 27 Decision	Reference documents	
		Input	Output
For details regarding previous development stages refer to the 2 nd page of this explanatory report.			
ISO/IEC NP 18045 1 st WD	54th WG 3 meeting, April 2017, Recommendations 5,10 11, 14 (N17041 = WG 3 N1413).	SoV (N17030).	Liaisons to: CCDB (WG 3 N1391); The Open Group (WG 3 N1394); ISO/TC 22/SC 32 (N17373); Text f. 1st WD (WG 3 N1440).
ISO/IEC 18045 2 nd WD	55th WG 3 meeting, October / November 2017, Recommendations 8, 10, 15 (N17666 = WG 3 N1494).	SoCom (WG 3 N1476); Draft DoC (WG 3 N1501).	Liaison to ISO/TC 22/SC 32/WG 11 (N18103); Status (WG 3 N1465); DoC (WG 3 N1462); Text f. 2 nd WD (WG 3 N1478).
ISO/IEC 18045 1 st CD	56th WG 3 meeting, April 2018, Recommendations 10, 12 / 30 th SC 27 Plenary, April 2018, Resolution 6 (N18710) (N18471 = WG 3 N1557).	SoCom (WG 3 N1536); Late Com (WG 3 N1567); Draft DoC (WG 3 N15).	DoC (WG 3 N1527); Text f. 1 st CD (N18705).
ISO/IEC 18045 2 nd CD	57th WG 3 meeting / CRM for WG 3 projects, Sep / Oct 2018, Recommendations 11, 14, 15 (N18820 = WG 3 N1610).	SoV (N18860).	Liaison to CCDB (WG 3 N1619); DoC (N18802); Text f. 2 nd CD (N18808).
ISO/IEC 18045 3 rd CD	59th WG 3 meeting / CRM for WG 3 projects, April 2019, Recommendations 12, 14, 17 (N19523 = WG 3 N1676).	SoV (N19436).	Liaison to CCDB (WG 3 N1680); DoC (N19504); Text f. 3 rd CD (N19510).
3 rd CD Consideration			
In accordance with Recommendation 14 (see SC 27 N19523 = WG 3 N1676) of the 58 th SC 27/WG 3 meeting held in Tel Aviv, Israel, 2019-04-01/05 the hereby attached document is being circulated for a 8-week 3 rd CD letter ballot closing by			
2019-10-08			
Medium: http://isotc.iso.org/livelink/livelink/open/jtc1sc27			
No. of pages: 2 + 426			

Explanatory Report (2 nd page)			
Status	SC 27 Decision	Reference documents	
		Input	Output
Study Period IT security testing, evaluation and assurance standards and techniques	51 st WG 3 meeting, Oct. 2015, Recommendations 5, 6 (N15594 = WG 3 N1251).		Terms of Reference (WG 5 N1258); 1 st /2 nd call f. contr. (WG 3 N1259 /1317)..
	52 nd WG 3 meeting, April 2016, Recommendation 5, 7 (N16026 = WG 3 N1296).	Expert contr. (WG 3 N1299, 1301).	3 rd call f. contr. (WG 3 N1377); Rapporteur's report (WG 3 N1320); Liaison to: PRIPARE (WG 5 N = N16266).
ISO/IEC NP 18045	53 rd WG 3 meeting, Oct. 2016, Recommendations 6, 15 (N16800 = WG 5 N600).	Expert contr. (WG 3 N1368, N1371, N1373).	SP report (WG 3 N1363); Call f. editor (WG 3 N1387 = N16886); Liaisons to: CCDB (WG 3 N1330); The Open Group (WG 3 N1332); Text f. NWIP (N16884).

i. ISO/IEC JTC 1/SC 27 N19510

ISO/IEC JTC 1/SC 27/WG 3 N1654

Date: 2018-12-24

ISO/IEC CD 18045:####(EN)

ISO/IEC JTC 1/SC 27 IT Security techniques

Secretariat: DIN

IT security techniques — Evaluation criteria for IT security — Methodology for IT security evaluation

Techniques de sécurité IT — Critères d'évaluation pour la sécurité des technologies de l'information — Méthodologie pour l'évaluation de sécurité TI

CD stage

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard

Document subtype:

Document stage: (30.20) Preparatory

Document language: E

19
20
21
22
23

24
25
26
27
28
29
30

31
32

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
copyright@iso.org
www.iso.org

33

Legal Notice:

The text for the legal notice agreed between ISO/IEC and the CCDB will be included here.

34	Contents		Page
35	1	Scope	1
36	2	Normative references	1
37	3	Terms and definitions	1
38	4	Symbols and abbreviated terms	1
39	5	Overview	2
40	5.1	Organisation of this International Standard	Error! Bookmark not defined.
41	6	Document Conventions	2
42	6.1	Terminology	2
43	6.2	Verb usage	2
44	6.3	General evaluation guidance	2
45	6.4	Relationship between ISO/IEC 15408 and ISO/IEC 18045 structures	3
46	7	Evaluation process and related tasks	3
47	7.1	Introduction	3
48	7.2	Evaluation process overview	4
49	7.2.1	Objectives	4
50	7.2.2	Responsibilities of the roles	4
51	7.2.3	Relationship of roles	4
52	7.2.4	General evaluation model	4
53	7.2.5	Evaluator verdicts	5
54	7.3	Evaluation input task	7
55	7.3.1	Objectives	7
56	7.3.2	Application notes	7
57	7.3.3	Management of evaluation evidence sub-task	8
58	7.4	Evaluation sub-activities	8
59	7.5	Evaluation output task	8
60	7.5.1	Objectives	8
61	7.5.2	Management of evaluation outputs	9
62	7.5.3	Application notes	9
63	7.5.4	Write OR sub-task	9
64	7.5.5	Write ETR sub-task	10
65	8	Class APE: Protection Profile evaluation	16
66	8.1	Introduction	16
67	8.2	Application notes	Error! Bookmark not defined.
68	8.2.1	Re-using the evaluation results of certified PPs	16
69	8.3	PP introduction (APE_INT)	16
70	8.3.1	Evaluation of sub-activity (APE_INT.1)	16
71	8.4	Conformance claims (APE_CCL)	18
72	8.4.1	Evaluation of sub-activity (APE_CCL.1)	18
73	8.5	Security problem definition (APE_SPD)	28
74	8.5.1	Evaluation of sub-activity (APE_SPD.1)	28
75	8.6	Security objectives (APE_OBJ)	29
76	8.6.1	Evaluation of sub-activity (APE_OBJ.1)	29
77	8.6.2	Evaluation of sub-activity (APE_OBJ.2)	30
78	8.7	Extended components definition (APE_ECD)	32
79	8.7.1	Evaluation of sub-activity (APE_ECD.1)	32
80	8.8	Security requirements (APE_REQ)	37
81	8.8.1	Evaluation of sub-activity (APE_REQ.1)	37
82	8.8.2	Evaluation of sub-activity (APE_REQ.2)	43
83	9	Class ACE: Protection Profile Configuration evaluation	48

84	9.1	Introduction	48
85	9.2	PP-Module introduction (ACE_INT)	49
86	9.2.1	Evaluation of sub-activity (ACE_INT.1)	49
87	9.3	PP-Module conformance claims (ACE_CCL)	50
88	9.3.1	Evaluation of sub-activity (ACE_CCL.1)	50
89	9.4	PP-Module Security problem definition (ACE_SPD)	53
90	9.4.1	Evaluation of sub-activity (ACE_SPD.1)	Error! Bookmark not defined.
91	9.5	PP-Module Security objectives (ACE_OBJ)	54
92	9.5.1	Evaluation of sub-activity (ACE_OBJ.1)	54
93	9.5.2	Evaluation of sub-activity (ACE_OBJ.2)	55
94	9.6	PP-Module extended components definition (ACE_ECD)	55
95	9.6.1	Evaluation of sub-activity (ACE_ECD.1)	55
96	9.7	PP-Module security requirements (ACE_REQ)	55
97	9.7.1	Evaluation of sub-activity (ACE_REQ.1)	55
98	9.7.2	Evaluation of sub-activity (ACE_REQ.1)	55
99	9.8	PP-Module consistency (ACE_MCO)	55
100	9.8.1	Evaluation of sub-activity (ACE_MCO.1)	55
101	9.9	PP-Configuration consistency (ACE_CCO)	57
102	9.9.1	Evaluation of sub-activity (ACE_CCO.1)	57
103	10	Class ASE: Security Target evaluation	60
104	10.1	Introduction	60
105	10.2	Application notes	60
106	10.2.1	Re-using the evaluation results of certified PPs	60
107	10.3	ST introduction (ASE_INT)	61
108	10.3.1	Evaluation of sub-activity (ASE_INT.1)	61
109	10.4	Conformance claims (ASE_CCL)	64
110	10.4.1	Evaluation of sub-activity (ASE_CCL.1)	64
111	10.5	Security problem definition (ASE_SPD)	77
112	10.5.1	Evaluation of sub-activity (ASE_SPD.1)	77
113	10.6	Security objectives (ASE_OBJ)	78
114	10.6.1	Evaluation of sub-activity (ASE_OBJ.1)	78
115	10.6.2	Evaluation of sub-activity (ASE_OBJ.2)	78
116	10.7	Extended components definition (ASE_ECD)	81
117	10.7.1	Evaluation of sub-activity (ASE_ECD.1)	81
118	10.8	Security requirements (ASE_REQ)	85
119	10.8.1	Evaluation of sub-activity (ASE_REQ.1)	85
120	10.8.2	Evaluation of sub-activity (ASE_REQ.2)	92
121	10.9	TOE summary specification (ASE_TSS)	97
122	10.9.1	Evaluation of sub-activity (ASE_TSS.1)	97
123	10.9.2	Evaluation of sub-activity (ASE_TSS.2)	97
124	10.10	Consistency of composite product Security Target (ASE_COMP)	99
125	10.10.1	Evaluation of sub-activity (ASE_COMP.1)	99
126	11	Class ADV: Development	105
127	11.1	Introduction	105
128	11.2	Application notes	105
129	11.3	Security Architecture (ADV_ARC)	106
130	11.3.1	Evaluation of sub-activity (ADV_ARC.1)	106
131	11.4	Functional specification (ADV_FSP)	110
132	11.4.1	Evaluation of sub-activity (ADV_FSP.1)	110
133	11.4.2	Evaluation of sub-activity (ADV_FSP.2)	114
134	11.4.3	Evaluation of sub-activity (ADV_FSP.3)	118
135	11.4.4	Evaluation of sub-activity (ADV_FSP.4)	124
136	11.4.5	Evaluation of sub-activity (ADV_FSP.5)	129
137	11.4.6	Evaluation of sub-activity (ADV_FSP.6)	135
138	11.5	Implementation representation (ADV_IMP)	135
139	11.5.1	Evaluation of sub-activity (ADV_IMP.1)	135
140	11.5.2	Evaluation of sub-activity (ADV_IMP.2)	138
141	11.6	TSF internals (ADV_INT)	141
142	11.6.1	Evaluation of sub-activity (ADV_INT.1)	141

143	11.6.2	Evaluation of sub-activity (ADV_INT.2).....	143
144	11.6.3	Evaluation of sub-activity (ADV_INT.3).....	145
145	11.7	Security policy modelling (ADV_SPM).....	148
146	11.7.1	Evaluation of sub-activity (ADV_SPM.1).....	148
147	11.8	TOE design (ADV_TDS).....	153
148	11.8.1	Evaluation of sub-activity (ADV_TDS.1).....	153
149	11.8.2	Evaluation of sub-activity (ADV_TDS.2).....	157
150	11.8.3	Evaluation of sub-activity (ADV_TDS.3).....	162
151	11.8.4	Evaluation of sub-activity (ADV_TDS.4).....	171
152	11.8.5	Evaluation of sub-activity (ADV_TDS.5).....	181
153	11.8.6	Evaluation of sub-activity (ADV_TDS.6).....	188
154	11.9	Composite design compliance (ADV_COMP).....	189
155	11.9.1	Evaluation of sub-activity (ADV_COMP.1).....	189
156	12	Class AGD: Guidance documents.....	191
157	12.1	Introduction.....	191
158	12.2	Application notes.....	191
159	12.3	Operational user guidance (AGD_OPE).....	191
160	12.3.1	Evaluation of sub-activity (AGD_OPE.1).....	191
161	12.4	Preparative procedures (AGD_PRE).....	194
162	12.4.1	Evaluation of sub-activity (AGD_PRE.1).....	194
163	13	Class ALC: Life-cycle support.....	196
164	13.1	Introduction.....	196
165	13.2	CM capabilities (ALC_CMC).....	197
166	13.2.1	Evaluation of sub-activity (ALC_CMC.1).....	197
167	13.2.2	Evaluation of sub-activity (ALC_CMC.2).....	198
168	13.2.3	Evaluation of sub-activity (ALC_CMC.3).....	200
169	13.2.4	Evaluation of sub-activity (ALC_CMC.4).....	204
170	13.2.5	Evaluation of sub-activity (ALC_CMC.5).....	210
171	13.3	CM scope (ALC_CMS).....	217
172	13.3.1	Evaluation of sub-activity (ALC_CMS.1).....	217
173	13.3.2	Evaluation of sub-activity (ALC_CMS.2).....	218
174	13.3.3	Evaluation of sub-activity (ALC_CMS.3).....	219
175	13.3.4	Evaluation of sub-activity (ALC_CMS.4).....	220
176	13.3.5	Evaluation of sub-activity (ALC_CMS.5).....	221
177	13.4	Delivery (ALC_DEL).....	222
178	13.4.1	Evaluation of sub-activity (ALC_DEL.1).....	222
179	13.5	Development security (ALC_DVS).....	224
180	13.5.1	Evaluation of sub-activity (ALC_DVS.1).....	224
181	13.5.2	Evaluation of sub-activity (ALC_DVS.2).....	227
182	13.6	Flaw remediation (ALC_FLR).....	230
183	13.6.1	Evaluation of sub-activity (ALC_FLR.1).....	230
184	13.6.2	Evaluation of sub-activity (ALC_FLR.2).....	232
185	13.6.3	Evaluation of sub-activity (ALC_FLR.3).....	236
186	13.7	Life-cycle definition (ALC_LCD).....	241
187	13.7.1	Evaluation of sub-activity (ALC_LCD.1).....	241
188	13.7.2	Evaluation of sub-activity (ALC_LCD.2).....	242
189	13.8	TOE Development Artifacts (ALC_TDA).....	244
190	13.8.1	Evaluation of sub-activity (ALC_TDA.1).....	244
191	13.9	Tools and techniques (ALC_TAT).....	255
192	13.9.1	Evaluation of sub-activity (ALC_TAT.1).....	255
193	13.9.2	Evaluation of sub-activity (ALC_TAT.2).....	257
194	13.9.3	Evaluation of sub-activity (ALC_TAT.3).....	260
195	13.10	Integration of composition parts and consistency check of delivery procedures (ALC_COMP).....	263
196	13.10.1	Evaluation of sub-activity (ALC_COMP.1).....	264
197	14	Class ATE: Tests.....	265
198	14.1	Introduction.....	265
199	14.2	Application notes.....	265
200	14.2.1	Understanding the expected behaviour of the TOE.....	266

201	14.2.2	Testing vs. alternate approaches to verify the expected behaviour of functionality.....	266
202	14.2.3	Verifying the adequacy of tests	266
203	14.3	Coverage (ATE_COV)	267
204	14.3.1	Evaluation of sub-activity (ATE_COV.1).....	267
205	14.3.2	Evaluation of sub-activity (ATE_COV.2).....	268
206	14.3.3	Evaluation of sub-activity (ATE_COV.3).....	269
207	14.4	Depth (ATE_DPT)	271
208	14.4.1	Evaluation of sub-activity (ATE_DPT.1)	271
209	14.4.2	Evaluation of sub-activity (ATE_DPT.2)	274
210	14.4.3	Evaluation of sub-activity (ATE_DPT.3)	277
211	14.4.4	Evaluation of sub-activity (ATE_DPT.4)	279
212	14.5	Functional tests (ATE_FUN)	279
213	14.5.1	Evaluation of sub-activity (ATE_FUN.1).....	279
214	14.5.2	Evaluation of sub-activity (ATE_FUN.2).....	282
215	14.6	Independent testing (ATE_IND)	286
216	14.6.1	Evaluation of sub-activity (ATE_IND.1)	286
217	14.6.2	Evaluation of sub-activity (ATE_IND.2)	291
218	14.6.3	Evaluation of sub-activity (ATE_IND.3)	296
219	14.7	Composite functional testing (ATE_COMP)	296
220	14.7.1	Evaluation of sub-activity (ATE_COMP.1)	297
221	15	Class AVA: Vulnerability assessment	298
222	15.1	Introduction	298
223	15.1.1	Evaluation of sub-activity (AVA_VAN.1)	298
224	15.1.2	Evaluation of sub-activity (AVA_VAN.2)	303
225	15.1.3	Evaluation of sub-activity (AVA_VAN.3)	310
226	15.1.4	Evaluation of sub-activity (AVA_VAN.4)	319
227	15.1.5	Evaluation of sub-activity (AVA_VAN.5)	328
228	15.2	Composite vulnerability assessment (AVA_COMP).....	336
229	15.2.1	Evaluation of sub-activity (AVA_COMP.1).....	336
230	16	Class ACO: Composition.....	337
231	16.1	Introduction	337
232	16.2	Application notes.....	337
233	16.3	Composition rationale (ACO_COR).....	338
234	16.3.1	Evaluation of sub-activity (ACO_COR.1)	338
235	16.4	Development evidence (ACO_DEV)	345
236	16.4.1	Evaluation of sub-activity (ACO_DEV.1)	345
237	16.4.2	Evaluation of sub-activity (ACO_DEV.2)	346
238	16.4.3	Evaluation of sub-activity (ACO_DEV.3)	348
239	16.5	Reliance of dependent component (ACO_REL)	351
240	16.5.1	Evaluation of sub-activity (ACO_REL.1)	351
241	16.5.2	Evaluation of sub-activity (ACO_REL.2)	353
242	16.6	Composed TOE testing (ACO_CTT)	356
243	16.6.1	Evaluation of sub-activity (ACO_CTT.1).....	356
244	16.6.2	Evaluation of sub-activity (ACO_CTT.2)	359
245	16.7	Composition vulnerability analysis (ACO_VUL)	362
246	16.7.1	Evaluation of sub-activity (ACO_VUL.1)	362
247	16.7.2	Evaluation of sub-activity (ACO_VUL.2)	365
248	16.7.3	Evaluation of sub-activity (ACO_VUL.3)	369
249	Annex A	(informative) General evaluation guidance	374
250	A.1	Objectives	374
251	A.2	Sampling	374
252	A.3	Dependencies.....	376
253	A.3.1	Dependencies between activities	376
254	A.3.2	Dependencies between sub-activities	376
255	A.3.3	Dependencies between actions.....	377
256	A.4	Site Visits	377
257	A.4.1	Introduction	377
258	A.4.2	General Approach.....	377
259	A.4.3	Orientation Guide for the Preparation of the Check List	378

260	A.4.4	Example of a checklist	380
261	A.5	Scheme Responsibilities	382
262	Annex B	(informative) Vulnerability Assessment (AVA)	384
263	B.1	What is Vulnerability Analysis	384
264	B.2	Evaluator construction of a Vulnerability Analysis	385
265	B.2.1	Generic vulnerability guidance	385
266	B.2.2	Identification of Potential Vulnerabilities	393
267	B.3	When attack potential is used	396
268	B.3.1	Developer	396
269	B.3.2	Evaluator	397
270	B.4	Calculating attack potential	398
271	B.4.1	Application of attack potential	398
272	B.4.2	Characterising attack potential	399
273	B.5	Example calculation for direct attack	405
274	Annex C	Evaluation Techniques and Tools (informative)	407
275	C.1	Semiformal and formal methods	407
276	C.1.1	Description of styles	407
277	C.1.2	Security policy models and styles	411
278			

Editor Note

Experts in SC27/WG3 agree with the editors that, since this document needs to reflect the evaluation requirements arising from the various parts of ISO/IEC 15408 the CD for which have only just been completed, it is inevitable that the 18045 draft will lag behind the 15408 parts and that some editing will be needed when the other parts are complete.

The aim expressed at WG3 meetings is to have the whole set of documents clearly and comfortably support the co-existence of the different ways of using the criteria for evaluations. In particular the document set should support without conflict, contradiction, or interference, ways of providing assurance that accommodate both detailed specification with transparent, conformance checking (generally the iTC/cPP route), and also the investigative, judgement-based examination. Evaluations generally combine both approaches to different extents, and different balances are currently preferred by different groups of users and schemes.

This document is intended to meet that aim.

Notes for CD1

A new element ACE_CCO.1.6C has been added in this version of 18045 (in order to more clearly specify the requirement for its related work units – previously these were attached to ACE_CCO.1.3C but the connection was not clear or convincing). This new element therefore needs to be added to 15408-3.

Optional SFRs have been removed from 18045 (but will be replaced if discussion on other parts necessitates that step)

Note

ISO/IEC 15408-3 CD1 needs to reflect the updated ASE_REQ.1.9C

The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) counter all threats for the TOE.

Edits have introduced a new ACE_CCO.1.6C and then renumbered ACE_CCO.1-3a and ACE_CCO.1-3b as ACE_CCO.1-6 and ACE_CCO.1-7 as its work units. This means that the old ACE_CCO.1-6 is now renumbered as ACE_CCO.1-8.

This requires a future update to part 3 to introduce ACE_CCO.1.6C.

APE_CCL.1.13C addresses only the identification of allowed PP-modules whereas the related Work Unit APE_CCL.1-17 covers more, i.e. subject PP's conformance statement / aspect 'allowed with' other base-PPs.

ISO/IEC CD3 18045:20XX (E)

~~~~This seems to be a mismatch, i.e. in APE\_CCL.1.13C the goal and content of Work Unit APE\_CCL.1-17 is not covered. – expert text awaited

Clarification to what a PP may claim conformance. Corresponding update of ISO/IEC 15408-1, ISO/IEC 15408-3 and / or ISO/IEC 18045. – deferred to incorporate updates

Check as proposed the new subchapters for AVA\_VAN.5, ADV\_SPM.1, ADV\_TDS.5, ADV\_IMP.2, ADV\_INT.3, ATE\_COV.3 and ATE\_FUN.2 for consistency to ISO/IEC 15408-1, ISO/IEC 15408-3 and ISO/IEC 18045 (for the latter one check against the other already existing subchapters in AVA, ADV and ATE). Corresponding update of the subchapters where necessary. – expert check awaited (from authors of AIS 34 in particular)

### Notes for CD2

As in comment 003 on CD1 the action elements regarding ASE\_COMP, ALC\_COMP, ADV\_COMP, ATE\_COMP, AVA\_COMP implemented from Appendix 1.1 of [JIL Composite product evaluation for Smart Cards and similar devices] (version 1.5.1 May 2018) were incorporated. The structure of that appendix was kept broadly the same. Certification specific items were omitted. This section needs a close check by relevant experts.

There were also a number of changes that could not be made without reference to CD2 versions of other parts and will need to be incorporated in the next round of editing actions. Appropriate detailed comment/changes are invited.

**Deleted: ATE\_MTK, ATE\_MTT, ADV\_MTC\_ASE\_AMA**

**Added: ACE\_OBJ.2, ACE\_REQ.2, ASE\_COMP, ADV\_COMP, ALC\_TDA, ALC\_COMP, ATE\_COMP, AVA\_COMP**

**Re-located: ASE\_COMP, ADV\_COMP, ALC\_TDA, ALC\_COMP, ATE\_COMP, AVA\_COMP (to sync up with 15408-3)**

**Need additional contribution or text: ALC\_TDA, ALC\_COMP, ATE\_COMP**

**Resolve the existing cross-reference label issue with TOE design (ADV\_TDS), Independent testing (ATE\_IND), Depth (ATE\_DPT), Class ACO: Composition, TSF internals (ADV\_INT)**

### **December 24 update**

- Item 1) Updated to sync up with the 15408-3 (complete for the part of the class most done but need remaining few chapters such as APE, ACE, ALC, ATE, AVA, ACO)

- Item 2) Resolved the existing cross-reference label issue with TOE design (ADV\_TDS), Independent testing (ATE\_IND), Depth (ATE\_DPT), Class ACO: Composition, TSF internals (ADV\_INT)

- Item 3) Reformatting the \*\_COMP

### Notes for CD3

This version has addressed the majority of comments although in some cases no input text was supplied. For a few of the comments the location of the errors could not be found (e.g. 'Missing period at the end of sentence' where the line referenced appeared not to show this) The editors generated their own text to address some of the comments and significant input was helpfully provided by some of the editors of 15408. In the incorporation of those however the overall fragility of the 18045 document was highlighted as the document became unusable. Following advice from other editors the document, which had a multiplicity of styles, was simplified to a very small number of styles and the use of inter and intra document references removed. This has left a more robust document but it still suffers from a tendency to renumber all lists consecutively when significant changes get made. The lists have been reset by hand and should be correct. However, as part of the simplification of styles only 3 list types are now defined (letter, number, and bulleted) and this means that the indentation of sub lists is not always as might be expected. This need not be commented upon since, as helpfully explained by the ISO editor at the Tel Aviv meeting, the existing formatting gets stripped out and consistent new formatting incorporated when the document is moved into a publication state.

Also during the briefing about ISO formatting rules the WG3 experts noted that 18045 used more sub-heading levels than permitted. The 18045 editors have addressed this in the area where this was present by converting the lowest level subheadings into a table format (Table 1 in ACO\_COR.1-3).

362

363  
364  
365  
366

The removal of cross references improved the robustness of the document but could lead to a slight risk of having incorrect references – this will be addressed by automated checking and should any errors be found these will be included in the comments, as will outstanding comments where suitable text is still awaited.

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives)).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see [www.iso.org/patents](http://www.iso.org/patents)).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html).

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 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.commoncriteriaportal.org/cc/>

This fourth edition cancels and replaces the third edition (ISO/IEC 18045:-2009), which has been technically revised.

The main changes compared to the previous edition are as follows:

- The document has been revised to comply with ISO/IEC Directives
- Technical changes have been introduced:
- New security assurance components have been introduced

Commented [A1]: Needs updating

399 **Introduction**

400 The target audience for this International Standard is primarily evaluators applying ISO/IEC 15408:20xx and  
401 certifiers confirming evaluator actions; evaluation sponsors, developers, PP, PP-Module, PP-Configuration, and ST  
402 authors, and other parties interested in IT security, may be a secondary audience.

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

407



# IT security techniques — Evaluation criteria for IT securityInformation technology — Security techniques — Methodology for IT security evaluation

## 1 Scope

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

## 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 15408-1:20XX, *IT Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:20XX, *IT Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:20XX, *IT Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

## 3 Terms and definitions

For the purposes of this document, the terms, definitions, symbols and abbreviated terms given in ISO/IEC 15408-1 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

Terms and definitions previously located in this clause of 18045 are now found in ISO/IEC 15408

## 4 Symbols and abbreviated terms

For the purposes of this document, the terms, definitions, symbols and abbreviated terms given in ISO/IEC 15408-1 apply.

Symbols and abbreviations previously located in this clause of 18045 are now found in ISO/IEC 15408

## 5 Overview

Clause 6 defines the conventions used in this document.

Clause 7 describes general evaluation tasks with no verdicts associated with them as they do not map to ISO/IEC 15408 evaluator action elements.

Clauses 8 to 10 address the work necessary for reaching an evaluation result on a PP.

Clauses 10 to 16 define the evaluation activities, organised by Assurance Classes.

Annex A covers the basic evaluation techniques used to provide technical evidence of evaluation results.

Annex B provides an explanation of the Vulnerability Analysis criteria and examples of their application

## 6 Document Conventions

### 6.1 Terminology

Unlike ISO/IEC 15408, where each element maintains the last digit of its identifying symbol for all components within the family, this document may introduce new work units when an ISO/IEC 15408 evaluator action element changes from sub-activity to sub-activity; as a result, the last digit of the work unit's identifying symbol may change although the work unit remains unchanged.

Any methodology-specific evaluation work required that is not derived directly from ISO/IEC 15408 requirements is termed *task* or *sub-task*.

### 6.2 Verb usage

All work unit and sub-task verbs are preceded by the auxiliary verb *shall* and by presenting both the verb and the *shall* in ***bold italic*** type face. The auxiliary verb *shall* is used only when the provided text is mandatory and therefore only within the work units and sub-tasks. The work units and sub-tasks contain mandatory activities that the evaluator must perform in order to assign verdicts.

Guidance text accompanying work units and sub-tasks gives further explanation on how to apply ISO/IEC 15408 words in an evaluation. The verb usage is in accordance with ISO definitions for these verbs. The auxiliary verb *should* is used when the described method is strongly preferred. All other auxiliary verbs, including *may*, are used where the described method(s) is allowed but is neither recommended nor strongly preferred; it is merely explanation.

The verbs *check*, *examine*, *report* and *record* are used with a precise meaning within this part of this document and Clause 3 should be referenced for their definitions.

### 6.3 General evaluation guidance

Material that has applicability to more than one sub-activity is collected in one place. Guidance whose applicability is widespread (across activities and EALs) has been collected into Annex A. Guidance that pertains to multiple sub-activities within a single activity has been provided in the introduction to that activity. If guidance pertains to only a single sub-activity, it is presented within that sub-activity.



#### 6.4 Relationship between ISO/IEC 15408 and ISO/IEC 18045 structures

There are direct relationships between ISO/IEC 15408 structure (i.e. class, family, component and element) and the structure of this document. Figure 1 illustrates the correspondence between ISO/IEC 15408 constructs of class, family and evaluator action elements and evaluation methodology activities, sub-activities and actions. However, several evaluation methodology work units may result from the requirements noted in ISO/IEC 15408 developer action and content and presentation elements.

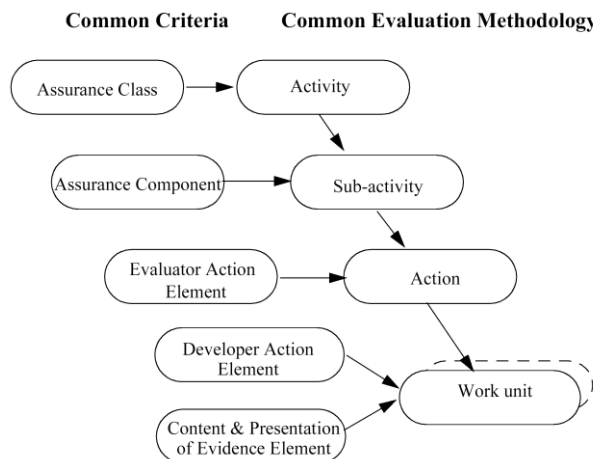


Figure 1 — Mapping of ISO/IEC 15408 and ISO/IEC 18045 structures

## 7 Evaluation process and related tasks

### 7.1 Introduction

This clause provides an overview of the evaluation process and defines the tasks an evaluator is intended to perform when conducting an evaluation.

Each evaluation, whether of a PP, PP-Configuration, or TOE (including ST), follows the same process, and has four evaluator tasks in common: the input task, the output task, the evaluation sub-activities, and the demonstration of the technical competence to the evaluation authority task.

The input task and the output tasks, which are related to management of evaluation evidence and to report generation, are entirely described in this clause. Each task has associated sub-tasks that apply to, and are normative for all ISO/IEC 15408 evaluations (evaluation of a PP or a TOE).

The evaluation sub-activities are only introduced in this clause, and fully described in the remainder of 7..

In contrast to the evaluation sub-activities, input and output tasks have no verdicts associated with them as they do not map to ISO/IEC 15408 evaluator action elements; they are performed in order to ensure conformance with the universal principles and to comply with this document.

The demonstration of the technical competence to the evaluation authority task may be fulfilled by the evaluation authority analysis of the output tasks results, or may include the demonstration by the evaluators of their understanding of the inputs for the evaluation sub-activities. This task has

## ISO/IEC 18045:2008(E)

no associated evaluator verdict, but has an evaluator authority verdict. The detailed criteria to pass this task are left to the discretion of the evaluation authority, as noted in Annex A.5.

Evaluation activities defined in conformance with ISO/IEC15408-4 may be used in place of work units defined within this document provided that this is made clear within the evaluation and certification reports.

## 7.2 Evaluation process overview

### 7.2.1 Objectives

This subclause presents the general model of the methodology and identifies:

- a) roles and responsibilities of the parties involved in the evaluation process;
- b) the general evaluation model.

### 7.2.2 Responsibilities of the roles

The general model defines the following roles: sponsor, developer, evaluator and evaluation authority.

The sponsor is responsible for requesting and supporting an evaluation. This means that the sponsor establishes the different agreements for the evaluation (e.g. commissioning the evaluation). Moreover, the sponsor is responsible for ensuring that the evaluator is provided with the evaluation evidence.

The developer produces the TOE and is responsible for providing the evidence required for the evaluation (e.g. training, design information), on behalf of the sponsor.

The evaluator performs the evaluation tasks required in the context of an evaluation: the evaluator receives the evaluation evidence from the developer on behalf of the sponsor or directly from the sponsor, performs the evaluation sub-activities and provides the results of the evaluation assessment to the evaluation authority.

The evaluation authority establishes and maintains the scheme, monitors the evaluation conducted by the evaluator, and issues certification/validation reports as well as certificates based on the evaluation results provided by the evaluator.

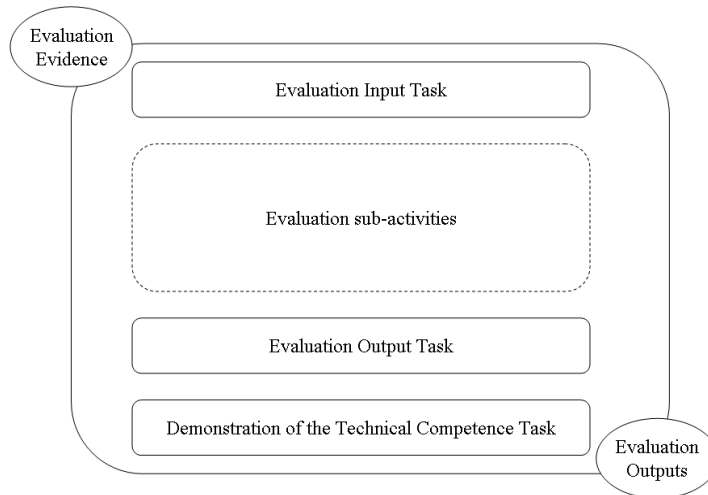
### 7.2.3 Relationship of roles

To prevent undue influence from improperly affecting an evaluation, some separation of roles is required. This implies that the roles described above are fulfilled by different entities, except that the roles of developer and sponsor may be satisfied by a single entity.

Moreover, some evaluations (e.g. EAL1 evaluation) may not require the developer to be involved in the project. In this case, it is the sponsor who provides the TOE to the evaluator and who generates the evaluation evidence.

### 7.2.4 General evaluation model

The evaluation process consists of the evaluator performing the evaluation input task, the evaluation output task and the evaluation sub-activities. Figure 2 provides an overview of the relationship between these tasks and sub-activities.

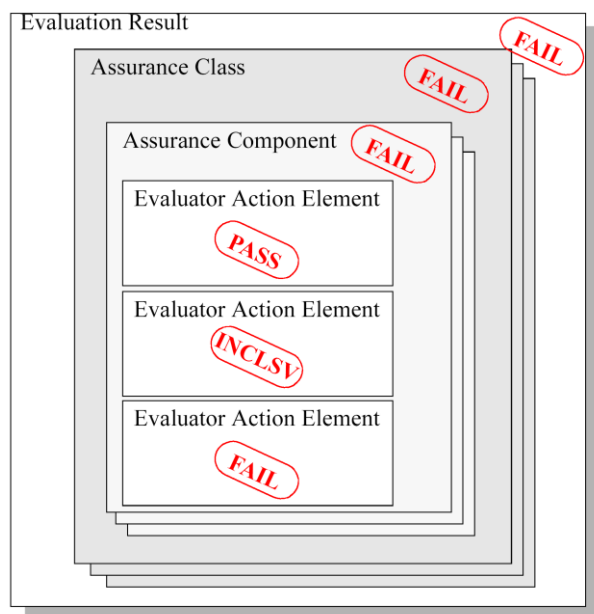


**Figure 2 — Generic evaluation model**

The evaluation process may be preceded by a preparation phase where initial contact is made between the sponsor and the evaluator. The work that is performed and the involvement of the different roles during this phase may vary. It is typically during this step that the evaluator performs a feasibility analysis to assess the likelihood of a successful evaluation.

#### 7.2.5 Evaluator verdicts

The evaluator assigns verdicts to the requirements of ISO/IEC 15408 and not to those of this document. The most granular ISO/IEC 15408 structure to which a verdict is assigned is the evaluator action element (explicit or implied). A verdict is assigned to an applicable ISO/IEC 15408 evaluator action element as a result of performing the corresponding evaluation methodology action and its constituent work units. Finally, an evaluation result is assigned, as described in ISO/IEC 15408-1:20xx, Clause 9, Evaluation results.



**Figure 3 — Example of the verdict assignment rule**

This document recognises three mutually exclusive verdict states:

- a) Conditions for a pass verdict are defined as an evaluator completion of ISO/IEC 15408 evaluator action element and determination that the requirements for the PP, ST or TOE under evaluation are met. The conditions for passing the element are defined as:
  - 1) the constituent work units of the related evaluation methodology action, and;
  - 2) all evaluation evidence required for performing these work units is coherent, that is it can be fully and completely understood by the evaluator, and
  - 3) all evaluation evidence required for performing these work units does not have any obvious internal inconsistencies or inconsistencies with other evaluation evidence. Note that obvious means here that the evaluator discovers this inconsistency while performing the work units: the evaluator should not undertake a full consistency analysis across the entire evaluation evidence every time a work unit is performed.
- b) Conditions for a *fail* verdict are defined as an evaluator completion of ISO/IEC 15408 evaluator action element and determination that the requirements for the PP, ST, or TOE under evaluation are not met, or that the evidence is incoherent, or an obvious inconsistency in the evaluation evidence has been found;
- c) All verdicts are initially *inconclusive* and remain so until either a *pass* or *fail* verdict is assigned.

The overall verdict is *pass* if and only if all the constituent verdicts are also *pass*. In the example illustrated in Figure 3, if the verdict for one evaluator action element is *fail* then the verdicts for the corresponding assurance component, assurance class, and overall verdict are also *fail*.

#### 7.2.6 Evaluation input task

#### 7.2.7 Objectives

The objective of this task is to ensure that the evaluator has available the correct version of the evaluation evidence necessary for the evaluation and that it is adequately protected. Otherwise, the technical accuracy of the evaluation cannot be assured, nor can it be assured that the evaluation is being conducted in a way to provide repeatable and reproducible results.

#### 7.2.8 Application notes

The responsibility to provide all the required evaluation evidence lies with the sponsor. However, most of the evaluation evidence is likely to be produced and supplied by the developer, on behalf of the sponsor.

Since the assurance requirements apply to the entire TOE, all evaluation evidence pertaining to all parts of the TOE is to be made available to the evaluator. The scope and required content of such evaluation evidence is independent of the level of control that the developer has over each of the parts of the TOE. For example, if design is required, then the TOE design (ADV\_TDS) requirements will apply to all subsystems that are part of the TSF. In addition, assurance requirements that call for procedures to be in place (for example, CM capabilities (ALC\_CMC) and Delivery (ALC\_DEL)) will also apply to the entire TOE (including any part produced by another developer).

It is recommended that the evaluator, in conjunction with the sponsor, produce an index to required evaluation evidence. This index may be a set of references to the documentation. This index should contain enough information (e.g. a brief summary of each document, or at least an explicit title, indication of the subclauses of interest) to help the evaluator to find easily the required evidence.

It is the information contained in the evaluation evidence that is required, not any particular document structure. Evaluation evidence for a sub-activity may be provided by separate documents, or a single document may satisfy several of the input requirements of a sub-activity.

The evaluator requires stable and formally-issued versions of evaluation evidence. However, draft evaluation evidence may be provided during an evaluation, for example, to help an evaluator make an early, informal assessment, but is not used as the basis for verdicts. It may be helpful for the evaluator to see draft versions of particular appropriate evaluation evidence, such as:

- a) test documentation, to allow the evaluator to make an early assessment of tests and test procedures;
- b) design documents, to provide the evaluator with background for understanding the TOE design;
- c) source code or hardware drawings, to allow the evaluator to assess the application of the developer's standards.

Draft evaluation evidence is more likely to be encountered where the evaluation of a TOE is performed concurrently with its development. However, it may also be encountered during the evaluation of an already-developed TOE where the developer has had to perform additional work to address a problem identified by the evaluator (e.g. to correct an error in design or implementation) or to provide evaluation evidence of security that is not provided in the existing

## ISO/IEC 18045:2008(E)

618 documentation (e.g. in the case of a TOE not originally developed to meet the requirements of  
619 ISO/IEC 15408).

### 620 7.2.9 Management of evaluation evidence sub-task

#### 621 7.2.9.1 Configuration control

622 The evaluator **shall perform** configuration control of the evaluation evidence.

623 ISO/IEC 15408 implies that the evaluator is able to identify and locate each item of evaluation  
624 evidence after it has been received and is able to determine whether a specific version of a  
625 document is in the evaluator's possession.

626 The evaluator **shall protect** the evaluation evidence from alteration or loss while it is in the  
627 evaluator's possession.

#### 628 7.2.9.2 Disposal

629 Schemes may wish to control the disposal of evaluation evidence at the conclusion of an evaluation.  
630 The disposal of the evaluation evidence should be achieved by one or more of:

631 a) returning the evaluation evidence;

632 b) archiving the evaluation evidence;

633 c) destroying the evaluation evidence.

#### 634 7.2.9.3 Confidentiality

635 An evaluator may have access to sponsor and developer commercially-sensitive information (e.g.  
636 TOE design information, specialist tools), and may have access to nationally-sensitive information  
637 during the course of an evaluation. Schemes may wish to impose requirements for the evaluator to  
638 maintain the confidentiality of the evaluation evidence. The sponsor and evaluator may mutually  
639 agree to additional requirements as long as these are consistent with the scheme.

640 Confidentiality requirements affect many aspects of evaluation work, including the receipt,  
641 handling, storage and disposal of evaluation evidence.

### 642 7.3 Evaluation sub-activities

643 The evaluation sub-activities vary depending on whether it is a PP or a TOE evaluation. Moreover,  
644 in the case of a TOE evaluation, the sub-activities depend upon the selected assurance  
645 requirements.

### 646 7.4 Evaluation output task

#### 647 7.4.1 Objectives

648 The objective of this subclause is to describe the Observation Report (OR) and the Evaluation  
649 Technical Report (ETR). Schemes may require additional evaluator reports such as reports on  
650 individual units of work, or may require additional information to be contained in the OR and the  
651 ETR. This document does not preclude the addition of information into these reports as this  
652 International Standard specifies only the minimum information content.

653 Consistent reporting of evaluation results facilitates the achievement of the universal principle of  
654 repeatability and reproducibility of results. The consistency covers the type and the amount of

information reported in the ETR and OR. The consistency of ETR and OR among different evaluations is the responsibility of the evaluation authority.

The evaluator performs the two following sub-tasks in order to meet the requirements of this document for the information content of reports:

a) write OR sub-task (if needed in the context of the evaluation);

b) write ETR sub-task.

#### 7.4.2 Management of evaluation outputs

The evaluator delivers the ETR to the evaluation authority, as well as any ORs as they become available. Requirements for controls on handling the ETR and ORs are established by the scheme which may include delivery to the sponsor or developer. The ETR and ORs may include sensitive or proprietary information and may need to be sanitised before they are given to the sponsor.

#### 7.4.3 Application notes

In this edition of this document, the requirements for the provision of evaluator evidence to support re-evaluation and re-use have not been explicitly stated. Where information for re-evaluation or re-use is required by the sponsor, the scheme under which the evaluation is being performed should be consulted.

#### 7.4.4 Write OR sub-task

ORs provide the evaluator with a mechanism to request a clarification (e.g. from the evaluation authority on the application of a requirement) or to identify a problem with an aspect of the evaluation.

In the case of a fail verdict, the evaluator **shall provide** an OR to reflect the evaluation result. Otherwise, the evaluator may use ORs as one way of expressing clarification needs.

For each OR, the evaluator **shall report** the following:

- a) the identifier of the PP or TOE evaluated;
- b) the evaluation task/sub-activity during which the observation was generated;
- c) the observation;
- d) the assessment of its severity (e.g. implies a fail verdict, holds up progress on the evaluation, requires a resolution prior to evaluation being completed);
- e) the identification of the organisation responsible for resolving the issue;
- f) the recommended timetable for resolution;
- g) the assessment of the impact on the evaluation of failure to resolve the observation.

The intended audience of an OR and procedures for handling the report depend on the nature of the report's content and on the scheme. Schemes may distinguish different types of ORs or define

## ISO/IEC 18045:2008(E)

688 additional types, with associated differences in required information and distribution (e.g.  
689 evaluation ORs to evaluation authorities and sponsors).

### 690 7.4.5 Write ETR sub-task

#### 691 7.4.5.1 Objectives

692 The evaluator **shall provide** an ETR to present technical justification of the verdicts.

693 This document defines the ETR's minimum content requirement; however, schemes may specify  
694 additional content and specific presentational and structural requirements. For instance, schemes  
695 may require that certain introductory material (e.g. disclaimers and copyright Clauses) be reported  
696 in the ETR.

697 The reader of the ETR is assumed to be familiar with general concepts of information security,  
698 ISO/IEC 15408, this document, evaluation approaches and IT.

699 The ETR supports the evaluation authority to confirm that the evaluation was done to the required  
700 standard, but it is anticipated that the documented results may not provide all of the necessary  
701 information, so additional information specifically requested by the scheme may be necessary. This  
702 aspect is outside the scope of this document.



7.4.5.2 ETR for a PP Evaluation

7.4.5.2.1 General

This Subclause describes the minimum content of the ETR for a PP evaluation. The contents of the ETR are portrayed in Figure 4; this figure may be used as a guide when constructing the structural outline of the ETR document.

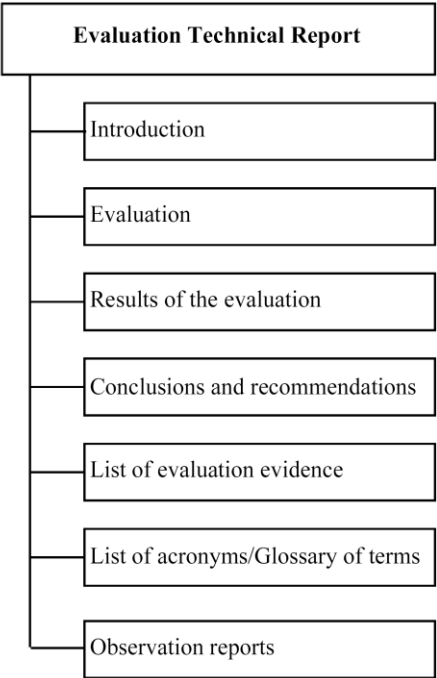


Figure 4 —ETR information content for a PP evaluation

7.4.5.2.2 Introduction

The evaluator **shall report** evaluation scheme identifiers.

Evaluation scheme identifiers (e.g. logos) are the information required to unambiguously identify the scheme responsible for the evaluation oversight.

The evaluator **shall report** ETR configuration control identifiers.

The ETR configuration control identifiers contain information that identifies the ETR (e.g. name, date and version number).

The evaluator **shall report** PP configuration control identifiers.

PP configuration control identifiers (e.g. name, date and version number) are required to identify what is being evaluated in order for the evaluation authority to verify that the verdicts have been assigned correctly by the evaluator.

## ISO/IEC 18045:2008(E)

- 721 The evaluator **shall report** the identity of the developer.
- 722 The identity of the PP developer is required to identify the party responsible for producing the PP.
- 723 The evaluator **shall report** the identity of the sponsor.
- 724 The identity of the sponsor is required to identify the party responsible for providing evaluation  
725 evidence to the evaluator.
- 726 The evaluator **shall report** the identity of the evaluator.
- 727 The identity of the evaluator is required to identify the party performing the evaluation and  
728 responsible for the evaluation verdicts.
- 729 **7.4.5.2.3 Evaluation**
- 730 The evaluator **shall report** the evaluation methods, techniques, tools and standards used.
- 731 The evaluator references the evaluation criteria, methodology and interpretations used to evaluate  
732 the PP.
- 733 The evaluator **shall report** any constraints on the evaluation, constraints on the handling of  
734 evaluation results and assumptions made during the evaluation that have an impact on the  
735 evaluation results.
- 736 The evaluator may include information in relation to legal or statutory aspects, organisation,  
737 confidentiality, etc.
- 738 **7.4.5.2.4 Results of the evaluation**
- 739 The evaluator **shall report** a verdict and a supporting rationale for each assurance component that  
740 constitutes an APE activity, as a result of performing the corresponding evaluation methodology  
741 action and its constituent work units.
- 742 The rationale justifies the verdict using ISO/IEC 15408, this document, any interpretations and the  
743 evaluation evidence examined and shows how the evaluation evidence does or does not meet each  
744 aspect of the criteria. It contains a description of the work performed, the method used, and any  
745 derivation of results. The rationale may provide detail to the level of an evaluation methodology  
746 work unit.
- 747 **7.4.5.2.5 Conclusions and recommendations**
- 748 The evaluator **shall report** the conclusions of the evaluation, in particular the overall verdict as  
749 defined in ISO/IEC 15408-1:20xx, Clause 12, Evaluation results, and determined by application of  
750 the verdict assignment described in 7.2.5.
- 751 The evaluator provides recommendations that may be useful for the evaluation authority. These  
752 recommendations may include shortcomings of the PP discovered during the evaluation or  
753 mention of features which are particularly useful.
- 754 **7.4.5.2.6 List of evaluation evidence**
- 755 The evaluator **shall report** for each item of evaluation evidence the following information:
- 756 • the issuing body (e.g. the developer, the sponsor);
- 757 • the title;

- the unique reference (e.g. issue date and version number).

**7.4.5.2.7 List of acronyms/Glossary of terms**

The evaluator **shall report** any acronyms or abbreviations used in the ETR.

Glossary definitions already defined by ISO/IEC 15408 or by this document need not be repeated in the ETR.

**7.4.5.2.8 Observation reports**

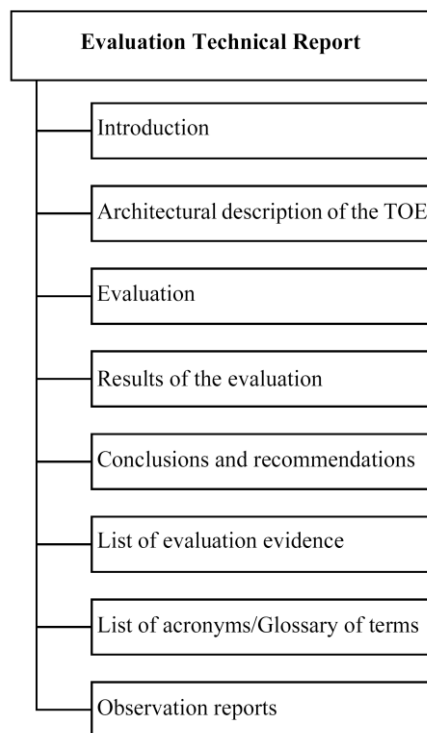
The evaluator **shall report** a complete list that uniquely identifies the ORs raised during the evaluation and their status.

For each OR, the list should contain its identifier as well as its title or a brief summary of its content.

**7.4.5.3 ETR for a TOE Evaluation**

**7.4.5.3.1 General**

This Subclause describes the minimum content of the ETR for a TOE evaluation. The contents of the ETR are portrayed in Figure 5; this figure may be used as a guide when constructing the structural outline of the ETR document.



**Figure 5 — ETR information content for a TOE evaluation**

774 **7.4.5.3.2 Introduction**

775 The evaluator **shall report** evaluation scheme identifiers.

776 Evaluation scheme identifiers (e.g. logos) are the information required to unambiguously identify  
777 the scheme responsible for the evaluation oversight.

778 The evaluator **shall report** ETR configuration control identifiers.

779 The ETR configuration control identifiers contain information that identifies the ETR (e.g. name,  
780 date and version number).

781 The evaluator **shall report** ST and TOE configuration control identifiers.

782 ST and TOE configuration control identifiers identify what is being evaluated in order for the  
783 evaluation authority to verify that the verdicts have been assigned correctly by the evaluator.

784 If the ST claims that the TOE conforms to the requirements of one or more PPs, the ETR shall  
785 report the reference of the corresponding PPs.

786 The PPs reference contains information that uniquely identifies the PPs (e.g. title, date, and version  
787 number).

788 The evaluator **shall report** the identity of the developer.

789 The identity of the TOE developer is required to identify the party responsible for producing the  
790 TOE.

791 The evaluator **shall report** the identity of the sponsor.

792 The identity of the sponsor is required to identify the party responsible for providing evaluation  
793 evidence to the evaluator.

794 The evaluator **shall report** the identity of the evaluator.

795 The identity of the evaluator is required to identify the party performing the evaluation and  
796 responsible for the evaluation verdicts.

797 **7.4.5.3.3 Architectural description of the TOE**

798 The evaluator **shall report** a high level description of the TOE and its major components based on  
799 the evaluation evidence described in ISO/IEC 15408 assurance family entitled TOE design  
800 (ADV\_TDS), where applicable.

801 The intent of this Subclause is to characterise the degree of architectural separation of the major  
802 components. If there is no TOE design (ADV\_TDS) requirement in the ST, this is not applicable and  
803 is considered to be satisfied.

804 **7.4.5.3.4 Evaluation**

805 The evaluator **shall report** the evaluation methods, techniques, tools and standards used.

806 The evaluator may reference the evaluation criteria, methodology and interpretations used to  
807 evaluate the TOE or the devices used to perform the tests.

808 The evaluator **shall report** any constraints on the evaluation, constraints on the distribution of  
809 evaluation results and assumptions made during the evaluation that have an impact on the  
810 evaluation results.

811 The evaluator may include information in relation to legal or statutory aspects, organisation,  
812 confidentiality, etc.

#### 813 7.4.5.3.5 Results of the evaluation

814 For each activity on which the TOE is evaluated, the evaluator *shall report*:

- 815 • the title of the activity considered;
- 816 • a verdict and a supporting rationale for each assurance component that constitutes this  
817 activity, as a result of performing the corresponding evaluation methodology action and  
818 its constituent work units.

819 The rationale justifies the verdict using ISO/IEC 15408, this document, any interpretations and the  
820 evaluation evidence examined and shows how the evaluation evidence does or does not meet each  
821 aspect of the criteria. It contains a description of the work performed, the method used, and any  
822 derivation of results. The rationale may provide detail to the level of an evaluation methodology  
823 work unit.

824 The evaluator *shall report* all information specifically required by a work unit.

825 For the AVA and ATE activities, work units that identify information to be reported in the ETR have  
826 been defined.

#### 827 7.4.5.3.6 Conclusions and recommendations

828 The evaluator *shall report* the conclusions of the evaluation, which will relate to whether the TOE  
829 has satisfied its associated ST, in particular the overall verdict as defined in ISO/IEC 15408-1:20xx,  
830 Clause 9, Evaluation results, and determined by application of the verdict assignment described in  
831 7.2.5.

832 The evaluator provides recommendations that may be useful for the evaluation authority. These  
833 recommendations may include shortcomings of the IT product discovered during the evaluation or  
834 mention of features which are particularly useful.

#### 835 7.4.5.3.7 List of evaluation evidence

836 The evaluator *shall report* for each item of evaluation evidence the following information:

- 837 • the issuing body (e.g. the developer, the sponsor);
- 838 • the title;
- 839 • the unique reference (e.g. issue date and version number).

#### 840 7.4.5.3.8 List of acronyms/Glossary of terms

841 The evaluator *shall report* any acronyms or abbreviations used in the ETR.

842 Glossary definitions already defined by ISO/IEC 15408 or by this document need not be repeated  
843 in the ETR.

#### 844 7.4.5.3.9 Observation reports

845 The evaluator *shall report* a complete list that uniquely identifies the ORs raised during the  
846 evaluation and their status.

For each OR, the list should contain its identifier as well as its title or a brief summary of its content.

## **8 Class APE: Protection Profile evaluation**

### **8.1 Introduction**

This Clause describes the evaluation of a PP. The requirements and methodology for PP evaluation are identical for each PP evaluation, regardless of the EAL (or other set of assurance requirements) that is claimed in the PP. The evaluation methodology in this Clause is based on the requirements on the PP as specified in ISO/IEC 15408-3 class APE.

This Clause should be used in conjunction with Annexes A, B and C in ISO/IEC 15408-1, as these Annexes clarify the concepts here and provide many examples.

### **8.2 Re-using the evaluation results of certified PPs**

While evaluating a PP that is based on one or more certified PPs, it may be possible to re-use the fact that these PPs were certified. The potential for re-use of the result of a certified PP is greater if the PP under evaluation does not add threats, OSPs, security objectives and/or security requirements to those of the PP that conformance is being claimed to. If the PP under evaluation contains much more than the certified PP, re-use may not be useful at all.

The evaluator is allowed to re-use the PP evaluation results by doing certain analyses only partially or not at all if these analyses or parts thereof were already done as part of the PP evaluation. While doing this, the evaluator should assume that the analyses in the PP were performed correctly.

An example would be where the PP that conformance is being claimed to contain a set of security requirements, and these were determined to be internally consistent during its evaluation. If the PP under evaluation uses the exact same requirements, the consistency analysis does not have to be repeated during the PP evaluation. If the PP under evaluation adds one or more requirements, or performs operations on these requirements, the analysis will have to be repeated. However, it may be possible to save work in this consistency analysis by using the fact that the original requirements are internally consistent. If the original requirements are internally consistent, the evaluator only has to determine that:

a) the set of all new and/or changed requirements is internally consistent, and

b) the set of all new and/or changed requirements is consistent with the original requirements.

The evaluator notes in the ETR each case where analyses are not done or only partially done for this reason.

### **8.3 PP introduction (APE\_INT)**

#### **8.3.1 Evaluation of sub-activity (APE\_INT.1)**

##### **8.3.1.1 Objectives**

The objective of this sub-activity is to determine whether the PP is correctly identified, and whether the PP reference and TOE overview are consistent with each other.

##### **8.3.1.2 Input**

The evaluation evidence for this sub-activity is:

885 a) the PP.

886 **8.3.1.3 Action APE\_INT.1.1E**

887 **8.3.1.3.1 General**

888 ISO/IEC 15408-3 APE\_INT.1.1C: *The PP introduction shall contain a PP reference and a TOE*  
889 *overview.*

890 **8.3.1.3.2 Work unit APE\_INT.1-1**

891 The evaluator **shall check** that the PP introduction contains a PP reference and a TOE overview.

892 ISO/IEC 15408-3 APE\_INT.1.2C: *The PP reference shall uniquely identify the PP.*

893 **8.3.1.3.3 Work unit APE\_INT.1-2**

894 The evaluator **shall examine** the PP reference to determine that it uniquely identifies the PP.

895 The evaluator determines that the PP reference identifies the PP itself, so that it may be easily  
896 distinguished from other PPs, and that it also uniquely identifies each version of the PP, e.g. by  
897 including a version number and/or a date of publication.

898 The PP should have some referencing system that is capable of supporting unique references (e.g.  
899 use of numbers, letters or dates).

900 ISO/IEC 15408-3 APE\_INT.1.3C: *The TOE overview shall summarise the usage and major security*  
901 *features of the TOE.*

902 **8.3.1.3.4 Work unit APE\_INT.1-3**

903 The evaluator **shall examine** the TOE overview to determine that it describes the usage and major  
904 security features of the TOE.

905 The TOE overview should briefly (i.e. several paragraphs) describe the usage and major security  
906 features expected of the TOE. The TOE overview should enable consumers and potential TOE  
907 developers to quickly determine whether the PP is of interest to them.

908 The evaluator determines that the overview is clear enough for TOE developers and consumers,  
909 and sufficient to give them a general understanding of the intended usage and major security  
910 features of the TOE.

911 ISO/IEC 15408-3 APE\_INT.1.4C: *The TOE overview shall identify the TOE type.*

912 **8.3.1.3.5 Work unit APE\_INT.1-4**

913 The evaluator **shall check** that the TOE overview identifies the TOE type.

914 ISO/IEC 15408-3 APE\_INT.1.5C: *The TOE overview shall identify any non-TOE*  
915 *hardware/software/firmware available to the TOE.*

916 **8.3.1.3.6 Work unit APE\_INT.1-5**

917 The evaluator **shall examine** the TOE overview to determine that it identifies any non-TOE  
918 hardware/software/firmware available to the TOE.

919 While some TOEs may run stand-alone, other TOEs (notably software TOEs) need additional  
920 hardware, software or firmware to operate. In this subclause of the PP, the PP author lists all  
921 hardware, software, and/or firmware that will be available for the TOE to run on.

922 This identification should be detailed enough for potential consumers and TOE developers to  
923 determine whether their TOE may operate with the listed hardware, software and firmware.

#### 924 **8.4 Conformance claims (APE\_CCL)**

##### 925 **8.4.1 Evaluation of sub-activity (APE\_CCL.1)**

###### 926 **8.4.1.1 Objectives**

927 The objective of this sub-activity is to determine the validity of various conformance claims. These  
928 describe how the PP conforms to ISO/IEC 15408, other PPs and packages.

###### 929 **8.4.1.2 Input**

930 The evaluation evidence for this sub-activity is:

- 931 a) the PP
- 932 b) the content of the PP configuration
- 933 c) the package(s) that the PP claims conformance to.

###### 934 **8.4.1.3 Action APE\_CCL.1.1E**

###### 935 **8.4.1.3.1 General**

936 ISO/IEC 15408-3 APE\_CCL.1.1C: *The conformance claim shall contain an ISO/IEC 15408*  
937 *conformance claim that identifies the edition of ISO/IEC 15408 to which the PP claims conformance.*

###### 938 **8.4.1.3.2 Work unit APE\_CCL.1-1**

939 The evaluator **shall check** that the conformance claim contains an ISO/IEC 15408 conformance  
940 claim that identifies the edition of ISO/IEC 15408 to which the PP claims conformance.

941 The evaluator determines that ISO/IEC 15408 conformance claim identifies the edition of ISO/IEC  
942 15408 that was used to develop this PP. This should include the edition number of ISO/IEC 15408  
943 and, unless the International English edition of ISO/IEC 15408 was used, the language of the  
944 edition of ISO/IEC 15408 that was used.

945 ISO/IEC 15408-3 APE\_CCL.1.2C: *ISO/IEC 15408 conformance claim shall describe the conformance of*  
946 *the PP to ISO/IEC 15408-2 as either ISO/IEC 15408-2 conformant or ISO/IEC 15408-2 extended.*

###### 947 **8.4.1.3.3 Work unit APE\_CCL.1-2**

948 The evaluator **shall check** that ISO/IEC 15408 conformance claim states a claim of either ISO/IEC  
949 15408-2 conformant or ISO/IEC 15408-2 extended for the PP.

950 ISO/IEC 15408-3 APE\_CCL.1.3C: *ISO/IEC 15408 conformance claim shall describe the conformance of*  
951 *the PP to ISO/IEC 15408-3 as either ISO/IEC 15408-3 conformant or ISO/IEC 15408-3 extended.*



952 **8.4.1.3.4 Work unit APE\_CCL.1-3**

953 The evaluator **shall check** that ISO/IEC 15408 conformance claim states a claim of either ISO/IEC  
954 15408-3 conformant or ISO/IEC 15408-3 extended for the PP.

955 ISO/IEC 15408-3 APE\_CCL.1.4C: *ISO/IEC 15408 conformance claim shall be consistent with the*  
956 *extended components definition.*

957 **8.4.1.3.5 Work unit APE\_CCL.1-4**

958 The evaluator **shall examine** ISO/IEC 15408 conformance claim for ISO/IEC 15408-2 to determine  
959 that it is consistent with the extended components definition.

960 If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-2 conformant, the evaluator  
961 determines that the extended components definition does not define functional components.

962 If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-2 extended, the evaluator determines  
963 that the extended components definition defines at least one extended functional component.

964 **8.4.1.3.6 Work unit APE\_CCL.1-5**

965 The evaluator **shall examine** ISO/IEC 15408 conformance claim for ISO/IEC 15408-3 to determine  
966 that it is consistent with the extended components definition.

967 If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-3 conformant, the evaluator  
968 determines that the extended components definition does not define assurance components.

969 If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-3 extended, the evaluator determines  
970 that the extended components definition defines at least one extended assurance component.

971 ISO/IEC 15408-3 APE\_CCL.1.5C: *The conformance claim shall identify all PPs and security*  
972 *requirement packages to which the PP claims conformance.*

973 **8.4.1.3.7 Work unit APE\_CCL.1-6**

974 The evaluator **shall check** that the conformance claim contains a PP claim that identifies all PPs for  
975 which the PP claims conformance.

976 If the PP does not claim conformance to another PP, this work unit is not applicable and therefore  
977 considered to be satisfied.

978 The evaluator determines that any referenced PPs are unambiguously identified (e.g. by title and  
979 version number, or by the identification included in the introduction of that PP).

980 The evaluator is reminded that claims of partial conformance to a PP are not permitted.

981 **8.4.1.3.8 Work unit APE\_CCL.1-6a**

982 The evaluator **shall check** that any functional or assurance packages claimed by the PP are  
983 identified.

984 If the PP does not claim conformance to a package, then this work unit is not applicable and  
985 considered to be satisfied.

986 The evaluator ensures that the identification of all packages is unambiguous, and references each  
987 package's defined identity (and version, if applicable)

## ISO/IEC 18045:2008(E)

988 ISO/IEC 15408-3 APE\_CCL.1.6C: *The conformance claim shall describe any conformance of the PP to*  
989 *a package as one of: package-conformant, package-augmented, or package tailored.*

### 990 8.4.1.3.9 Work unit APE\_CCL.1-7

991 The evaluator **shall examine** the PP, each identified package, and the conformance claim for each  
992 package to determine that the claim is either package-name conformant or package-name  
993 augmented, and that the claim is accurate.

994 If the PP does not claim conformance to a package, this work unit is not applicable and therefore  
995 considered to be satisfied.

996 There are two methods for a PP author to represent a package to which they are claiming  
997 conformance. The first method is to include the package by reference, in which case the PP only  
998 provides a (unique) reference to the package, and clearly identifies any changes, modifications,  
999 restrictions, etc. that are made to the package contents when it is included in the PP. The second  
1000 method is to transcribe the contents of the package directly into the PP. The specific  
1001 representation will be taken into account by the evaluator in performing the following examination.

1002 If the package conformance claim contains or references package-name conformance, the evaluator  
1003 determines that:

1004 a) If the package is an assurance package, then the PP contains all SARs included in the  
1005 package, but no additional SARs.

1006 b) If the package is a functional package, then all assumptions, threats, OSPs, security  
1007 objectives and SFRs included in the package are included in identical form in the PP  
1008 (after allowing for iteration, refinement, assignments and selections from the  
1009 package to be completed as required by the PP).

1010 If the package conformance claim contains package-name tailored, the evaluator determines that:

1011 a) all assumptions, threats, OPSs, Security Objectives, and SFRs included in the package  
1012 are included in identical form in the PP (after allowing for iteration, refinement,  
1013 assignments and selections from the package to be completed as required by the  
1014 PP);

1015 b) the PP may have at least one additional SFR or one SFR that is hierarchically higher  
1016 than an SFR in the functional package;

1017 c) the PP shall have at least one additional (not present in the SFR in the package)  
1018 selection item in one of the SFRs in the functional package.

1019 In the case of package-name tailored, the evaluator additionally examines the selection (and other  
1020 selections in that requirement) to ensure that the requirement still meets its security objective (or  
1021 the associated SPD element in the direct rationale approach) with the addition of (and potentially  
1022 deletion of) the selection item.

1023 If the package conformance claim contains package-name augmented, the evaluator determines  
1024 that:

1025 a) If the package is an assurance package, then the PP contains all SARs included in the package,  
1026 and at least one additional SAR or at least one SAR that is hierarchical to a SAR in the package.

1027 b) If the package is a functional package, then all assumptions, threats, OPSs, Security Objectives,  
1028 and SFRs included in the package are included (either by reference or transcription) in  
1029 identical form in the PP (after allowing for iteration, refinement, assignments and selections  
1030 from the package to be completed as required by the PP) except that the PP shall have at least  
1031 one additional SFR or one SFR that is hierarchically higher than an SFR in the functional  
1032 package.

#### 1033 8.4.1.3.10 Work unit APE\_CCL.1-8

1034 The evaluator shall check, for each identified functional package, that the package definition is  
1035 complete.

1036 If the PP does not claim conformance to a package, this work unit is not applicable and therefore  
1037 considered to be satisfied.

1038 The evaluator determines that the package definition is conformant to the requirements from  
1039 ISO/IEC 15408-1, clause 8 "Packages" by checking that the functional package includes:

1040 a) A functional package identification, giving a unique name, optional short name,  
1041 version, date, sponsor, and the ISO/IEC 15408 edition;

1042 b) A functional package overview, giving a narrative description of the security  
1043 functionality;

1044 c) The ISO/IEC 15408 edition used;

1045 d) If the package defines an SPD then it also either

1046 1) if using the Direct Rationale approach: include a security functional requirements  
1047 rationale that maps all threats, OSPs and assumptions in the SPD directly to the  
1048 SFRs and Security Objectives for the operational environment; or else

1049 2) if not using the Direct Rationale approach: include Security Objectives for the  
1050 TOE and the operational environment and the Security Objectives rationale; The  
1051 functional package SFRs shall also include a security requirements rationale if the  
1052 package includes any Security Objectives for the TOE.

1053 e) Application notes, describing additional information in regard to the package  
1054 including a reference to any evaluation methods(s) and/or activities specified to be  
1055 used in conjunction with the package;

1056 f) If extended components have been specified then the package includes an extended  
1057 components definition;

1058 g) A rationale for the selection of the components in the package.

1059 ISO/IEC 15408-3 APE\_CCL.1.7C: *The conformance claim rationale shall demonstrate that the TOE*  
1060 *type is consistent with the TOE type in the PPs for which conformance is being claimed.*

#### 1061 8.4.1.3.11 Work unit APE\_CCL.1-9

1062 The evaluator **shall examine** the conformance claim rationale to determine that the TOE type of  
1063 the TOE is consistent with all TOE types of the PPs.

## ISO/IEC 18045:2008(E)

1064 If the PP does not claim conformance to another PP, this work unit is not applicable and therefore  
1065 considered to be satisfied.

1066 The relation between the types may be simple: a firewall PP claiming conformance to another  
1067 firewall PP, or more complex: a smart card PP claiming conformance to a number of other PPs at  
1068 the same time: a PP for the integrated circuit, a PP for the smart card OS, and two PPs for two  
1069 applications on the smart card.

1070 ISO/IEC 15408-3 APE\_CCL.1.8C: *The conformance claim rationale shall demonstrate that the*  
1071 *statement of the security problem definition is consistent with the statement of the security problem*  
1072 *definition in the PPs for which conformance is being claimed.*

### 1073 8.4.1.3.12 Work unit APE\_CCL.1-10

1074 The evaluator **shall examine** the conformance claim rationale to determine that it demonstrates  
1075 that the statement of security problem definition is consistent, as defined by the conformance  
1076 statement of the PP, with the statements of security problem definition stated in the PPs to which  
1077 conformance is being claimed.

1078 If the PP under evaluation does not claim conformance with another PP, this work unit is not  
1079 applicable and therefore considered to be satisfied.

1080 If the PP to which conformance is being claimed does not have a statement of security problem  
1081 definition, this work unit is not applicable and therefore considered to be satisfied.

1082 If the PP to which conformance is being claimed contains functional packages, the evaluator  
1083 determines that the security problem definition of the PP under evaluation includes (in terms of  
1084 consideration for the assessment of this work unit) all assumptions, threats and OSPs of all  
1085 functional packages.

1086 The terms exact, strict and demonstrable conformance are defined in ISO/IEC 15408-1.

1087 If packages are used, the rules defined in the following paragraphs concerning exact, strict and  
1088 demonstrable conformance also hold for the SPD descriptions taken from the packages.

1089 Note that since a PP can only claim conformance to another PP whose conformance statement  
1090 requires strict or demonstrable conformance, those are the only cases covered in the following  
1091 paragraphs. If strict conformance is required by the PP to which conformance is being claimed, no  
1092 conformance claim rationale is required. Instead, the evaluator determines whether:

1093 a) the threats in the PP under evaluation are a superset of or identical to the threats in  
1094 the PP to which conformance is being claimed;

1095 b) the OSPs in the PP under evaluation are a superset of or identical to the OSPs in the  
1096 PP to which conformance is being claimed;

1097 c) the assumptions in the PP claiming conformance are identical to the assumptions in  
1098 the PP to which conformance is being claimed, with two possible exceptions  
1099 described in the following two bullet points;

1100 • an assumption (or part of an assumption) from the PP to which conformance is claimed,  
1101 can be omitted, if all security objectives for the operational environment addressing this  
1102 assumption (or part of an assumption) are replaced by security objectives for the TOE;

1103 • an assumption can be added to the assumptions defined in the PP to which conformance  
1104 is claimed, if a justification is given, why the new assumption neither mitigates a threat

- 1105 (or a part of a threat) meant to be addressed by security objectives for the TOE in the PP  
 1106 to which conformance is claimed, nor fulfils an OSP (or part of an OSP) meant to be  
 1107 addressed by security objectives for the TOE in the PP to which conformance is claimed.
- 1108 For items "a" and "b", it is allowed to omit SPD elements associated with optional requirements  
 1109 that are not included in the ST and still claim exact conformance.
- 1110 When examining a PP, which omits assumptions from another PP to which conformance is claimed,  
 1111 or adds new assumptions, the evaluator shall carefully determine, if the conditions given above are  
 1112 fulfilled. The following discussion gives some motivation and examples for these cases:
- 1113 • Example for omitting an assumption: A PP to which conformance is claimed, may  
 1114 contain an assumption stating that the operational environment prevents unauthorized  
 1115 modification or interception of data sent to an external interface of the TOE. This may be  
 1116 the case if the TOE accepts data in clear text and without integrity protection at this  
 1117 interface and is assumed to be located in a secure operational environment, which will  
 1118 prevent attackers from accessing these data. The assumption will then be mapped in the  
 1119 PP, to which conformance is claimed, to some objective for the operational environment  
 1120 stating that the data interchanged at this interface are protected by adequate measures in  
 1121 the operational environment. If a PP claiming this PP, defines a more secure TOE, which  
 1122 has an additional security objective stating that the TOE itself protects these data, for  
 1123 example by providing a secure channel for encryption and integrity protection of all data  
 1124 transferred via this interface, the corresponding objective and assumption for the  
 1125 operational environment can be omitted from the PP claiming conformance. This is also  
 1126 called re-assigning of the objective, since the objective is re-assigned from the  
 1127 operational environment to the TOE. Note, that this TOE is still secure in an operational  
 1128 environment fulfilling the omitted assumption and therefore still fulfils the PP to which  
 1129 conformance is claimed.
  - 1130 • Example for adding an assumption: In this example, the PP to which conformance is  
 1131 claimed, is designed to specify requirements for a TOE of type "Firewall" and the author  
 1132 of another PP wishes to claim conformance to this PP for a TOE, which implements a  
 1133 firewall, but additionally provides the functionality of a virtual private network (VPN)  
 1134 component. For the VPN functionality, the TOE needs cryptographic keys and these keys  
 1135 may also have to be handled securely by the operational environment (e. g. if symmetric  
 1136 keys are used to secure the network connection and therefore need to be provided in  
 1137 some secure way to other components in the network). In this case, it is acceptable to add  
 1138 an assumption that the cryptographic keys used by the VPN are handled securely by the  
 1139 operational environment. This assumption does not address threats or OSPs of the PP to  
 1140 which conformance is claimed, and therefore fulfils the conditions stated above.
  - 1141 • Counterexample for adding an assumption: In a variant of the first example a PP to which  
 1142 conformance is claimed, may already contain an objective for the TOE to provide a  
 1143 secure channel for one of its interfaces, and this objective is mapped to a threat of  
 1144 unauthorized modification or reading of the data on this interface. In this case, it is  
 1145 clearly not allowed for another PP claiming this PP, to add an assumption for the  
 1146 operational environment, which assumes that the operational environment protects data  
 1147 on this interface against modification or unauthorized reading of the data. This  
 1148 assumption would reduce a threat, which is meant to be addressed by the TOE.  
 1149 Therefore, a TOE fulfilling a PP with this added assumption would not automatically  
 1150 fulfil the PP to which conformance is claimed, anymore and this addition is therefore not  
 1151 allowed.

- 1152 • Second counterexample for adding an assumption: In the example above of a TOE  
1153 implementing a firewall it would not be admissible to add a general assumption that the  
1154 TOE is only connected to trusted devices, because this would obviously remove essential  
1155 threats relevant for a firewall (namely that there is untrusted IP traffic, which needs to be  
1156 filtered). Therefore, this addition would not be allowed.

1157 If demonstrable conformance is required by the PP to which conformance is being claimed, the  
1158 evaluator examines the conformance claim rationale to determine that it demonstrates that the  
1159 statement of security problem definition of the PP under evaluation is equivalent or more  
1160 restrictive than the statement of security problem definition in the PP to which conformance is  
1161 being claimed.

1162 For this, the conformance claim rationale needs to demonstrate that the security problem  
1163 definition in the PP claiming conformance is equivalent (or more restrictive) than the security  
1164 problem definition in the PP to which conformance is claimed. This means that:

- 1165 • all TOEs that would meet the security problem definition in the PP claiming conformance  
1166 also meet the security problem definition in the PP to which conformance is claimed.  
1167 This can also be shown indirectly by demonstrating that every event, which realizes a  
1168 threat defined in the PP to which conformance is claimed, or violates an OSP defined in  
1169 the PP to which conformance is claimed, would also realize a threat stated in the PP  
1170 claiming conformance or violate an OSP defined in the PP claiming conformance. Note  
1171 that fulfilling an OSP stated in the PP claiming conformance may avert a threat stated in  
1172 the PP to which conformance is claimed, or that averting a threat stated in the PP  
1173 claiming conformance may fulfil an OSP stated in the PP to which conformance is  
1174 claimed, so threats and OSPs can substitute each other;

- 1175 • all operational environments that would meet the security problem definition in the PP to  
1176 which conformance is claimed, would also meet the security problem definition in the PP  
1177 claiming conformance (with one exception in the next bullet);

- 1178 • besides a set of assumptions in the PP claiming conformance needed to demonstrate  
1179 conformance to the SPD of the PP to which conformance is claimed, an PP claiming  
1180 conformance may specify further assumptions, but only if these additional assumptions  
1181 are independent of and do not affect the security problem definition as defined in the PP  
1182 to which conformance is claimed. More detailed, there are no assumptions in the PP  
1183 claiming conformance that exclude threats to the TOE that need to be countered by the  
1184 TOE according to the PP to which conformance is claimed. Similarly, there are no  
1185 assumptions in the PP claiming conformance that realize aspects of an OSP stated in the  
1186 PP to which conformance is claimed, which are meant to be fulfilled by the TOE  
1187 according to the PP to which conformance is claimed.

1188 ISO/IEC 15408-3 APE\_CCL.1.9C: *The conformance claim rationale shall demonstrate that the*  
1189 *statement of security objectives is consistent with the statement of security objectives in the PPs for*  
1190 *which conformance is being claimed.*

#### 1191 8.4.1.3.13 Work unit APE\_CCL.1-11

1192 The evaluator **shall examine** the conformance claim rationale to determine that the statement of  
1193 security objectives is consistent, as defined by the conformance statement of the PPs, with the  
1194 statement of security objectives in the PPs.

1195 If the PP does not claim conformance to another PP, this work unit is not applicable and therefore  
1196 considered to be satisfied.

- 1197 If the PP to which conformance is being claimed contains functional packages, the evaluator  
1198 determines that the security objectives of the PP under evaluation include (in terms of  
1199 consideration for the assessment of this work unit) all security objectives of all functional packages.
- 1200 If packages are used, the rules defined in the following paragraphs concerning exact, strict and  
1201 demonstrable conformance also hold for the security objectives taken from the packages.
- 1202 Note that since a PP can only claim conformance to another PP whose conformance statement  
1203 requires strict or demonstrable conformance, those are the only cases covered in the following  
1204 paragraphs. If strict conformance is required by the PP to which conformance is being claimed, no  
1205 conformance claim rationale is required. Instead, the evaluator determines whether:
- 1206 • The PP under evaluation contains all security objectives for the TOE of the PP to which  
1207 conformance is being claimed. Note that it is allowed for the PP under evaluation to have  
1208 additional security objectives for the TOE;
  - 1209 • The security objectives for the operational environment in the PP claiming conformance  
1210 are identical to the security objectives for the operational environment in the PP to which  
1211 conformance is being claimed, with two possible exceptions described in the following  
1212 two bullet points;
  - 1213 • a security objective for the operational environment (or part of such security objective)  
1214 from the PP to which conformance is claimed, can be replaced by the same (part of the)  
1215 security objective stated for the TOE;
  - 1216 • a security objective for the operational environment can be added to the objectives  
1217 defined in the PP to which conformance is claimed, if a justification is given, why the  
1218 new objective neither mitigates a threat (or a part of a threat) meant to be addressed by  
1219 security objectives for the TOE in the PP to which conformance is claimed, nor fulfils an  
1220 OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the  
1221 PP to which conformance is claimed.
- 1222 When examining a PP claiming another PP which omits security objectives for the operational  
1223 environment from the PP to which conformance is claimed, or adds new security objectives for the  
1224 operational environment, the evaluator shall carefully determine, if the conditions given above are  
1225 fulfilled. The examples given for the case of assumptions in the preceding work unit are also valid  
1226 here.
- 1227 If demonstrable conformance is required by the PP to which conformance is being claimed, the  
1228 evaluator examines the conformance claim rationale to determine that it demonstrates that the  
1229 statement of security objectives of the PP under evaluation is equivalent or more restrictive than  
1230 the statement of security objectives in the PP to which conformance is being claimed.
- 1231 For this the conformance claim rationale needs to demonstrate that the security objectives in the  
1232 PP claiming conformance are equivalent (or more restrictive) than the security objectives in the PP  
1233 to which conformance is claimed. This means that:
- 1234 • all TOEs that would meet the security objectives for the TOE in the PP claiming  
1235 conformance also meet the security objectives for the TOE in the PP to which  
1236 conformance is claimed;
  - 1237 • all operational environments that would meet the security objectives for the operational  
1238 environment in the PP to which conformance is claimed, would also meet the security  
1239 objectives for the operational environment in the PP claiming conformance (with one  
1240 exception in the next bullet);

## ISO/IEC 18045:2008(E)

- 1241 • besides a set of security objectives for the operational environment in the PP claiming  
1242 conformance, which are used to demonstrate conformance to the set of security  
1243 objectives defined in the PP to which conformance is claimed, an PP claiming  
1244 conformance may specify further security objectives for the operational environment, but  
1245 only if these security objectives neither affect the original set of security objectives for  
1246 the TOE nor the security objectives for the operational environment as defined in the PP  
1247 to which conformance is claimed.

1248 ISO/IEC 15408-3 APE\_CCL.1.10C: *The conformance claim rationale shall demonstrate that the*  
1249 *statement of security requirements is consistent with the statement of security requirements in the*  
1250 *PPs for which conformance is being claimed.*

### 1251 8.4.1.3.14 Work unit APE\_CCL.1-12

1252 The evaluator **shall examine** the PP to determine that it is consistent, as defined by the  
1253 conformance statement of the PP, with all security requirements in the PPs for which conformance  
1254 is being claimed.

1255 If the PP does not claim conformance to another PP, this work unit is not applicable and therefore  
1256 considered to be satisfied.

1257 If the PP to which conformance is being claimed contains functional packages, the evaluator  
1258 determines that the SFRs of the PP under evaluation includes (in terms of consideration for the  
1259 assessment of this work unit).all SFRs (or hierarchical SFRs) of all functional packages.

1260 If packages are used, the rules defined in the following paragraphs concerning exact, strict and  
1261 demonstrable conformance also hold for the SFRs taken from the packages.

- 1262 • Note that since a PP can only claim conformance to another PP whose conformance  
1263 statement requires strict or demonstrable conformance, those are the only cases covered  
1264 in the following paragraphs.

1265 If strict conformance is required by the PP to which conformance is being claimed, no conformance  
1266 claim rationale is required. Instead, the evaluator determines whether the statement of security  
1267 requirements in the PP under evaluation is a superset of or identical to the statement of security  
1268 requirements in the PP to which conformance is being claimed (for strict conformance).

1269 If demonstrable conformance is required by the PP to which conformance is being claimed, the  
1270 evaluator examines the conformance claim rationale to determine that it demonstrates that the  
1271 statement of security requirements of the PP under evaluation is equivalent or more restrictive  
1272 than the statement of security requirements in the PP to which conformance is being claimed.

1273 For:

- 1274 • SFRs: The conformance rationale in the PP claiming conformance shall demonstrate that  
1275 the overall set of requirements defined by the SFRs in the PP claiming conformance is  
1276 equivalent (or more restrictive) than the overall set of requirements defined by the SFRs  
1277 in the PP to which conformance is claimed. This means that all TOEs that would meet the  
1278 requirements defined by the set of all SFRs in the PP claiming conformance would also  
1279 meet the requirements defined by the set of all SFRs in the PP to which conformance is  
1280 claimed;

- 1281 • SARs: The PP claiming conformance shall contain all SARs in the PP to which  
1282 conformance is claimed, but may claim additional SARs or replace SARs by  
1283 hierarchically stronger SARs. The completion of operations in the PP claiming  
1284 conformance must be consistent with that in the PP to which conformance is claimed;



- 1285 either the same completion will be used in the PP claiming conformance as that in the PP  
1286 to which conformance is claimed or a completion that makes the SAR more restrictive  
1287 (the rules of refinement apply).
- 1288 ISO/IEC 15408-3 APE\_CCL.1.11C: *The conformance statement shall describe the conformance*  
1289 *required of any PPs/STs to the PP as exact-PP, strict-PP or demonstrable-PP conformance.*
- 1290 **8.4.1.3.15 Work unit APE\_CCL.1-13**
- 1291 The evaluator **shall check** that the PP conformance statement states a claim of exact-PP, strict-PP  
1292 or demonstrable-PP conformance.
- 1293 ISO/IEC 15408-3 APE\_CCL.1.12C: *The conformance statement shall identify the set of other PPs (if*  
1294 *any) to which, in combination with the PP under evaluation, exact conformance is allowed to be*  
1295 *claimed.*
- 1296 **8.4.1.3.16 Work unit APE\_CCL.1-14**
- 1297 The evaluator **shall check** the conformance statement to determine that it lists the set of PPs to  
1298 which, in combination with the PP being evaluated, an exact conformance claim (in an ST or PP  
1299 Configuration) is allowed.
- 1300 If the PP does not require exact conformance in its conformance statement, this work unit does not  
1301 apply and is therefore considered satisfied.
- 1302 If the PP does not allow claims of exact conformance to it in combination with any other PPs, then  
1303 no list of PPs is required and this work unit is considered satisfied.
- 1304 There are no other actions for the evaluator other than determining that the list is present.
- 1305 **8.4.1.3.17 Work unit APE\_CCL.1-15**
- 1306 The evaluator **shall check** the conformance statement to determine that it lists the set of derived  
1307 Evaluation Methods and Evaluation Activities (if any) that shall be used with the PP under  
1308 evaluation, and that the list is sufficiently structured and detailed to identify every member.
- 1309 15408-3 APE\_CCL.1.14C *The conformance statement shall identify the set of derived Evaluation*  
1310 *Methods and Evaluation Activities (if any) that shall be used with the PP under evaluation. This list*  
1311 *shall contain:"*
- 1312 **8.4.1.3.18 Work unit APE\_CCL.1-16**
- 1313 The evaluator shall check the conformance statement to determine that it lists the set of PP-  
1314 Modules that can be used with the PP under evaluation in a PP-Configuration.
- 1315 If the PP does not require exact conformance in its conformance statement, this work unit does not  
1316 apply and is therefore considered satisfied.
- 1317 If the PP is not allowed to be used with any PP-Module in a PP-Configuration, then the evaluator  
1318 confirms that no PP-modules are listed.
- 1319 There are no other actions for the evaluator other than determining that the list is present.

1320 **8.4.1.3.19 Work unit APE\_CCL.1-17**

1321 The evaluator **shall check** that, for each other PP to which the PP being evaluated claims  
1322 conformance, the conformance statement of that other PP requires strict or demonstrable  
1323 conformance.

1324 If the PP does not claim conformance to another PP, this work unit is not applicable and therefore  
1325 considered to be satisfied.

1326 If the PP requires exact conformance, the evaluator ensures that it does not claim conformance to  
1327 any other PPs.

1328 If the PP claims conformance to another PP, the evaluator ensures that all PPs it is claiming  
1329 conformance to, require either strict or demonstrable conformance.

1330 **8.5 Security problem definition (APE\_SPD)**

1331 **8.5.1 Evaluation of sub-activity (APE\_SPD.1)**

1332 **8.5.1.1 Objectives**

1333 The objective of this sub-activity is to determine that the security problem intended to be  
1334 addressed by the TOE and its operational environment is clearly defined.

1335 **8.5.1.2 Input**

1336 The evaluation evidence for this sub-activity is:

1337 a) the PP.

1338 **8.5.1.3 Action APE\_SPD.1.1E**

1339 **8.5.1.3.1 General**

1340 ISO/IEC 15408-3 APE\_SPD.1.1C: *The security problem definition shall describe the threats.*

1341 **8.5.1.3.2 Work unit APE\_SPD.1-1**

1342 The evaluator **shall check** that the security problem definition describes the threats.

1343 If all security objectives are derived from assumptions and/or OSPs only, the statement of threats  
1344 need not be present in the PP. In this case, this work unit is not applicable and therefore considered  
1345 to be satisfied.

1346 The evaluator determines that the security problem definition describes the threats that must be  
1347 countered by the TOE and/or its operational environment.

1348 Note that if optional requirements are defined by the PP, there may be associated threats that are  
1349 covered by this work unit.

1350 ISO/IEC 15408-3 APE\_SPD.1.2C: *All threats shall be described in terms of a threat agent, an asset,*  
1351 *and an adverse action.*

1352 **8.5.1.3.3 Work unit APE\_SPD.1-2**

1353 The evaluator **shall examine** the security problem definition to determine that all threats are  
1354 described in terms of a threat agent, an asset, and an adverse action.

1355 If all security objectives are derived from assumptions and OSPs only, the statement of threats  
1356 need not be present in the PP. In this case, this work unit is not applicable and therefore considered  
1357 to be satisfied.

1358 Threat agents may be further described by aspects such as expertise, resource, opportunity, and  
1359 motivation.

1360 ISO/IEC 15408-3 APE\_SPD.1.3C: *The security problem definition shall describe the OSPs.*

#### 1361 **8.5.1.3.4 Work unit APE\_SPD.1-3**

1362 The evaluator **shall examine** that the security problem definition describes the OSPs.

1363 If all security objectives are derived from assumptions and/or threats only, OSPs need not be  
1364 present in the PP. In this case, this work unit is not applicable and therefore considered to be  
1365 satisfied.

1366 The evaluator determines that OSP statements are made in terms of rules or guidelines that must  
1367 be followed by the TOE and/or its operational environment.

1368 The evaluator determines that each OSP is explained and/or interpreted in sufficient detail to make  
1369 it clearly understandable; a clear presentation of policy statements is necessary to permit tracing  
1370 security objectives to them.

1371 Note that if optional requirements are defined by the PP, there may be associated OSPs that are  
1372 covered by this work unit.

1373 ISO/IEC 15408-3:20XX APE\_SPD.1.4C: *The security problem definition shall describe the assumptions*  
1374 *about the operational environment of the TOE.*

#### 1375 **8.5.1.3.5 Work unit APE\_SPD.1-4**

1376 The evaluator **shall examine** the security problem definition to determine that it describes the  
1377 assumptions about the operational environment of the TOE.

1378 If there are no assumptions, this work unit is not applicable and is therefore considered to be  
1379 satisfied.

1380 The evaluator determines that each assumption about the operational environment of the TOE is  
1381 explained in sufficient detail to enable consumers to determine that their operational environment  
1382 matches the assumption. If the assumptions are not clearly understood, the end result may be that  
1383 the TOE is used in an operational environment in which it will not function in a secure manner.

### 1384 **8.6 Security objectives (APE\_OB)**

#### 1385 **8.6.1 Evaluation of sub-activity (APE\_OB.1)**

##### 1386 **8.6.1.1 Objectives**

1387 The objective of this sub-activity is to determine whether the security objectives for the  
1388 operational environment are clearly defined.

##### 1389 **8.6.1.2 Input**

1390 The evaluation evidence for this sub-activity is:

1391 a) the PP.

## ISO/IEC 18045:2008(E)

### 1392 8.6.1.3 Action APE\_OBJ.1.1E

#### 1393 8.6.1.3.1 General

1394 ISO/IEC 15408-3:20XX APE\_OBJ.1.1C: *The statement of security objectives shall describe the security*  
1395 *objectives for the operational environment.*

#### 1396 8.6.1.3.2 Work unit APE\_OBJ.1-1

1397 The evaluator **shall check** that the statement of security objectives defines the security objectives  
1398 for the operational environment.

1399 The evaluator checks that the security objectives for the operational environment are identified.

### 1400 8.6.2 Evaluation of sub-activity (APE\_OBJ.2)

#### 1401 8.6.2.1 Objectives

1402 The objective of this sub-activity is to determine whether the security objectives adequately and  
1403 completely address the security problem definition and that the division of this problem between  
1404 the TOE and its operational environment is clearly defined.

#### 1405 8.6.2.2 Input

1406 The evaluation evidence for this sub-activity is:

1407 a) the PP.

### 1408 8.6.2.3 Action APE\_OBJ.2.1E

#### 1409 8.6.2.3.1 General

1410 ISO/IEC 15408-3:20XX APE\_OBJ.2.1C: *The statement of security objectives shall describe the security*  
1411 *objectives for the TOE and the security objectives for the operational environment.*

#### 1412 8.6.2.3.2 Work unit APE\_OBJ.2-1

1413 The evaluator **shall check** that the statement of security objectives defines the security objectives  
1414 for the TOE and the security objectives for the operational environment.

1415 The evaluator checks that both categories of security objectives are clearly identified and  
1416 separated from the other category.

1417 ISO/IEC 15408-3:20XX APE\_OBJ.2.2C: *The security objectives rationale shall trace each security*  
1418 *objective for the TOE back to threats countered by that security objective and OSPs enforced by that*  
1419 *security objective.*

#### 1420 8.6.2.3.3 Work unit APE\_OBJ.2-2

1421 The evaluator **shall check** that the security objectives rationale traces all security objectives for the  
1422 TOE back to threats countered by the objectives and/or OSPs enforced by the objectives.

1423 Each security objective for the TOE may trace back to threats or OSPs, or a combination of threats  
1424 and OSPs, but it must trace back to at least one threat or OSP. Optional requirements may require  
1425 Threats/OSPs to be specified, and security objectives associated with these SPD elements are also  
1426 covered by this work unit.

1427 Failure to trace implies that either the security objectives rationale is incomplete, the security  
1428 problem definition is incomplete, or the security objective for the TOE has no useful purpose.

1429 ISO/IEC 15408-3 APE\_OBJ.2.3C: *The security objectives rationale shall trace each security objective*  
1430 *for the operational environment back to threats countered by that security objective, OSPs enforced*  
1431 *by that security objective, and assumptions upheld by that security objective.*

#### 1432 8.6.2.3.4 Work unit APE\_OBJ.2-3

1433 The evaluator **shall check** that the security objectives rationale traces the security objectives for  
1434 the operational environment back to threats countered by that security objective, to OSPs enforced  
1435 by that security objective, and to assumptions upheld by that security objective.

1436 Each security objective for the operational environment may trace back to threats, OSPs,  
1437 assumptions, or a combination of threats, OSPs and/or assumptions, but it must trace back to at  
1438 least one threat, OSP or assumption.

1439 Failure to trace implies that either the security objectives rationale is incomplete, the security  
1440 problem definition is incomplete, or the security objective for the operational environment has no  
1441 useful purpose.

1442 ISO/IEC 15408-3:20XX APE\_OBJ.2.4C: *The security objectives rationale shall demonstrate that the*  
1443 *security objectives counter all threats.*

#### 1444 8.6.2.3.5 Work unit APE\_OBJ.2-4

1445 The evaluator **shall examine** the security objectives rationale to determine that it justifies for each  
1446 threat that the security objectives are suitable to counter that threat.

1447 If no security objectives trace back to the threat, the evaluator action related to this work unit is  
1448 assigned a fail verdict.

1449 The evaluator determines that the justification for a threat shows whether the threat is removed,  
1450 diminished or mitigated.

1451 The evaluator determines that the justification for a threat demonstrates that the security  
1452 objectives are sufficient: if all security objectives that trace back to the threat are achieved, the  
1453 threat is removed, sufficiently diminished, or the effects of the threat are sufficiently mitigated.

1454 Note that the tracings from security objectives to threats provided in the security objectives  
1455 rationale may be part of a justification, but do not constitute a justification by themselves. Even in  
1456 the case that a security objective is merely a statement reflecting the intent to prevent a particular  
1457 threat from being realised, a justification is required, but this justification may be as minimal as  
1458 "Security Objective X directly counters Threat Y".

1459 The evaluator also determines that each security objective that traces back to a threat is necessary:  
1460 when the security objective is achieved it actually contributes to the removal, diminishing or  
1461 mitigation of that threat.

1462 ISO/IEC 15408-3:20XX, APE\_OBJ.2.5C: *The security objectives rationale shall demonstrate that the*  
1463 *security objectives enforce all OSPs.*

#### 1464 8.6.2.3.6 Work unit APE\_OBJ.2-5

1465 The evaluator **shall examine** the security objectives rationale to determine that for each OSP it  
1466 justifies that the security objectives are suitable to enforce that OSP.

## ISO/IEC 18045:2008(E)

1467 If no security objectives trace back to the OSP, the evaluator action related to this work unit is  
1468 assigned a fail verdict.

1469 The evaluator determines that the justification for an OSP demonstrates that the security  
1470 objectives are sufficient: if all security objectives that trace back to that OSP are achieved, the OSP  
1471 is enforced.

1472 The evaluator also determines that each security objective that traces back to an OSP is necessary:  
1473 when the security objective is achieved it actually contributes to the enforcement of the OSP.

1474 Note that the tracings from security objectives to OSPs provided in the security objectives rationale  
1475 may be part of a justification, but do not constitute a justification by themselves. In the case that a  
1476 security objective is merely a statement reflecting the intent to enforce a particular OSP, a  
1477 justification is required, but this justification may be as minimal as "Security Objective X directly  
1478 enforces OSP Y".

1479 ISO/IEC 15408-3:20XX, APE\_OBJ.2.6C: *The security objectives rationale shall demonstrate that the*  
1480 *security objectives for the operational environment uphold all assumptions.*

### 1481 8.6.2.3.7 Work unit APE\_OBJ.2-6

1482 The evaluator **shall examine** the security objectives rationale to determine that for each  
1483 assumption for the operational environment it contains an appropriate justification that the  
1484 security objectives for the operational environment are suitable to uphold that assumption.

1485 If no security objectives for the operational environment trace back to the assumption, the  
1486 evaluator action related to this work unit is assigned a fail verdict.

1487 The evaluator determines that the justification for an assumption about the operational  
1488 environment of the TOE demonstrates that the security objectives are sufficient: if all security  
1489 objectives for the operational environment that trace back to that assumption are achieved, the  
1490 operational environment upholds the assumption.

1491 The evaluator also determines that each security objective for the operational environment that  
1492 traces back to an assumption about the operational environment of the TOE is necessary: when the  
1493 security objective is achieved it actually contributes to the operational environment upholding the  
1494 assumption.

1495 Note that the tracings from security objectives for the operational environment to assumptions  
1496 provided in the security objectives rationale may be a part of a justification, but do not constitute a  
1497 justification by themselves. Even in the case that a security objective of the operational  
1498 environment is merely a restatement of an assumption, a justification is required, but this  
1499 justification may be as minimal as "Security Objective X directly upholds Assumption Y".

## 1500 8.7 Extended components definition (APE\_ECD)

### 1501 8.7.1 Evaluation of sub-activity (APE\_ECD.1)

#### 1502 8.7.1.1 Objectives

1503 The objective of this sub-activity is to determine whether extended components have been clearly  
1504 and unambiguously defined, and whether they are necessary, i.e. they may not be clearly expressed  
1505 using existing ISO/IEC 15408-2 or ISO/IEC 15408-3 components.

#### 1506 8.7.1.2 Input

1507 The evaluation evidence for this sub-activity is:

- 1508 a) the PP.
- 1509 **8.7.1.3 Action APE\_ECD.1.1E**
- 1510 **8.7.1.3.1 General**
- 1511 ISO/IEC 15408-3:20XX, APE\_ECD.1.1C: *The statement of security requirements shall identify all*  
 1512 *extended security requirements.*
- 1513 **8.7.1.3.2 Work unit APE\_ECD.1-1**
- 1514 The evaluator **shall check** that all security requirements in the statement of security requirements  
 1515 that are not identified as extended requirements are present in ISO/IEC 15408-2 or in ISO/IEC  
 1516 15408-3.
- 1517 ISO/IEC 15408-3:20XX, APE\_ECD.1.2C: *The extended components definition shall define an extended*  
 1518 *component for each extended security requirement.*
- 1519 **8.7.1.3.3 Work unit APE\_ECD.1-2**
- 1520 The evaluator **shall check** that the extended components definition defines an extended  
 1521 component for each extended security requirement.
- 1522 If the PP does not contain extended security requirements, this work unit is not applicable and  
 1523 therefore considered to be satisfied.
- 1524 A single extended component may be used to define multiple iterations of an extended security  
 1525 requirement, it is not necessary to repeat this definition for each iteration.
- 1526 ISO/IEC 15408-3:20XX, APE\_ECD.1.3C: *The extended components definition shall describe how each*  
 1527 *extended component is related to the existing ISO/IEC 15408 components, families, and classes.*
- 1528 **8.7.1.3.4 Work unit APE\_ECD.1-3**
- 1529 The evaluator **shall examine** the extended components definition to determine that it describes  
 1530 how each extended component fits into the existing ISO/IEC 15408 components, families, and  
 1531 classes.
- 1532 If the PP does not contain extended security requirements, this work unit is not applicable and  
 1533 therefore considered to be satisfied.
- 1534 The evaluator determines that each extended component is either:
- 1535 a) a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 family, or
- 1536 b) a member of a new family defined in the PP.
- 1537 If the extended component is a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 family,  
 1538 the evaluator determines that the extended components definition adequately describes why the  
 1539 extended component should be a member of that family and how it relates to other components of  
 1540 that family.
- 1541 If the extended component is a member of a new family defined in the PP, the evaluator confirms  
 1542 that the extended component is not appropriate for an existing family.
- 1543 If the PP defines new families, the evaluator determines that each new family is either:

## ISO/IEC 18045:2008(E)

- 1544 a) a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 class, or
- 1545 b) a member of a new class defined in the PP.
- 1546 If the family is a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 class, the evaluator  
1547 determines that the extended components definition adequately describes why the family should  
1548 be a member of that class and how it relates to other families in that class.
- 1549 If the family is a member of a new class defined in the PP, the evaluator confirms that the family is  
1550 not appropriate for an existing class.
- 1551 **8.7.1.3.5 Work unit APE\_ECD.1-4**
- 1552 The evaluator **shall examine** the extended components definition to determine that each definition  
1553 of an extended component identifies all applicable dependencies of that component.
- 1554 If the PP does not contain extended security requirements, this work unit is not applicable and  
1555 therefore considered to be satisfied.
- 1556 The evaluator confirms that no applicable dependencies have been overlooked by the PP author.
- 1557 ISO/IEC 15408-3:20XX, APE\_ECD.1.4C: *The extended components definition shall use the existing*  
1558 *ISO/IEC 15408 components, families, classes, and methodology as a model for presentation.*
- 1559 **8.7.1.3.6 Work unit APE\_ECD.1-5**
- 1560 The evaluator **shall examine** the extended components definition to determine that each extended  
1561 functional component uses the existing ISO/IEC 15408-2 components as a model for presentation.
- 1562 If the PP does not contain extended SFRs, this work unit is not applicable and therefore considered  
1563 to be satisfied.
- 1564 The evaluator determines that the extended functional component is consistent with ISO/IEC  
1565 15408-2:20XX 6.1.3, Component structure.
- 1566 If the extended functional component uses operations, the evaluator determines that the extended  
1567 functional component is consistent with ISO/IEC 15408-1 Subclause 7.1, Operations.
- 1568 If the extended functional component is hierarchical to an existing functional component, the  
1569 evaluator determines that the extended functional component is consistent with ISO/IEC 15408-  
1570 2:20XX, 6.2.1, Component changes highlighting.
- 1571 **8.7.1.3.7 Work unit APE\_ECD.1-6**
- 1572 The evaluator **shall examine** the extended components definition to determine that each definition  
1573 of a new functional family uses the existing ISO/IEC 15408 functional families as a model for  
1574 presentation.
- 1575 If the PP does not define new functional families, this work unit is not applicable and therefore  
1576 considered to be satisfied.
- 1577 The evaluator determines that all new functional families are defined consistent with ISO/IEC  
1578 15408-2:20XX, 6.1.2, Family structure.



1579 **8.7.1.3.8 Work unit APE\_ECD.1-7**

1580 The evaluator *shall examine* the extended components definition to determine that each definition  
1581 of a new functional class uses the existing ISO/IEC 15408 functional classes as a model for  
1582 presentation.

1583 If the PP does not define new functional classes, this work unit is not applicable and therefore  
1584 considered to be satisfied.

1585 The evaluator determines that all new functional classes are defined consistent with ISO/IEC  
1586 15408-2:20XX, 6.1.1, Class structure

1587 **8.7.1.3.9 Work unit APE\_ECD.1-8**

1588 The evaluator *shall examine* the extended components definition to determine that each definition  
1589 of an extended assurance component uses the existing ISO/IEC 15408-3 components as a model  
1590 for presentation.

1591 If the PP does not contain extended SARs, this work unit is not applicable and therefore considered  
1592 to be satisfied.

1593 The evaluator determines that the extended assurance component definition is consistent with  
1594 ISO/IEC 15408-3:20XX, 6.1.3, Assurance component structure.

1595 If the extended assurance component uses operations, the evaluator determines that the extended  
1596 assurance component is consistent with ISO/IEC 15408-1:20XX, 7.1, Operations.

1597 If the extended assurance component is hierarchical to an existing assurance component, the  
1598 evaluator determines that the extended assurance component is consistent with ISO/IEC 15408-  
1599 3:20XX, 6.1.3, Assurance component structure.

1600 **8.7.1.3.10 Work unit APE\_ECD.1-9**

1601 The evaluator *shall examine* the extended components definition to determine that, for each  
1602 defined extended assurance component, applicable methodology has been provided.

1603 If the PP does not contain extended SARs, this work unit is not applicable and therefore considered  
1604 to be satisfied.

1605 The evaluator determines that, for each evaluator action element of each extended SAR, one or  
1606 more work units are provided and that successfully performing all work units for a given evaluator  
1607 action element will demonstrate that the element has been achieved.

1608 **8.7.1.3.11 Work unit APE\_ECD.1-10**

1609 The evaluator *shall examine* the extended components definition to determine that each definition  
1610 of a new assurance family uses the existing ISO/IEC 15408 assurance families as a model for  
1611 presentation.

1612 If the PP does not define new assurance families, this work unit is not applicable and therefore  
1613 considered to be satisfied.

1614 The evaluator determines that all new assurance families are defined consistent with ISO/IEC  
1615 15408-3:20XX, 6.1.2, Assurance family structure.

## ISO/IEC 18045:2008(E)

### 1616 8.7.1.3.12 Work unit APE\_ECD.1-11

1617 The evaluator **shall examine** the extended components definition to determine that each definition  
1618 of a new assurance class uses the existing ISO/IEC 15408 assurance classes as a model for  
1619 presentation.

1620 If the PP does not define new assurance classes, this work unit is not applicable and therefore  
1621 considered to be satisfied.

1622 The evaluator determines that all new assurance classes are defined consistent with ISO/IEC  
1623 15408-3:20XX, 6.1.1, Assurance class structure.

1624 ISO/IEC 15408-3 APE\_ECD.1.5C: *The extended components shall consist of measurable and objective*  
1625 *elements such that conformance or nonconformance to these elements can be demonstrated.*

### 1626 8.7.1.3.13 Work unit APE\_ECD.1-12

1627 The evaluator **shall examine** the extended components definition to determine that each element  
1628 in each extended component is measurable and states objective evaluation requirements, such that  
1629 conformance or nonconformance can be demonstrated.

1630 If the PP does not contain extended security requirements, this work unit is not applicable and  
1631 therefore considered to be satisfied.

1632 The evaluator determines that elements of extended functional components are stated in such a  
1633 way that they are testable, and traceable through the appropriate TSF representations.

1634 The evaluator also determines that elements of extended assurance components avoid the need for  
1635 subjective evaluator judgement.

1636 The evaluator is reminded that whilst being measurable and objective is appropriate for all  
1637 evaluation criteria, it is acknowledged that no formal method exists to prove such properties.  
1638 Therefore the existing ISO/IEC 15408 functional and assurance components are to be used as a  
1639 model for determining what constitutes conformance to this requirement.

### 1640 8.7.1.4 Action APE\_ECD.1.2E

#### 1641 8.7.1.4.1 Work unit APE\_ECD.1-13

1642 The evaluator **shall examine** the extended components definition to determine that each extended  
1643 component may not be clearly expressed using existing components.

1644 If the PP does not contain extended security requirements, this work unit is not applicable and  
1645 therefore considered to be satisfied.

1646 The evaluator should take components from ISO/IEC 15408-2 and ISO/IEC 15408-3, other  
1647 extended components that have been defined in the PP, combinations of these components, and  
1648 possible operations on these components into account when making this determination.

1649 The evaluator is reminded that the role of this work unit is to preclude unnecessary duplication of  
1650 components, that is, components that may be clearly expressed by using other components. The  
1651 evaluator should not undertake an exhaustive search of all possible combinations of components  
1652 including operations in an attempt to find a way to express the extended component by using  
1653 existing components.

1654 **8.8 Security requirements (APE\_REQ)**

1655 **8.8.1 Evaluation of sub-activity (APE\_REQ.1)**

1656 **8.8.1.1 Objectives**

1657 The objective of this sub-activity is to determine whether the SFRs and SARs are clear,  
1658 unambiguous and well-defined, whether they are internally consistent, and whether the SFRs  
1659 counter the threats and implement the organisational security policies of the TOE.

1660 **8.8.1.2 Input**

1661 The evaluation evidence for this sub-activity is:

1662 a) the PP.

1663 **8.8.1.3 Action APE\_REQ.1.1E**

1664 **8.8.1.3.1 General**

1665 ISO/IEC 15408-3:20XX, APE\_REQ.1.1C: *The statement of security requirements shall describe the*  
1666 *SFRs and the SARs.*

1667 **8.8.1.3.2 Work unit APE\_REQ.1-1**

1668 The evaluator **shall check** that the statement of security requirements describes the SFRs.

1669 The evaluator determines that each SFR is identified by one of the following means:

1670 a) by reference to an individual component in ISO/IEC 15408-2;

1671 b) by reference to an extended component in the extended components definition of the  
1672 PP;

1673 c) by reference to a PP that the PP claims to be conformant with including any optional  
1674 requirements defined in the PP;

1675 d) by reference to a security requirements package that the PP claims to be conformant  
1676 with;

1677 e) by reproduction in the PP.

1678 It is not required to use the same means of identification for all SFRs.

1679 **8.8.1.3.3 Work unit APE\_REQ.1-2**

1680 The evaluator **shall check** that the statement of security requirements describes the SARs.

1681 The evaluator determines that each SAR is identified by one of the following means:

1682 a) by reference to an individual component in ISO/IEC 15408-3;

1683 b) by reference to an extended component in the extended components definition of the  
1684 PP;

## ISO/IEC 18045:2008(E)

- 1685 c) by reference to a PP that the PP claims to be conformant with;
- 1686 d) by reference to a security requirements package that the PP claims to be conformant  
1687 with;
- 1688 e) by reproduction in the PP.
- 1689 It is not required to use the same means of identification for all SARs.
- 1690 ISO/IEC 15408-3:20XX, APE\_REQ.1.2C: *All subjects, objects, operations, security attributes, external*  
1691 *entities and other terms that are used in the SFRs and the SARs shall be defined.*
- 1692 **8.8.1.3.4 Work unit APE\_REQ.1-3**
- 1693 The evaluator **shall examine** the PP to determine that all subjects, objects, operations, security  
1694 attributes, external entities and other terms that are used in the SFRs and the SARs are defined.
- 1695 The evaluator determines that the PP defines all:
- 1696 • (types of) subjects and objects that are used in the SFRs;
- 1697 • (types of) security attributes of subjects, users, objects, information, sessions and/or  
1698 resources, possible values that these attributes may take and any relations between these  
1699 values (e.g. top\_secret is “higher” than secret);
- 1700 • (types of) operations that are used in the SFRs, including the effects of these operations;
- 1701 • (types of) external entities in the SFRs;
- 1702 • other terms that are introduced in the SFRs and/or SARs by completing operations, if  
1703 these terms are not immediately clear, or are used outside their dictionary definition.
- 1704 The goal of this work unit is to ensure that the SFRs and SARs are well-defined and that no  
1705 misunderstanding may occur due to the introduction of vague terms. This work unit should not be  
1706 taken into extremes, by forcing the PP author to define every single word. The general audience of  
1707 a set of security requirements should be assumed to have a reasonable knowledge of IT, security  
1708 and “Evaluation criteria for IT security”.
- 1709 All of the above may be presented in groups, classes, roles, types or other groupings or  
1710 characterisations that allow easy understanding.
- 1711 The evaluator is reminded that these lists and definitions do not have to be part of the statement of  
1712 security requirements, but may be placed (in part or in whole) in different subclauses. This may be  
1713 especially applicable if the same terms are used in the rest of the PP.
- 1714 ISO/IEC 15408-3:20XX, APE\_REQ.1.3C: *The statement of security requirements shall include a*  
1715 *natural language description, part of which describes how the SFRs combine together to provide*  
1716 *security functionality in terms of the architecture that is visible to Administrators and other users.*
- 1717 **8.8.1.3.5 Work unit APE\_REQ.1-4**
- 1718 The evaluator **shall check** that the statement of security requirements includes a natural language  
1719 description, part of which describes how the SFRs combine together to provide security  
1720 functionality in terms of the architecture that is visible to Administrators and other users.

1721 The description is intended to make clear connections between SFRs and to provide a view of how  
 1722 they provide security functionality that is recognizable to Administrators and other types of user.  
 1723 The description in terms of the architecture that is "visible to Administrators and other users"  
 1724 means that the description must relate the security behavior to visible elements, but the  
 1725 mechanisms themselves need not be visible. For example: when describing authentication using a  
 1726 biometric mechanism, the calculation of the match or score might not be visible, but (a) might  
 1727 relate to a referenced description of a matching algorithm, (b) might be based on specific template  
 1728 files maintained by the Administrator, and (c) will result in acceptance or rejection of the  
 1729 authentication attempt – therefore the description might make use of any or all of these items (a) –  
 1730 (c). No specific format for this information is prescribed, and the description need not all be located  
 1731 alongside the SFRs themselves (e.g. some of it might be in the PP Introduction). The intention of the  
 1732 requirement is to make the meaning of the SFRs clearer and more easily understood by readers of  
 1733 the PP who may not have deep knowledge of the CC but who are familiar with the product type.

1734 The evaluator determines that all operations are identified in each SFR or SAR where such an  
 1735 operation is used. This includes both completed operations and uncompleted operations.  
 1736 Identification may be achieved by typographical distinctions, or by explicit identification in the  
 1737 surrounding text, or by any other distinctive means.

1738 ISO/IEC 15408-3:20XX, APE\_REQ.1.4C: *The statement of security requirements shall identify all*  
 1739 *operations on the security requirements.*

#### 1740 **8.8.1.3.6 Work unit APE\_REQ.1-5**

1741 The evaluator **shall check** that the statement of security requirements identifies all operations on  
 1742 the security requirements.

1743 The evaluator determines that all operations are identified in each SFR or SAR where such an  
 1744 operation is used. This includes both completed operations and uncompleted operations.  
 1745 Identification may be achieved by typographical distinctions, or by explicit identification in the  
 1746 surrounding text, or by any other distinctive means.

1747 If the PP defines *selection-based* SFRs, the evaluator determines that the PP clearly identifies the  
 1748 dependencies between the selection in an SFR and the selection-based SFR(s) to be included in the  
 1749 PP/ST should that selection be chosen by the PP/ST author.

1750 ISO/IEC 15408-3:20XX, APE\_REQ.1.5C: *All operations shall be performed correctly.*

#### 1751 **8.8.1.3.7 Work unit APE\_REQ.1-6**

1752 The evaluator **shall examine** the statement of security requirements to determine that all  
 1753 assignment operations are performed correctly.

1754 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C.

#### 1755 **8.8.1.3.8 Work unit APE\_REQ.1-7**

1756 The evaluator **shall examine** the statement of security requirements to determine that all iteration  
 1757 operations are performed correctly.

1758 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C.

#### 1759 **8.8.1.3.9 Work unit APE\_REQ.1-8**

1760 The evaluator **shall examine** the statement of security requirements to determine that all selection  
 1761 operations are performed correctly.

1762 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C.

## ISO/IEC 18045:2008(E)

### 1763 8.8.1.3.10 Work unit APE\_REQ.1-9

1764 The evaluator **shall examine** the statement of security requirements to determine that all  
1765 refinement operations are performed correctly.

1766 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C.

1767 ISO/IEC 15408-3:20XX, APE\_REQ.1.6C: *Each dependency of the security requirements shall either be*  
1768 *satisfied, or the security requirements rationale shall justify the dependency not being satisfied.*

### 1769 8.8.1.3.11 Work unit APE\_REQ.1-10

1770 The evaluator **shall examine** the statement of security requirements to determine that each  
1771 dependency of the security requirements is either satisfied, or that the security requirements  
1772 rationale justifies the dependency not being satisfied.

1773 A dependency is satisfied by the inclusion of the relevant component (or one that is hierarchical to  
1774 it) within the statement of security requirements. The component used to satisfy the dependency  
1775 should, if necessary, be modified by operations to ensure that it actually satisfies that dependency.

1776 A justification that a dependency is not met should address either:

1777 a) why the dependency is not necessary or useful, in which case no further information  
1778 is required; or

1779 b) that the dependency has been addressed by the operational environment of the TOE,  
1780 in which case the justification should describe how the security objectives for the  
1781 operational environment address this dependency.

1782 If a functional package identifies dependences on its requirements that need to be satisfied by the  
1783 underlying PP, the evaluator ensures that their analysis covers these dependencies as well.

1784 ISO/IEC 15408-3:20XX, APE\_REQ.1.7C: *The security requirements rationale shall trace each SFR*  
1785 *back to the threats countered by that SFR and OSPs enforced by that SFR.*

### 1786 8.8.1.3.12 Work unit APE\_REQ.1-11

1787 The evaluator **shall check** that the security requirements rationale traces each SFR back to the  
1788 threats countered by that SFR and OSPs enforced by that SFR.

1789 The evaluator determines that each SFR is traced back to at least one threat or OSP for the TOE.

1790 Failure to trace implies that either the security requirements rationale is incomplete, the security  
1791 objectives for the TOE are incomplete, or the SFR has no useful purpose.

1792 There is no prescribed location where this tracing element of the rationale must be placed: for  
1793 example, the relevant parts may be located under each threat and OSP in order to help make the  
1794 security argument clearer and easier to read.

1795 ISO/IEC 15408-3:20XX, APE\_REQ.1.8C: *The security requirements rationale shall trace each security*  
1796 *objective for the operational environment back to threats countered by that security objective, OSPs*  
1797 *enforced by that security objective, and assumptions upheld by that security objective.*

1798 **8.8.1.3.13 Work unit APE\_REQ.1-12**

1799 The evaluator **shall check** that the security objectives requirements rationale traces the security  
 1800 objectives for the operational environment back to threats countered by that security objective, to  
 1801 OSPs enforced by that security objective, and to assumptions upheld by that security objective.

1802 Each security objective for the operational environment may trace back to threats, OSPs,  
 1803 assumptions, or a combination of threats, OSPs and/or assumptions, but it must trace back to at  
 1804 least one threat, OSP or assumption.

1805 Failure to trace implies that either the security objectives requirements rationale is incomplete, the  
 1806 security problem definition is incomplete, or the security objective for the operational  
 1807 environment has no useful purpose.

1808 There is no prescribed location where this tracing element of the rationale must be placed: for  
 1809 example, the relevant parts may be located under each threat, OSP and assumption in order to help  
 1810 make the security argument clearer and easier to read.

1811 ISO/IEC 15408-3:20XX, APE\_REQ.1.9C: *The security requirements rationale shall demonstrate that*  
 1812 *the SFRs (in conjunction with the security objectives for the environment) counter all threats for the*  
 1813 *TOE.*

1814 **8.8.1.3.14 Work unit APE\_REQ.1-13**

1815 The evaluator **shall examine** the security requirements rationale to determine that for each threat  
 1816 it demonstrates that the SFRs are suitable to meet that threat.

1817 If no SFRs trace back to a threat, the evaluator action related to this work unit is assigned a fail  
 1818 verdict.

1819 The evaluator determines that the justification for a threat shows whether the threat is removed,  
 1820 diminished or mitigated.

1821 The evaluator determines that the justification for a threat demonstrates that the SFRs are  
 1822 sufficient: if all SFRs that trace back to the threat are achieved then, in the context of any applicable  
 1823 OSPs and assumptions, the threat is removed, sufficiently diminished, or the effects of the threat  
 1824 are sufficiently mitigated.

1825 Note that simply listing in the security requirements rationale the SFRs associated with each threat  
 1826 may be part of a justification, but does not constitute a justification by itself. A descriptive  
 1827 justification is required, although in simple cases this justification may be as minimal as "SFR X  
 1828 directly counters Threat Y".

1829 The evaluator also determines that each SFR that traces back to a threat is necessary: when the SFR  
 1830 is implemented it actually contributes to the removal, diminishing or mitigation of that threat.

1831 ISO/IEC 15408-3:20XX, APE\_REQ.1.10C: *The security requirements rationale shall demonstrate that*  
 1832 *the SFRs (in conjunction with the security objectives for the environment) enforce all OSPs for the TOE.*

1833 **8.8.1.3.15 Work unit APE\_REQ.1-14**

1834 The evaluator **shall examine** the security requirements rationale to determine that for each OSP it  
 1835 justifies that the SFRs are suitable to enforce that OSP.

1836 If no SFRs or security objectives for the operational environment trace back to the OSP, the  
 1837 evaluator action related to this work unit is assigned a fail verdict.

## ISO/IEC 18045:2008(E)

1838 The evaluator determines that the justification for an OSP demonstrates that the security  
1839 objectives are sufficient: if all SFRs that trace back to that OSP are achieved then, in the context of  
1840 any applicable assumptions, the OSP is enforced.

1841 The evaluator also determines that each SFR that traces back to an OSP is necessary: when the SFR  
1842 is implemented it actually contributes to the enforcement of the OSP.

1843 Note that simply listing in the security requirements rationale the SFRs associated with each OSP  
1844 may be part of a justification, but does not constitute a justification by itself. A descriptive  
1845 justification is required, although in simple cases this justification may be as minimal as "SFR X  
1846 directly enforces OSP Y".

1847 ISO/IEC 15408-3:20XX, APE\_REQ.1.11C: The security requirements rationale shall demonstrate  
1848 that the SFRs (in conjunction with the security objectives for the environment) enforce all OSPs for  
1849 the TOE.

### 1850 8.8.1.3.16 Work unit APE\_REQ.1-15

1851 The evaluator **shall examine** the security requirements rationale to determine that for each  
1852 assumption for the operational environment it contains an appropriate justification that the  
1853 security objectives for the operational environment are suitable to uphold that assumption.

1854 If no security objectives for the operational environment trace back to the assumption, the  
1855 evaluator action related to this work unit is assigned a fail verdict.

1856 The evaluator determines that the justification for an assumption about the operational  
1857 environment of the TOE demonstrates that the security objectives are sufficient: if all security  
1858 objectives for the operational environment that trace back to that assumption are achieved, the  
1859 operational environment upholds the assumption.

1860 The evaluator also determines that each security objective for the operational environment that  
1861 traces back to an assumption about the operational environment of the TOE is necessary: when the  
1862 security objective is achieved it actually contributes to the operational environment upholding the  
1863 assumption.

1864 Note that simply listing in the security requirements rationale the security objectives for the  
1865 operational environment associated with each assumption may be a part of a justification, but does  
1866 not constitute a justification by itself. A descriptive justification is required, although in simple  
1867 cases this justification may be as minimal as "Security Objective X directly upholds Assumption Y".

1868

1869 ISO/IEC 15408-3:20XX, APE\_REQ.1.12C: *The statement of security requirements shall be internally*  
1870 *consistent.*

### 1871 8.8.1.3.17 Work unit APE\_REQ.1-16

1872 The evaluator **shall examine** the statement of security requirements to determine that it is  
1873 internally consistent.

1874 The evaluator determines that the combined set of all SFRs and SARs is internally consistent. With  
1875 respect to optional requirements, the evaluator determines that:

- 1876 a) All optional requirements either trace to an SPD element that is itself not optional, or trace  
1877 to an SPD element that is clearly associated with that optional SFR;



1878 b) All optional requirements are clearly identified as being required if a conformant TOE  
 1879 implements the functionality covered by the requirement, or as being “purely optional”;  
 1880 and

1881 c) All optional requirements do not conflict with non-optional requirements (a capability  
 1882 cannot be both required and optional; however, a base capability can be required with  
 1883 enhancements to that capability being specified as optional).

1884 The evaluator determines that on all occasions where different security requirements apply to the  
 1885 same types of developer evidence, events, operations, data, tests to be performed etc. or to “all  
 1886 objects”, “all subjects” etc., that these requirements do not conflict.

1887 Some possible conflicts are:

1888 a) an extended SAR specifying that the design of a certain cryptographic algorithm is to  
 1889 be kept secret, and another extended SAR specifying an open source review;

1890 b) FAU\_Gen.1 Audit data generation specifying that subject identity is to be logged,  
 1891 FDP\_ACC.1 Subset access control specifying who has access to these logs, and  
 1892 FPR\_UNO.1 Unobservability specifying that some actions of subjects should be  
 1893 unobservable to other subjects. If the subject that should not be able to see an  
 1894 activity may access logs of this activity, these SFRs conflict;

1895 c) FDP\_RIP.1 Subset residual information protection specifying deletion of information  
 1896 no longer needed, and FDP\_ROL.1 Basic rollback specifying that a TOE may return to  
 1897 a previous state. If the information that is needed for the rollback to the previous  
 1898 state has been deleted, these requirements conflict;

1899 d) Multiple iterations of FDP\_ACC.1 Subset access control, especially where some  
 1900 iterations cover the same subjects, objects, or operations. If one access control SFR  
 1901 allows a subject to perform an operation on an object, while another access control  
 1902 SFR does not allow this, these requirements conflict.

## 1903 **8.8.2 Evaluation of sub-activity (APE\_REQ.2)**

### 1904 **8.8.2.1 Objectives**

1905 The objective of this sub-activity is to determine whether the SFRs and SARs are clear,  
 1906 unambiguous and well-defined, whether they are internally consistent, and whether the SFRs meet  
 1907 the security objectives of the TOE.

### 1908 **8.8.2.2 Input**

1909 The evaluation evidence for this sub-activity is:

1910 a) the PP.

### 1911 **8.8.2.3 Action APE\_REQ.2.1E**

#### 1912 **8.8.2.3.1 General**

1913 ISO/IEC 15408-3:20XX, APE\_REQ.2.1C: *The statement of security requirements shall describe the*  
 1914 *SFRs and the SARs.*

## ISO/IEC 18045:2008(E)

### 1915 8.8.2.3.2 Work unit APE\_REQ.2-1

1916 The evaluator **shall check** that the statement of security requirements describes the SFRs.

1917 The evaluator determines that each SFR is identified by one of the following means:

1918 a) by reference to an individual component in ISO/IEC 15408-2;

1919 b) by reference to an extended component in the extended components definition of the  
1920 PP;

1921 c) by reference to an individual component in a PP that the PP claims to be conformant  
1922 with, including any optional requirements defined in the PP;

1923 d) by reference to an individual component in a security requirements package that the  
1924 PP claims to be conformant with;

1925 e) by reproduction in the PP.

1926 It is not required to use the same means of identification for all SFRs.

### 1927 8.8.2.3.3 Work unit APE\_REQ.2-2

1928 The evaluator **shall check** that the statement of security requirements describes the SARs.

1929 The evaluator determines that each SAR is identified by one of the following means:

1930 a) by reference to an individual component in ISO/IEC 15408-3;

1931 b) by reference to an extended component in the extended components definition of the  
1932 PP;

1933 c) by reference to an individual component in a PP that the PP claims to be conformant  
1934 with;

1935 d) by reference to an individual component in a security requirements package that the  
1936 PP claims to be conformant with;

1937 e) by reproduction in the PP.

1938 It is not required to use the same means of identification for all SARs.

1939 Note that if optional requirements are defined by the PP, there may be associated threats that are  
1940 covered by this work unit.

1941 ISO/IEC 15408-3 APE\_REQ.2.2C: *All subjects, objects, operations, security attributes, external entities*  
1942 *and other terms that are used in the SFRs and the SARs shall be defined.*

### 1943 8.8.2.3.4 Work unit APE\_REQ.2-3

1944 The evaluator **shall examine** the PP to determine that all subjects, objects, operations, security  
1945 attributes, external entities and other terms that are used in the SFRs and the SARs are defined.

- 1946 The evaluator determines that the PP defines all:
- 1947 • (types of) subjects and objects that are used in the SFRs;
  - 1948 • (types of) security attributes of subjects, users, objects, information, sessions and/or  
1949 resources, possible values that these attributes may take and any relations between these  
1950 values (e.g. top\_secret is “higher” than secret);
  - 1951 • (types of) operations that are used in the SFRs, including the effects of these operations;
  - 1952 • (types of) external entities in the SFRs;
  - 1953 • other terms that are introduced in the SFRs and/or SARs by completing operations, if  
1954 these terms are not immediately clear, or are used outside their dictionary definition.
- 1955 The goal of this work unit is to ensure that the SFRs and SARs are well-defined and that no  
1956 misunderstanding may occur due to the introduction of vague terms. This work unit should not be  
1957 taken into extremes, by forcing the PP author to define every single word. The general audience of  
1958 a set of security requirements should be assumed to have a reasonable knowledge of IT, security  
1959 and “Evaluation criteria for IT security”.
- 1960 All of the above may be presented in groups, classes, roles, types or other groupings or  
1961 characterisations that allow easy understanding.
- 1962 The evaluator is reminded that these lists and definitions do not have to be part of the statement of  
1963 security requirements, but may be placed (in part or in whole) in different subclauses. This may be  
1964 especially applicable if the same terms are used in the rest of the PP.
- 1965 ISO/IEC 15408-3 APE\_REQ.2.3C: *The statement of security requirements shall identify all operations*  
1966 *on the security requirements.*
- 1967 **8.8.2.3.5 Work unit APE\_REQ.2-4**
- 1968 The evaluator **shall check** that the statement of security requirements identifies all operations on  
1969 the security requirements.
- 1970 The evaluator determines that all operations are identified in each SFR or SAR where such an  
1971 operation is used. This includes both completed operations and uncompleted operations.  
1972 Identification may be achieved by typographical distinctions, or by explicit identification in the  
1973 surrounding text, or by any other distinctive means.
- 1974 If the PP defines *selection-based* SFRs, the evaluator determines that the PP clearly identifies the  
1975 dependencies between the selection in an SFR and the selection-based SFR(s) to be included in the  
1976 PP/ST should that selection be chosen by the PP/ST author.
- 1977 ISO/IEC 15408-3 APE\_REQ.2.4C: *All operations shall be performed correctly.*
- 1978 **8.8.2.3.6 Work unit APE\_REQ.2-5**
- 1979 The evaluator **shall examine** the statement of security requirements to determine that all  
1980 assignment operations are performed correctly.
- 1981 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C..

## ISO/IEC 18045:2008(E)

### 1982 8.8.2.3.7 Work unit APE\_REQ.2-6

1983 The evaluator **shall examine** the statement of security requirements to determine that all iteration  
1984 operations are performed correctly.

1985 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C.

### 1986 8.8.2.3.8 Work unit APE\_REQ.2-7

1987 The evaluator **shall examine** the statement of security requirements to determine that all selection  
1988 operations are performed correctly.

1989 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C.

### 1990 8.8.2.3.9 Work unit APE\_REQ.2-8

1991 The evaluator **shall examine** the statement of security requirements to determine that all  
1992 refinement operations are performed correctly.

1993 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C.

1994 ISO/IEC 15408-3 APE\_REQ.2.5C: *Each dependency of the security requirements shall either be*  
1995 *satisfied, or the security requirements rationale shall justify the dependency not being satisfied.*

### 1996 8.8.2.3.10 Work unit APE\_REQ.2-9

1997 The evaluator **shall examine** the statement of security requirements to determine that each  
1998 dependency of the security requirements is either satisfied, or that the security requirements  
1999 rationale justifies the dependency not being satisfied.

2000 A dependency is satisfied by the inclusion of the relevant component (or one that is hierarchical to  
2001 it) within the statement of security requirements. The component used to satisfy the dependency  
2002 should, if necessary, be modified by operations to ensure that it actually satisfies that dependency.

2003 A justification that a dependency is not met should address either:

2004 a) why the dependency is not necessary or useful, in which case no further information  
2005 is required; or

2006 b) that the dependency has been addressed by the operational environment of the TOE,  
2007 in which case the justification should describe how the security objectives for the  
2008 operational environment address this dependency.

2009 If a functional package identifies dependencies on its requirements that need to be satisfied by the  
2010 underlying PP, the evaluator ensures that their analysis covers these dependencies as well.

2011 ISO/IEC 15408-3 APE\_REQ.2.6C: *The security requirements rationale shall trace each SFR back to*  
2012 *the security objectives for the TOE.*

### 2013 8.8.2.3.11 Work unit APE\_REQ.2-10

2014 The evaluator **shall check** that the security requirements rationale traces each SFR back to the  
2015 security objectives for the TOE.

2016 Optional requirements may require Threats/OSPs to be specified, and security objectives  
2017 associated with these SPD elements are also covered by this work unit.

- 2018 The evaluator determines that each SFR is traced back to at least one security objective for the TOE.
- 2019 Failure to trace implies that either the security requirements rationale is incomplete, the security  
2020 objectives for the TOE are incomplete, or the SFR has no useful purpose.
- 2021 ISO/IEC 15408-3 APE\_REQ.2.7C: *The security requirements rationale shall demonstrate that the*  
2022 *SFRs meet all security objectives for the TOE.*
- 2023 **8.8.2.3.12 Work unit APE\_REQ.2-11**
- 2024 The evaluator **shall examine** the security requirements rationale to determine that for each  
2025 security objective for the TOE it justifies that the SFRs are suitable to meet that security objective  
2026 for the TOE.
- 2027 If no SFRs trace back to the security objective for the TOE, the evaluator action related to this work  
2028 unit is assigned a fail verdict.
- 2029 The evaluator determines that the justification for a security objective for the TOE demonstrates  
2030 that the SFRs are sufficient: if all SFRs that trace back to the objective are satisfied, the security  
2031 objective for the TOE is achieved.
- 2032 If the SFRs that trace back to a security objective for the TOE have any uncompleted assignments,  
2033 or uncompleted or restricted selections, the evaluator determines that for every conceivable  
2034 completion or combination of completions of these operations, the security objective is still met.
- 2035 The evaluator also determines that each SFR that traces back to a security objective for the TOE is  
2036 necessary: when the SFR is satisfied, it actually contributes to achieving the security objective.
- 2037 Note that the tracings from SFRs to security objectives for the TOE provided in the security  
2038 requirements rationale may be a part of the justification, but do not constitute a justification by  
2039 themselves.
- 2040 ISO/IEC 15408-3 APE\_REQ.2.8C: *The security requirements rationale shall explain why the SARs*  
2041 *were chosen.*
- 2042 **8.8.2.3.13 Work unit APE\_REQ.2-12**
- 2043 The evaluator **shall check** that the security requirements rationale explains why the SARs were  
2044 chosen.
- 2045 The evaluator is reminded that any explanation is correct, as long as it is coherent and neither the  
2046 SARs nor the explanation have obvious inconsistencies with the remainder of the PP.
- 2047 An example of an obvious inconsistency between the SARs and the remainder of the PP would be to  
2048 have threat agents that are very capable, but an AVA\_VAN SAR that does not protect against these  
2049 threat agents.
- 2050 ISO/IEC 15408-3 APE\_REQ.2.9C: *The statement of security requirements shall be internally*  
2051 *consistent.*
- 2052 **8.8.2.3.14 Work unit APE\_REQ.2-13**
- 2053 The evaluator **shall examine** the statement of security requirements to determine that it is  
2054 internally consistent.
- 2055 The evaluator determines that the combined set of all SFRs and SARs is internally consistent. With  
2056 respect to optional requirements, the evaluator determines that:

## ISO/IEC 18045:2008(E)

- 2057 a) All optional requirements either trace to an SPD element that is itself not optional, or trace  
2058 to an SPD element that is clearly associated with that optional SFR;
- 2059 b) All optional requirements are clearly identified as being required if a conformant TOE  
2060 implements the functionality covered by the requirement, or as being "purely optional";  
2061 and
- 2062 c) All optional requirements do not conflict with non-optional requirements (a capability  
2063 cannot be both required and optional; however, a base capability can be required with  
2064 enhancements to that capability being specified as optional).

2065

2066 The evaluator determines that on all occasions where different security requirements apply to the  
2067 same types of developer evidence, events, operations, data, tests to be performed etc. or to "all  
2068 objects", "all subjects" etc., that these requirements do not conflict.

2069 Some possible conflicts are:

- 2070 a) an extended SAR specifying that the design of a certain cryptographic algorithm is to  
2071 be kept secret, and another extended SAR specifying an open source review;
- 2072 b) FAU\_Gen.1 Audit data generation specifying that subject identity is to be logged,  
2073 FDP\_ACC.1 Subset access control specifying who has access to these logs, and **Error!**  
2074 **Reference source not found.** specifying that some actions of subjects should be  
2075 unobservable to other subjects. If the subject that should not be able to see an  
2076 activity may access logs of this activity, these SFRs conflict;
- 2077 c) FDP\_RIP.1 Subset residual information protection specifying deletion of information  
2078 no longer needed, and FDP\_ROL.1 Basic rollback specifying that a TOE may return to  
2079 a previous state. If the information that is needed for the rollback to the previous  
2080 state has been deleted, these requirements conflict;
- 2081 d) Multiple iterations of FDP\_ACC.1 Subset access control, especially where some  
2082 iterations cover the same subjects, objects, or operations. If one access control SFR  
2083 allows a subject to perform an operation on an object, while another access control  
2084 SFR does not allow this, these requirements conflict.

## 2085 9 Class ACE: Protection Profile Configuration evaluation

### 2086 9.1 Introduction

2087 All Base-PP(s) referenced in the PP-Module must be evaluated before the evaluation of a PP-  
2088 Configuration.

2089 A possibility for efficient evaluation of a PP-Configuration composed of several PP-Modules  
2090 proceeds PP-Module by PP-Module, iteratively. Considering a PP-Configuration composed of the  
2091 Protection Profiles  $P_i$  and the PP-Modules  $M_j$ , evaluation of the PP-Configuration proceeds with the  
2092 following steps, illustrated in Figure 6

- 2093 1) first evaluating independently all Protection Profiles  $P_i$ ;
- 2094 2) evaluating the PP-Configuration  $C_1$  composed of the PP-Module  $M_1$  with the  
2095 Protection Profiles  $P_i$ ;

2096 3) evaluating the PP-Configuration  $C_{i+1}$  composed of the PP-Module  $M_{i+1}$  with the  
2097 PP-Configuration  $C_i$  considered as a standard PP (cf. Section B.14 in ISO/IEC  
2098 15408-1);

2099 4) iterating the step 3) for all the PP-Modules

2100 Steps 2) and 3) are themselves performed in two steps:

2101 a) Evaluation of the PP-Module with its Base-PP(s) (Evaluation of sub-activity  
2102 (ACE\_MCO.1))

2103 b) Extension of the evaluation (consistency assessment) to the other elements of the PP-  
2104 Configuration (Evaluation of sub-activity (ACE\_CC0.1))

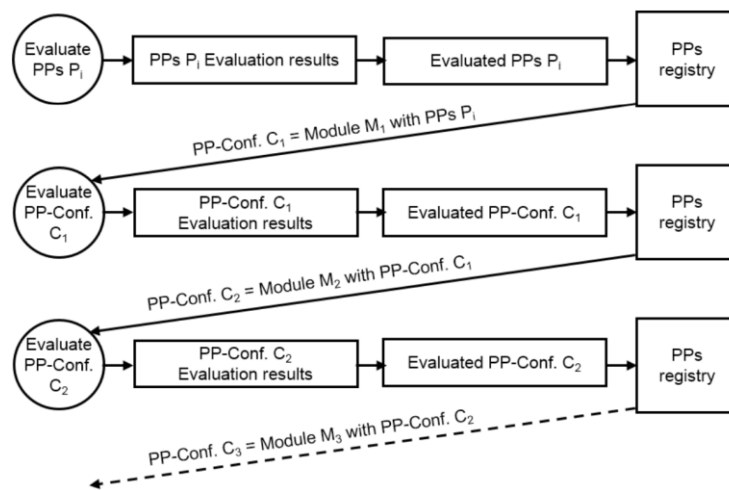


Figure 6 - Evaluation of a PP-Configuration

## 9.2 PP-Module introduction (ACE\_INT)

### 9.2.1 Evaluation of sub-activity (ACE\_INT.1)

#### 9.2.1.1 Objectives

The objective of this sub-activity is to determine whether the PP-Module is correctly identified, and whether the Base-PP(s) and TOE overview are consistent with each other.

#### 9.2.1.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP-Module;
- b) its Base-PP(s)

## ISO/IEC 18045:2008(E)

### 2117 9.2.1.3 Action ACE\_INT.1.1E

#### 2118 9.2.1.3.1 General

2119 ISO/IEC 15408-3 ACE\_INT.1.1C *The PP-Module introduction shall uniquely identify all the Base-PPs*  
2120 *on which the PP-Module relies, including their logical structuring and relationship to the PP-Module*  
2121 *according to ISO/IEC 15408 Part 1, section B.13.3.2.*

#### 2122 9.2.1.3.2 Work unit ACE\_INT.1-1

2123 *The evaluator shall check that the PP-Module introduction identifies the Base-PP(s) on which the PP-*  
2124 *Module relies.*

2125 ISO/IEC 15408-3 ACE\_INT.1.2C *The TOE overview shall identify the differences introduced by the PP-*  
2126 *Module with respect to the TOE overview of its Base-PP(s).*

#### 2127 9.2.1.3.3 Work unit ACE\_INT.1-2

2128 *The evaluator shall check that the TOE overview identifies the differences introduced by the PP-*  
2129 *Module with respect to the TOE overview of its Base-PP(s).*

### 2130 9.3 PP-Module conformance claims (ACE\_CCL)

#### 2131 9.3.1 Evaluation of sub-activity (ACE\_CCL.1)

##### 2132 9.3.1.1 Objectives

2133 The objective of this sub-activity is to determine the validity of various conformance claims. These  
2134 describe how the PP-Module conforms to the ISO/IEC 15408 Part 2 and SFR packages.

##### 2135 9.3.1.2 Input

2136 The evaluation evidence for this sub-activity is:

- 2137 a) the PP-Module;
- 2138 b) the SFR package(s) that the PP claims conformance to;
- 2139 c) the PP-Configuration.

#### 2140 9.3.1.3 Action ACE\_CCL.1.1E

2141 ISO/IEC 15408-3 ACE\_CCL.1.1C The conformance claim shall contain a ISO/IEC 15408  
2142 conformance claim that identifies the edition of the ISO/IEC 15408 to which the PP-Module claims  
2143 conformance.

#### 2144 9.3.1.3.1 Work unit ACE\_CCL.1-1

2145 The evaluator *shall check* that the conformance claim contains a ISO/IEC 15408 conformance  
2146 claim that identifies the edition of the ISO/IEC 15408 to which the PP-Module claims conformance.

2147 The evaluator determines that the ISO/IEC 15408 conformance claim identifies the edition of the  
2148 ISO/IEC 15408 that was used to develop this PP-Module. This should include the edition number of  
2149 the ISO/IEC 15408 and, unless the International English edition of the ISO/IEC 15408 was used, the  
2150 language of the edition of the ISO/IEC 15408 that was used.



## ISO/IEC 18045:2008(E)

2151 ISO/IEC 15408-3 ACE\_CCL.1.2C: The ISO/IEC 15408 conformance claim shall describe the  
2152 conformance of the PP-Module to ISO/IEC 15408 Part 2 as either ISO/IEC 15408 Part 2 conformant  
2153 or ISO/IEC 15408 Part 2 extended.

### 2154 9.3.1.3.2 Work unit ACE\_CCL.1-2

2155 The evaluator **shall check** that the ISO/IEC 15408 conformance claim states a claim of either  
2156 ISO/IEC 15408 Part 2 conformant or ISO/IEC 15408 Part 2 extended for the PP-Module.

2157 ISO/IEC 15408-3 ACE\_CCL.1.3C: *The conformance claim shall identify all security functional*  
2158 *requirement packages to which the PP-Module claims conformance.*

### 2159 9.3.1.3.3 Work unit ACE\_CCL.1-3

2160 The evaluator **shall check** that, for each identified package, the conformance claim contains a  
2161 package claim that identifies all security functional requirement packages to which the PP-Module  
2162 claims conformance.

2163 If the PP-Module does not claim conformance to a security functional requirement package, this  
2164 work unit is not applicable and therefore considered to be satisfied.

2165 The evaluator determines that any referenced security functional requirement packages are  
2166 unambiguously identified (e.g. by title and version number, or by the identification included in the  
2167 introduction of that security functional requirement package).

2168 The evaluator ensures that the PP-Module only claims conformance to functional packages that:

- 2169 a) Are not claimed by one of its Base PPs; or
- 2170 b) are augmented from the claim in one of its Base PPs.

2171 Any augmentations will need to be explained in the security functional package claim in the PP-  
2172 module. If a package is claimed by a Base PP and is not modified by the PP-Module, then the PP-  
2173 Module does not include this functional package in its package conformance claim section."

2174 The evaluator is reminded that claims of partial conformance to a security functional requirement  
2175 package are not permitted.

2176 ISO/IEC 15408-3 ACE\_CCL.1.4C: *The ISO/IEC 15408 conformance claim shall be consistent with the*  
2177 *extended components definition.*

### 2178 9.3.1.3.4 Work unit ACE\_CCL.1-4

2179 The evaluator **shall examine** the ISO/IEC 15408 conformance claim for ISO/IEC 15408 Part 2 to  
2180 determine that it is consistent with the extended components definition

2181 If the ISO/IEC 15408 conformance claim contains ISO/IEC 15408 Part 2 conformant, the evaluator  
2182 determines that the extended components definition does not define functional components.

2183 If the ISO/IEC 15408 conformance claim contains ISO/IEC 15408 Part 2 extended, the evaluator  
2184 determines that the extended components definition defines at least one extended functional  
2185 component.

2186 ISO/IEC 15408-3 ACE\_CCL.1.8C The conformance statement shall identify the set of PPs and PP-  
2187 Modules to which, in combination with the PP-Module under evaluation, exact conformance is  
2188 allowed to be claimed.

## ISO/IEC 18045:2008(E)

### 2189 9.3.1.3.5 Work unit ACE\_CCL.1-5

2190 The evaluator **shall check** the conformance statement to determine that it lists the set of other PP-  
2191 modules that can be specified in the components statement of a PP-Configuration that includes the  
2192 PP-module.

2193 If no PPs in the PP-Configuration's component statement require exact conformance in their  
2194 conformance statements then this work unit does not apply and is therefore considered satisfied.

2195 If the PP-module does not allow its use (in a PP-Configuration) with other PP-modules, then there  
2196 will be no other PP-modules identified in the PP-module's conformance statement, and the  
2197 evaluator ensures the PP-Configuration contains no other PP-modules in the PP-Configuration's  
2198 components statement.

2199 If the PP-Configuration's components statement does include other PP-modules, then the evaluator  
2200 ensures that all PP-modules listed in the PP-Configuration's components statement are identified  
2201 as allowed with the PP-module in its conformance statement.

### 2202 9.3.1.3.6 Work unit ACE\_CCL.1-6

2203 The evaluator shall check the conformance statement to determine that it lists PPs identified in the  
2204 PP-Configuration's component statements that are not included in the PP-Module's set of Base-PPs  
2205 as identified in the PP-Configuration's component statements.

2206 If a PP in the PP-Configuration's component statement does not require exact conformance in its  
2207 conformance statement, this work unit does not apply and is therefore considered satisfied.

2208 If PP-Module does not identify (in its conformance statement) any PPs other than those that make  
2209 up the set of Base-PPs for the PP-Module identified in the PP-Configuration's component statement,  
2210 the evaluator ensures the PP-Configuration contains no other (non-Base-) PPs in the PP-  
2211 Configuration's components statement.

2212 If the PP-Configuration's components statement does include PPs that are not part of the PP-  
2213 Module's set of Base-PPs, then the evaluator ensures that all such PPs listed in the PP-  
2214 Configuration's components statement are identified as allowed with the PP-Module in its  
2215 conformance statement.

2216 ISO/IEC 15408-3 ACE\_CCL.1.6C: *The conformance claim shall describe any conformance of the PP*  
2217 *Module to a package as one of: package-conformant, package-augmented, or package tailored.*

### 2218 9.3.1.3.7 Work unit ACE\_CCL.1-7

2219 The evaluator **shall check** that, for each identified package, the conformance claim states a claim of  
2220 one of: package-name conformant, package-name augmented, or package-name tailored.

2221 If the PP-Module does not claim conformance to a package, this work unit is not applicable and  
2222 therefore considered to be satisfied. PP-Modules can only claim conformance to functional  
2223 packages and therefore only this type of package is considered in the description below.

2224 If the functional package conformance claim contains package-name conformant, the evaluator  
2225 determines that all assumptions, threats, OSPs, security objectives and SFRs included in the  
2226 package are included in identical form by the PP-Module (including via its base-PP(s)).

2227 If the functional package conformance claim contains package-name augmented, the evaluator  
2228 determines that all all assumptions, threats, OSPs, security objectives and SFRs included in the  
2229 package are included in identical form by the PP-Module except that the PP-Module shall have at  
2230 least one additional SFR or one SFR that is hierarchically higher than an SFR in the functional  
2231 package.

2232 If the functional package conformance claim contains package-name tailored, the evaluator  
2233 determines that:

2234 a) all assumptions, threats, OPSs, Security Objectives, and SFRs included in the package  
2235 are included in identical form in the PP-Module (after allowing for iteration,  
2236 refinement, assignments and selections from the package to be completed as  
2237 required by the PP-Module);

2238 b) the PP-Module may have at least one additional SFR or one SFR that is hierarchically  
2239 higher than an SFR in the functional package;

2240 c) the PP-Module shall have at least one additional (not present in the SFR in the  
2241 package) selection item in one of the SFRs in the functional package.

2242 In the case of package-name tailored, the evaluator additionally examines the selection (and other  
2243 selections in that requirement) to ensure that the requirement still meets its security objective (or  
2244 the associated SPD element in the direct rationale approach) with the addition of (and potentially  
2245 deletion of) the selection item.

#### 2246 **9.4 PP-Module Security problem definition (ACE\_SPD)**

##### 2247 **9.4.1 Evaluation of sub-activity (ACE\_SPD.1)**

###### 2248 **9.4.1.1 Objectives**

2249 The objective of this sub-activity is to determine that the security problem intended to be  
2250 addressed by the PP Module and its operational environment is clearly defined.

###### 2251 **9.4.1.2 Input**

2252 The evaluation evidence for this sub-activity is:

2253 a) the PP Module.

###### 2254 **9.4.1.3 Action ACE\_SPD.1.1E**

###### 2255 **9.4.1.3.1 General**

2256 ISO/IEC 15408-3 ACE\_SPD.1.1C: *The security problem definition shall describe the threats.*

###### 2257 **9.4.1.3.2 Work unit ACE\_SPD.1-1**

2258 The evaluator **shall check** that the security problem definition describes the threats.

2259 If all security objectives are derived from assumptions and/or OSPs only, the statement of threats  
2260 need not be present in the PP. In this case, this work unit is not applicable and therefore considered  
2261 to be satisfied.

2262 The evaluator determines that the security problem definition describes the threats that must be  
2263 countered by the TOE and/or its operational environment.

2264 Note that if optional requirements are defined by the PP, there may be associated threats that are  
2265 covered by this work unit.

2266 ISO/IEC 15408-3 ACE\_SPD.1.2C: *All threats shall be described in terms of a threat agent, an asset,  
2267 and an adverse action.*

## ISO/IEC 18045:2008(E)

### 2268 9.4.1.3.3 Work unit ACE\_SPD.1-2

2269 The evaluator **shall examine** the security problem definition to determine that all threats are  
2270 described in terms of a threat agent, an asset, and an adverse action.

2271 If all security objectives are derived from assumptions and OSPs only, the statement of threats  
2272 need not be present in the PP Module. In this case, this work unit is not applicable and therefore  
2273 considered to be satisfied.

2274 Threat agents may be further described by aspects such as expertise, resource, opportunity, and  
2275 motivation.

2276 ISO/IEC 15408-3 ACE\_SPD.1.3C: *The security problem definition shall describe the OSPs.*

### 2277 9.4.1.3.4 Work unit ACE\_SPD.1-3

2278 The evaluator **shall examine** that the security problem definition describes the OSPs.

2279 If all security objectives are derived from assumptions and/or threats only, OSPs need not be  
2280 present in the PP Module. In this case, this work unit is not applicable and therefore considered to  
2281 be satisfied.

2282 The evaluator determines that OSP statements are made in terms of rules or guidelines that must  
2283 be followed by the TOE and/or its operational environment.

2284 The evaluator determines that each OSP is explained and/or interpreted in sufficient detail to make  
2285 it clearly understandable; a clear presentation of policy statements is necessary to permit tracing  
2286 security objectives to them.

2287 Note that if optional requirements are defined by the PP Module, there may be associated OSPs that  
2288 are covered by this work unit.

2289 ISO/IEC 15408-3:20XX ACE\_SPD.1.4C: *The security problem definition shall describe the assumptions  
2290 about the operational environment of the TOE.*

### 2291 9.4.1.3.5 Work unit ACE\_SPD.1-4

2292 The evaluator **shall examine** the security problem definition to determine that it describes the  
2293 assumptions about the operational environment of the TOE.

2294 If there are no assumptions, this work unit is not applicable and is therefore considered to be  
2295 satisfied.

2296 The evaluator determines that each assumption about the operational environment of the TOE is  
2297 explained in sufficient detail to enable consumers to determine that their operational environment  
2298 matches the assumption. If the assumptions are not clearly understood, the end result may be that  
2299 the TOE is used in an operational environment in which it will not function in a secure manner.

## 2300 9.5 PP-Module Security objectives (ACE\_OBJ)

### 2301 9.5.1 Evaluation of sub-activity (ACE\_OBJ.1)

#### 2302 9.5.1.1 Application notes

2303 If the PP-Configuration uses the Direct Rationale approach (as determined in ACE\_CCO.1-2) then all  
2304 actions of APE\_OBJ.1.1E hold.

|      |                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------|
| 2305 | <b>9.5.2 Evaluation of sub-activity (ACE_OBJ.2)</b>                                                   |
| 2306 | <b>9.5.2.1 Application notes</b>                                                                      |
| 2307 | All actions of APE_OBJ.2.1E hold.                                                                     |
| 2308 | <b>9.6 PP-Module extended components definition (ACE_ECD)</b>                                         |
| 2309 | <b>9.6.1 Evaluation of sub-activity (ACE_ECD.1)</b>                                                   |
| 2310 | <b>9.6.1.1 Application notes</b>                                                                      |
| 2311 | All actions of APE_ECD.1.1E and APE_ECD.1.2E hold.                                                    |
| 2312 | <b>9.7 PP-Module security requirements (ACE_REQ)</b>                                                  |
| 2313 | <b>9.7.1 Evaluation of sub-activity (ACE_REQ.1)</b>                                                   |
| 2314 | <b>9.7.1.1 Application notes</b>                                                                      |
| 2315 | If the PP-Configuration uses the Direct Rationale approach (as determined in ACE_CCO.1-2) then all    |
| 2316 | actions of APE_REQ.1.1E hold. The SAR part is not considered because it is empty in PP-Modules.       |
| 2317 | <b>9.7.2 Evaluation of sub-activity (ACE_REQ.1)</b>                                                   |
| 2318 | <b>9.7.2.1 Application notes</b>                                                                      |
| 2319 | All actions of APE_REQ.2.1E hold. The SAR part is not considered because it is empty in PP-Modules.   |
| 2320 | <b>9.8 PP-Module consistency (ACE_MCO)</b>                                                            |
| 2321 | <b>9.8.1 Evaluation of sub-activity (ACE_MCO.1)</b>                                                   |
| 2322 | <b>9.8.1.1 Objectives</b>                                                                             |
| 2323 | The objective of this sub-activity is to determine the consistency of the PP-Module regarding its     |
| 2324 | Base-PP(s).                                                                                           |
| 2325 | <b>9.8.1.2 Input</b>                                                                                  |
| 2326 | The evaluation evidence for this sub-activity is:                                                     |
| 2327 | a) the PP-Module;                                                                                     |
| 2328 | b) its Base-PP(s)                                                                                     |
| 2329 | <b>9.8.1.3 Action ACE_MCO.1.1E</b>                                                                    |
| 2330 | <b>9.8.1.3.1 General</b>                                                                              |
| 2331 | ISO/IEC 15408-3 ACE_MCO.1.1C: <i>The consistency rationale shall demonstrate that the TOE type of</i> |
| 2332 | <i>the PP-Module is consistent with the TOE type(s) in the Base-PPs identified in the PP-Module</i>   |
| 2333 | <i>introduction.</i>                                                                                  |

2334 **9.8.1.3.2 Work unit ACE\_MCO.1-1**

2335 The evaluator **shall examine** the consistency rationale to determine that the TOE type of the PP-  
2336 Module is consistent with all the TOE types of the Base-PP(s).

2337 The relation between the types may be simple: a PP-Module may consider a TOE that provides  
2338 additional security functionality, or more complex: a TOE that provides a given security  
2339 functionality in a specific way.

2340 ISO/IEC 15408-3 ACE\_MCO.1.2C: *The consistency rationale shall demonstrate that the statement of*  
2341 *the security problem definition is consistent with the statement of the security problem definition in*  
2342 *the Base-PPs identified in the PP-Module introduction.*

2343 **9.8.1.3.3 Work unit ACE\_MCO.1-2**

2344 The evaluator **shall examine** the PP-Module consistency rationale to determine that it  
2345 demonstrates that the statement of security problem definition of the PP-Module is consistent with  
2346 the statements of security problem definition stated in its Base-PPs.

2347 In particular, the evaluator examines the consistency rationale to determine that:

2348 a) the statements of threats, assumptions and OSPs in the PP-Module do not contradict  
2349 those from the Base-PP(s). It may be the case that the PP-Module eliminates or  
2350 changes SPD elements in the Base PP. While allowed, the evaluator confirms that  
2351 such modifications do not adversely affect the security problem statement of the  
2352 Base PP in the context of the PP-Module/Base PP construct.

2353 b) the statement of assumptions in the PP-Module addresses aspects out of scope of the  
2354 Base-PP, in which case, the addition of elements is allowed.

2355 ISO/IEC 15408-3 ACE\_MCO.1.3C: *The consistency rationale shall demonstrate that the statement of*  
2356 *security objectives is consistent with the statement of security objectives in the Base-PPs identified in*  
2357 *the PP-Module introduction.*

2358 **9.8.1.3.4 Work unit ACE\_MCO.1-3**

2359 The evaluator **shall examine** the PP-Module consistency rationale to determine that it  
2360 demonstrates that the statement of security objectives of the PP-Module is consistent with the  
2361 statement of security objectives of its Base-PP(s).

2362 Where the PP-Module and its Base-PP(s) use the Direct Rationale approach then this work unit is  
2363 trivially satisfied for the TOE objectives (because these are not included under the Direct Rationale  
2364 approach). If *any* of the PP-Module or its Base-PPs use the Direct Rationale approach then the PP-  
2365 Module *and all* of its Base-PPs must use the Direct Rationale approach, otherwise the evaluator  
2366 action related to this work unit is assigned a fail verdict.

2367 In particular, the evaluator examines the consistency rationale to determine that:

2368 a) the statements of the security objectives for the TOE and the security objectives for  
2369 the operational environment in the PP-Module do not contradict those from the  
2370 Base-PPs.

2371 b) the statement of the security objectives for the operational environment in the PP-  
2372 Module addresses aspects out of scope of the Base-PP, in which case, the addition of  
2373 elements is allowed.

2374 ISO/IEC 15408-3 ACE\_MCO.1.4C: *The consistency rationale shall demonstrate that the statement of*  
 2375 *security requirements is consistent with the statement of security requirements in the Base-PPs*  
 2376 *identified in the PP-Module introduction.*

2377 **9.8.1.3.5 Work unit ACE\_MCO.1-4**

2378 The evaluator **shall examine** the consistency rationale to determine that the statement of security  
 2379 requirements of the PP-Module is consistent with the statement of security requirements of its  
 2380 Base-PPs, that is, the SFRs of the PP-Module either complete or refine the SFRs of the Base-PP(s)  
 2381 and that no contradiction arises from the whole set of SFRs of the PP-Module and the Base-PP(s).

2382 **9.9 PP-Configuration consistency (ACE\_CCO)**

2383 **9.9.1 Evaluation of sub-activity (ACE\_CCO.1)**

2384 **9.9.1.1 Objectives**

2385 The objective of this sub-activity is to determine whether the PP-Configuration and its  
 2386 components are correctly identified.

2387 The objective of this sub-activity is also to determine the consistency of the PP-Configuration  
 2388 regarding the whole set of Protection Profiles and PP-Modules.

2389 For the consistency analysis required by this activity Section 10.2.1 (Re-using the evaluation  
 2390 results of certified PPs), is applicable to determine which parts of the Base-PPs are to be re-  
 2391 evaluated during the evaluation of PP-Configuration.

2392 **9.9.1.2 Input**

2393 The evaluation evidence for this sub-activity is:

- 2394 a) the PP-Configuration reference;
- 2395 b) the PP-Configuration components statement;
- 2396 c) the PP(s) and PP-Modules identified in the components statement.

2397 **9.9.1.3 Action ACE\_CCO.1.1E**

2398 ISO/IEC 15408-3 ACE\_CCO.1.1C: *The PP-Configuration reference shall uniquely identify the PP-*  
 2399 *Configuration.*

2400 **9.9.1.3.1 Work unit ACE\_CCO.1-1**

2401 The evaluator shall examine the PP-Configuration reference to determine that it uniquely identifies  
 2402 the PP-Configuration.

2403 The evaluator determines that the PP-Configuration reference identifies the PP-Configuration itself,  
 2404 so that it may be easily distinguished from other PPs, PP-Configurations and PP-Modules, and that  
 2405 it also uniquely identifies each version of the PP-Configuration, e.g. by including a version number  
 2406 and/or a date of publication.

2407 The PP-Configuration should have some referencing system that is capable of supporting unique  
 2408 references (e.g. use of numbers, letters or dates).

## ISO/IEC 18045:2008(E)

2409 ISO/IEC 15408-3 ACE\_CCO.1.2C: *The components statements shall uniquely identify the Protection*  
2410 *Profiles and the PP-Modules that compose the PP-Configuration.*

### 2411 9.9.1.3.2 Work unit ACE\_CCO.1-2

2412 The evaluator shall examine the PP-Configuration components statement to determine that it  
2413 uniquely identifies the Protection Profiles and PP-Modules contained in the PP-Configuration.

2414 The evaluator shall check that if *any* of the Base-PPs or PP-Modules in the PP-Configuration use the  
2415 Direct Rationale Approach then *all* Base-PPs and PP-Modules in the PP-Configuration use the  
2416 Direct Rationale approach.

2417 The Protection Profiles should have been certified and available for use in security targets.

2418 ISO/IEC 15408-3 ACE\_CCO.1.3C: *The conformance statement shall specify the required conformance*  
2419 *to the PP-Configuration as one of exact, strict, or demonstrable. The conformance claim shall contain*  
2420 *a ISO/IEC 15408 conformance claim that identifies the edition of the ISO/IEC 15408 to which the PP-*  
2421 *Configuration and its underlying Protection Profiles and PP-Module claim conformance.*

### 2422 9.9.1.3.3 Work unit ACE\_CCO.1-3

2423 The evaluator shall examine the PP-Configuration conformance statement to determine that it  
2424 specifies the kind of conformance required: exact, strict, or demonstrable.

2425 The evaluator shall check that the conformance claim contains a ISO/IEC 15408 conformance claim  
2426 that identifies the edition of the ISO/IEC 15408 to which the PP-Configuration and its underlying  
2427 Protection Profile(s) and PP-Module(s) claim conformance.

2428 The evaluator shall examine the PP-Configuration conformance claim to determine the  
2429 compatibility between all ISO/IEC 15408 editions that are related to the PP-Configuration and its  
2430 underlying Protection Profile(s) and PP-Module(s).

2431 If at least one of the Protection Profiles identified in the PP-Configuration components statement  
2432 requires exact conformance, then the PP-Configuration conformance statement shall also require  
2433 exact conformance. If none of the PPs identified in the PP-Configuration components statement  
2434 requires exact conformance but at least one of the Protection Profiles identified in the PP-  
2435 Configuration components statement claims strict conformance, then the PP-Configuration  
2436 conformance statement shall also require strict conformance also.

2437 ISO/IEC 15408 editions used in a PP-Configuration and its underlying Protection Profile(s) and  
2438 PP-Module(s) have to be compatible. If compatibility is not obvious, guidance from the certification  
2439 scheme should be asked.

2440 ISO/IEC 15408-3 ACE\_CCO.1.4C: *The SAR statement shall specify the set of SAR or predefined EAL*  
2441 *that applies to this PP-Configuration.*

### 2442 9.9.1.3.4 Work unit ACE\_CCO.1-4

2443 The evaluator shall examine the PP-Configuration SAR statement to determine that it specifies a  
2444 well-formed package of assurance requirements drawn from ISO/IEC 15408-3. The SAR package  
2445 can be built with components from ISO/IEC 15408-3 or can refer to a specific SAR package stated  
2446 in one of the Protection Profiles composing the PP-Configuration.

2447 If the package comes from ISO/IEC 15408-3 then the evaluator shall check that it is well-formed: it  
2448 is closed by dependencies or the SAR statements provide a sound discarding rationale.

2449 The evaluator shall check that the package of SAR of the PP-Configuration is consistent with  
2450 respect to the SARs of each of the Protection Profiles contained in the PP-Configuration: for any



2451 SAR component in each of the Protection Profile, the PP-Configuration provides either the same  
 2452 component or a higher component in the family hierarchy. If the SAR component in the Protection  
 2453 Profile is a refinement of a standard component, then the correspondent SAR component in the PP-  
 2454 Configuration has to include these refinements. If two Protection Profiles refine the same SAR  
 2455 component, the evaluator shall check that the refinements are not contradictory and that the  
 2456 corresponding SAR component in the PP-Configuration meets both.

2457 ISO/IEC 15408-3 ACE\_CCO.1.5C: *The Base-PP(s) on which the PP-Modules relies shall belong to the*  
 2458 *Protection Profiles identified in the components statement of the PP-Configuration.*

#### 2459 **9.9.1.3.5 Work unit ACE\_CCO.1-5**

2460 The evaluator shall check that the Base-PP(s) of each PP-Module in the PP-Configuration are  
 2461 included in the set of Protection Profiles identified in the PP-Configuration's component statement.  
 2462 Where a PP-Module specifies alternative sets of Base-PP(s) then only one of these sets must be  
 2463 referred to in the PP-Configuration.

2464 ISO/IEC 15408-3 ACE\_CCO.1.6C: *The conformance statement of each Base-PPs and PP in the*  
 2465 *components statement of the PP-Configuration shall identify other PP-Modules and PPs that can be*  
 2466 *used in combination with the PP in a PP-Configuration.*

#### 2467 **9.9.1.3.6 Work unit ACE\_CCO.1-6**

2468 For each Protection Profile listed in the PP-Configuration's components statement, the evaluator  
 2469 shall check the PP's conformance statement to determine that all PP-modules specified in the PP-  
 2470 Configuration's components statement are listed as allowed to be used with that PP. If the PP-  
 2471 Configuration does not require exact conformance in its conformance statement, this work unit  
 2472 does not apply and is therefore considered satisfied.

2473 The evaluator checks each PP in the PP-Configuration's components statement. For each PP, the  
 2474 evaluator determines that each PP-Module listed in the PP-Configuration's components statement  
 2475 is also listed in the PP's conformance statement as allowed to be used with that PP.

#### 2476 **9.9.1.3.7 Work unit ACE\_CCO.1-7**

2477 For each Protection Profile listed in the PP-Configuration's components statement, the evaluator  
 2478 shall check the PP's conformance statement to determine that all other PPs specified in the PP-  
 2479 Configuration's components statement are listed as allowed to be used with that PP.

2480 If the PP-Configuration does not require exact conformance in its conformance statement, this  
 2481 work unit does not apply and is therefore considered satisfied.

2482 If there is only one PP identified in the PP-Configuration's component statement, then this work  
 2483 unit does not apply and is therefore considered satisfied.

#### 2484 **9.9.1.4 Action ACE\_CCO.1.2E**

##### 2485 **9.9.1.4.1 Work unit ACE\_CCO.1-8**

2486 The evaluator shall check that the PP-Configuration made up of all the Protection Profiles and PP-  
 2487 Modules identified in the components statement of the PP-Configuration is consistent. That is, the  
 2488 evaluator shall check that no contradiction arises from the whole set of Protection Profiles and PP-  
 2489 Modules included in the PP-Configuration.

2490 The evaluator can organise this work in many ways; the actual organisation may depend on the  
 2491 will to derive evaluation results for more than one PP-Configuration at a time

2492 For instance, the evaluator can process in two steps as follows:

## ISO/IEC 18045:2008(E)

- 2493 a) Assess the consistency of the set of Protection Profiles composing the PP-  
2494 Configuration,
- 2495 b) Then proceed with the assessment of the PP-Configuration consistency incrementally,  
2496 by adding one PP-Module at a time.
- 2497 An alternative is to proceed incrementally but mixing PPs and PP-Modules or to flatten/serialise  
2498 the definition of the PP-Configuration (cf. Annex B in ISO/IEC 15408-1), duplicating as required,  
2499 and to assess the consistency of the whole set of elements.
- 2500 Any incremental consistency analysis step where C is a subset of the PP-Configuration and X is  
2501 a PP or a PP-Module that has to be added to C consists of:
- 2502 • assessing that the SPD, the objectives and the SFRs of X do not contradict the statements  
2503 in C;
  - 2504 • the assumptions and objectives for the environment in X either are the same as in C or  
2505 address security aspects that are out of the scope of C.
- 2506 If the PP-Configuration is a Direct Rationale PP-Configuration (as determined in ACE\_CCO.1-2) then  
2507 the TOE objectives are not required in the consistency analysis.
- 2508 Note that if X is a PP-Module, C contains all its Base-PP(s) and Evaluation of sub-activity  
2509 (ACE\_MCO.1) has succeed for X, then the consistency analysis step has to be performed with  
2510 respect to the components of C different from these Base-PP(s) only.
- 2511 **10 Class ASE: Security Target evaluation**
- 2512 **10.1 Introduction**
- 2513 This Clause describes the evaluation of an ST. The ST evaluation should be started prior to any TOE  
2514 evaluation sub-activities since the ST provides the basis and context to perform these sub-activities.  
2515 The evaluation methodology in this subclause is based on the requirements on the ST as specified  
2516 in ISO/IEC 15408-3 class ASE.
- 2517 This Clause should be used in conjunction with Annexes A, B and C, Guidance for Operations in  
2518 ISO/IEC 15408-1, as these Annexes clarify the concepts here and provide many examples.
- 2519 **10.2 Application notes**
- 2520 **10.2.1 Re-using the evaluation results of certified PPs**
- 2521 While evaluating an ST that is based on one or more certified PPs, it may be possible to re-use the  
2522 fact that these PPs were certified. The potential for re-use of the result of a certified PP is greater if  
2523 the ST does not add threats, OSPs, assumptions, security objectives and/or security requirements  
2524 to those of the PP. If the ST contains much more than the certified PP, re-use may not be useful at  
2525 all.
- 2526 The evaluator is allowed to re-use the PP evaluation results by doing certain analyses only partially  
2527 or not at all if these analyses or parts thereof were already done as part of the PP evaluation. While  
2528 doing this, the evaluator should assume that the analyses in the PP were performed correctly.
- 2529 An example would be where the PP contains a set of security requirements, and these were  
2530 determined to be internally consistent during the PP evaluation. If the ST uses the exact same  
2531 requirements, the consistency analysis does not have to be repeated during the ST evaluation. If  
2532 the ST adds one or more requirements, or performs operations on these requirements, the analysis

2533 will have to be repeated. However, it may be possible to save work in this consistency analysis by  
2534 using the fact that the original requirements are internally consistent. If the original requirements  
2535 are internally consistent, the evaluator only has to determine that:

2536 a) the set of all new and/or changed requirements is internally consistent, and

2537 b) the set of all new and/or changed requirements is consistent with the original  
2538 requirements.

2539 The evaluator notes in the ETR each case where analyses are not done or only partially done for  
2540 this reason.

2541 The same re-use discussion applies to an ST claiming conformance to a certified PP-Configuration.

### 2542 **10.3 ST introduction (ASE\_INT)**

#### 2543 **10.3.1 Evaluation of sub-activity (ASE\_INT.1)**

##### 2544 **10.3.1.1 Objectives**

2545 The objective of this sub-activity is to determine whether the ST and the TOE are correctly  
2546 identified, whether the TOE is correctly described in a narrative way at three levels of abstraction  
2547 (TOE reference, TOE overview and TOE description), and whether these three descriptions are  
2548 consistent with each other.

##### 2549 **10.3.1.2 Input**

2550 The evaluation evidence for this sub-activity is:

2551 a) the ST.

##### 2552 **10.3.1.3 Action ASE\_INT.1.1E**

2553 ISO/IEC 15408-3 ASE\_INT.1.1C: *The ST introduction shall contain an ST reference, a TOE reference, a*  
2554 *TOE overview and a TOE description.*

##### 2555 **10.3.1.3.1 Work unit ASE\_INT.1-1**

2556 The evaluator **shall check** that the ST introduction contains an ST reference, a TOE reference, a  
2557 TOE overview and a TOE description.

2558 ISO/IEC 15408-3 ASE\_INT.1.2C: *The ST reference shall uniquely identify the ST.*

##### 2559 **10.3.1.3.2 Work unit ASE\_INT.1-2**

2560 The evaluator **shall examine** the ST reference to determine that it uniquely identifies the ST.

2561 The evaluator determines that the ST reference identifies the ST itself, so that it may be easily  
2562 distinguished from other STs, and that it also uniquely identifies each version of the ST, e.g. by  
2563 including a version number and/or a date of publication.

2564 In evaluations where a CM system is provided, the evaluator may validate the uniqueness of the  
2565 reference by checking the configuration list. In the other cases, the ST should have some  
2566 referencing system that is capable of supporting unique references (e.g. use of numbers, letters or  
2567 dates).

## ISO/IEC 18045:2008(E)

- 2568 ISO/IEC 15408-3 ASE\_INT.1.3C: *The TOE reference shall uniquely identify the TOE.*
- 2569 **10.3.1.3.3 Work unit ASE\_INT.1-3**
- 2570 The evaluator **shall examine** the TOE reference to determine that it uniquely identifies the TOE.
- 2571 The evaluator determines that the TOE reference uniquely identifies the TOE, so that it is clear to  
2572 which TOE the ST refers, and that it also identifies the version of the TOE, e.g. by including a  
2573 version/release/build number, or a date of release.
- 2574 In the end of the evaluation, the evaluator **shall check** the TOE reference, and any unique  
2575 identifiers associated with the TOE physical components are consistent with the identifier(s)  
2576 assigned to the TOE evaluated in work units related to ALC\_CMC.x.1C and the configuration list  
2577 evaluated in work units related to ALC\_CMS.x.2C.
- 2578 **10.3.1.3.4 Work unit ASE\_INT.1-4**
- 2579 The evaluator **shall examine** the TOE reference to determine that it is not misleading.
- 2580 If the TOE is related to one or more well-known products, it is allowed to reflect this in the TOE  
2581 reference. However, this should not be used to mislead consumers and it must be made clear which  
2582 part of the product has been evaluated.
- 2583 When a TOE needs some required non-TOE hardware/software/firmware to run properly, the TOE  
2584 reference may include the name of the non-TOE hardware/software/firmware used by the TOE,  
2585 however it must be made clear that the non-TOE hardware/software/firmware has not been  
2586 evaluated.
- 2587 ISO/IEC 15408-3 ASE\_INT.1.4C: *The TOE overview shall summarise the usage and major security  
2588 features of the TOE.*
- 2589 **10.3.1.3.5 Work unit ASE\_INT.1-5**
- 2590 The evaluator **shall examine** the TOE overview to determine that it describes the usage and major  
2591 security features of the TOE.
- 2592 The TOE overview may describe security features that are provided by the product, and/or those  
2593 that users may expect in that product type, but it must clearly distinguish those features that are  
2594 evaluated and those that are not evaluated.
- 2595 The TOE overview shall be consistent with information provided in other sections of the Security  
2596 Target such as the TOE description, the security objectives, the security functional requirements,  
2597 and the TOE summary specification. In addition to ensuring the evaluated security features are  
2598 consistently described throughout the ST, this means that any security feature that is not evaluated  
2599 is only discussed within the ST introduction, or else is explicitly identified as not evaluated in each  
2600 other place where it is mentioned (failure to make this identification means that this work unit is  
2601 assigned a fail verdict).
- 2602 The TOE overview in an ST for a composed TOE should describe the usage and major security  
2603 feature of the composed TOE, rather than those of the individual component TOEs.
- 2604 The evaluator determines that the overview is clear enough for consumers, and sufficient to give  
2605 them a general understanding of the intended usage and major security features of the TOE.
- 2606 ISO/IEC 15408-3 ASE\_INT.1.5C: *The TOE overview shall identify the TOE type.*

2607 **10.3.1.3.6 Work unit ASE\_INT.1-6**

2608 The evaluator *shall check* that the TOE overview identifies the TOE type.

2609 **10.3.1.3.7 Work unit ASE\_INT.1-7**

2610 The evaluator *shall examine* the TOE overview to determine that the TOE type is not misleading.

2611 There are situations where the general consumer would expect certain functionality of the TOE  
2612 because of its TOE type. If this functionality is absent in the TOE, the evaluator determines that the  
2613 TOE overview adequately discusses this absence.

2614 There are also TOEs where the general consumer would expect that the TOE should be able to  
2615 operate in a certain operational environment because of its TOE type. If the TOE is unable to  
2616 operate in such an operational environment, the evaluator determines that the TOE overview  
2617 adequately discusses this.

2618 ISO/IEC 15408-3 ASE\_INT.1.6C: The TOE overview shall identify any non-TOE  
2619 hardware/software/firmware required by the TOE.

2620 **10.3.1.3.8 Work unit ASE\_INT.1-8**

2621 The evaluator *shall examine* the TOE overview to determine that it identifies any non-TOE  
2622 hardware/software/firmware required by the TOE.

2623 While some TOEs are able to run stand-alone, other TOEs (notably software TOEs) need additional  
2624 hardware, software or firmware to operate. If the TOE does not require any hardware, software or  
2625 firmware, this work unit is not applicable and therefore considered to be satisfied.

2626 The evaluator determines that the TOE overview identifies any additional hardware, software and  
2627 firmware needed by the TOE to operate. This identification does not have to be exhaustive, but  
2628 detailed enough for potential consumers of the TOE to determine whether their current hardware,  
2629 software and firmware support use of the TOE, and, if this is not the case, which additional  
2630 hardware, software and/or firmware is needed.

2631 ISO/IEC 15408-3 ASE\_INT.1.7C: *The TOE description shall describe the physical scope of the TOE.*

2632 **10.3.1.3.9 Work unit ASE\_INT.1-9**

2633 The evaluator *shall examine* the TOE description to determine that it describes the physical scope  
2634 of the TOE.

2635 The evaluator determines that the TOE description lists the hardware, firmware, software and  
2636 guidance parts that constitute the TOE and describes them at a level of detail that is sufficient to  
2637 give the reader a general understanding of those parts.

2638 As a minimum, the TOE description will cover the following elements:

2639 a) Each separately delivered part of the TOE, which will be identified by its unique  
2640 identifier and the current format (binary, wafer, inlay, \*.pdf, \*.doc, \*.chm etc.).

2641 b) The delivery method used by the developer to make available each part to the TOE  
2642 consumer (Web site download, courier delivery, etc.).

2643 The physical description will also include some clear statements about the evaluated TOE  
2644 configuration. In the case where a product could have multiple physical components, and therefore  
2645 multiple configurations, the evaluated configurations must be briefly described and identified.

## ISO/IEC 18045:2008(E)

2646 The evaluator also determines that there is no possible misunderstanding as to whether any  
2647 hardware, firmware, software or guidance part is part of the TOE or not.

2648 ISO/IEC 15408-3 ASE\_INT.1.8C: *The TOE description shall describe the logical scope of the TOE.*

### 2649 **10.3.1.3.10 Work unit ASE\_INT.1-10**

2650 The evaluator **shall examine** the TOE description to determine that it describes the logical scope of  
2651 the TOE.

2652 The evaluator determines that the TOE description discusses the logical security features offered  
2653 by the TOE at a level of detail that is sufficient to give the reader a general understanding of those  
2654 features.

2655 The evaluator also determines that there is no possible misunderstanding as to whether any logical  
2656 security feature is offered by the TOE or not.

2657 An ST for a composed TOE may refer out to the description of the logical scope of the component  
2658 TOEs, provided in the component TOE STs to provide the majority of this description for the  
2659 composed TOE. However, the evaluator determines that the composed TOE ST clearly discusses  
2660 which features of the individual components are not within the composed TOE, and therefore not a  
2661 feature of the composed TOE.

### 2662 **10.3.1.4 Action ASE\_INT.1.2E**

#### 2663 **10.3.1.4.1 Work unit ASE\_INT.1-11**

2664 The evaluator **shall examine** the TOE reference, TOE overview and TOE description to determine  
2665 that they are consistent with each other.

## 2666 **10.4 Conformance claims (ASE\_CCL)**

### 2667 **10.4.1 Evaluation of sub-activity (ASE\_CCL.1)**

#### 2668 **10.4.1.1 Objectives**

2669 The objective of this sub-activity is to determine the validity of various conformance claims. These  
2670 describe how the ST and the TOE conform to ISO/IEC 15408 and how the ST conforms to a PP-  
2671 Configuration, PPs and packages.

#### 2672 **10.4.1.2 Input**

2673 The evaluation evidence for this sub-activity is:

- 2674 a) the ST;
- 2675 b) the Base-PP(s) that the ST claims conformance to;
- 2676 c) the package(s) that the ST claims conformance to.

#### 2677 **10.4.1.3 Action ASE\_CCL.1.1E**

2678 ISO/IEC 15408-3 ASE\_CCL.1.1C: *The conformance claim shall contain an ISO/IEC 15408*  
2679 *conformance claim that identifies the edition of ISO/IEC 15408 to which the ST and the TOE claim*  
2680 *conformance.*

2681 **10.4.1.3.1 Work unit ASE\_CCL.1-1**

2682 The evaluator **shall check** that the conformance claim contains an ISO/IEC 15408 conformance  
2683 claim that identifies the edition of ISO/IEC 15408 to which the ST and the TOE claim conformance.

2684 The evaluator determines that ISO/IEC 15408 conformance claim identifies the edition of ISO/IEC  
2685 15408 that was used to develop this ST. This should include the edition number of ISO/IEC 15408  
2686 and, unless the International English edition of ISO/IEC 15408 was used, the language of the  
2687 edition of ISO/IEC 15408 that was used.

2688 For a composed TOE, the evaluator will consider any differences between the edition of ISO/IEC  
2689 15408 claimed for a component and the edition of ISO/IEC 15408 claimed for the composed TOE. If  
2690 the edition differ the evaluator will assess whether the differences between the editions will lead to  
2691 conflicting claims.

2692 For instances where ISO/IEC 15408 conformance claims for the base TOE and dependent TOE are  
2693 for different major releases of ISO/IEC 15408 (e.g. one component TOE conformance claim is  
2694 ISO/IEC 15408 v2.x and the other component TOE conformance claim is ISO/IEC 15408 v3.x), the  
2695 conformance claim for the composed TOE will be the earlier release of ISO/IEC 15408, as ISO/IEC  
2696 15408 is developed with an aim to provide backwards compatibility (although this may not be  
2697 achieved in the strictest sense, it is understood to be achieved in principle).

2698 ISO/IEC 15408-3 ASE\_CCL.1.2C: *ISO/IEC 15408 conformance claim shall describe the conformance of*  
2699 *the ST to ISO/IEC 15408-2 as either ISO/IEC 15408-2 conformant or ISO/IEC 15408-2 extended.*

2700 **10.4.1.3.2 Work unit ASE\_CCL.1-2**

2701 The evaluator **shall check** that ISO/IEC 15408 conformance claim states a claim of either ISO/IEC  
2702 15408-2 conformant or ISO/IEC 15408-2 extended for the ST.

2703 For a composed TOE, the evaluator will consider whether this claim is consistent not only with  
2704 ISO/IEC 15408-2, but also with the claims of conformance to ISO/IEC 15408-2 by each of the  
2705 component TOEs. I.e. if one or more component TOEs claims to be ISO/IEC 15408-2 extended, then  
2706 the composed TOE should also claim to be ISO/IEC 15408-2 extended.

2707 ISO/IEC 15408 conformance claim for the composed TOE may be ISO/IEC 15408-2 extended, even  
2708 though the component TOEs are ISO/IEC 15408-2 conformant, in the event that additional SFRs  
2709 are claimed for the base TOE (see composed TOE guidance for ASE\_CCL.1.6C)

2710 ISO/IEC 15408-3 ASE\_CCL.1.3C: *ISO/IEC 15408 conformance claim shall describe the conformance of*  
2711 *the ST to ISO/IEC 15408-3 as either ISO/IEC 15408-3 conformant or ISO/IEC 15408-3 extended.*

2712 **10.4.1.3.3 Work unit ASE\_CCL.1-3**

2713 The evaluator **shall check** that ISO/IEC 15408 conformance claim states a claim of either ISO/IEC  
2714 15408-3 conformant or ISO/IEC 15408-3 extended for the ST.

2715 ISO/IEC 15408-3 ASE\_CCL.1.4C: *ISO/IEC 15408 conformance claim shall be consistent with the*  
2716 *extended components definition.*

2717 **10.4.1.3.4 Work unit ASE\_CCL.1-4**

2718 The evaluator **shall examine** ISO/IEC 15408 conformance claim for ISO/IEC 15408-2 to determine  
2719 that it is consistent with the extended components definition.

2720 If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-2 conformant, the evaluator  
2721 determines that the extended components definition does not define functional components.

## ISO/IEC 18045:2008(E)

2722 If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-2 extended, the evaluator determines  
2723 that the extended components definition defines at least one extended functional component.

### 2724 10.4.1.3.5 Work unit ASE\_CCL.1-5

2725 The evaluator **shall examine** ISO/IEC 15408 conformance claim for ISO/IEC 15408-3 to determine  
2726 that it is consistent with the extended components definition.

2727 If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-3 conformant, the evaluator  
2728 determines that the extended components definition does not define assurance components.

2729 If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-3 extended, the evaluator determines  
2730 that the extended components definition defines at least one extended assurance component.

2731 ISO/IEC 15408-3 ASE\_CCL.1.5C: *The conformance claim shall identify a PP-Configuration, or all PPs*  
2732 *and security requirement packages to which the ST claims conformance.*

### 2733 10.4.1.3.6 Work unit ASE\_CCL.1-6

2734 The evaluator **shall check** that the conformance claim contains a PP claim that identifies all PPs for  
2735 which the ST claims conformance.

2736 If the ST does not claim conformance to a PP, this work unit is not applicable and therefore  
2737 considered to be satisfied.

2738 The evaluator determines that any referenced PPs are unambiguously identified (e.g. by title and  
2739 version number, or by the identification included in the introduction of that PP).

2740 For conformance claims to PPs containing functional packages, the evaluator examines that:

- 2741 • The ST does not include conformance claims to any PP that also claims conformance to  
2742 any of the packages to which the ST is also claiming conformance. all dependencies  
2743 between the selected packages have been resolved.

2744 The evaluator is reminded that claims of partial conformance to a PP are not permitted. Therefore,  
2745 conformance to a PP requiring a composite solution may be claimed in an ST for a composed TOE.  
2746 Conformance to such a PP would not have been possible during the evaluation of the component  
2747 TOEs, as these components would not have satisfied the composed solution. This is only possible in  
2748 the instances where the “composite” PP permits use of the composition evaluation approach (use  
2749 of ACO components).

2750 For PPs containing functional packages, partial conformance means that not all packages have been  
2751 included in the ST, a functional package has only been partially included into the ST, or a  
2752 dependency requirement between functional packages has not been met. Note that exclusion of  
2753 optional requirements that the ST either chooses not to, or is not required to, claim does not result  
2754 in “partial conformance” to the PP, and so is allowed.

### 2755 10.4.1.3.7 Work unit ASE\_CCL.1-6a

2756 The evaluator **shall check** that, for each PP to which the ST claims conformance, the conformance  
2757 statement of that PP allows all other PPs in the conformance claim to be allowed to be claimed with  
2758 that PP.

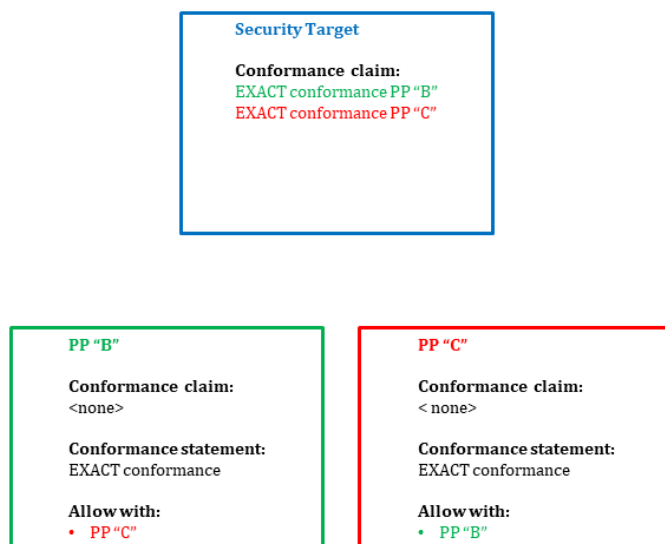
2759 If the ST does not claim conformance to a PP, or claims conformance to only one PP, this work unit  
2760 is not applicable and therefore considered to be satisfied.



2761 If the ST is not claiming exact conformance to a PP, this work unit is not applicable and therefore  
 2762 considered to be satisfied.

2763 The evaluator determines that the conformance statement of the PP to which conformance is being  
 2764 claimed lists each of the PPs identified in the conformance claim section of the ST as being "allowed  
 2765 to be claimed with" that PP. Note that this is only applicable in cases where that PP requires exact  
 2766 conformance and the ST claims exact conformance.

2767 EXAMPLE: consider the case where an ST is being evaluated and claims conformance to PPs B and  
 2768 C; this is depicted in Figure 7. The ST is claiming exact conformance, so all PPs require exact  
 2769 conformance in their conformance statements. Under this work unit, the evaluator determines that  
 2770 PP B lists (in its conformance statement) "PP C" as being a PP that can be claimed (by an ST) with  
 2771 PP B. Likewise, the evaluator determines that PP C lists (in its conformance statement) "PP B" as  
 2772 being a PP that can be claimed (by an ST) with PP C.



2773  
 2774 **Figure 7 — Example of exact conformance relationships between an ST and PPs**

2775 **10.4.1.3.8 Work unit ASE\_CCL.1-6b**

2776 The evaluator shall check that the conformance claim contains a PP-Configuration claim that  
 2777 identifies the PP-Configuration(s) for which the ST claims conformance.

2778 If the ST does not claim conformance to a PP-Configuration, this work unit is not applicable and  
 2779 therefore considered to be satisfied.

2780 If the ST claims conformance to multiple PP-Configurations, the evaluator ensures that the  
 2781 conformance statement for all PP-Configurations is either "strict" or "demonstrable"; an ST cannot  
 2782 claim exact conformance to multiple PP-Configurations.

2783 If the ST claims conformance to a PP-Configuration and a PP (that is not part of the PP-  
 2784 Configuration), the evaluator ensures that the conformance statement for all PP-Configurations  
 2785 and the PP is either "strict" or "demonstrable"; an ST cannot claim exact conformance to a PP-  
 2786 Configuration and a PP that is not part of the PP-Configuration. The evaluator determines that any

## ISO/IEC 18045:2008(E)

2787 referenced PP-Configuration(s) are unambiguously identified (e.g. by title and version number, or  
2788 by the identification included in the introduction of that PP).

2789 For conformance claims to PP-Configurations containing functional packages, the evaluator  
2790 examines that:

- 2791 • all dependencies between the selected packages have been resolved.

2792 The evaluator is reminded that claims of partial conformance to a PP are not permitted. For PP-  
2793 Configurations containing functional packages, partial conformance means that a functional  
2794 package has only been partially included into the ST, or a dependency requirement between  
2795 functional packages has not been met.

### 2796 10.4.1.3.9 Work unit ASE\_CCL.1-7

2797 The evaluator **shall check** that the conformance claim contains a package claim that identifies all  
2798 packages to which the ST claims conformance.

2799 If the ST does not claim conformance to a package, this work unit is not applicable and therefore  
2800 considered to be satisfied.

2801 The evaluator determines that any packages to which the ST claims conformance are not also  
2802 claimed conformance to by a PP, Base-PP, or PP-Module that the ST is claiming conformance to.

2803 The evaluator also determines that if the ST is claiming exact conformance to a PP or PP-  
2804 Configuration, then no packages are claimed conformance to by the ST. The evaluator determines  
2805 that the component TOE STs from which the composed TOE is derived are also unambiguously  
2806 identified.

2807 The evaluator is reminded that claims of partial conformance to a package are not permitted.

### 2808 10.4.1.3.10 Work unit ASE\_CCL.1-8

2809 The evaluator **shall check** that, for each identified package, the conformance claim states a claim of  
2810 either package-name conformant or package-name augmented.

2811 If the ST claims conformance to a PP and the PP itself claims conformance to one or more  
2812 functional packages then the ST shall not separately make a conformance claim to the same  
2813 packages. If the ST does not claim conformance to a package, this work unit is not applicable and  
2814 therefore considered to be satisfied.

2815 If the package conformance claim contains package-name conformant, the evaluator determines  
2816 that:

2817 a) If the package is an assurance package, then the ST contains all SARs included in the  
2818 package, but no additional SARs.

2819 b) If the package is a functional package, then all assumptions, threats, OSPs, security  
2820 objectives and SFRs included in the package are identical to those included in the ST  
2821 (after allowing any remaining iterations, refinements, assignments or selections  
2822 from the package to be made in the ST).

2823 If the package conformance claim contains package-name augmented, the evaluator determines  
2824 that:

- 2825 a) If the package is an assurance package then the ST contains all SARs included in the  
2826 package, and at least one additional SAR or at least one SAR that is hierarchical to a  
2827 SAR in the package.
- 2828 b) If the package is a functional package, then the constituent parts (security problem  
2829 definition, security objectives, SFRs) of that ST contain all constituent parts  
2830 (security problem definition, security objectives, SFRs) of that specific package, but  
2831 additionally contain at least one enhancement of the security  
2832 functionality defined by that specific package (finally resulting in an additional SFR  
2833 or one an SFR that is hierarchically higher than an SFR in the package).
- 2834 The evaluator determines that, if the ST claims exact conformance to the PPs/PP-Configuration,  
2835 only claims of <package name>-conformant are present.
- 2836 ISO/IEC 15408-3 ASE\_CCL.1.7C: *The conformance claim rationale shall demonstrate that the TOE*  
2837 *type is consistent with the TOE type in the PP-Configuration or PPs for which conformance is being*  
2838 *claimed.*
- 2839 **10.4.1.3.11 Work unit ASE\_CCL.1-9**
- 2840 In this work unit, the term “PP” shall be understood to mean “PP or PP-Configuration component”.
- 2841 The evaluator **shall examine** the conformance claim rationale to determine that the TOE type of  
2842 the TOE is consistent with all TOE types of the PPs.
- 2843 If the ST does not claim conformance to a PP, this work unit is not applicable and therefore  
2844 considered to be satisfied.
- 2845 The relation between the types may be simple: a firewall ST claiming conformance to a firewall PP,  
2846 or more complex: a smart card ST claiming conformance to a number of PPs at the same time (a PP  
2847 for the integrated circuit, a PP for the smart card OS, and two PPs for two applications on the smart  
2848 card).
- 2849 For a composed TOE, the evaluator will determine whether the conformance claim rationale  
2850 demonstrates that the TOE types of the component TOEs are consistent with the composed TOE  
2851 type. This does not mean that both the component and the composed TOE types have to be the  
2852 same, but rather that the component TOEs are suitable for integration to provide the composed  
2853 TOE. It should be made clear in the composed TOE ST which SFRs are only included as a result of  
2854 composition, and were not examined as SFRs in the base and dependent TOE (e.g. EALx) evaluation.
- 2855 ISO/IEC 15408-3 ASE\_CCL.1.8C: *The conformance claim rationale shall demonstrate that the*  
2856 *statement of the security problem definition is consistent with the statement of the security problem*  
2857 *definition in the PP-Configuration or PPs for which conformance is being claimed.*
- 2858 **10.4.1.3.12 Work unit ASE\_CCL.1-10**
- 2859 In this work unit, the term “PP” shall be understood to mean “PP or PP-Configuration component”.
- 2860 The evaluator **shall examine** the conformance claim rationale to determine that it demonstrates  
2861 that the statement of security problem definition is consistent, as defined by the conformance  
2862 statement of the PP, with the statements of security problem definition stated in the PPs to which  
2863 conformance is being claimed.
- 2864 If the ST does not claim conformance with a PP, this work unit is not applicable and therefore  
2865 considered to be satisfied.

## ISO/IEC 18045:2008(E)

2866 If the PP does not have a statement of security problem definition, this work unit is not applicable  
2867 and therefore considered to be satisfied.

2868 If the PP contains functional packages, the evaluator determines that the security problem  
2869 definition of the ST consists of all assumptions, threats and OSPs of all functional packages.

2870 If packages are used, the rules defined in the following paragraphs concerning exact, strict and  
2871 demonstrable conformance also hold for the SPD descriptions taken from the packages.

2872 If exact conformance is required by the PP to which conformance is being claimed, no conformance  
2873 claim rationale is required. Instead, the evaluator determines whether:

2874 a) the threats in the ST are identical (no fewer threats, no additional threats) to the threats in  
2875 the PP to which conformance is being claimed. If exact conformance is being claimed to  
2876 more than one PP, then the set of threats in the ST must be identical to the union of the  
2877 threats in all PPs to which conformance is being claimed.

2878 b) the OSPs in the ST are identical (no fewer OSPs, no additional OSPs) to the OSPs in the PP  
2879 to which conformance is being claimed. If exact conformance is being claimed to more than  
2880 one PP, then the set of OSPs in the ST must be identical to the union of the OSPs in all PPs  
2881 to which conformance is being claimed.

2882 c) the assumptions in the ST are identical (no fewer assumptions, no additional assumptions)  
2883 to the assumptions in the PP to which conformance is being claimed. If exact conformance  
2884 is being claimed to more than one PP, then the set of assumptions in the ST must be  
2885 identical to the union of the assumptions in all PPs to which conformance is being claimed,  
2886 with the following possible exception;

2887 • an assumption (or part of an assumption) from a PP can be omitted, if all security  
2888 objectives for the operational environment addressing this assumption (or part of an  
2889 assumption) are replaced by security objectives for the TOE that are identical to (taken  
2890 from) another of the PPs to which the ST is claiming conformance;

2891 When examining an ST in these circumstances (assumptions from one PP are replaced by security  
2892 objectives on the TOE from one of the other PPs) the evaluator shall carefully determine that the  
2893 condition given above is fulfilled. The following discussion gives an example:

2894 EXAMPLE: an ST is claiming exact conformance to two PPs. As determined in previous work units,  
2895 both PPs require exact conformance in their conformance statements, and both PPs list the other  
2896 as being "allowed with" the PP in a conformance claim by an ST. One PP to which the ST claims  
2897 conformance contains an assumption stating that the operational environment prevents  
2898 unauthorised modification or interception of data sent to an external interface of the TOE. This  
2899 may be the case if the TOE accepts data in clear text and without integrity protection at this  
2900 interface and is assumed to be located in a secure operational environment, which will prevent  
2901 attackers from accessing this data. The assumption will then be mapped in the PP to some objective  
2902 for the operational environment stating that the data interchanged at this interface are protected  
2903 by adequate measures in the operational environment. Suppose there is another PP that specifies  
2904 that conformant TOEs must protect data sent over the TOEs external interfaces, and has  
2905 appropriate threats and security objectives addressing this threat. The ST author can then replace  
2906 the assumption and security objective for the environment related to the protection of data over  
2907 the external interfaces of the TOE from one PP with the security objective stating that the TOE itself  
2908 protects these data, for example by providing a secure channel for encryption and integrity  
2909 protection of all data transferred via this interface from the other PP; the corresponding objective  
2910 and assumption for the operational environment from the other PP is thus omitted from the ST.  
2911 This is also called re-assigning of the objective, since the objective is re-assigned from the  
2912 operational environment to the TOE. Note, that this TOE is still secure in an operational  
2913 environment fulfilling the omitted assumption and therefore still fulfils the PP. Further, the set of

2914 threats and objectives in the ST is still no broader than the union of threats and objectives in the  
 2915 PPs to which it is claiming exact conformance.

2916 If strict conformance is required by the PP to which conformance is being claimed no conformance  
 2917 claim rationale is required. Instead, the evaluator determines whether:

2918 a) the threats in the ST are a superset of or identical to the threats in the PP to which  
 2919 conformance is being claimed;

2920 b) the OSPs in the ST are a superset of or identical to the OSPs in the PP to which  
 2921 conformance is being claimed;

2922 c) the assumptions in the ST are identical to the assumptions in the PP to which  
 2923 conformance is being claimed, with two possible exceptions described in the  
 2924 following two bullet points;

- 2925 • an assumption (or part of an assumption) from the PP can be omitted, if all security  
 2926 objectives for the operational environment addressing this assumption (or part of an  
 2927 assumption) are replaced by security objectives for the TOE;

- 2928 • an assumption can be added to the assumptions defined in the PP, if a rationale is given,  
 2929 why the new assumption neither mitigates a threat (or a part of a threat) meant to be  
 2930 addressed by security objectives for the TOE in the PP, nor fulfils an OSP (or part of an  
 2931 OSP) meant to be addressed by security objectives for the TOE in the PP.

2932 When examining an ST claiming a PP, which omits assumptions from the PP or adds new  
 2933 assumptions, the evaluator shall carefully determine, if the conditions given above are fulfilled. The  
 2934 following discussion gives some motivation and examples for these cases:

- 2935 • Example for omitting an assumption: A PP may contain an assumption stating that the  
 2936 operational environment prevents unauthorised modification or interception of data sent  
 2937 to an external interface of the TOE. This may be the case if the TOE accepts data in clear  
 2938 text and without integrity protection at this interface and is assumed to be located in a  
 2939 secure operational environment, which will prevent attackers from accessing these data.  
 2940 The assumption will then be mapped in the PP to some objective for the operational  
 2941 environment stating that the data interchanged at this interface are protected by adequate  
 2942 measures in the operational environment. If an ST claiming this PP defines a more secure  
 2943 TOE, which has an additional security objective stating that the TOE itself protects these  
 2944 data, for example by providing a secure channel for encryption and integrity protection of  
 2945 all data transferred via this interface, the corresponding objective and assumption for the  
 2946 operational environment can be omitted from the ST. This is also called re-assigning of  
 2947 the objective, since the objective is re-assigned from the operational environment to the  
 2948 TOE. Note, that this TOE is still secure in an operational environment fulfilling the  
 2949 omitted assumption and therefore still fulfils the PP.

- 2950 • Example for adding an assumption: In this example, the PP is designed to specify  
 2951 requirements for a TOE of type "Firewall" and an ST author wishes to claim this PP for a  
 2952 TOE, which implements a firewall, but additionally provides the functionality of a virtual  
 2953 private network (VPN) component. For the VPN functionality, the TOE needs  
 2954 cryptographic keys and these keys may also have to be handled securely by the  
 2955 operational environment (e. g. if symmetric keys are used to secure the network  
 2956 connection and therefore need to be provided in some secure way to other components in  
 2957 the network). In this case, it is acceptable to add an assumption that the cryptographic  
 2958 keys used by the VPN are handled securely by the operational environment. This

## ISO/IEC 18045:2008(E)

- 2959 assumption does not address threats or OSPs of the PP and therefore fulfils the conditions  
2960 stated above.
- 2961 • Counterexample for adding an assumption: In a variant of the first example a PP may  
2962 already contain an objective for the TOE to provide a secure channel for one of its  
2963 interfaces, and this objective is mapped to a threat of unauthorised modification or  
2964 reading of the data on this interface. In this case, it is clearly not allowed for an ST  
2965 claiming this PP to add an assumption for the operational environment, which assumes  
2966 that the operational environment protects data on this interface against modification or  
2967 unauthorised reading of the data. This assumption would reduce a threat, which is meant  
2968 to be addressed by the TOE. Therefore a TOE fulfilling an ST with this added assumption  
2969 would not automatically fulfil the PP any more and this addition is therefore not  
2970 allowed. Second counterexample for adding an assumption: In the example above of a  
2971 TOE implementing a firewall it would not be admissible to add a general assumption that  
2972 the TOE is only connected to trusted devices, because this would obviously remove  
2973 essential threats relevant for a firewall (namely that there is untrusted IP traffic, which  
2974 needs to be filtered). Therefore, this addition would not be allowed.
- 2975 If demonstrable conformance is required by the PP, the evaluator examines the conformance claim  
2976 rationale to determine that it demonstrates that the statement of security problem definition of the  
2977 ST is equivalent or more restrictive than the statement of security problem definition in the PP to  
2978 which conformance is being claimed.
- 2979 For this, the conformance claim rationale needs to demonstrate that the security problem  
2980 definition in the ST is equivalent (or more restrictive) than the security problem definition in the  
2981 PP. This means that:
- 2982 • all TOEs that would meet the security problem definition in the ST also meet the security  
2983 problem definition in the PP. This can also be shown indirectly by demonstrating that  
2984 every event, which realises a threat defined in the PP or violates an OSP defined in the  
2985 PP, would also realise a threat stated in the ST or violate an OSP defined in the ST. Note  
2986 that fulfilling an OSP stated in the ST may avert a threat stated in the PP or that averting  
2987 a threat stated in the ST may fulfil an OSP stated in the PP, so threats and OSPs can  
2988 substitute each other;
- 2989 • all operational environments that would meet the security problem definition in the PP  
2990 would also meet the security problem definition in the ST (with one exception in the next  
2991 bullet);
- 2992 • besides a set of assumptions in the ST needed to demonstrate conformance to the SPD of  
2993 the PP, an ST may specify further assumptions, but only if these additional assumptions  
2994 are independent of and do not affect the security problem definition as defined in the PP.  
2995 More detailed, there are no assumptions in the ST that exclude threats to the TOE that  
2996 need to be countered by the TOE according to the PP. Similarly, there are no assumptions  
2997 in the ST that realise aspects of an OSP stated in the PP, which are meant to be fulfilled  
2998 by the TOE according to the PP."
- 2999 For a composed TOE, the evaluator will consider whether the security problem definition of the  
3000 composed TOE is consistent with that specified in the STs for the component TOEs. This is  
3001 determined in terms of demonstrable conformance. In particular, the evaluator examines the  
3002 conformance claim rationale to determine that:
- 3003 a) Threat statements and OSPs in the composed TOE ST do not contradict those from the  
3004 component STs.

- 3005 b) Any assumptions made in the component STs are upheld in the composed TOE ST.  
 3006 That is, either the assumption should also be present in the composed ST, or the  
 3007 assumption should be positively addressed in the composed ST. The assumption  
 3008 may be positively addressed through specification of requirements in the composed  
 3009 TOE to provide functionality fulfilling the concern captured in the assumption.
- 3010 ISO/IEC 15408-3 ASE\_CCL.1.9C: *The conformance claim rationale shall demonstrate that the*  
 3011 *statement of security objectives is consistent with the statement of security objectives in the PP-*  
 3012 *Configuration or PPs for which conformance is being claimed.*
- 3013 **10.4.1.3.13 Work unit ASE\_CCL.1-11**
- 3014 In this work unit, the term “PP” shall be understood to mean “PP or PP-Configuration component”.
- 3015 The evaluator ***shall examine*** the conformance claim rationale to determine that the statement of  
 3016 security objectives is consistent, as defined by the conformance statement of the PP, with the  
 3017 statement of security objectives in the PPs to which conformance is being claimed.
- 3018 If the ST does not claim conformance to a PP, this work unit is not applicable and therefore  
 3019 considered to be satisfied.
- 3020 If the PP to which conformance is being claimed contains functional packages, the evaluator  
 3021 determines that the security objectives of the ST consist of all security objectives of all functional  
 3022 packages.
- 3023 If packages are used, the rules defined in the following paragraphs concerning exact, strict and  
 3024 demonstrable conformance also hold for the security objectives taken from the packages.
- 3025 If exact conformance is required by the PP to which conformance is being claimed, no conformance  
 3026 claim rationale is required. Instead, the evaluator determines whether:
- 3027 a) The ST contains all security objectives for the TOE of the PP to which conformance is  
 3028 being claimed. Note that in the exact conformance case, it is not allowed for the ST  
 3029 under evaluation to have additional security objectives for the TOE. If conformance  
 3030 is being claimed to more than one PP, the set of security objectives for the TOE must  
 3031 be identical to the union of the security objectives for the TOE in the PPs to which  
 3032 conformance is being claimed. It should be noted that in the case that optional  
 3033 requirements have associated SPD elements, exact conformance can still be claimed  
 3034 if objectives associated with the SPD elements are omitted when the associated  
 3035 optional SFRs are also omitted.
- 3036 b) The security objectives for the operational environment in the ST are identical to the  
 3037 security objectives for the operational environment in the PP to which conformance  
 3038 is being claimed. If conformance is being claimed to more than one PP, the set of  
 3039 security objectives for the operational environment must be identical to the union of  
 3040 the security objectives for the operational environment in the PPs to which  
 3041 conformance is being claimed with the possible exception that a security objective  
 3042 for the operational environment (or part of such security objective) from one PP can  
 3043 be replaced by the same (part of the) security objective for the TOE from another PP.
- 3044 If strict conformance is required by the PP to which conformance is being claimed, no conformance  
 3045 claim rationale is required. Instead, the evaluator determines whether:
- 3046 a) The ST contains all security objectives for the TOE of the PP to which conformance is  
 3047 being claimed. Note that it is allowed for the ST under evaluation to have additional  
 3048 security objectives for the TOE;

## ISO/IEC 18045:2008(E)

- 3049 b) The security objectives for the operational environment in the ST are identical to the  
3050 security objectives for the operational environment in the PP to which conformance  
3051 is being claimed, with two possible exceptions described in the following two bullet  
3052 points;
- 3053 c) a security objective for the operational environment (or part of such security  
3054 objective) from the PP can be replaced by the same (part of the) security objective  
3055 stated for the TOE;
- 3056 d) a security objective for the operational environment can be added to the objectives  
3057 defined in the PP, if a justification is given, why the new objective neither mitigates a  
3058 threat (or a part of a threat) meant to be addressed by security objectives for the  
3059 TOE in the PP, nor fulfils an OSP (or part of an OSP) meant to be addressed by  
3060 security objectives for the TOE in the PP.
- 3061 When examining an ST claiming a PP, which omits security objectives for the operational  
3062 environment from the PP or adds new security objectives for the operational environment, the  
3063 evaluator shall carefully determine, if the conditions given above are fulfilled. The examples given  
3064 for the case of assumptions in the preceding work unit are also valid here.
- 3065 If demonstrable conformance is required by the PP to which conformance is being claimed, the  
3066 evaluator examines the conformance claim rationale to determine that it demonstrates that the  
3067 statement of security objectives of the ST is equivalent or more restrictive than the statement of  
3068 security objectives in the PP to which conformance is being claimed.
- 3069 For this the conformance claim rationale needs to demonstrate that the security objectives in the  
3070 ST are equivalent (or more restrictive) than the security objectives in the PP. This means that:
- 3071 • all TOEs that would meet the security objectives for the TOE in the ST also meet the  
3072 security objectives for the TOE in the PP;
- 3073 • all operational environments that would meet the security objectives for the operational  
3074 environment in the PP would also meet the security objectives for the operational  
3075 environment in the ST (with one exception in the next bullet);
- 3076 • besides a set of security objectives for the operational environment in the ST, which are  
3077 used to demonstrate conformance to the set of security objectives defined in the PP, an  
3078 ST may specify further security objectives for the operational environment, but only if  
3079 these security objectives neither affect the original set of security objectives for the TOE  
3080 nor the security objectives for the operational environment as defined in the PP to which  
3081 conformance is claimed."
- 3082 For a composed TOE, the evaluator will consider whether the security objectives of the composed  
3083 TOE are consistent with that specified in the STs for the component TOEs. This is determined in  
3084 terms of demonstrable conformance. In particular, the evaluator examines the conformance claim  
3085 rationale to determine that:
- 3086 a) The statement of security objectives in the dependent TOE ST relevant to any IT in  
3087 the operational environment are consistent with the statement of security objectives  
3088 for the TOE in the base TOE ST. It is not expected that the statement of security  
3089 objectives for the environment within in the dependent TOE ST will cover all aspects  
3090 of the statement of security objectives for the TOE in the base TOE ST.
- 3091 b) The statement of security objectives in the composed ST is consistent with the  
3092 statements of security objectives in the STs for the component TOEs.



3093 If demonstrable conformance is required by the PP, the evaluator examines the conformance claim  
3094 rationale to determine that it demonstrates that the statement of security objectives of the ST is at  
3095 least equivalent to the statement of security objectives in the PP, or component TOE ST in the case  
3096 of a composed TOE ST.

3097 ISO/IEC 15408-3 ASE\_CCL.1.10C: *The conformance claim rationale shall demonstrate that the*  
3098 *statement of security requirements is consistent with the statement of security requirements in the*  
3099 *PP-Configuration or PPs for which conformance is being claimed.*

#### 3100 **10.4.1.3.14 Work unit ASE\_CCL.1-12**

3101 In this work unit, the term "PP" shall be understood to mean "PP or PP-Configuration component".

3102 The evaluator **shall examine** the ST to determine that it is consistent, as defined by the  
3103 conformance statement of the PP, with all security requirements in the PPs for which conformance  
3104 is being claimed.

3105 If the ST does not claim conformance to a PP, this work unit is not applicable and therefore  
3106 considered to be satisfied.

3107 If the PP to which conformance is being claimed contains functional packages, the evaluator  
3108 determines that the SFRs of the ST consist of all SFRs (or hierarchical SFRs) of all functional  
3109 packages.

3110 If packages are used, the rules defined in the following paragraphs concerning exact, strict and  
3111 demonstrable conformance also hold for the SFRs taken from the packages.

3112 If exact conformance is required by the PP to which conformance is being claimed, no conformance  
3113 claim rationale is required. Instead, the evaluator determines that the statement of security  
3114 requirements in the PP to which conformance is being claimed is exactly reproduced in the ST,  
3115 with the following allowances:

- 3116 a) an SFR from the PP may be iterated or refined in the ST,
- 3117 b) all SFRs that are defined in the PP to which conformance is being claimed as  
3118 selection-based upon a particular selection shall be included if and only if that  
3119 selection on which inclusion is based is present in the ST. If a selection is not chosen  
3120 by the ST author, then the selection-based SFRs associated with that selection are  
3121 not included in the ST.
- 3122 c) There are no additional security requirements (SFRs or SARs) that are included in the  
3123 ST that are not also present in the PP.
- 3124 d) Optional requirements (and associated SPD elements) that 1) the ST wishes to claim  
3125 and/or 2) the ST is required to claim (as stipulated in the PP/PP-Module) due to the  
3126 TOE implementation are included; other optional requirements may be excluded  
3127 while maintaining the exact conformance claim.
- 3128 e) In the case where exact conformance is being claimed to multiple PPs, the evaluator  
3129 determines there are no additional security requirements included in the ST that are  
3130 not in at least one of the PPs, and that all of the requirements (with the allowances  
3131 described above) in all of the PPs have been included in the ST.

3132 If strict conformance is required by the PP to which conformance is being claimed, no conformance  
3133 claim rationale is required. Instead, the evaluator determines whether the statement of security

## ISO/IEC 18045:2008(E)

3134 requirements in the ST is a superset of or identical to the statement of security requirements in the  
3135 PP to which conformance is being claimed (for strict conformance).

3136 If demonstrable conformance is required by the PP to which conformance is being claimed, the  
3137 evaluator examines the conformance claim rationale to determine that it demonstrates that the  
3138 statement of security requirements of the ST is equivalent or more restrictive than the statement of  
3139 security requirements in the PP to which conformance is being claimed.

3140 For:

- 3141 • SFRs: The conformance rationale in the ST shall demonstrate that the overall set of  
3142 requirements defined by the SFRs in the ST is equivalent (or more restrictive) than the  
3143 overall set of requirements defined by the SFRs in the PP. This means that all TOEs that  
3144 would meet the requirements defined by the set of all SFRs in the ST would also meet the  
3145 requirements defined by the set of all SFRs in the PP;
- 3146 • SARs: The ST shall contain all SARs in the PP, but may claim additional SARs or  
3147 replace SARs by hierarchically stronger SARs. The completion of operations in the ST  
3148 must be consistent with that in the PP; either the same completion will be used in the ST  
3149 as that in the PP or a completion that makes the SAR more restrictive (the rules of  
3150 refinement apply).

3151 For a composed TOE, the evaluator will consider whether the security requirements of the  
3152 composed TOE are consistent with that specified in the STs for the component TOEs. This is  
3153 determined in terms of demonstrable conformance. In particular, the evaluator examines the  
3154 conformance rationale to determine that:

- 3155 a) The statement of security requirements in the dependent TOE ST relevant to any IT in  
3156 the operational environment is consistent with the statement of security  
3157 requirements for the TOE in the base TOE ST. It is not expected that the statement of  
3158 security requirements for the environment within in the dependent TOE ST will  
3159 cover all aspects of the statement of security requirements for the TOE in the base  
3160 TOE ST, as some SFRs may need to be added to the statement of security  
3161 requirements in the composed TOE ST. However, the statement of security  
3162 requirements in the base should support the operation of the dependent component.
- 3163 b) The statement of security objectives in the dependent TOE ST relevant to any IT in  
3164 the operational environment is consistent with the statement of security  
3165 requirements for the TOE in the base TOE ST. It is not expected that the statement of  
3166 security objectives for the environment within in the dependent TOE ST will cover  
3167 all aspects of the statement of security requirements for the TOE in the base TOE ST.
- 3168 c) The statement of security requirements in the composed is consistent with the  
3169 statements of security requirements in the STs for the component TOEs.

3170 If demonstrable conformance is required by the PP to which conformance is being claimed, the  
3171 evaluator examines the conformance claim rationale to determine that it demonstrates that the  
3172 statement of security requirements of the ST is at least equivalent to the statement of security  
3173 requirements in the PP, or component TOE ST in the case of a composed TOE ST.

3174 **10.5 Security problem definition (ASE\_SPD)**

3175 **10.5.1 Evaluation of sub-activity (ASE\_SPD.1)**

3176 **10.5.1.1 Objectives**

3177 The objective of this sub-activity is to determine that the security problem intended to be  
3178 addressed by the TOE and its operational environment is clearly defined.

3179 **10.5.1.2 Input**

3180 The evaluation evidence for this sub-activity is:

3181 a) the ST.

3182 **10.5.1.3 Action ASE\_SPD.1.1E**

3183 **10.5.1.3.1 General**

3184 ISO/IEC 15408-3 ASE\_SPD.1.1C: *The security problem definition shall describe the threats.*

3185 **10.5.1.3.2 Work unit ASE\_SPD.1-1**

3186 The evaluator **shall check** that the security problem definition describes the threats.

3187 If all security objectives are derived from assumptions and/or OSPs only, the statement of threats  
3188 need not be present in the ST. In this case, this work unit is not applicable and therefore considered  
3189 to be satisfied.

3190 The evaluator determines that the security problem definition describes the threats that must be  
3191 countered by the TOE and/or operational environment.

3192 ISO/IEC 15408-3 ASE\_SPD.1.2C: *All threats shall be described in terms of a threat agent, an asset,*  
3193 *and an adverse action.*

3194 **10.5.1.3.3 Work unit ASE\_SPD.1-2**

3195 The evaluator **shall examine** the security problem definition to determine that all threats are  
3196 described in terms of a threat agent, an asset, and an adverse action.

3197 If all security objectives are derived from assumptions and/or OSPs only, the statement of threats  
3198 need not be present in the ST. In this case, this work unit is not applicable and therefore considered  
3199 to be satisfied.

3200 Threat agents may be further described by aspects such as expertise, resource, opportunity, and  
3201 motivation.

3202 ISO/IEC 15408-3 ASE\_SPD.1.3C: *The security problem definition shall describe the OSPs.*

3203 **10.5.1.3.4 Work unit ASE\_SPD.1-3**

3204 The evaluator **shall examine** that the security problem definition describes the OSPs.

3205 If all security objectives are derived from assumptions and threats only, OSPs need not be present  
3206 in the ST. In this case, this work unit is not applicable and therefore considered to be satisfied.

3207 The evaluator determines that OSP statements are made in terms of rules or guidelines that must  
3208 be followed by the TOE and/or its operational environment.

## ISO/IEC 18045:2008(E)

3209 The evaluator determines that each OSP is explained and/or interpreted in sufficient detail to make  
3210 it clearly understandable; a clear presentation of policy statements is necessary to permit tracing  
3211 security objectives to them.

3212 ISO/IEC 15408-3 ASE\_SPD.1.4C: *The security problem definition shall describe the assumptions*  
3213 *about the operational environment of the TOE.*

### 3214 **10.5.1.3.5 Work unit ASE\_SPD.1-4**

3215 The evaluator **shall examine** the security problem definition to determine that it describes the  
3216 assumptions about the operational environment of the TOE.

3217 If there are no assumptions, this work unit is not applicable and is therefore considered to be  
3218 satisfied.

3219 The evaluator determines that each assumption about the operational environment of the TOE is  
3220 explained in sufficient detail to enable consumers to determine that their operational environment  
3221 matches the assumption. If the assumptions are not clearly understood, the end result may be that  
3222 the TOE is used in an operational environment in which it will not function in a secure manner.

## 3223 **10.6 Security objectives (ASE\_OBJ)**

### 3224 **10.6.1 Evaluation of sub-activity (ASE\_OBJ.1)**

#### 3225 **10.6.1.1 Objectives**

3226 The objective of this sub-activity is to determine whether the security objectives for the  
3227 operational environment are clearly defined.

#### 3228 **10.6.1.2 Input**

3229 The evaluation evidence for this sub-activity is:

3230 a) the ST.

### 3231 **10.6.1.3 Action ASE\_OBJ.1.1E**

#### 3232 **10.6.1.3.1 General**

3233 ISO/IEC 15408-3 ASE\_OBJ.1.1C: *The statement of security objectives shall describe the security*  
3234 *objectives for the operational environment.*

#### 3235 **10.6.1.3.2 Work unit ASE\_OBJ.1-1**

3236 The evaluator **shall check** that the statement of security objectives defines the security objectives  
3237 for the operational environment.

3238 The evaluator checks that the security objectives for the operational environment are identified.

### 3239 **10.6.2 Evaluation of sub-activity (ASE\_OBJ.2)**

#### 3240 **10.6.2.1 Objectives**

3241 The objective of this sub-activity is to determine whether the security objectives adequately and  
3242 completely address the security problem definition and that the division of this problem between  
3243 the TOE and its operational environment is clearly defined.

3244 **10.6.2.2 Input**

3245 The evaluation evidence for this sub-activity is:

3246 a) the ST.

3247 **10.6.2.3 Action ASE\_OBJ.2.1E**

3248 **10.6.2.3.1 General**

3249 ISO/IEC 15408-3 ASE\_OBJ.2.1C: *The statement of security objectives shall describe the security*  
3250 *objectives for the TOE and the security objectives for the operational environment.*

3251 **10.6.2.3.2 Work unit ASE\_OBJ.2-1**

3252 The evaluator **shall check** that the statement of security objectives defines the security objectives  
3253 for the TOE and the security objectives for the operational environment.

3254 The evaluator checks that both categories of security objectives are clearly identified and  
3255 separated from the other category.

3256 ISO/IEC 15408-3 ASE\_OBJ.2.2C: *The security objectives rationale shall trace each security objective*  
3257 *for the TOE back to threats countered by that security objective and OSPs enforced by that security*  
3258 *objective.*

3259 **10.6.2.3.3 Work unit ASE\_OBJ.2-2**

3260 The evaluator **shall check** that the security objectives rationale traces all security objectives for the  
3261 TOE back to threats countered by the objectives and/or OSPs enforced by the objectives.

3262 Each security objective for the TOE may trace back to threats or OSPs, or a combination of threats  
3263 and OSPs, but it must trace back to at least one threat or OSP.

3264 Failure to trace implies that either the security objectives rationale is incomplete, the security  
3265 problem definition is incomplete, or the security objective for the TOE has no useful purpose.

3266 ISO/IEC 15408-3 ASE\_OBJ.2.3C: *The security objectives rationale shall trace each security objective*  
3267 *for the operational environment back to threats countered by that security objective, OSPs enforced*  
3268 *by that security objective, and assumptions upheld by that security objective.*

3269 **10.6.2.3.4 Work unit ASE\_OBJ.2-3**

3270 The evaluator **shall check** that the security objectives rationale traces the security objectives for  
3271 the operational environment back to threats countered by that security objective, to OSPs enforced  
3272 by that security objective, and to assumptions upheld by that security objective.

3273 Each security objective for the operational environment may trace back to threats, OSPs,  
3274 assumptions, or a combination of threats, OSPs and/or assumptions, but it must trace back to at  
3275 least one threat, OSP or assumption.

3276 Failure to trace implies that either the security objectives rationale is incomplete, the security  
3277 problem definition is incomplete, or the security objective for the operational environment has no  
3278 useful purpose.

3279 ISO/IEC 15408-3 ASE\_OBJ.2.4C: *The security objectives rationale shall demonstrate that the security*  
3280 *objectives counter all threats.*

## ISO/IEC 18045:2008(E)

### 3281 10.6.2.3.5 Work unit ASE\_OBJ.2-4

3282 The evaluator **shall examine** the security objectives rationale to determine that it justifies for each  
3283 threat that the security objectives are suitable to counter that threat.

3284 If no security objectives trace back to the threat, the evaluator action related to this work unit is  
3285 assigned a fail verdict.

3286 The evaluator determines that the justification for a threat shows whether the threat is removed,  
3287 diminished or mitigated.

3288 The evaluator determines that the justification for a threat demonstrates that the security  
3289 objectives are sufficient: if all security objectives that trace back to the threat are achieved, the  
3290 threat is removed, sufficiently diminished, or the effects of the threat are sufficiently mitigated.

3291 Note that the tracings from security objectives to threats provided in the security objectives  
3292 rationale may be part of a justification, but do not constitute a justification by themselves. Even in  
3293 the case that a security objective is merely a statement reflecting the intent to prevent a particular  
3294 threat from being realised, a justification is required, but this justification may be as minimal as  
3295 "Security Objective X directly counters Threat Y".

3296 The evaluator also determines that each security objective that traces back to a threat is necessary:  
3297 when the security objective is achieved it actually contributes to the removal, diminishing or  
3298 mitigation of that threat.

3299 ISO/IEC 15408-3 ASE\_OBJ.2.5C: *The security objectives rationale shall demonstrate that the security*  
3300 *objectives enforce all OSPs.*

### 3301 10.6.2.3.6 Work unit ASE\_OBJ.2-5

3302 The evaluator **shall examine** the security objectives rationale to determine that for each OSP it  
3303 justifies that the security objectives are suitable to enforce that OSP.

3304 If no security objectives trace back to the OSP, the evaluator action related to this work unit is  
3305 assigned a fail verdict.

3306 The evaluator determines that the justification for an OSP demonstrates that the security  
3307 objectives are sufficient: if all security objectives that trace back to that OSP are achieved, the OSP  
3308 is enforced.

3309 The evaluator also determines that each security objective that traces back to an OSP is necessary:  
3310 when the security objective is achieved it actually contributes to the enforcement of the OSP.

3311 Note that the tracings from security objectives to OSPs provided in the security objectives rationale  
3312 may be part of a justification, but do not constitute a justification by themselves. In the case that a  
3313 security objective is merely a statement reflecting the intent to enforce a particular OSP, a  
3314 justification is required, but this justification may be as minimal as "Security Objective X directly  
3315 enforces OSP Y".

3316 ISO/IEC 15408-3 ASE\_OBJ.2.6C: *The security objectives rationale shall demonstrate that the security*  
3317 *objectives for the operational environment uphold all assumptions.*

### 3318 10.6.2.3.7 Work unit ASE\_OBJ.2-6

3319 The evaluator **shall examine** the security objectives rationale to determine that for each  
3320 assumption for the operational environment it contains an appropriate justification that the  
3321 security objectives for the operational environment are suitable to uphold that assumption.

3322 If no security objectives for the operational environment trace back to the assumption, the  
3323 evaluator action related to this work unit is assigned a fail verdict.

3324 The evaluator determines that the justification for an assumption about the operational  
3325 environment of the TOE demonstrates that the security objectives are sufficient: if all security  
3326 objectives for the operational environment that trace back to that assumption are achieved, the  
3327 operational environment upholds the assumption.

3328 The evaluator also determines that each security objective for the operational environment that  
3329 traces back to an assumption about the operational environment of the TOE is necessary: when the  
3330 security objective is achieved it actually contributes to the operational environment upholding the  
3331 assumption.

3332 Note that the tracings from security objectives for the operational environment to assumptions  
3333 provided in the security objectives rationale may be a part of a justification, but do not constitute a  
3334 justification by themselves. Even in the case that a security objective of the operational  
3335 environment is merely a restatement of an assumption, a justification is required, but this  
3336 justification may be as minimal as "Security Objective X directly upholds Assumption Y".

## 3337 10.7 Extended components definition (ASE\_ECD)

### 3338 10.7.1 Evaluation of sub-activity (ASE\_ECD.1)

#### 3339 10.7.1.1 Objectives

3340 The objective of this sub-activity is to determine whether extended components have been clearly  
3341 and unambiguously defined, and whether they are necessary, i.e. they may not be clearly expressed  
3342 using existing ISO/IEC 15408-2 or ISO/IEC 15408-3 components.

#### 3343 10.7.1.2 Input

3344 The evaluation evidence for this sub-activity is:

3345 a) the ST.

#### 3346 10.7.1.3 Action ASE\_ECD.1.1E

##### 3347 10.7.1.3.1 General

3348 ISO/IEC 15408-3 ASE\_ECD.1.1C: *The statement of security requirements shall identify all extended*  
3349 *security requirements.*

##### 3350 10.7.1.3.2 Work unit ASE\_ECD.1-1

3351 The evaluator **shall check** that all security requirements in the statement of security requirements  
3352 that are not identified as extended requirements are present in ISO/IEC 15408-2 or in ISO/IEC  
3353 15408-3.

3354 ISO/IEC 15408-3 ASE\_ECD.1.2C: *The extended components definition shall define an extended*  
3355 *component for each extended security requirement.*

##### 3356 10.7.1.3.3 Work unit ASE\_ECD.1-2

3357 The evaluator **shall check** that the extended components definition defines an extended  
3358 component for each extended security requirement.

## ISO/IEC 18045:2008(E)

3359 If the ST does not contain extended security requirements, this work unit is not applicable and  
3360 therefore considered to be satisfied.

3361 A single extended component may be used to define multiple iterations of an extended security  
3362 requirement, it is not necessary to repeat this definition for each iteration.

3363 ISO/IEC 15408-3 ASE\_ECD.1.3C: *The extended components definition shall describe how each*  
3364 *extended component is related to the existing ISO/IEC 15408 components, families, and classes.*

### 3365 **10.7.1.3.4 Work unit ASE\_ECD.1-3**

3366 The evaluator ***shall examine*** the extended components definition to determine that it describes  
3367 how each extended component fits into the existing ISO/IEC 15408 components, families, and  
3368 classes.

3369 If the ST does not contain extended security requirements, this work unit is not applicable and  
3370 therefore considered to be satisfied.

3371 The evaluator determines that each extended component is either:

3372 a) a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 family, or

3373 b) a member of a new family defined in the ST.

3374 If the extended component is a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 family,  
3375 the evaluator determines that the extended components definition adequately describes why the  
3376 extended component should be a member of that family and how it relates to other components of  
3377 that family.

3378 If the extended component is a member of a new family defined in the ST, the evaluator confirms  
3379 that the extended component is not appropriate for an existing family.

3380 If the ST defines new families, the evaluator determines that each new family is either:

3381 a) a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 class, or

3382 b) a member of a new class defined in the ST.

3383 If the family is a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 class, the evaluator  
3384 determines that the extended components definition adequately describes why the family should  
3385 be a member of that class and how it relates to other families in that class.

3386 If the family is a member of a new class defined in the ST, the evaluator confirms that the family is  
3387 not appropriate for an existing class.

### 3388 **10.7.1.3.5 Work unit ASE\_ECD.1-4**

3389 The evaluator ***shall examine*** the extended components definition to determine that each definition  
3390 of an extended component identifies all applicable dependencies of that component.

3391 If the ST does not contain extended security requirements, this work unit is not applicable and  
3392 therefore considered to be satisfied.

3393 The evaluator confirms that no applicable dependencies have been overlooked by the ST author.



3394 ISO/IEC 15408-3 ASE\_ECD.1.4C: *The extended components definition shall use the existing ISO/IEC*  
3395 *15408 components, families, classes, and methodology as a model for presentation.*

3396 **10.7.1.3.6 Work unit ASE\_ECD.1-5**

3397 The evaluator ***shall examine*** the extended components definition to determine that each extended  
3398 functional component uses the existing ISO/IEC 15408-2 components as a model for presentation.

3399 If the ST does not contain extended SFRs, this work unit is not applicable and therefore considered  
3400 to be satisfied.

3401 The evaluator determines that the extended functional component is consistent with ISO/IEC  
3402 15408-2 Subclause 6.1.3, Component structure.

3403 If the extended functional component uses operations, the evaluator determines that the extended  
3404 functional component is consistent with ISO/IEC 15408-1 Subclause 7.1, Operations.

3405 If the extended functional component is hierarchical to an existing functional component, the  
3406 evaluator determines that the extended functional component is consistent with ISO/IEC 15408-2  
3407 Subclause 6.2.1, Component changes highlighting.

3408 **10.7.1.3.7 Work unit ASE\_ECD.1-6**

3409 The evaluator ***shall examine*** the extended components definition to determine that each definition  
3410 of a new functional family uses the existing ISO/IEC 15408 functional families as a model for  
3411 presentation.

3412 If the ST does not define new functional families, this work unit is not applicable and therefore  
3413 considered to be satisfied.

3414 The evaluator determines that all new functional families are defined consistent with ISO/IEC  
3415 15408-2 Subclause 6.1.2, Family structure.

3416 **10.7.1.3.8 Work unit ASE\_ECD.1-7**

3417 The evaluator ***shall examine*** the extended components definition to determine that each definition  
3418 of a new functional class uses the existing ISO/IEC 15408 functional classes as a model for  
3419 presentation.

3420 If the ST does not define new functional classes, this work unit is not applicable and therefore  
3421 considered to be satisfied.

3422 The evaluator determines that all new functional classes are defined consistent with ISO/IEC  
3423 15408-2 Subclause 6.1.1, Class structure.

3424 **10.7.1.3.9 Work unit ASE\_ECD.1-8**

3425 The evaluator ***shall examine*** the extended components definition to determine that each definition  
3426 of an extended assurance component uses the existing ISO/IEC 15408-3 components as a model  
3427 for presentation.

3428 If the ST does not contain extended SARs, this work unit is not applicable and therefore considered  
3429 to be satisfied.

3430 The evaluator determines that the extended assurance component definition is consistent with  
3431 ISO/IEC 15408-3 Subclause 6.1.3, Assurance component structure.

## ISO/IEC 18045:2008(E)

3432 If the extended assurance component uses operations, the evaluator determines that the extended  
3433 assurance component is consistent with ISO/IEC 15408-1 Subclause 7.1, Operations.

3434 If the extended assurance component is hierarchical to an existing assurance component, the  
3435 evaluator determines that the extended assurance component is consistent with ISO/IEC 15408-3  
3436 Subclause 6.1.3, Assurance component structure.

### 3437 10.7.1.3.10 Work unit ASE\_ECD.1-9

3438 The evaluator **shall examine** the extended components definition to determine that, for each  
3439 defined extended assurance component, applicable methodology has been provided.

3440 If the ST does not contain extended SARs, this work unit is not applicable and therefore considered  
3441 to be satisfied.

3442 The evaluator determines that, for each evaluator action element of each extended SAR, one or  
3443 more work units are provided and that successfully performing all work units for a given evaluator  
3444 action element will demonstrate that the element has been achieved.

### 3445 10.7.1.3.11 Work unit ASE\_ECD.1-10

3446 The evaluator **shall examine** the extended components definition to determine that each definition  
3447 of a new assurance family uses the existing ISO/IEC 15408 assurance families as a model for  
3448 presentation.

3449 If the ST does not define new assurance families, this work unit is not applicable and therefore  
3450 considered to be satisfied.

3451 The evaluator determines that all new assurance families are defined consistent with ISO/IEC  
3452 15408-3 Subclause 6.1.2, Assurance family structure.

### 3453 10.7.1.3.12 Work unit ASE\_ECD.1-11

3454 The evaluator **shall examine** the extended components definition to determine that each definition  
3455 of a new assurance class uses the existing ISO/IEC 15408 assurance classes as a model for  
3456 presentation.

3457 If the ST does not define new assurance classes, this work unit is not applicable and therefore  
3458 considered to be satisfied.

3459 The evaluator determines that all new assurance classes are defined consistent with ISO/IEC  
3460 15408-3 Subclause 6.1.1, Assurance class structure.

3461 ISO/IEC 15408-3 ASE\_ECD.1.5C: *The extended components shall consist of measurable and objective*  
3462 *elements such that conformance or nonconformance to these elements can be demonstrated.*

### 3463 10.7.1.3.13 Work unit ASE\_ECD.1-12

3464 The evaluator **shall examine** the extended components definition to determine that each element  
3465 in each extended component is measurable and states objective evaluation requirements, such that  
3466 conformance or nonconformance can be demonstrated.

3467 If the ST does not contain extended security requirements, this work unit is not applicable and  
3468 therefore considered to be satisfied.

3469 The evaluator determines that elements of extended functional components are stated in such a  
3470 way that they are testable, and traceable through the appropriate TSF representations.

3471 The evaluator also determines that elements of extended assurance components avoid the need for  
3472 subjective evaluator judgement.

3473 The evaluator is reminded that whilst being measurable and objective is appropriate for all  
3474 evaluation criteria, it is acknowledged that no formal method exists to prove such properties.  
3475 Therefore the existing ISO/IEC 15408 functional and assurance components are to be used as a  
3476 model for determining what constitutes conformance with this requirement.

#### 3477 **10.7.1.4 Action ASE\_ECD.1.2E**

##### 3478 **10.7.1.4.1 Work unit ASE\_ECD.1-13**

3479 The evaluator *shall examine* the extended components definition to determine that each extended  
3480 component cannot be clearly expressed using existing components.

3481 If the ST does not contain extended security requirements, this work unit is not applicable and  
3482 therefore considered to be satisfied.

3483 The evaluator should take components from ISO/IEC 15408-2 and ISO/IEC 15408-3, other  
3484 extended components that have been defined in the ST, combinations of these components, and  
3485 possible operations on these components into account when making this determination.

3486 The evaluator is reminded that the role of this work unit is to preclude unnecessary duplication of  
3487 components, that is, components that may be clearly expressed by using other components. The  
3488 evaluator should not undertake an exhaustive search of all possible combinations of components  
3489 including operations in an attempt to find a way to express the extended component by using  
3490 existing components.

### 3491 **10.8 Security requirements (ASE\_REQ)**

#### 3492 **10.8.1 Evaluation of sub-activity (ASE\_REQ.1)**

##### 3493 **10.8.1.1 Objectives**

3494 The objective of this sub-activity is to determine whether the SFRs and SARs are clear,  
3495 unambiguous and well-defined, whether they are internally consistent, and whether the SFRs  
3496 counter the threats and implement the organisational security policies of the TOE.

##### 3497 **10.8.1.2 Input**

3498 The evaluation evidence for this sub-activity is:

3499 a) the ST.

##### 3500 **10.8.1.3 Action ASE\_REQ.1.1E**

3501 ISO/IEC 15408-3 ASE\_REQ.1.1C: *The statement of security requirements shall describe the SFRs and*  
3502 *the SARs.*

##### 3503 **10.8.1.3.1 Work unit ASE\_REQ.1-1**

3504 The evaluator *shall check* that the statement of security requirements describes the SFRs.

3505 The evaluator determines that each SFR is identified by one of the following means:

3506 a) by reference to an individual component in ISO/IEC 15408-2;

## ISO/IEC 18045:2008(E)

- 3507 b) by reference to an extended component in the extended components definition of the  
3508 ST;
- 3509 c) by reference to a PP that the ST claims to be conformant with, including any optional  
3510 requirements defined in the PP;
- 3511 d) by reference to a security requirements package that the ST claims to be conformant  
3512 with;
- 3513 e) by reproduction in the ST.
- 3514 It is not required to use the same means of identification for all SFRs.
- 3515 **10.8.1.3.2 Work unit ASE\_REQ.1-2**
- 3516 The evaluator **shall check** that the statement of security requirements describes the SARs.
- 3517 The evaluator determines that each SAR is identified by one of the following means:
- 3518 a) by reference to an individual component in ISO/IEC 15408-3;
- 3519 b) by reference to an extended component in the extended components definition of the  
3520 ST;
- 3521 c) by reference to a PP that the ST claims to be conformant with;
- 3522 d) by reference to a security requirements package that the ST claims to be conformant  
3523 with;
- 3524 e) by reproduction in the ST.
- 3525 It is not required to use the same means of identification for all SARs.
- 3526 Note that if optional requirements are defined by the PP, there may be associated threats that are  
3527 covered by this work unit.
- 3528 ISO/IEC 15408-3 ASE\_REQ.1.2C: *All subjects, objects, operations, security attributes, external entities*  
3529 *and other terms that are used in the SFRs and the SARs shall be defined.*
- 3530 **10.8.1.3.3 Work unit ASE\_REQ.1-3**
- 3531 The evaluator **shall examine** the ST to determine that all subjects, objects, operations, security  
3532 attributes, external entities and other terms that are used in the SFRs and the SARs are defined.
- 3533 The evaluator determines that the ST defines all:
- 3534 • (types of) subjects and objects that are used in the SFRs;
- 3535 • (types of) security attributes of subjects, users, objects, information, sessions and/or  
3536 resources, possible values that these attributes may take and any relations between these  
3537 values (e.g. top\_secret is “higher” than secret);

- 3538 • (types of) operations that are used in the SFRs, including the effects of these operations;
- 3539 • (types of) external entities in the SFRs;
- 3540 • other terms that are introduced in the SFRs and/or SARs by completing operations, if
- 3541 these terms are not immediately clear, or are used outside their dictionary definition.

3542 The goal of this work unit is to ensure that the SFRs and SARs are well-defined and that no  
 3543 misunderstanding may occur due to the introduction of vague terms. This work unit should not be  
 3544 taken into extremes, by forcing the ST author to define every single word. The general audience of  
 3545 a set of security requirements should be assumed to have a reasonable knowledge of IT, security  
 3546 and "Evaluation criteria for IT security".

3547 All of the above may be presented in groups, classes, roles, types or other groupings or  
 3548 characterisations that allow easy understanding.

3549 The evaluator is reminded that these lists and definitions do not have to be part of the statement of  
 3550 security requirements, but may be placed (in part or in whole) in different subclauses. This may be  
 3551 especially applicable if the same terms are used in the rest of the ST.

3552 ISO/IEC 15408-3 ASE\_REQ.1.3C: *The statement of security requirements shall include a natural*  
 3553 *language description, part of which describes how the SFRs combine together to provide security*  
 3554 *functionality in terms of the architecture that is visible to Administrators and other users.*

#### 3555 10.8.1.3.4 Work unit ASE\_REQ.1-4

3556 The evaluator **shall check** that the statement of security requirements includes a natural language  
 3557 description, part of which describes how the SFRs combine together to provide security  
 3558 functionality in terms of the architecture that is visible to Administrators and other users.

3559 The description is intended to make clear connections between SFRs and to provide a view of how  
 3560 they provide security functionality that is recognizable to Administrators and other types of user.  
 3561 The description in terms of the architecture that is "visible to Administrators and other users"  
 3562 means that the description must relate the security behavior to visible elements, but the  
 3563 mechanisms themselves need not be visible. For example: when describing authentication using a  
 3564 biometric mechanism, the calculation of the match or score might not be visible, but (a) might  
 3565 relate to a referenced description of a matching algorithm, (b) might be based on specific template  
 3566 files maintained by the Administrator, and (c) will result in acceptance or rejection of the  
 3567 authentication attempt – therefore the description might make use of any or all of these items (a) –  
 3568 (c). No specific format for this information is prescribed, and the description need not all be located  
 3569 alongside the SFRs themselves (e.g. some of it might be in the ST Introduction and/or in the TSS).  
 3570 The intention of the requirement is to make the meaning of the SFRs clearer and more easily  
 3571 understood by readers of the ST who may not have deep knowledge of the CC but who are familiar  
 3572 with the product type.

3573 The evaluator determines that all operations are identified in each SFR or SAR where such an  
 3574 operation is used. This includes both completed operations and uncompleted operations.  
 3575 Identification may be achieved by typographical distinctions, or by explicit identification in the  
 3576 surrounding text, or by any other distinctive means.

3577 ISO/IEC 15408-3 ASE\_REQ.1.4C: *The statement of security requirements shall identify all operations*  
 3578 *on the security requirements.*

#### 3579 10.8.1.3.5 Work unit ASE\_REQ.1-5

3580 The evaluator **shall check** that the statement of security requirements identifies all operations on  
 3581 the security requirements.

## ISO/IEC 18045:2008(E)

3582 The evaluator determines that all operations are identified in each SFR or SAR where such an  
3583 operation is used. Identification may be achieved by typographical distinctions, or by explicit  
3584 identification in the surrounding text, or by any other distinctive means.

3585 ISO/IEC 15408-3 ASE\_REQ.1.5C: *All operations shall be performed correctly.*

### 3586 10.8.1.3.6 Work unit ASE\_REQ.1-6

3587 The evaluator **shall examine** the statement of security requirements to determine that all  
3588 assignment operations are performed correctly.

3589 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C,  
3590 Guidance for Operations.

### 3591 10.8.1.3.7 Work unit ASE\_REQ.1-7

3592 The evaluator **shall examine** the statement of security requirements to determine that all iteration  
3593 operations are performed correctly.

3594 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C,  
3595 Guidance for Operations.

### 3596 10.8.1.3.8 Work unit ASE\_REQ.1-8

3597 The evaluator **shall examine** the statement of security requirements to determine that all selection  
3598 operations are performed correctly.

3599 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C,  
3600 Guidance for Operations.

### 3601 10.8.1.3.9 Work unit ASE\_REQ.1-9

3602 The evaluator **shall examine** the statement of security requirements to determine that all  
3603 refinement operations are performed correctly.

3604 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C,  
3605 Guidance for Operations.

3606 ISO/IEC 15408-3 ASE\_REQ.1.6C: *Each dependency of the security requirements shall either be*  
3607 *satisfied, or the security requirements rationale shall justify the dependency not being satisfied.*

### 3608 10.8.1.3.10 Work unit ASE\_REQ.1-10

3609 The evaluator **shall examine** the statement of security requirements to determine that each  
3610 dependency of the security requirements is either satisfied, or that a security requirements  
3611 rationale is provided which justifies the dependency not being satisfied.

3612 A dependency is satisfied by the inclusion of the relevant component (or one that is hierarchical to  
3613 it) within the statement of security requirements. The component used to satisfy the dependency  
3614 should, if necessary, be modified by operations to ensure that it actually satisfies that dependency.

3615 A justification that a dependency is not met should address either:

- 3616 a) why the dependency is not necessary or useful, in which case no further information  
3617 is required; or

- 3618 b) that the dependency has been addressed by the operational environment of the TOE,  
3619 in which case the justification should describe how the security objectives for the  
3620 operational environment address this dependency.
- 3621 ISO/IEC 15408-3 ASE\_REQ.1.7C: The security requirements rationale shall trace each SFR back to  
3622 the threats countered by that SFR and OSPs enforced by that SFR.
- 3623 **10.8.1.3.11 Work unit ASE\_REQ.1-11**
- 3624 The evaluator **shall check** that the security requirements rationale traces each SFR back to the  
3625 threats countered by that SFR and OSPs enforced by that SFR.
- 3626 The evaluator determines that each SFR is traced back to at least one threat or OSP for the TOE.
- 3627 Failure to trace implies that either the security requirements rationale is incomplete, the security  
3628 objectives for the TOE are incomplete, or the SFR has no useful purpose.
- 3629 There is no prescribed location where this tracing element of the rationale must be placed: for  
3630 example, the relevant parts may be located under each threat and OSP in order to help make the  
3631 security argument clearer and easier to read.
- 3632 Optional requirements may require Threats/OSP to be specified, and security objectives  
3633 associated with these SPD elements are also covered by this work unit.
- 3634 ISO/IEC 15408-3 ASE\_REQ.1.8C: *The security requirements rationale shall trace each security*  
3635 *objective for the operational environment back to threats countered by that security objective, OSPs*  
3636 *enforced by that security objective, and assumptions upheld by that security objective.*
- 3637 **10.8.1.3.12 Work unit ASE\_REQ.1-12**
- 3638 The evaluator **shall check** that the security objectives requirements rationale traces the security  
3639 objectives for the operational environment back to threats countered by that security objective, to  
3640 OSPs enforced by that security objective, and to assumptions upheld by that security objective.
- 3641 Each security objective for the operational environment may trace back to threats, OSPs,  
3642 assumptions, or a combination of threats, OSPs and/or assumptions, but it must trace back to at  
3643 least one threat, OSP or assumption.
- 3644 Failure to trace implies that either the security objectives requirements rationale is incomplete, the  
3645 security problem definition is incomplete, or the security objective for the operational  
3646 environment has no useful purpose.
- 3647 There is no prescribed location where this tracing element of the rationale must be placed: for  
3648 example, the relevant parts may be located under each threat, OSP and assumption in order to help  
3649 make the security argument clearer and easier to read.
- 3650 ISO/IEC 15408-3 ASE\_REQ.1.9C: The security requirements rationale shall demonstrate that the  
3651 SFRs (in conjunction with the security objectives for the environment) counter all threats for the  
3652 TOE.
- 3653 **10.8.1.3.13 Work unit ASE\_REQ.1-13**
- 3654 The evaluator **shall examine** the security requirements rationale to determine that for each threat  
3655 it demonstrates that the SFRs are suitable to meet that threat.
- 3656 If no SFRs trace back to a threat, the evaluator action related to this work unit is assigned a fail  
3657 verdict.

## ISO/IEC 18045:2008(E)

3658 The evaluator determines that the justification for a threat shows whether the threat is removed,  
3659 diminished or mitigated.

3660 The evaluator determines that the justification for a threat demonstrates that the SFRs are  
3661 sufficient: if all SFRs that trace back to the threat are achieved then, in the context of any applicable  
3662 OSPs and assumptions, the threat is removed, sufficiently diminished, or the effects of the threat  
3663 are sufficiently mitigated.

3664 Note that simply listing in the security requirements rationale the SFRs associated with each threat  
3665 may be part of a justification, but does not constitute a justification by itself. A descriptive  
3666 justification is required, although in simple cases this justification may be as minimal as "SFR X  
3667 directly counters Threat Y".

3668 The evaluator also determines that each SFR that traces back to a threat is necessary: when the SFR  
3669 is implemented it actually contributes to the removal, diminishing or mitigation of that threat.

3670 ISO/IEC 15408-3 ASE\_REQ.1.10C: The security requirements rationale shall demonstrate that the  
3671 SFRs (in conjunction with the security objectives for the environment) enforce all OSPs for the TOE.

### 3672 10.8.1.3.14 Work unit ASE\_REQ.1-14

3673 The evaluator **shall examine** the security requirements rationale to determine that for each OSP it  
3674 justifies that the SFRs are suitable to enforce that OSP.

3675 If no SFRs or security objectives for the operational environment trace back to the OSP, the  
3676 evaluator action related to this work unit is assigned a fail verdict.

3677 The evaluator determines that the justification for an OSP demonstrates that the security  
3678 objectives are sufficient: if all SFRs that trace back to that OSP are achieved then, in the context of  
3679 any applicable assumptions, the OSP is enforced.

3680 The evaluator also determines that each SFR that traces back to an OSP is necessary: when the SFR  
3681 is implemented it actually contributes to the enforcement of the OSP.

3682 Note that simply listing in the security requirements rationale the SFRs associated with each OSP  
3683 may be part of a justification, but does not constitute a justification by itself. A descriptive  
3684 justification is required, although in simple cases this justification may be as minimal as "SFR X  
3685 directly enforces OSP Y".

3686 ISO/IEC 15408-3 ASE\_REQ.1.11C: The security requirements rationale shall demonstrate that the  
3687 SFRs (in conjunction with the security objectives for the environment) enforce all OSPs for the TOE.

### 3688 10.8.1.3.15 Work unit ASE\_REQ.1-15

3689 The evaluator **shall examine** the security requirements rationale to determine that for each  
3690 assumption for the operational environment it contains an appropriate justification that the  
3691 security objectives for the operational environment are suitable to uphold that assumption.

3692 If no security objectives for the operational environment trace back to the assumption, the  
3693 evaluator action related to this work unit is assigned a fail verdict.

3694 The evaluator determines that the justification for an assumption about the operational  
3695 environment of the TOE demonstrates that the security objectives are sufficient: if all security  
3696 objectives for the operational environment that trace back to that assumption are achieved, the  
3697 operational environment upholds the assumption.

3698 The evaluator also determines that each security objective for the operational environment that  
3699 traces back to an assumption about the operational environment of the TOE is necessary: when the



3700 security objective is achieved it actually contributes to the operational environment upholding the  
3701 assumption.

3702 Note that simply listing in the security requirements rationale the security objectives for the  
3703 operational environment associated with each assumption may be a part of a justification, but does  
3704 not constitute a justification by itself. A descriptive justification is required, although in simple  
3705 cases this justification may be as minimal as "Security Objective X directly upholds Assumption Y".

3706 ISO/IEC 15408-3 ASE\_REQ.1.12C: *The statement of security requirements shall be internally*  
3707 *consistent.*

#### 3708 **10.8.1.3.16 Work unit ASE\_REQ.1-16**

3709 The evaluator ***shall examine*** the statement of security requirements to determine that it is  
3710 internally consistent.

3711 The evaluator determines that the combined set of all SFRs and SARs is internally consistent. With  
3712 respect to optional requirements, the evaluator determines that:

3713 a) All optional requirements either trace to an SPD element that is itself not optional, or  
3714 trace to an SPD element that is clearly associated with that optional SFR;

3715 b) All optional requirements are clearly identified as being required if a conformance  
3716 TOE implements the functionality covered by the requirement, or as being "purely  
3717 optional"; and

3718 c) All optional requirements do not conflict with non-optional requirements (a  
3719 capability cannot be both required and optional; however, a base capability can be  
3720 required with enhancements to that capability being specified as optional).

3721

3722 The evaluator determines that on all occasions where different security requirements apply to the  
3723 same types of developer evidence, events, operations, data, tests to be performed etc. or to "all  
3724 objects", "all subjects" etc., that these requirements do not conflict.

3725 Some possible conflicts are:

3726 a) an extended SAR specifying that the design of a certain cryptographic algorithm is to  
3727 be kept secret, and another extended SAR specifying an open source review;

3728 b) FAU\_GEN.1 Audit data generation specifying that subject identity is to be logged,  
3729 FDP\_ACC.1 Subset access control specifying who has access to these logs, and  
3730 FPR\_UNO.1 Unobservability specifying that some actions of subjects should be  
3731 unobservable to other subjects. If the subject that should not be able to see an  
3732 activity may access logs of this activity, these SFRs conflict;

3733 c) FDP\_RIP.1 Subset residual information protection specifying deletion of information  
3734 no longer needed, and FDP\_ROL.1 Basic rollback specifying that a TOE may return to  
3735 a previous state. If the information that is needed for the rollback to the previous  
3736 state has been deleted, these requirements conflict;

3737 d) Multiple iterations of FDP\_ACC.1 Subset access control especially where some  
3738 iterations cover the same subjects, objects, or operations. If one access control SFR

## ISO/IEC 18045:2008(E)

- 3739 allows a subject to perform an operation on an object, while another access control  
3740 SFR does not allow this, these requirements conflict.
- 3741 **10.8.2 Evaluation of sub-activity (ASE\_REQ.2)**
- 3742 **10.8.2.1 Objectives**
- 3743 The objective of this sub-activity is to determine whether the SFRs and SARs are clear,  
3744 unambiguous and well-defined, whether they are internally consistent, and whether the SFRs meet  
3745 the security objectives of the TOE.
- 3746 **10.8.2.2 Input**
- 3747 The evaluation evidence for this sub-activity is:
- 3748 a) the ST.
- 3749 **10.8.2.3 Action ASE\_REQ.2.1E**
- 3750 **10.8.2.3.1 General**
- 3751 ISO/IEC 15408-3 ASE\_REQ.2.1C: *The statement of security requirements shall describe the SFRs and*  
3752 *the SARs.*
- 3753 **10.8.2.3.2 Work unit ASE\_REQ.2-1**
- 3754 The evaluator **shall check** that the statement of security requirements describes the SFRs.
- 3755 The evaluator determines that each SFRs is identified by one of the following means:
- 3756 a) by reference to an individual component in ISO/IEC 15408-2;
- 3757 b) by reference to an extended component in the extended components definition of the  
3758 ST;
- 3759 c) by reference to an individual component in a PP that the ST claims to be conformant  
3760 with, including any optional requirements defined in the PP;
- 3761 d) by reference to an individual component in a security requirements package that the  
3762 ST claims to be conformant with;
- 3763 e) by reproduction in the ST.
- 3764 It is not required to use the same means of identification for all SFRs.
- 3765 **10.8.2.3.3 Work unit ASE\_REQ.2-2**
- 3766 The evaluator **shall check** that the statement of security requirements describes the SARs.
- 3767 The evaluator determines that all SARs are identified by one of the following means:
- 3768 a) by reference to an individual component in ISO/IEC 15408-3;

- 3769 b) by reference to an extended component in the extended components definition of the  
3770 ST;
- 3771 c) by reference to an individual component in a PP that the ST claims to be conformant  
3772 with;
- 3773 d) by reference to an individual component in a security requirements package that the  
3774 ST claims to be conformant with;
- 3775 e) by reproduction in the ST.
- 3776 It is not required to use the same means of identification for all SARs.
- 3777 Note that if optional requirements are defined by the PP, there may be associated threats that are  
3778 covered by this work unit.
- 3779 ISO/IEC 15408-3 ASE\_REQ.2.2C: *All subjects, objects, operations, security attributes, external entities*  
3780 *and other terms that are used in the SFRs and the SARs shall be defined.*
- 3781 **10.8.2.3.4 Work unit ASE\_REQ.2-3**
- 3782 The evaluator **shall examine** the ST to determine that all subjects, objects, operations, security  
3783 attributes, external entities and other terms that are used in the SFRs and the SARs are defined.
- 3784 The evaluator determines that the ST defines all:
- 3785 • (types of) subjects and objects that are used in the SFRs;
- 3786 • (types of) security attributes of subjects, users, objects, information, sessions and/or  
3787 resources, possible values that these attributes may take and any relations between these  
3788 values (e.g. top\_secret is “higher” than secret);
- 3789 • (types of) operations that are used in the SFRs, including the effects of these operations;
- 3790 • (types of) external entities in the SFRs;
- 3791 • other terms that are introduced in the SFRs and/or SARs by completing operations, if  
3792 these terms are not immediately clear, or are used outside their dictionary definition.
- 3793 The goal of this work unit is to ensure that the SFRs and SARs are well-defined and that no  
3794 misunderstanding may occur due to the introduction of vague terms. This work unit should not be  
3795 taken into extremes, by forcing the ST author to define every single word. The general audience of  
3796 a set of security requirements should be assumed to have a reasonable knowledge of IT, security  
3797 and “Evaluation criteria for IT security”.
- 3798 All of the above may be presented in groups, classes, roles, types or other groupings or  
3799 characterisations that allow easy understanding.
- 3800 The evaluator is reminded that these lists and definitions do not have to be part of the statement of  
3801 security requirements, but may be placed (in part or in whole) in different subclauses. This may be  
3802 especially applicable if the same terms are used in the rest of the ST.
- 3803 ISO/IEC 15408-3 ASE\_REQ.2.3C: *The statement of security requirements shall identify all operations*  
3804 *on the security requirements.*

## ISO/IEC 18045:2008(E)

### 3805 10.8.2.3.5 Work unit ASE\_REQ.2-4

3806 The evaluator **shall check** that the statement of security requirements identifies all operations on  
3807 the security requirements.

3808 The evaluator determines that all operations are identified in each SFR or SAR where such an  
3809 operation is used. Identification may be achieved by typographical distinctions, or by explicit  
3810 identification in the surrounding text, or by any other distinctive means.

3811 ISO/IEC 15408-3 ASE\_REQ.2.4C: *All operations shall be performed correctly.*

### 3812 10.8.2.3.6 Work unit ASE\_REQ.2-5

3813 The evaluator **shall examine** the statement of security requirements to determine that all  
3814 assignment operations are performed correctly.

3815 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C,  
3816 Guidance for Operations.

### 3817 10.8.2.3.7 Work unit ASE\_REQ.2-6

3818 The evaluator **shall examine** the statement of security requirements to determine that all iteration  
3819 operations are performed correctly.

3820 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C,  
3821 Guidance for Operations.

### 3822 10.8.2.3.8 Work unit ASE\_REQ.2-7

3823 The evaluator **shall examine** the statement of security requirements to determine that all selection  
3824 operations are performed correctly.

3825 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C,  
3826 Guidance for Operations.

### 3827 10.8.2.3.9 Work unit ASE\_REQ.2-8

3828 The evaluator **shall examine** the statement of security requirements to determine that all  
3829 refinement operations are performed correctly.

3830 Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C,  
3831 Guidance for Operations.

3832 ISO/IEC 15408-3 ASE\_REQ.2.5C: *Each dependency of the security requirements shall either be*  
3833 *satisfied, or the security requirements rationale shall justify the dependency not being satisfied.*

### 3834 10.8.2.3.10 Work unit ASE\_REQ.2-9

3835 The evaluator **shall examine** the statement of security requirements to determine that each  
3836 dependency of the security requirements is either satisfied, or that the security requirements  
3837 rationale justifies the dependency not being satisfied.

3838 A dependency is satisfied by the inclusion of the relevant component (or one that is hierarchical to  
3839 it) within the statement of security requirements. The component used to satisfy the dependency  
3840 should, if necessary, be modified by operations to ensure that it actually satisfies that dependency.

3841 A justification that a dependency is not met should address either:

- 3842 a) why the dependency is not necessary or useful, in which case no further information  
3843 is required; or
- 3844 b) that the dependency has been addressed by the operational environment of the TOE,  
3845 in which case the justification should describe how the security objectives for the  
3846 operational environment address this dependency.
- 3847 ISO/IEC 15408-3 ASE\_REQ.2.6C: *The security requirements rationale shall trace each SFR back to the*  
3848 *SPD elements for the TOE.*
- 3849 **10.8.2.3.11 Work unit ASE\_REQ.2-10**
- 3850 The evaluator **shall check** that the security requirements rationale traces each SFR back to the  
3851 security objectives for the TOE.
- 3852 Optional requirements may require Threats/OSPs to be specified, and security objectives  
3853 associated with these SPD elements are also covered by this work unit.
- 3854 The evaluator determines that each SFR is traced back to at least one security objective for the TOE.
- 3855 Failure to trace implies that either the security requirements rationale is incomplete, the security  
3856 objectives for the TOE are incomplete, or the SFR has no useful purpose.
- 3857 ISO/IEC 15408-3 ASE\_REQ.2.7C: *The security requirements rationale shall demonstrate that the*  
3858 *SFRs meet all security objectives for the TOE.*
- 3859 **10.8.2.3.12 Work unit ASE\_REQ.2-11**
- 3860 The evaluator **shall examine** the security requirements rationale to determine that for each  
3861 security objective for the TOE it demonstrates that the SFRs are suitable to meet that security  
3862 objective for the TOE.
- 3863 If no SFRs trace back to the security objective for the TOE, the evaluator action related to this work  
3864 unit is assigned a fail verdict.
- 3865 The evaluator determines that the justification for a security objective for the TOE demonstrates  
3866 that the SFRs are sufficient: if all SFRs that trace back to the objective are satisfied, the security  
3867 objective for the TOE is achieved.
- 3868 The evaluator also determines that each SFR that traces back to a security objective for the TOE is  
3869 necessary: when the SFR is satisfied, it actually contributes to achieving the security objective.
- 3870 Note that the tracings from SFRs to security objectives for the TOE provided in the security  
3871 requirements rationale may be a part of the justification, but do not constitute a justification by  
3872 themselves.
- 3873 ISO/IEC 15408-3 ASE\_REQ.2.8C: *The security requirements rationale shall explain why the SARs*  
3874 *were chosen.*
- 3875 **10.8.2.3.13 Work unit ASE\_REQ.2-12**
- 3876 The evaluator **shall check** that the security requirements rationale explains why the SARs were  
3877 chosen.
- 3878 The evaluator is reminded that any explanation is correct, as long as it is coherent and neither the  
3879 SARs nor the explanation have obvious inconsistencies with the remainder of the ST.

## ISO/IEC 18045:2008(E)

3880 An example of an obvious inconsistency between the SARs and the remainder of the ST would be to  
3881 have threat agents that are very capable, but an AVA\_VAN SAR that does not protect against these  
3882 threat agents.

3883 ISO/IEC 15408-3 ASE\_REQ.2.9C: *The statement of security requirements shall be internally*  
3884 *consistent.*

### 3885 10.8.2.3.14 Work unit ASE\_REQ.2-13

3886 The evaluator **shall examine** the statement of security requirements to determine that it is  
3887 internally consistent.

3888 The evaluator determines that the combined set of all SFRs and SARs is internally consistent. With  
3889 respect to optional requirements, the evaluator determines that:

- 3890 a) All optional requirements either trace to an SPD element that is itself not optional, or trace  
3891 to an SPD element that is clearly associated with that optional SFR;
- 3892 b) All optional requirements are clearly identified as being required if a conformance TOE  
3893 implements the functionality covered by the requirement, or as being "purely optional";  
3894 and
- 3895 c) All optional requirements do not conflict with non-optional requirements (a capability  
3896 cannot be both required and optional; however, a base capability can be required with  
3897 enhancements to that capability being specified as optional).

3898

3899 The evaluator determines that on all occasions where different security requirements apply to the  
3900 same types of developer evidence, events, operations, data, tests to be performed etc. or to "all  
3901 objects", "all subjects" etc., that these requirements do not conflict.

3902 Some possible conflicts are:

- 3903 a) an extended SAR specifying that the design of a certain cryptographic algorithm is to  
3904 be kept secret, and another extended SAR specifying an open source review;
- 3905 b) FAU\_GEN.1 Audit data generation specifying that subject identity is to be logged,  
3906 FDP\_ACC.1 Subset access control specifying who has access to these logs, and  
3907 FPR\_UNO.1 Unobservability specifying that some actions of subjects should be  
3908 unobservable to other subjects. If the subject that should not be able to see an  
3909 activity may access logs of this activity, these SFRs conflict;
- 3910 c) FDP\_RIP.1 Subset residual information protection specifying deletion of information  
3911 no longer needed, and FDP\_ROL.1 Basic rollback specifying that a TOE may return to  
3912 a previous state. If the information that is needed for the rollback to the previous  
3913 state has been deleted, these requirements conflict;
- 3914 d) Multiple iterations of FDP\_ACC.1 Subset access control especially where some  
3915 iterations cover the same subjects, objects, or operations. If one access control SFR  
3916 allows a subject to perform an operation on an object, while another access control  
3917 SFR does not allow this, these requirements conflict.

3918 **10.9 TOE summary specification (ASE\_TSS)**3919 **10.9.1 Evaluation of sub-activity (ASE\_TSS.1)**3920 **10.9.1.1 Objectives**

3921 The objective of this sub-activity is to determine whether the TOE summary specification  
 3922 addresses all SFRs, and whether the TOE summary specification is consistent with other narrative  
 3923 descriptions of the TOE.

3924 **10.9.1.2 Input**

3925 The evaluation evidence for this sub-activity is:

3926 a) the ST.

3927 **10.9.1.3 Action ASE\_TSS.1.1E**

3928 ISO/IEC 15408-3 ASE\_TSS.1.1C: *The TOE summary specification shall describe how the TOE meets*  
 3929 *each SFR.*

3930 **10.9.1.3.1 Work unit ASE\_TSS.1-1**

3931 The evaluator *shall examine* the TOE summary specification to determine that it describes how  
 3932 the TOE meets each SFR.

3933 The evaluator determines that the TOE summary specification provides, for each SFR from the  
 3934 statement of security requirements, a description on how that SFR is met.

3935 The evaluator is reminded that the objective of each description is to provide potential consumers  
 3936 of the TOE with a high-level view of how the developer intends to satisfy each SFR and that the  
 3937 descriptions therefore should not be overly detailed. Often several SFRs will be implemented in  
 3938 one context; for instance, a password authentication mechanism may implement FIA\_UAU.1,  
 3939 FIA\_SOS.1 and FIA\_UID.1. Therefore, usually the TSS will not consist of a long list with texts for each  
 3940 single SFR, but complete groups of SFRs may be covered by one text passage.

3941 For a composed TOE, the evaluator also determines that it is clear which component provides each  
 3942 SFR or how the components combine to meet each SFR.

3943 **10.9.1.4 Action ASE\_TSS.1.2E**3944 **10.9.1.4.1 Work unit ASE\_TSS.1-2**

3945 The evaluator *shall examine* the TOE summary specification to determine that it is consistent with  
 3946 the TOE overview and the TOE description.

3947 The TOE overview, TOE description, and TOE summary specification describe the TOE in a  
 3948 narrative form at increasing levels of detail. These descriptions therefore need to be consistent.

3949 **10.9.2 Evaluation of sub-activity (ASE\_TSS.2)**3950 **10.9.2.1 Objectives**

3951 The objective of this sub-activity is to determine whether the TOE summary specification  
 3952 addresses all SFRs, whether the TOE summary specification addresses interference, logical  
 3953 tampering and bypass, and whether the TOE summary specification is consistent with other  
 3954 narrative descriptions of the TOE.

## ISO/IEC 18045:2008(E)

### 3955 10.9.2.2 Input

3956 The evaluation evidence for this sub-activity is:

3957 a) the ST.

### 3958 10.9.2.3 Action ASE\_TSS.2.1E

#### 3959 10.9.2.3.1 General

3960 ISO/IEC 15408-3 ASE\_TSS.2.1C: *The TOE summary specification shall describe how the TOE meets*  
3961 *each SFR.*

#### 3962 10.9.2.3.2 Work unit ASE\_TSS.2-1

3963 The evaluator **shall examine** the TOE summary specification to determine that it describes how  
3964 the TOE meets each SFR.

3965 The evaluator determines that the TOE summary specification provides, for each SFR from the  
3966 statement of security requirements, a description on how that SFR is met.

3967 The evaluator is reminded that the objective of each description is to provide potential consumers  
3968 of the TOE with a high-level view of how the developer intends to satisfy each SFR and that the  
3969 descriptions therefore should not be overly detailed. Often several SFRs will be implemented in  
3970 one context; for instance a password authentication mechanism may implement FIA\_UAU.1,  
3971 FIA\_SOS.1 and FIA\_UID.1. Therefore usually the TSS will not consist of a long list with texts for each  
3972 single SFR, but complete groups of SFRs may be covered by one text passage.

3973 For a composed TOE, the evaluator also determines that it is clear which component provides each  
3974 SFR or how the components combine to meet each SFR.

3975 ISO/IEC 15408-3 ASE\_TSS.2.2C: *The TOE summary specification shall describe how the TOE protects*  
3976 *itself against interference and logical tampering.*

#### 3977 10.9.2.3.3 Work unit ASE\_TSS.2-2

3978 The evaluator **shall examine** the TOE summary specification to determine that it describes how  
3979 the TOE protects itself against interference and logical tampering.

3980 The evaluator is reminded that the objective of each description is to provide potential consumers  
3981 of the TOE with a high-level view of how the developer intends to provide protection against  
3982 interference and logical tampering and that the descriptions therefore should not be overly  
3983 detailed.

3984 For a composed TOE, the evaluator also determines that it is clear which component provides the  
3985 protection or how the components combine to provide protection.

3986 ISO/IEC 15408-3 ASE\_TSS.2.3C: *The TOE summary specification shall describe how the TOE protects*  
3987 *itself against bypass.*

#### 3988 10.9.2.3.4 Work unit ASE\_TSS.2-3

3989 The evaluator **shall examine** the TOE summary specification to determine that it describes how  
3990 the TOE protects itself against bypass.



3991 The evaluator is reminded that the objective of each description is to provide potential consumers  
 3992 of the TOE with a high-level view of how the developer intends to provide protection against  
 3993 bypass and that the descriptions therefore should not be overly detailed.

3994 For a composed TOE, the evaluator also determines that it is clear which component provides the  
 3995 protection or how the components combine to provide protection.

#### 3996 **10.9.2.4 Action ASE\_TSS.2.2E**

##### 3997 **10.9.2.4.1 Work unit ASE\_TSS.2-4**

3998 The evaluator *shall examine* the TOE summary specification to determine that it is consistent with  
 3999 the TOE overview and the TOE description.

4000 The TOE overview, TOE description, and TOE summary specification describe the TOE in a  
 4001 narrative form at increasing levels of detail. These descriptions therefore need to be consistent.

#### 4002 **10.10 Consistency of composite product Security Target (ASE\_COMP)**

4003 The composite-specific work units defined in this chapter are intended to be integrated as  
 4004 refinements to the evaluation activities of the ASE class listed in the following table. The other  
 4005 activities of ASE class do not require composite-specific work units.

| CC assurance family | Evaluation activity | Evaluation work unit | Composite-specific work |
|---------------------|---------------------|----------------------|-------------------------|
| ASE_OBJ             | ASE_OBJ.2.1C        | ASE_OBJ.2-1          | ASE_COMP.1-5            |
|                     | ASE_OBJ.2.1C        | ASE_OBJ.2-1          | ASE_COMP.1-6            |
|                     | ASE_OBJ.2.3C        | ASE_OBJ.2-3          | ASE_COMP.1-6            |
| ASE_REQ             | ASE_REQ.1.6C        | ASE_REQ.1-10         | ASE_COMP.1-1            |
|                     | ASE_REQ.2.9C.       | ASE_REQ.2-13         | ASE_COMP.1-1            |
|                     | ASE_REQ.1.6C        | ASE_REQ.1-10         | ASE_COMP.1-2            |
|                     | ASE_REQ.2.9C        | ASE_REQ.2-13         | ASE_COMP.1-2            |
|                     | ASE_REQ.2.8C        | ASE_REQ.2-12         | ASE_COMP.1-3            |
|                     | ASE_REQ.2.3C        | ASE_REQ.2-4          | ASE_COMP.1-4            |

4006

#### 4007 **10.10.1 Evaluation of sub-activity (ASE\_COMP.1)**

##### 4008 **10.10.1.1 Objectives**

4009 The aim of this activity is to determine whether the Security Target of the composite product<sup>1</sup> does  
 4010 not contradict the Security Target of the underlying platform<sup>2</sup>.

---

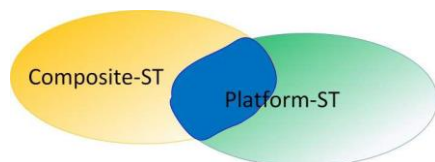
<sup>1</sup> denoted by Composite-ST in the following

4011 **10.10.1.2 Application notes**

4012 These application notes aid the developer to create as well as the evaluator to analyse a composite  
4013 Security Target and describe a general methodology for it. For detailed information/guidance  
4014 please refer to the single work units below. In order to create a composite Security Target the  
4015 developer should perform the following steps:

4016 Step 1: The developer formulates a preliminary Security Target for the composite product (the  
4017 Composite-ST) using the standard code of practice. The Composite-ST can be formulated  
4018 independently of the Security Target of the underlying platform (Platform-ST) – at least as long as  
4019 there are no formal PP conformance claims.

4020 Step 2: The developer determines the overlap between Platform-ST and Composite-ST through  
4021 analysing and comparing their TOE Security Functionality (TSF)<sup>3,4</sup>:



4022  
4023 Step 3: The developer determines under which conditions they can trust in and rely on the  
4024 Platform-TSF being used by the Composite-ST without a new examination.

4025 Having undertaken these steps the developer completes the preliminary Security Target for the  
4026 composite product.

4027 It is not mandatory that the platform and the composite TOE are being certified according to same  
4028 edition of the 15408. It is due to the fact that the application can rely on some security services of  
4029 the platform, if (i) the assurance level of the platform covers the intended assurance level of the  
4030 composite TOE and (ii) the platform's security certificate is valid and up-to-date. Equivalence of  
4031 single assurance components (and, hence, of assurance levels) belonging to different ISO/IEC  
4032 editions shall be established / acknowledged by the Composite Product Certification Body.

4033 If a PP conformance is claimed (e.g. composite ST claim conformance to a PP that claims  
4034 conformance to a hardware PP), the consistency check can be reduced to the elements of the  
4035 Security Target having not already been covered by these Protection Profiles.

4036 The fact of compliance to a PP is not sufficient to avoid inconsistencies. Assume the following  
4037 situation, where → stands for "complies with"

4038 Composite-ST → SW PP → HW PP ← platform-ST

4039 The SW PP may require any kind of conformance, but this does not change the 'additional  
4040 elements' that the platform-ST may introduce to the HW PP. In conclusion, these additions are not

<sup>2</sup> denoted by Platform-ST in the following. Generally, a Security Target expresses a security policy for the TOE defined.

<sup>3</sup> because the TSF enforce the Security Target (together with organisational measures enforcing security objectives for the operational environment of the TOE).

<sup>4</sup> The comparison shall be performed on the abstraction level of SFRs. If the developer defined security functionality groups (TSF-groups) in the TSS part of his Security Target, the evaluator should also consider them in order to get a better understanding for the context of the security services offered by the TOE.

4041 necessarily consistent with the composite-ST/SW PP additions: There is no scenario that ensures  
4042 the consistency 'by construction'.

4043 Note that consistency may not be direct matching: e.g. objectives for the platform environment may  
4044 become objectives for the composite TOE.

### 4045 **10.10.1.3 Action ASE\_COMP.1.1E**

#### 4046 **10.10.1.3.1 General**

4047 The evaluator shall confirm that the information provided meets all requirements for content and  
4048 presentation of evidence.

4049 *ISO/IEC 15408-3 ASE\_COMP.1.1C: The statement of compatibility shall describe the separation of the*  
4050 *Platform-TSF into relevant Platform-TSF being used by the Composite-ST and others.*

#### 4051 **10.10.1.3.2 Work unit ASE\_COMP.1-1**

4052 The evaluator shall check that the statement of compatibility describes the separation of the  
4053 Platform-TSF into relevant Platform-TSF being used by the Composite-ST and others.

4054 Please note that TSF means 'TOE Security Functionality', whereby the TSF content is represented  
4055 by SFRs. The respective TOE summary specification (TSS) shall provide, for each SFR, a description  
4056 on how each SFR is met. The evaluator shall use this description in order to understand the  
4057 contextual frame of the SFRs.

4058 If the developer defined security functionality groups (TSF groups) in the TSS part of his Security  
4059 Target as such contextual frame of the SFRs, the evaluator should also consider them in order to  
4060 get a better understanding for the context of the security services offered by the TOE.

4061 This work unit relates to the Step 2 of the Application Notes above. In order to determine the  
4062 intersection area the evaluator considers the list of the Platform-SFRs (given in the ST of the  
4063 underlying platform) as single properties of the platform's security services.

4064 To give an example, let us assume that there are the following Platform-SFRs: Cryptographic  
4065 operations FCS\_COP.1/RSA, FCS\_COP.1/AES, FCS\_COP.1/EC as well as tamper-resistance  
4066 FPT\_PHP.3 and limited capabilities and availability FMT\_LIM.1 and FMT\_LIM.2

4067 These Platform-SFRs shall be separated in three groups:

4068 – **IP\_SFR:** Irrelevant Platform-SFRs not being used by the Composite-ST.

4069 – **RP\_SFR-SERV:** Relevant Platform-SFRs being used by the Composite-ST to implement a security  
4070 service with associated TSFI. –

4071 **RP\_SFR-MECH:** Relevant Platform-SFRs being used by the Composite-ST because of its security  
4072 properties providing protection against attacks to the TOE as a whole and are addressed in  
4073 ADV\_ARC. These required security properties are a result of the security mechanisms and services  
4074 that are implemented in the Platform TOE.

4075 The second and third group RP\_SFR-SERV and RP\_SFR-MECH exactly represent the intersection  
4076 area in question. For example, IP\_SFR = {FCS\_COP.1/AES}, RP\_SFR-SERV= {FCS\_COP.1/RSA,  
4077 FCS\_COP.1/EC} and RP\_SFR-MECH = {FPT\_PHP.3, FMT\_LIM.1, FMT\_LIM.2}, i.e. AES is not used by  
4078 the composite TOE, but all other Platform-SFRs are used. However, the RP\_SFR-MECH cannot be  
4079 directly connected to SFRs in the Composite-ST.

4080 The size of the overlapping area (i.e. the content of the group RP\_SFR-SERV and RP\_SFR-MECH)  
4081 results from the concrete properties of the Platform-ST and the Composite-ST. If the Composite-ST

4082 does not use any property of the Platform-ST and, hence, the intersection area is an empty set  
4083  $(RP\_SFR-MECH \cup RP\_SFR-SERV) = \{\emptyset\}$ , no further composite evaluation activities are necessary at  
4084 all: In such a case there is a technical, but not a security composition.

4085 The result of this work unit shall be integrated to the result of ASE\_REQ.1.6C/ ASE\_REQ.1-10 (or  
4086 the equivalent higher components if a higher assurance level is selected) and ASE\_REQ.2.9C/  
4087 ASE\_REQ.2-13.

#### 4088 **10.10.1.3.3 Work unit ASE\_COMP.1-2**

4089 The evaluator shall examine the statement of compatibility to determine that the Platform-TSF  
4090 being used by the Composite-ST is complete and consistent for the current composite TOE.

4091 In order to determine the completeness of the list of the Platform-TSF being used by the  
4092 Composite-ST, the evaluator shall verify that:

- 4093
- Platform-SFR =  $IP\_SFR \cup RP\_SFR-SERV \cup RP\_SFR-MECH$
  - Elements that belong to  $RP\_SFR-SERV$  and  $RP\_SFR-MECH$  are taken into account during the evaluation of the composite TOE. The  $IP\_SFR$  are obviously part of the Platform-TOE but they are not considered during the evaluation of the composite TOE
- 4094  
4095  
4096

4097 In order to determine the consistency of the list of the Platform TSF being used by the Composite-  
4098 ST, the evaluator shall verify that there are no ambiguities and contradictory statements.

4099 The result of this work unit shall be integrated to the result of ASE\_REQ.1.6C/ ASE\_REQ.1-10 (or  
4100 the equivalent higher components if a higher assurance level is selected) and ASE\_REQ.2.9C/  
4101 ASE\_REQ.2-13.

#### 4102 **10.10.1.3.4 Work unit ASE\_COMP.1-3**

4103 The evaluator shall check that the security assurance requirements of the composite evaluation  
4104 represent a subset of the security assurance requirements of the underlying platform.

4105 This work unit relates to the Step 2 of the Application Notes above. In order to ensure a sufficient  
4106 degree of trustworthiness of the Platform-TSF the evaluator compares the TOE security assurance  
4107 requirements of the composite evaluation with those of the underlying platform. The evaluator  
4108 decides that the degree of trustworthiness of the Platform-TSF is sufficient, if the Composite-SAR  
4109 represent a subset of the Platform-SAR:

4110  $Platform-SAR \supseteq Composite-SAR,$

4111 e.g. the EAL chosen for the composite evaluation does not exceed the EAL applied to the evaluation  
4112 of the platform.

4113 The result of this work unit shall be integrated to the result of ASE\_REQ.2.8C/ ASE\_REQ.2-12.

#### 4114 **10.10.1.3.5 Work unit ASE\_COMP.1-4**

4115 The evaluator shall examine the statement of compatibility to determine that all performed  
4116 operations on the relevant TOE security functional requirements of the platform are appropriate  
4117 for the Composite-ST.

4118 This work unit relates to Step 3 of the Application Notes above. The relevant TOE security  
4119 functional requirements of the platform comprise at least the elements of the group  $RP\_SFR-SERV$   
4120 (cf. the work unit ASE\_COMP.1-1) but also the  $RP\_SFR-MECH$  may be presented as relevant TOE  
4121 security functional requirements. The non-relevant TOE security functional requirements belong  
4122 to  $IP\_SFR$ .

4123 In order to perform this work unit the evaluator compares single parameters of the relevant SFRs  
 4124 of the platform with those of the composite evaluation. For example, the evaluator compares the  
 4125 properties of the respective components FCS\_COP.1/RSA and determines that the Composite-ST  
 4126 requires a key length of 2048 bit and the Platform-ST enforces the RSA-function with a key length  
 4127 of 1024 and 2048 bit, i.e. this parameter of the platform is appropriate for the Composite-ST. Note,  
 4128 that the Composite-SFRs need not necessarily be the same as the Platform-SFRs, e.g. a trusted  
 4129 channel (FTP\_ITC.1) in the composite product can be built using an RSA implementation  
 4130 (FCS\_COP.1/RSA) of the platform.

4131 The result of this work unit shall be integrated to the result of ASE\_REQ.2.3C/ ASE\_REQ.2-4.

#### 4132 **10.10.1.3.6 Work unit ASE\_COMP.1-5**

4133 The evaluator shall examine the statement of compatibility to determine that the relevant TOE  
 4134 security objectives of the Platform-ST are not contradictory to those of the Composite-ST.

4135 This work unit relates to Step 3 of the Application Notes above. The relevant TOE security  
 4136 objectives of the Platform-ST are those that are mapped to the relevant SFRs of the Platform-ST (cf.  
 4137 the work unit ASE\_COMP.1-1).

4138 In order to perform this work unit the evaluator compares the relevant TOE security objectives of  
 4139 the Platform-ST with those of the Composite-ST and determines whether they are not  
 4140 contradictory.

4141 The result of this work unit shall be integrated to the result of ASE\_OBJ.2.1C/ ASE\_OBJ.2-1.

#### 4142 **10.10.1.3.7 Work unit ASE\_COMP.1-6**

4143 The evaluator shall examine the statement of compatibility to determine that the significant  
 4144 security objectives for the operational environments of the Platform-ST are not contradictory to  
 4145 those of the Composite-ST.

4146 This work unit relates to Step 3 of the Application Notes above. In order to determine which  
 4147 assumptions of the Platform-ST are significant for the Composite-ST the evaluator analyses the  
 4148 objectives for the environment of the Platform-ST, and their separation, in the following groups:

- 4149 • **IrOE:** The objectives for the environment being not relevant for the Composite-ST, e.g. the  
 4150 objectives for the environment about the developing and manufacturing phases of the  
 4151 platform.
- 4152 • **CfPOE:** The objectives for the environment being fulfilled by the Composite-ST  
 4153 automatically. Such objectives of the environment of the Platform-ST can always be  
 4154 assigned to the TOE security objectives of the Composite-ST. Due to this fact they will be  
 4155 fulfilled either by the Composite-SFR or by the Composite-SAR automatically. To give an  
 4156 example, let there be an Objective for the environment OE.Resp-Appl of the Platform-ST:  
 4157 'All User Data are owned by Smartcard Embedded Software. Therefore, it must be assumed  
 4158 that security relevant User Data (especially cryptographic keys) are treated by the  
 4159 Smartcard Embedded Software as defined for the specific application context' and a TOE  
 4160 security objective OT.Key\_Secrecy of the Composite-ST: 'The secrecy of the signature  
 4161 private key used for signature generation is reasonably assured against attacks with a high  
 4162 attack potential.' If the private key is the only sensitive data element, then the Objective for  
 4163 the environment OE.Resp-Appl is covered by the TOE security objective OT.Key\_Secrecy  
 4164 automatically.
- 4165 • **SgOE:** The remaining Objectives for the environment of the Platform-ST belonging neither  
 4166 to the group IrOE nor CfOE Exactly this group makes up the significant objectives for the  
 4167 environment for the Composite-ST, which shall be addressed in the Composite-ST.

## ISO/IEC 18045:2008(E)

4168 In order to accomplish this work unit the evaluator compares the significant security objectives for  
4169 the operational environment of the Platform-ST with those of the Composite-ST and determines  
4170 whether they are not contradictory. If necessary, the significant security objectives for the  
4171 operational environment of the Platform-ST shall be included into the Composite-ST including the  
4172 related assumptions from which the objectives for the environment are drawn. The inclusion is not  
4173 necessary, if the Composite-ST already contains equivalent (or similar) security objectives  
4174 (covering all relevant aspects) and assumptions.

4175 Since assurance of the development and manufacturing environment of the platform is confirmed  
4176 by the platform certificate, the respective platform-objectives, if any, belong to the group IrOE.

4177 Assurance of development and manufacturing environment is usually completely addressed by the  
4178 assurance class ALC, and, hence, requires no explicit security objective.

4179 The result of this work unit shall be integrated to the result of ASE\_OBJ.2.1C/ ASE\_OBJ.2-1 and  
4180 ASE\_OBJ.2.3C/ ASE\_OBJ.2-3.

4181

## 11 Class ADV: Development

### 11.1 Introduction

The purpose of the development activity is to assess the design documentation in terms of its adequacy to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. This understanding is achieved through examination of increasingly refined descriptions of the TSF design documentation. Design documentation consists of a functional specification (which describes the interfaces of the TSF), a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed), and an implementation description (a source code level description). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed), an internals description (which describes how the TSF was constructed in a manner that encourages understandability), and a security policy model (which formally describes the security policies enforced by the TSF).

### 11.2 Application notes

ISO/IEC 15408 requirements for design documentation are levelled by the amount, and detail of information provided, and the degree of formality of the presentation of the information. At lower levels, the most security-critical portions of the TSF are described with the most detail, while less security-critical portions of the TSF are merely summarised; added assurance is gained by increasing the amount of information about the most security-critical portions of the TSF, and increasing the details about the less security-critical portions. The most assurance is achieved when thorough details and information of all portions are provided.

ISO/IEC 15408 considers a document's degree of formality (that is, whether it is informal or semiformal) to be hierarchical. An informal document is one that is expressed in a natural language. The methodology does not dictate the specific language that must be used; that issue is left for the scheme. The following paragraphs differentiate the contents of the different informal documents.

A functional specification provides a description of the purpose and method-of-use of interfaces to the TSF. For example, if an operating system presents the user with a means of self-identification, of creating files, of modifying or deleting files, of setting permissions defining what other users may access files, and of communicating with remote machines, its functional specification would contain descriptions of each of these and how they are realised through interactions with the externally-visible interfaces to the TSF. If there is also audit functionality that detects and record the occurrences of such events, descriptions of this audit functionality would also be expected to be part of the functional specification; while this functionality is technically not directly invoked by the user at the external interface, it certainly is affected by what occurs at the user's external interface.

A design description is expressed in terms of logical divisions (subsystems or modules) that each provide a comprehensible service or function. For example, a firewall might be composed of subsystems that deal with packet filtering, with remote administration, with auditing, and with connection-level filtering. The design description of the firewall would describe the actions that are taken, in terms of what actions each subsystem takes when an incoming packet arrives at the firewall.

4224 **11.3 Security Architecture (ADV\_ARC)**

4225 **11.3.1 Evaluation of sub-activity (ADV\_ARC.1)**

4226 **11.3.1.1 Objectives**

4227 The objective of this sub-activity is to determine whether the TSF is structured such that it cannot  
4228 be tampered with or bypassed, and whether TSFs that provide security domains isolate those  
4229 domains from each other.

4230 **11.3.1.2 Input**

4231 The evaluation evidence for this sub-activity is:

- 4232 a) the ST;
- 4233 b) the functional specification;
- 4234 c) the TOE design;
- 4235 d) the security architecture description;
- 4236 e) the implementation representation (if available);
- 4237 f) the operational user guidance.

4238 **11.3.1.3 Application notes**

4239 The notions of self-protection, domain separation, and non-bypassability are distinct from security  
4240 functionality expressed in ISO/IEC 15408-2 SFRs because self-protection and non-bypassability  
4241 largely have no directly observable interface at the TSF. Rather, they are properties of the TSF that  
4242 are achieved through the design of the TOE, and enforced by the correct implementation of that  
4243 design. Also, the evaluation of these properties is less straight-forward than the evaluation of  
4244 mechanisms; it is more difficult to check for the absence of functionality than for its presence.  
4245 However, the determination that these properties are being satisfied is just as critical as the  
4246 determination that the mechanisms are properly implemented.

4247 The overall approach used is that the developer provides a TSF that meets the above-mentioned  
4248 properties, and provides evidence (in the form of documentation) that can be analysed to show  
4249 that the properties are indeed met. The evaluator has the responsibility for looking at the evidence  
4250 and, coupled with other evidence delivered for the TOE, determining that the properties are  
4251 achieved. The work units can be characterised as those detailing with what information has to be  
4252 provided, and those dealing with the actual analysis the evaluator performs.

4253 The security architecture description describes how domains are defined and how the TSF keeps  
4254 them separate. It describes what prevents untrusted processes from getting to the TSF and  
4255 modifying it. It describes what ensures that all resources under the TSF's control are adequately  
4256 protected and that all actions related to the SFRs are mediated by the TSF. It explains any role the  
4257 environment plays in any of these (e.g. presuming it gets correctly invoked by its underlying  
4258 environment, how is its security functionality invoked?). In short, it explains how the TOE is  
4259 considered to be providing any kind of *security* service.

4260 The analyses the evaluator performs must be done in the context of all of the development  
4261 evidence provided for the TOE, at the level of detail the evidence is provided. At lower assurance  
4262 levels, there should not be the expectation that, for example, TSF self-protection is completely



4263 analysed, because only high-level design representations will be available. The evaluator also  
 4264 needs to be sure to use information gleaned from other portions of their analysis (e.g., analysis of  
 4265 the TOE design) in making their assessments for the properties being examined in the following  
 4266 work units.

#### 4267 **11.3.1.4 Action ADV\_ARC.1.1E**

##### 4268 **11.3.1.4.1 General**

4269 ISO/IEC 15408-3 ADV\_ARC.1.1C: *The security architecture description shall be at a level of detail*  
 4270 *commensurate with the description of the SFR-enforcing abstractions described in the TOE design*  
 4271 *document.*

##### 4272 **11.3.1.4.2 Work unit ADV\_ARC.1-1**

4273 The evaluator **shall examine** the security architecture description to determine that the  
 4274 information provided in the evidence is presented at a level of detail commensurate with the  
 4275 descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE  
 4276 design document.

4277 With respect to the functional specification, the evaluator should ensure that the self-protection  
 4278 functionality described cover those effects that are evident at the TSFI. Such a description might  
 4279 include protection placed upon the executable images of the TSF, and protection placed on objects  
 4280 (e.g., files used by the TSF). The evaluator ensures that the functionality that might be invoked  
 4281 through the TSFI is described.

4282 If Evaluation of sub-activity (ADV\_TDS.1) or Evaluation of sub-activity (ADV\_TDS.2) is included, the  
 4283 evaluator ensures the security architecture description contains information on how any  
 4284 subsystems that contribute to TSF domain separation work.

4285 If Evaluation of sub-activity (ADV\_TDS.3) or higher is available, the evaluator ensures that the  
 4286 security architecture description also contains implementation-dependent information. For  
 4287 example, such a description might contain information pertaining to coding conventions for  
 4288 parameter checking that would prevent TSF compromises (e.g. buffer overflows), and information  
 4289 on stack management for call and return operations. The evaluator checks the descriptions of the  
 4290 mechanisms to ensure that the level of detail is such that there is little ambiguity between the  
 4291 description in the security architecture description and the implementation representation.

4292 The evaluator action related to this work unit is assigned a fail verdict if the security architecture  
 4293 description mentions any module, subsystem, or interface that is not described in the functional  
 4294 specification or TOE design document.

4295 ISO/IEC 15408-3 ADV\_ARC.1.2C: *The security architecture description shall describe the security*  
 4296 *domains maintained by the TSF consistently with the SFRs.*

##### 4297 **11.3.1.4.3 Work unit ADV\_ARC.1-2**

4298 The evaluator **shall examine** the security architecture description to determine that it describes  
 4299 the security domains maintained by the TSF.

4300 Security domains refer to environments supplied by the TSF for use by potentially-harmful  
 4301 entities; for example, a typical secure operating system supplies a set of resources (address space,  
 4302 per-process environment variables) for use by processes with limited access rights and security  
 4303 properties. The evaluator determines that the developer's description of the security domains  
 4304 takes into account all of the SFRs claimed by the TOE.

4305 For some TOEs such domains do not exist because all of the interactions available to users are  
 4306 severely constrained by the TSF. A packet-filter firewall is an example of such a TOE. Users on the

## ISO/IEC 18045:2008(E)

4307 LAN or WAN do not interact with the TOE, so there need be no security domains; there are only  
4308 data structures maintained by the TSF to keep the users' packets separated. The evaluator ensures  
4309 that any claim that there are no domains is supported by the evidence and that no such domains  
4310 are, in fact, available.

4311 ISO/IEC 15408-3 ADV\_ARC.1.3C: *The security architecture description shall describe how the TSF*  
4312 *initialisation process is secure.*

### 4313 11.3.1.4.4 Work unit ADV\_ARC.1-3

4314 The evaluator **shall examine** the security architecture description to determine that the  
4315 initialisation process preserves security.

4316 The information provided in the security architecture description relating to TSF initialisation is  
4317 directed at the TOE components that are involved in bringing the TSF into an initial secure state  
4318 (i.e. when all parts of the TSF are operational) when power-on or a reset is applied. This discussion  
4319 in the security architecture description should list the system initialisation components and the  
4320 processing that occurs in transitioning from the "down" state to the initial secure state.

4321 It is often the case that the components that perform this initialisation function are not accessible  
4322 after the secure state is achieved; if this is the case then the security architecture description  
4323 identifies the components and explains how they are not reachable by untrusted entities after the  
4324 TSF has been established. In this respect, the property that needs to be preserved is that these  
4325 components either 1) cannot be accessed by untrusted entities after the secure state is achieved, or  
4326 2) if they provide interfaces to untrusted entities, these TSFI cannot be used to tamper with the  
4327 TSF.

4328 The TOE components related to TSF initialisation, then, are treated themselves as part of the TSF,  
4329 and analysed from that perspective. It should be noted that even though these are treated as part of  
4330 the TSF, it is likely that a justification (as allowed by TSF internals (ADV\_INT)) can be made that  
4331 they do not have to meet the internal structuring requirements of ADV\_INT.

4332 ISO/IEC 15408-3 ADV\_ARC.1.4C: *The security architecture description shall demonstrate that the*  
4333 *TSF protects itself from tampering.*

### 4334 11.3.1.4.5 Work unit ADV\_ARC.1-4

4335 The evaluator **shall examine** the security architecture description to determine that it contains  
4336 information sufficient to support a determination that the TSF is able to protect itself from  
4337 tampering by untrusted active entities.

4338 "Self-protection" refers to the ability of the TSF to protect itself from manipulation from external  
4339 entities that may result in changes to the TSF. For TOEs that have dependencies on other IT entities,  
4340 it is often the case that the TOE uses services supplied by the other IT entities in order to perform  
4341 its functions. In such cases, the TSF alone does not protect itself because it depends on the other IT  
4342 entities to provide some of the protection. For the purposes of the security architecture description,  
4343 the notion of *self-protection* applies only to the services provided by the TSF through its TSFI, and  
4344 not to services provided by underlying IT entities that it uses.

4345 Self-protection is typically achieved by a variety of means, ranging from physical and logical  
4346 restrictions on access to the TOE; to hardware-based means (e.g. "execution rings" and memory  
4347 management functionality); to software-based means (e.g. boundary checking of inputs on a  
4348 trusted server). The evaluator determines that all such mechanisms are described.

4349 The evaluator determines that the design description covers how user input is handled by the TSF  
4350 in such a way that the TSF does not subject itself to being corrupted by that user input. For example,  
4351 the TSF might implement the notion of privilege and protect itself by using privileged-mode  
4352 routines to handle user input. The TSF might make use of processor-based separation mechanisms

such as privilege levels or rings. The TSF might implement software protection constructs or coding conventions that contribute to implementing separation of software domains, perhaps by delineating user address space from system address space. And the TSF might have reliance its environment to provide some support to the protection of the TSF.

All of the mechanisms contributing to the domain separation functions are described. The evaluator should use knowledge gained from other evidence (functional specification, TOE design, TSF internals description, other parts of the security architecture description, or implementation representation, as included in the assurance package for the TOE) in determining if any functionality contributing to self-protection was described that is not present in the security architecture description.

Accuracy of the description of the self-protection mechanisms is the property that the description faithfully describes what is implemented. The evaluator should use other evidence (functional specification, TOE design, TSF Internals documentation, other parts of the security architecture description, implementation representation, as included in the ST for the TOE) in determining whether there are discrepancies in any descriptions of the self-protection mechanisms. If Implementation representation (ADV\_IMP) is included in the assurance package for the TOE, the evaluator will choose a sample of the implementation representation; the evaluator should also ensure that the descriptions are accurate for the sample chosen. If an evaluator cannot understand how a certain self-protection mechanism works or could work in the system architecture, it may be the case that the description is not accurate.

ISO/IEC 15408-3 ADV\_ARC.1.5C: *The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.*

#### 11.3.1.4.6 Work unit ADV\_ARC.1-5

The evaluator ***shall examine*** the security architecture description to determine that it presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

Non-bypassability is a property that the security functionality of the TSF (as specified by the SFRs) is always invoked. For example, if access control to files is specified as a capability of the TSF via an SFR, there must be no interfaces through which files can be accessed without invoking the TSF's access control mechanism (such as an interface through which a raw disk access takes place).

Describing how the TSF mechanisms cannot be bypassed generally requires a systematic argument based on the TSF and the TSFIs. The description of how the TSF works (contained in the design decomposition evidence, such as the functional specification, TOE design documentation) - along with the information in the TSS - provides the background necessary for the evaluator to understand what resources are being protected and what security functions are being provided. The functional specification provides descriptions of the TSFIs through which the resources/functions are accessed.

The evaluator assesses the description provided (and other information provided by the developer, such as the functional specification) to ensure that no available interface can be used to bypass the TSF. This means that every available interface must be either unrelated to the SFRs that are claimed in the ST (and does not interact with anything that is used to satisfy SFRs) or else uses the security functionality that is described in other development evidence in the manner described. For example, a game would likely be unrelated to the SFRs, so there must be an explanation of how it cannot affect security. Access to user data, however, is likely to be related to access control SFRs, so the explanation would describe how the security functionality works when invoked through the data-access interfaces. Such a description is needed for every available interface.

An example of a description follows. Suppose the TSF provides file protection. Further suppose that although the "traditional" system call TSFIs for open, read, and write invoke the file protection mechanism described in the TOE design, there exists a TSFI that allows access to a batch job facility (creating batch jobs, deleting jobs, modifying unprocessed jobs). The evaluator should be able to

determine from the vendor-provided description that this TSFI invokes the same protection mechanisms as do the “traditional” interfaces. This could be done, for example, by referencing the appropriate subclauses of the TOE design that discuss *how* the batch job facility TSFI achieves its security objectives.

Using this same example, suppose there is a TSFI whose sole purpose is to display the time of day. The evaluator should determine that the description adequately argues that this TSFI is not capable of manipulating any protected resources and should not invoke any security functionality.

Another example of bypass is when the TSF is supposed to maintain confidentiality of a cryptographic key (one is allowed to use it for cryptographic operations, but is not allowed to read/write it). If an attacker has direct physical access to the device, they might be able to examine side-channels such as the power usage of the device, the exact timing of the device, or even any electromagnetic emanations of the device and, from this, infer the key.

If such side-channels may be present, the demonstration should address the mechanisms that prevent these side-channels from occurring, such as random internal clocks, dual-line technology etc. Verification of these mechanisms would be verified by a combination of purely design-based arguments and testing.

For a final example using security functionality rather than a protected resource, consider an ST that contains FCO\_NRO.2 Enforced proof of origin, which requires that the TSF provides evidence of origination for information types specified in the ST. Suppose that the “information types” included all information that is sent by the TOE via e-mail. In this case, the evaluator should examine the description to ensure that all TSFI that can be invoked to send e-mail perform the “evidence of origination generation” function are detailed. The description might point to user guidance to show all places where e-mail can originate (e.g., e-mail program, notification from scripts/batch jobs) and then how each of these places invokes the evidence generation function.

The evaluator should also ensure that the description is comprehensive, in that each interface is analysed with respect to the entire set of claimed SFRs. This may require the evaluator to examine supporting information (functional specification, TOE design, other parts of the security architecture description, operational user guidance, and perhaps even the implementation representation, as provided for the TOE) to determine that the description has correctly capture all aspects of an interface. The evaluator should consider what SFRs each TSFI might affect (from the description of the TSFI and its implementation in the supporting documentation), and then examine the description to determine whether it covers those aspects.

#### 11.4 Functional specification (ADV\_FSP)

##### 11.4.1 Evaluation of sub-activity (ADV\_FSP.1)

###### 11.4.1.1 Objectives

The objective of this sub-activity is to determine whether the developer has provided a high-level description of at least the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their parameters. There is no other required evidence that can be expected to be available to measure the accuracy of these descriptions; the evaluator merely ensures the descriptions seem plausible.

###### 11.4.1.2 Input

The evaluation evidence for this sub-activity is:

- a) the ST;
- b) the functional specification;

4445 c) the operational user guidance;

#### 4446 11.4.1.3 Action ADV\_FSP.1.1E

4447 ISO/IEC 15408-3 ADV\_FSP.1.1C: *The functional specification shall describe the purpose and method*  
4448 *of use for each SFR-enforcing and SFR-supporting TSFI.*

##### 4449 11.4.1.3.1 Work unit ADV\_FSP.1-1

4450 The evaluator **shall examine** the functional specification to determine that it states the purpose of  
4451 each SFR-supporting and SFR-enforcing TSFI.

4452 The purpose of a TSFI is a general statement summarising the functionality provided by the  
4453 interface. It is not intended to be a complete statement of the actions and results related to the  
4454 interface, but rather a statement to help the reader understand in general what the interface is  
4455 intended to be used for. The evaluator should not only determine that the purpose exists, but also  
4456 that it accurately reflects the TSFI by taking into account other information about the interface,  
4457 such as the description of the parameters; this can be done in association with other work units for  
4458 this component.

4459 If an action available through an interface plays a role in enforcing any security policy on the TOE  
4460 (that is, if one of the actions of the interface can be traced to one of the SFRs levied on the TSF),  
4461 then that interface is *SFR-enforcing*. Such policies are not limited to the access control policies, but  
4462 also refer to any functionality specified by one of the SFRs contained in the ST. Note that it is  
4463 possible that an interface may have various actions and results, some of which may be SFR-  
4464 enforcing and some of which may not.

4465 Interfaces to (or actions available through an interface relating to) actions that SFR-enforcing  
4466 functionality depends on, but need only to function correctly in order for the security policies of  
4467 the TOE to be preserved, are termed *SFR supporting*. Interfaces to actions on which SFR-enforcing  
4468 functionality has no dependence are termed *SFR non-interfering*.

4469 It should be noted that in order for an interface to be SFR supporting or SFR non-interfering it must  
4470 have *no* SFR-enforcing actions or results. In contrast, an SFR-enforcing interface may have SFR-  
4471 supporting actions (for example, the ability to set the system clock may be an SFR-enforcing action  
4472 of an interface, but if that same interface is used to display the system date that action may only be  
4473 SFR supporting). An example of a purely SFR-supporting interface is a system call interface that is  
4474 used both by untrusted users and by a portion of the TSF that is running in user mode.

4475 At this level, it is unlikely that a developer will have expended effort to label interfaces as SFR-  
4476 enforcing and SFR-supporting. In the case that this has been done, the evaluator should verify to  
4477 the extent that supporting documentation (e.g., operational user guidance) allows that this  
4478 identification is correct. Note that this identification activity is necessary for several work units for  
4479 this component.

4480 In the more likely case that the developer has not labelled the interfaces, the evaluator must  
4481 perform their own identification of the interfaces first, and then determine whether the required  
4482 information (for this work unit, the purpose) is present. Again, because of the lack of supporting  
4483 evidence this identification will be difficult and have low assurance that all appropriate interfaces  
4484 have been correctly identified, but nonetheless the evaluator examines other evidence available for  
4485 the TOE to ensure as complete coverage as is possible.

##### 4486 11.4.1.3.2 Work unit ADV\_FSP.1-2

4487 The evaluator **shall examine** the functional specification to determine that the method of use for  
4488 each SFR-supporting and SFR-enforcing TSFI is given.

## ISO/IEC 18045:2008(E)

4489 See work unit ADV\_FSP.1-1 for a discussion on the identification of SFR-supporting and SFR-  
4490 enforcing TSFI.

4491 The method of use for a TSFI summarises how the interface is manipulated in order to invoke the  
4492 actions and obtain the results associated with the TSFI. The evaluator should be able to determine,  
4493 from reading this material in the functional specification, how to use each interface. This does not  
4494 necessarily mean that there needs to be a separate method of use for each TSFI, as it may be  
4495 possible to describe in general how kernel calls are invoked, for instance, and then identify each  
4496 interface using that general style. Different types of interfaces will require different method of use  
4497 specifications. APIs, network protocol interfaces, system configuration parameters, and hardware  
4498 bus interfaces all have very different methods of use, and this should be taken into account by the  
4499 developer when developing the functional specification, as well as by the evaluator evaluating the  
4500 functional specification.

4501 For administrative interfaces, whose functionality is documented as being inaccessible to  
4502 untrusted users, the evaluator ensures that the method of making the functions inaccessible is  
4503 described in the functional specification. It should be noted that this inaccessibility needs to be  
4504 tested by the developer in their test suite.

4505 ISO/IEC 15408-3 ADV\_FSP.1.2C: *The functional specification shall identify all parameters associated*  
4506 *with each SFR-enforcing and SFR-supporting TSFI.*

### 4507 11.4.1.3.3 Work unit ADV\_FSP.1-3

4508 The evaluator **shall examine** the presentation of the TSFI to determine that it identifies all  
4509 parameters associated with each SFR-enforcing and SFR-supporting TSFI.

4510 See work unit ADV\_FSP.1-1 for a discussion on the identification of SFR-supporting and SFR-  
4511 enforcing TSFI.

4512 The evaluator examines the functional specification to ensure that all of the parameters are  
4513 described for identified TSFI. Parameters are explicit inputs or outputs to an interface that control  
4514 the behaviour of that interface. For examples, parameters are the arguments supplied to an API;  
4515 the various fields in packet for a given network protocol; the individual key values in the Windows  
4516 Registry; the signals across a set of pins on a chip; etc.

4517 While difficult to obtain much assurance that all parameters for the applicable TSFI have been  
4518 identified, the evaluator should also check other evidence provided for the evaluation (e.g.,  
4519 operational user guidance) to see if behaviour or additional parameters are described there but not  
4520 in the functional specification.

4521 ISO/IEC 15408-3 ADV\_FSP.1.3C: *The functional specification shall provide rationale for the implicit*  
4522 *categorisation of interfaces as SFR-non-interfering.*

### 4523 11.4.1.3.4 Work unit ADV\_FSP.1-4

4524 The evaluator **shall examine** the rationale provided by the developer for the implicit  
4525 categorisation of interfaces as SFR-non-interfering to determine that it is accurate.

4526 In the case where the developer has provided adequate documentation to perform the analysis  
4527 called for by the rest of the work units for this component without explicitly identifying SFR-  
4528 enforcing and SFR-supporting interfaces, this work unit should be considered satisfied.

4529 This work unit is intended to apply to cases where the developer has not described a portion of the  
4530 TSFI, claiming that it is SFR-non-interfering and therefore not subject to other requirements of this  
4531 component. In such a case, the developer provides a rationale for this characterisation in sufficient  
4532 detail such that the evaluator understands the rationale, the characteristics of the interfaces  
4533 affected (e.g., their high-level function with respect to the TOE, such as "colour palette

manipulation”), and that the claim that these are SFR-non-interfering is supported. Given the level of assurance the evaluator should not expect more detail than is provided for the SFR-enforcing or SFR-supporting interfaces, and in fact the detail should be much less. In most cases, individual interfaces should not need to be addressed in the developer-provided rationale subclause.

ISO/IEC 15408-3 ADV\_FSP.1.4C: *The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.*

#### 11.4.1.3.5 Work unit ADV\_FSP.1-5

The evaluator **shall check** that the tracing links the SFRs to the corresponding TSFIs.

The tracing is provided by the developer to serve as a guide to which SFRs are related to which TSFIs. This tracing can be as simple as a table; it is used as input to the evaluator for use in the following work units, in which the evaluator verifies its completeness and accuracy.

#### 11.4.1.4 Action ADV\_FSP.1.2E

##### 11.4.1.4.1 Work unit ADV\_FSP.1-6

The evaluator **shall examine** the functional specification to determine that it is a complete instantiation of the SFRs.

To ensure that all SFRs are covered by the functional specification, as well as the test coverage analysis, the evaluator may build upon the developer's tracing (see ADV\_FSP.1-5 a map between the TOE security functional requirements and the TSFI). Note that this map may have to be at a level of detail below the component or even element level of the requirements, because of operations (assignments, refinements, selections) performed on the functional requirement by the ST author.

For example, the FDP\_ACC.1 component contains an element with assignments. If the ST contained, for instance, ten rules in the FDP\_ACC.1 assignment, and these ten rules were covered by three different TSFI, it would be inadequate for the evaluator to map FDP\_ACC.1 to TSFI A, B, and C and claim they had completed the work unit. Instead, the evaluator would map FDP\_ACC.1 (rule 1) to TSFI A; FDP\_ACC.1 (rule 2) to TSFI B; etc. It might also be the case that the interface is a wrapper interface (e.g., IOCTL), in which case the mapping would need to be specific to certain set of parameters for a given interface.

The evaluator must recognise that for requirements that have little or no manifestation at the TSF boundary (e.g., FDP\_RIP) it is not expected that they completely map those requirements to the TSFI. The analysis for those requirements will be performed in the analysis for the TOE design (ADV\_TDS) when included in the ST. It is also important to note that since the parameters associated with TSFIs must be fully specified, the evaluator should be able to determine if all aspects of an SFR appear to be implemented at the interface level.

##### 11.4.1.4.2 Work unit ADV\_FSP.1-7

The evaluator **shall examine** the functional specification to determine that it is an accurate instantiation of the SFRs.

For each functional requirement in the ST that results in effects visible at the TSF boundary, the information in the associated TSFI for that requirement specifies the required functionality described by the requirement. For example, if the ST contains a requirement for access control lists, and the only TSFI that map to that requirement specify functionality for Unix-style protection bits, then the functional specification is not accurate with respect to the requirements.

The evaluator must recognise that for requirements that have little or no manifestation at the TSF boundary (e.g., FDP\_RIP) it is not expected that the evaluator completely map those requirements

4578 to the TSFI. The analysis for those requirements will be performed in the analysis for the TOE  
4579 design (ADV\_TDS) when included in the ST.

4580 **11.4.2 Evaluation of sub-activity (ADV\_FSP.2)**

4581 **11.4.2.1 Objectives**

4582 The objective of this sub-activity is to determine whether the developer has provided a description  
4583 of the TSFIs in terms of their purpose, method of use, and parameters. In addition, the SFR-  
4584 enforcing actions, results and error messages of each TSFI that is SFR-enforcing are also described.

4585 **11.4.2.2 Input**

4586 The evaluation evidence for this sub-activity that is required by the work-units is:

- 4587 a) the ST;
- 4588 b) the functional specification;
- 4589 c) the TOE design.

4590 The evaluation evidence for this sub-activity that is used if included in the ST for the TOE is:

- 4591 a) the security architecture description;
- 4592 b) the operational user guidance;

4593 **11.4.2.3 Action ADV\_FSP.2.1E**

4594 **11.4.2.3.1 General**

4595 ISO/IEC 15408-3 ADV\_FSP.2.1C: *The functional specification shall completely represent the TSF.*

4596 **11.4.2.3.2 Work unit ADV\_FSP.2-1**

4597 The evaluator ***shall examine*** the functional specification to determine that the TSF is fully  
4598 represented.

4599 The identification of the TSFI is a necessary prerequisite to all other activities in this sub-activity.  
4600 The TSF must be identified (done as part of the TOE design (ADV\_TDS) work units) in order to  
4601 identify the TSFI. This activity can be done at a high level to ensure that no large groups of  
4602 interfaces have been missed (network protocols, hardware interfaces, configuration files), or at a  
4603 low level as the evaluation of the functional specification proceeds.

4604 In making an assessment for this work unit, the evaluator determines that all portions of the TSF  
4605 are addressed in terms of the interfaces listed in the functional specification. All portions of the TSF  
4606 should have a corresponding interface description, or if there are no corresponding interfaces for a  
4607 portion of the TSF, the evaluator determines that that is acceptable.

4608 ISO/IEC 15408-3 ADV\_FSP.2.2C: *The functional specification shall describe the purpose and method*  
4609 *of use for all TSFI.*



4610 **11.4.2.3.3 Work unit ADV\_FSP.2-2**

4611 The evaluator *shall examine* the functional specification to determine that it states the purpose of  
 4612 each TSFI.

4613 The purpose of a TSFI is a general statement summarising the functionality provided by the  
 4614 interface. It is not intended to be a complete statement of the actions and results related to the  
 4615 interface, but rather a statement to help the reader understand in general what the interface is  
 4616 intended to be used for. The evaluator should not only determine that the purpose exists, but also  
 4617 that it accurately reflects the TSFI by taking into account other information about the interface,  
 4618 such as the description of actions and error messages.

4619 **11.4.2.3.4 Work unit ADV\_FSP.2-3**

4620 The evaluator *shall examine* the functional specification to determine that the method of use for  
 4621 each TSFI is given.

4622 The method of use for a TSFI summarises how the interface is manipulated in order to invoke the  
 4623 actions and obtain the results associated with the TSFI. The evaluator should be able to determine,  
 4624 from reading this material in the functional specification, how to use each interface. This does not  
 4625 necessarily mean that there needs to be a separate method of use for each TSFI, as it may be  
 4626 possible to describe in general how kernel calls are invoked, for instance, and then identify each  
 4627 interface using that general style. Different types of interfaces will require different method of use  
 4628 specifications. APIs, network protocol interfaces, system configuration parameters, and hardware  
 4629 bus interfaces all have very different methods of use, and this should be taken into account by the  
 4630 developer when developing the functional specification, as well as by the evaluator evaluating the  
 4631 functional specification.

4632 For administrative interfaces, whose functionality is documented as being inaccessible to  
 4633 untrusted users, the evaluator ensures that the method of making the functions inaccessible is  
 4634 described in the functional specification. It should be noted that this inaccessibility needs to be  
 4635 tested by the developer in their test suite.

4636 The evaluator should not only determine that the set of method of use descriptions exist, but also  
 4637 that they accurately cover each TSFI.

4638 ISO/IEC 15408-3 ADV\_FSP.2.3C: *The functional specification shall identify and describe all*  
 4639 *parameters associated with each TSFI.*

4640 **11.4.2.3.5 Work unit ADV\_FSP.2-4**

4641 The evaluator *shall examine* the presentation of the TSFI to determine that it completely identifies  
 4642 all parameters associated with every TSFI.

4643 The evaluator examines the functional specification to ensure that all of the parameters are  
 4644 described for each TSFI. Parameters are explicit inputs or outputs to an interface that control the  
 4645 behaviour of that interface. For examples, parameters are the arguments supplied to an API; the  
 4646 various fields in packet for a given network protocol; the individual key values in the Windows  
 4647 Registry; the signals across a set of pins on a chip; etc.

4648 In order to determine that all of the parameters are present in the TSFI, the evaluator should  
 4649 examine the rest of the interface description (actions, error messages, etc.) to determine if the  
 4650 effects of the parameter are accounted for in the description. The evaluator should also check other  
 4651 evidence provided for the evaluation (e.g., TOE design, security architecture description,  
 4652 operational user guidance, implementation representation) to see if behaviour or additional  
 4653 parameters are described there but not in the functional specification.

4654 **11.4.2.3.6 Work unit ADV\_FSP.2-5**

4655 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
4656 accurately describes all parameters associated with every TSFI.

4657 Once all of the parameters have been identified, the evaluator needs to ensure that they are  
4658 accurately described, and that the description of the parameters is complete. A parameter  
4659 description tells what the parameter is in some meaningful way. For instance, the interface *foo(i)*  
4660 could be described as having “parameter i which is an integer”; this is not an acceptable parameter  
4661 description. A description such as “parameter i is an integer that indicates the number of users  
4662 currently logged in to the system” is much more acceptable.

4663 In order to determine that the description of the parameters is complete, the evaluator should  
4664 examine the rest of the interface description (purpose, method of use, actions, error messages, etc.)  
4665 to determine if the descriptions of the parameter(s) are accounted for in the description. The  
4666 evaluator should also check other evidence provided (e.g., TOE design, architectural design,  
4667 operational user guidance, implementation representation) to see if behaviour or additional  
4668 parameters are described there but not in the functional specification.

4669 ISO/IEC 15408-3 ADV\_FSP.2.4C: *For each SFR-enforcing TSFI, the functional specification shall*  
4670 *describe the SFR-enforcing actions associated with the TSFI.*

4671 **11.4.2.3.7 Work unit ADV\_FSP.2-6**

4672 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
4673 accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.

4674 If an action available through an interface can be traced to one of the SFRs levied on the TSF, then  
4675 that interface is *SFR-enforcing*. Such policies are not limited to the access control policies, but also  
4676 refer to any functionality specified by one of the SFRs contained in the ST. Note that it is possible  
4677 that an interface may have various actions and results, some of which may be SFR-enforcing and  
4678 some of which may not.

4679 The developer is not required to “label” interfaces as SFR-enforcing, and likewise is not required to  
4680 identify actions available through an interface as SFR-enforcing. It is the evaluator’s responsibility  
4681 to examine the evidence provided by the developer and determine that the required information is  
4682 present. In the case where the developer has identified the SFR-enforcing TSFI and SFR-enforcing  
4683 actions available through those TSFI, the evaluator must judge completeness and accuracy based  
4684 on other information supplied for the evaluation (e.g., TOE design, security architecture description,  
4685 operational user guidance), and on the other information presented for the interfaces (parameters  
4686 and parameter descriptions, error messages, etc.).

4687 In this case (where the developer has provided only the SFR-enforcing information for SFR-  
4688 enforcing TSFI) the evaluator also ensures that no interfaces have been mis-categorised. This is  
4689 done by examining other information supplied for the evaluation (e.g., TOE design, security  
4690 architecture description, operational user guidance), and the other information presented for the  
4691 interfaces (parameters and parameter descriptions, for example) not labelled as SFR-enforcing.

4692 In the case where the developer has provided the same level of information on all interfaces, the  
4693 evaluator performs the same type of analysis mentioned in the previous paragraphs. The evaluator  
4694 should determine which interfaces are SFR-enforcing and which are not, and subsequently ensure  
4695 that the SFR-enforcing aspects of the SFR-enforcing actions are appropriately described.

4696 The SFR-enforcing actions are those that are visible at any external interface and that provide for  
4697 the enforcement of the SFRs being claimed. For example, if audit requirements are included in the  
4698 ST, then audit-related actions would be SFR-enforcing and therefore must be described, even if the  
4699 result of that action is generally not visible through the invoked interface (as is often the case with

4700 audit, where a user action at one interface would produce an audit record visible at another  
4701 interface).

4702 The level of description that is required is that sufficient for the reader to understand what role the  
4703 TSFI actions play with respect to the SFR. The evaluator should keep in mind that the description  
4704 should be detailed enough to support the generation (and assessment) of test cases against that  
4705 interface. If the description is unclear or lacking detail such that meaningful testing cannot be  
4706 conducted against the TSFI, it is likely that the description is inadequate.

4707 ISO/IEC 15408-3 ADV\_FSP.2.5C: *For each SFR-enforcing TSFI, the functional specification shall*  
4708 *describe direct error messages resulting from processing associated with the SFR-enforcing actions.*

#### 4709 **11.4.2.3.8 Work unit ADV\_FSP.2-7**

4710 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
4711 accurately describes error messages that may result from SFR-enforcing actions associated with  
4712 each SFR-enforcing TSFI.

4713 This work unit should be performed in conjunction with, or after, work unit ADV\_FSP.2-6 in order  
4714 to ensure the set of SFR-enforcing TSFI and SFR-enforcing actions is correctly identified. The  
4715 developer may provide more information than is required (for example, all error messages  
4716 associated with each interface), in which the case the evaluator should restrict their assessment of  
4717 completeness and accuracy to only those that they determine to be associated with SFR-enforcing  
4718 actions of SFR-enforcing TSFI.

4719 Errors can take many forms, depending on the interface being described. For an API, the interface  
4720 itself may return an error code, set a global error condition, or set a certain parameter with an  
4721 error code. For a configuration file, an incorrectly configured parameter may cause an error  
4722 message to be written to a log file. For a hardware PCI card, an error condition may raise a signal  
4723 on the bus, or trigger an exception condition to the CPU.

4724 Errors (and the associated error messages) come about through the invocation of an interface. The  
4725 processing that occurs in response to the interface invocation may encounter error conditions,  
4726 which trigger (through an implementation-specific mechanism) an error message to be generated.  
4727 In some instances, this may be a return value from the interface itself; in other instances a global  
4728 value may be set and checked after the invocation of an interface. It is likely that a TOE will have a  
4729 number of low-level error messages that may result from fundamental resource conditions, such as  
4730 "disk full" or "resource locked". While these error messages may map to a large number of TSFI,  
4731 they could be used to detect instances where detail from an interface description has been omitted.  
4732 For instance, a TSFI that produces a "disk full" message, but has no obvious description of why that  
4733 TSFI should cause an access to the disk in its description of actions, might cause the evaluator to  
4734 examine other evidence (Security Architecture (ADV\_ARC), TOE design (ADV\_TDS)) related that  
4735 TSFI to determine if the description is accurate.

4736 In order to determine that the description of the error messages of a TSFI is accurate and complete,  
4737 the evaluator measures the interface description against the other evidence provided for the  
4738 evaluation (e.g., TOE design, security architecture description, operational user guidance), as well  
4739 as other evidence available for that TSFI (parameters, analysis from work unit ADV\_FSP.2-6).

4740 ISO/IEC 15408-3 ADV\_FSP.2.6C: *The tracing shall demonstrate that the SFRs trace to TSFIs in the*  
4741 *functional specification.*

#### 4742 **11.4.2.3.9 Work unit ADV\_FSP.2-8**

4743 The evaluator **shall check** that the tracing links the SFRs to the corresponding TSFIs.

## ISO/IEC 18045:2008(E)

4744 The tracing is provided by the developer to serve as a guide to which SFRs are related to which  
4745 TSFIs. This tracing can be as simple as a table; it is used as input to the evaluator for use in the  
4746 following work units, in which the evaluator verifies its completeness and accuracy.

### 4747 11.4.2.4 Action ADV\_FSP.2.2E

#### 4748 11.4.2.4.1 Work unit ADV\_FSP.2-9

4749 The evaluator *shall examine* the functional specification to determine that it is a complete  
4750 instantiation of the SFRs.

4751 To ensure that all SFRs are covered by the functional specification, as well as the test coverage  
4752 analysis, the evaluator may build upon the developer's tracing (see ADV\_FSP.2-8 a map between  
4753 the TOE security functional requirements and the TSFI. Note that this map may have to be at a level  
4754 of detail below the component or even element level of the requirements, because of operations  
4755 (assignments, refinements, selections) performed on the functional requirement by the ST author.

4756 For example, the FDP\_ACC.1 component contains an element with assignments. If the ST contained,  
4757 for instance, ten rules in the FDP\_ACC.1 assignment, and these ten rules were covered by three  
4758 different TSFI, it would be inadequate for the evaluator to map FDP\_ACC.1 to TSFI A, B, and C and  
4759 claim they had completed the work unit. Instead, the evaluator would map FDP\_ACC.1 (rule 1) to  
4760 TSFI A; FDP\_ACC.1 (rule 2) to TSFI B; etc. It might also be the case that the interface is a wrapper  
4761 interface (e.g., IOCTL), in which case the mapping would need to be specific to certain set of  
4762 parameters for a given interface.

4763 The evaluator must recognise that for requirements that have little or no manifestation at the TSF  
4764 boundary (e.g., FDP\_RIP) it is not expected that they completely map those requirements to the  
4765 TSFI. The analysis for those requirements will be performed in the analysis for the TOE design  
4766 (ADV\_TDS) when included in the ST. It is also important to note that since the parameters, actions,  
4767 and error messages associated with TSFIs must be fully specified, the evaluator should be able to  
4768 determine if all aspects of an SFR appear to be implemented at the interface level.

#### 4769 11.4.2.4.2 Work unit ADV\_FSP.2-10

4770 The evaluator *shall examine* the functional specification to determine that it is an accurate  
4771 instantiation of the SFRs.

4772 For each functional requirement in the ST that results in effects visible at the TSF boundary, the  
4773 information in the associated TSFI for that requirement specifies the required functionality  
4774 described by the requirement. For example, if the ST contains a requirement for access control lists,  
4775 and the only TSFI that map to that requirement specify functionality for Unix-style protection bits,  
4776 then the functional specification is not accurate with respect to the requirements.

4777 The evaluator must recognise that for requirements that have little or no manifestation at the TSF  
4778 boundary (e.g., FDP\_RIP) it is not expected that the evaluator completely map those requirements  
4779 to the TSFI. The analysis for those requirements will be performed in the analysis for the TOE  
4780 design (ADV\_TDS) when included in the ST.

### 4781 11.4.3 Evaluation of sub-activity (ADV\_FSP.3)

#### 4782 11.4.3.1 Objectives

4783 The objective of this sub-activity is to determine whether the developer has provided a description  
4784 of the TSFIs in terms of their purpose, method of use, and parameters. In addition, the actions,  
4785 results and error messages of each TSFI are also described sufficiently that it can be determined  
4786 whether they are SFR-enforcing, with the SFR-enforcing TSFI being described in more detail than  
4787 other TSFIs.

4788 **11.4.3.2 Input**

4789 The evaluation evidence for this sub-activity that is required by the work-units is:

- 4790 a) the ST;
- 4791 b) the functional specification;
- 4792 c) the TOE design.

4793 The evaluation evidence for this sub-activity that is used if included in the ST for the TOE is:

- 4794 a) the security architecture description;
- 4795 b) the implementation representation;
- 4796 c) the TSF internals description;
- 4797 d) the operational user guidance;

4798 **11.4.3.3 Action ADV\_FSP.3.1E**

4799 **11.4.3.3.1 General**

4800 ISO/IEC 15408-3 ADV\_FSP.3.1C: *The functional specification shall completely represent the TSF.*

4801 **11.4.3.3.2 Work unit ADV\_FSP.3-1**

4802 The evaluator **shall examine** the functional specification to determine that the TSF is fully  
4803 represented.

4804 The identification of the TSFI is a necessary prerequisite to all other activities in this sub-activity.  
4805 The TSF must be identified (done as part of the TOE design (ADV\_TDS) work units) in order to  
4806 identify the TSFI. This activity can be done at a high level to ensure that no large groups of  
4807 interfaces have been missed (network protocols, hardware interfaces, configuration files), or at a  
4808 low level as the evaluation of the functional specification proceeds.

4809 In making an assessment for this work unit, the evaluator determines that all portions of the TSF  
4810 are addressed in terms of the interfaces listed in the functional specification. All portions of the TSF  
4811 should have a corresponding interface description, or if there are no corresponding interfaces for a  
4812 portion of the TSF, the evaluator determines that that is acceptable.

4813 ISO/IEC 15408-3 ADV\_FSP.3.2C: *The functional specification shall describe the purpose and method*  
4814 *of use for all TSFI.*

4815 **11.4.3.3.3 Work unit ADV\_FSP.3-2**

4816 The evaluator **shall examine** the functional specification to determine that it states the purpose of  
4817 each TSFI.

4818 The purpose of a TSFI is a general statement summarising the functionality provided by the  
4819 interface. It is not intended to be a complete statement of the actions and results related to the  
4820 interface, but rather a statement to help the reader understand in general what the interface is  
4821 intended to be used for. The evaluator should not only determine that the purpose exists, but also

## ISO/IEC 18045:2008(E)

4822 that it accurately reflects the TSFI by taking into account other information about the interface,  
4823 such as the description of actions and error messages.

### 4824 11.4.3.3.4 Work unit ADV\_FSP.3-3

4825 The evaluator **shall examine** the functional specification to determine that the method of use for  
4826 each TSFI is given.

4827 The method of use for a TSFI summarises how the interface is manipulated in order to invoke the  
4828 actions and obtain the results associated with the TSFI. The evaluator should be able to determine,  
4829 from reading this material in the functional specification, how to use each interface. This does not  
4830 necessarily mean that there needs to be a separate method of use for each TSFI, as it may be  
4831 possible to describe in general how kernel calls are invoked, for instance, and then identify each  
4832 interface using that general style. Different types of interfaces will require different method of use  
4833 specifications. APIs, network protocol interfaces, system configuration parameters, and hardware  
4834 bus interfaces all have very different methods of use, and this should be taken into account by the  
4835 developer when developing the functional specification, as well as by the evaluator evaluating the  
4836 functional specification.

4837 For administrative interfaces whose functionality is documented as being inaccessible to untrusted  
4838 users, the evaluator ensures that the method of making the functions inaccessible is described in  
4839 the functional specification. It should be noted that this inaccessibility needs to be tested by the  
4840 developer in their test suite.

4841 The evaluator should not only determine that the set of method of use descriptions exist, but also  
4842 that they accurately cover each TSFI.

4843 ISO/IEC 15408-3 ADV\_FSP.3.3C: *The functional specification shall identify and describe all*  
4844 *parameters associated with each TSFI.*

### 4845 11.4.3.3.5 Work unit ADV\_FSP.3-4

4846 The evaluator **shall examine** the presentation of the TSFI to determine that it completely identifies  
4847 all parameters associated with every TSFI.

4848 The evaluator examines the functional specification to ensure that all of the parameters are  
4849 described for each TSFI. Parameters are explicit inputs or outputs to an interface that control the  
4850 behaviour of that interface. For examples, parameters are the arguments supplied to an API; the  
4851 various fields in packet for a given network protocol; the individual key values in the Windows  
4852 Registry; the signals across a set of pins on a chip; etc.

4853 In order to determine that all of the parameters are present in the TSFI, the evaluator should  
4854 examine the rest of the interface description (actions, error messages, etc.) to determine if the  
4855 effects of the parameter are accounted for in the description. The evaluator should also check other  
4856 evidence provided for the evaluation (e.g., TOE design, security architecture description,  
4857 operational user guidance, implementation representation) to see if behaviour or additional  
4858 parameters are described there but not in the functional specification.

### 4859 11.4.3.3.6 Work unit ADV\_FSP.3-5

4860 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
4861 accurately describes all parameters associated with every TSFI.

4862 Once all of the parameters have been identified, the evaluator needs to ensure that they are  
4863 accurately described, and that the description of the parameters is complete. A parameter  
4864 description tells what the parameter is in some meaningful way. For instance, the interface *foo(i)*  
4865 could be described as having "parameter i which is an integer"; this is not an acceptable parameter

description. A description such as "parameter i is an integer that indicates the number of users currently logged in to the system" is much more acceptable.

In order to determine that the description of the parameters is complete, the evaluator should examine the rest of the interface description (purpose, method of use, actions, error messages, etc.) to determine if the descriptions of the parameter(s) are accounted for in the description. The evaluator should also check other evidence provided (e.g., TOE design, architectural design, operational user guidance, implementation representation) to see if behaviour or additional parameters are described there but not in the functional specification.

ISO/IEC 15408-3 ADV\_FSP.3.4C: *For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.*

#### 11.4.3.3.7 Work unit ADV\_FSP.3-6

The evaluator **shall examine** the presentation of the TSFI to determine that it completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.

If an action available through an interface plays a role in enforcing any security policy on the TOE (that is, if one of the actions of the interface can be traced to one of the SFRs levied on the TSF), then that interface is *SFR-enforcing*. Such policies are not limited to the access control policies, but also refer to any functionality specified by one of the SFRs contained in the ST. Note that it is possible that an interface may have various actions and results, some of which may be SFR-enforcing and some of which may not.

The developer is not required to "label" interfaces as SFR-enforcing, and likewise is not required to identify actions available through an interface as SFR-enforcing. It is the evaluator's responsibility to examine the evidence provided by the developer and determine that the required information is present. In the case where the developer has identified the SFR-enforcing TSFI and SFR-enforcing actions available through those TSFI, the evaluator must judge completeness and accuracy based on other information supplied for the evaluation (e.g., TOE design, security architecture description, operational user guidance), and on the other information presented for the interfaces (parameters and parameter descriptions, error messages, etc.).

In this case (developer has provided only the SFR-enforcing information for SFR-enforcing TSFI) the evaluator also ensures that no interfaces have been mis-categorised. This is done by examining other information supplied for the evaluation (e.g., TOE design, security architecture description, operational user guidance), and the other information presented for the interfaces (parameters and parameter descriptions, for example) not labelled as SFR-enforcing. The analysis done for work units ADV\_FSP.3-7 and ADV\_FSP.3-8 are also used in making this determination.

In the case where the developer has provided the same level of information on all interfaces, the evaluator performs the same type of analysis mentioned in the previous paragraphs. The evaluator should determine which interfaces are SFR-enforcing and which are not, and subsequently ensure that the SFR-enforcing aspects of the SFR-enforcing actions are appropriately described. Note that in this case, the evaluator should be able to perform the bulk of the work associated with work unit ADV\_FSP.3-8 in the course of performing this SFR-enforcing analysis.

The SFR-enforcing actions are those that are visible at any external interface and that provide for the enforcement of the SFRs being claimed. For example, if audit requirements are included in the ST, then audit-related actions would be SFR-enforcing and therefore must be described, even if the result of that action is generally not visible through the invoked interface (as is often the case with audit, where a user action at one interface would produce an audit record visible at another interface).

The level of description that is required is that sufficient for the reader to understand what role the TSFI actions play with respect to the SFR. The evaluator should keep in mind that the description should be detailed enough to support the generation (and assessment) of test cases against that

## ISO/IEC 18045:2008(E)

4914 interface. If the description is unclear or lacking detail such that meaningful testing cannot be  
4915 conducted against the TSFI, it is likely that the description is inadequate.

4916 ISO/IEC 15408-3 ADV\_FSP.3.5C: *For each SFR-enforcing TSFI, the functional specification shall*  
4917 *describe direct error messages resulting from SFR-enforcing actions and exceptions associated with*  
4918 *invocation of the TSFI.*

### 4919 11.4.3.3.8 Work unit ADV\_FSP.3-7

4920 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
4921 accurately describes error messages that may result from an invocation of each SFR-enforcing TSFI.

4922 This work unit should be performed in conjunction with, or after, work unit ADV\_FSP.3-6 in order  
4923 to ensure the set of SFR-enforcing TSFI is correctly identified. The evaluator should note that the  
4924 requirement and associated work unit is that all direct error messages associated with an SFR-  
4925 enforcing TSFI must be described, that are associated with SFR-enforcing actions. This is because  
4926 at this level of assurance, the “extra” information provided by the error message descriptions  
4927 should be used in determining whether all of the SFR-enforcing aspects of an interface have been  
4928 appropriately described. For instance, if an error message associated with a TSFI (e.g., “access  
4929 denied”) indicated that an SFR-enforcing decision or action had taken place, but in the description  
4930 of the SFR-enforcing actions there was no mention of that particular SFR-enforcing mechanism,  
4931 then the description may not be complete.

4932 Errors can take many forms, depending on the interface being described. For an API, the interface  
4933 itself may return an error code, set a global error condition, or set a certain parameter with an  
4934 error code. For a configuration file, an incorrectly configured parameter may cause an error  
4935 message to be written to a log file. For a hardware PCI card, an error condition may raise a signal  
4936 on the bus, or trigger an exception condition to the CPU.

4937 Errors (and the associated error messages) come about through the invocation of an interface. The  
4938 processing that occurs in response to the interface invocation may encounter error conditions,  
4939 which trigger (through an implementation-specific mechanism) an error message to be generated.  
4940 In some instances this may be a return value from the interface itself; in other instances a global  
4941 value may be set and checked after the invocation of an interface. It is likely that a TOE will have a  
4942 number of low-level error messages that may result from fundamental resource conditions, such as  
4943 “disk full” or “resource locked”. While these error messages may map to a large number of TSFI,  
4944 they could be used to detect instances where detail from an interface description has been omitted.  
4945 For instance, a TSFI that produces a “disk full” message, but has no obvious description of why that  
4946 TSFI should cause an access to the disk in its description of actions, might cause the evaluator to  
4947 examine other evidence (Security Architecture (ADV\_ARC), TOE design (ADV\_TDS)) related that  
4948 TSFI to determine if the description is accurate.

4949 In order to determine that the description of the error messages of a TSFI is accurate and complete,  
4950 the evaluator measures the interface description against the other evidence provided for the  
4951 evaluation (e.g., TOE design, security architecture description, operational user guidance), as well  
4952 as for other evidence supplied for that TSFI (description of SFR-enforcing actions, summary of SFR-  
4953 supporting and SFR-non-interfering actions and results).

4954 ISO/IEC 15408-3 ADV\_FSP.3.6C: *The functional specification shall summarise the SFR-supporting*  
4955 *and SFR-non-interfering actions associated with each TSFI.*

### 4956 11.4.3.3.9 Work unit ADV\_FSP.3-8

4957 The evaluator **shall examine** the presentation of the TSFI to determine that it summarises the SFR-  
4958 supporting and SFR-non-interfering actions associated with each TSFI.

4959 The purpose of this work unit is to supplement the details about the SFR-enforcing actions  
4960 (provided in work unit ADV\_FSP.3-6) with a summary of the remaining actions (i.e., those that are



not SFR-enforcing). This covers *all* SFR-supporting and SFR-non-interfering actions, whether invocable through SFR-enforcing TSFI or through SFR-supporting or SFR-non-interfering TSFI. Such a summary about all SFR-supporting and SFR-non-interfering actions helps to provide a more complete picture of the functions provided by the TSF, and is to be used by the evaluator in determining whether an action or TSFI may have been mis-categorised.

The information to be provided is more abstract than that required for SFR-enforcing actions. While it should still be detailed enough so that the reader can understand what the action does, the description does not have to be detailed enough to support writing tests against it, for instance. For the evaluator, the key is that the information must be sufficient to make a positive determination that the action is SFR-supporting or SFR-non-interfering. If that level of information is missing, the summary is insufficient and more information must be obtained.

ISO/IEC 15408-3 ADV\_FSP.3.7C: *The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.*

#### 11.4.3.3.10 Work unit ADV\_FSP.3-9

The evaluator **shall check** that the tracing links the SFRs to the corresponding TSFIs.

The tracing is provided by the developer to serve as a guide to which SFRs are related to which TSFIs. This tracing can be as simple as a table; it is used as input to the evaluator for use in the following work units, in which the evaluator verifies its completeness and accuracy.

#### 11.4.3.4 Action ADV\_FSP.3.2E

##### 11.4.3.4.1 Work unit ADV\_FSP.3-10

The evaluator **shall examine** the functional specification to determine that it is a complete instantiation of the SFRs.

To ensure that all SFRs are covered by the functional specification, as well as the test coverage analysis, the evaluator may build upon the developer's tracing (see ADV\_FSP.3-9 a map between the TOE security functional requirements and the TSFI. Note that this map may have to be at a level of detail below the component or even element level of the requirements, because of operations (assignments, refinements, selections) performed on the functional requirement by the ST author.

For example, the FDP\_ACC.1 component contains an element with assignments. If the ST contained, for instance, ten rules in the FDP\_ACC.1 assignment, and these ten rules were covered by three different TSFI, it would be inadequate for the evaluator to map FDP\_ACC.1 to TSFI A, B, and C and claim they had completed the work unit. Instead, the evaluator would map FDP\_ACC.1 (rule 1) to TSFI A; FDP\_ACC.1 (rule 2) to TSFI B; etc. It might also be the case that the interface is a wrapper interface (e.g., IOCTL), in which case the mapping would need to be specific to certain set of parameters for a given interface.

The evaluator must recognise that for requirements that have little or no manifestation at the TSF boundary (e.g., FDP\_RIP) it is not expected that they completely map those requirements to the TSFI. The analysis for those requirements will be performed in the analysis for the TOE design (ADV\_TDS) when included in the ST. It is also important to note that since the parameters, actions, and error messages associated with TSFIs must be fully specified, the evaluator should be able to determine if all aspects of an SFR appear to be implemented at the interface level.

##### 11.4.3.4.2 Work unit ADV\_FSP.3-11

The evaluator **shall examine** the functional specification to determine that it is an accurate instantiation of the SFRs.

## ISO/IEC 18045:2008(E)

5004 For each functional requirement in the ST that results in effects visible at the TSF boundary, the  
5005 information in the associated TSFI for that requirement specifies the required functionality  
5006 described by the requirement. For example, if the ST contains a requirement for access control lists,  
5007 and the only TSFI that map to that requirement specify functionality for Unix-style protection bits,  
5008 then the functional specification is not accurate with respect to the requirements.

5009 The evaluator must recognise that for requirements that have little or no manifestation at the TSF  
5010 boundary (e.g., FDP\_RIP) it is not expected that the evaluator completely map those requirements  
5011 to the TSFI. The analysis for those requirements will be performed in the analysis for the TOE  
5012 design (ADV\_TDS) when included in the ST.

### 5013 **11.4.4 Evaluation of sub-activity (ADV\_FSP.4)**

#### 5014 **11.4.4.1 Objectives**

5015 The objective of this sub-activity is to determine whether the developer has completely described  
5016 all of the TSFI in a manner such that the evaluator is able to determine whether the TSFI are  
5017 completely and accurately described, and appears to implement the security functional  
5018 requirements of the ST.

#### 5019 **11.4.4.2 Input**

5020 The evaluation evidence for this sub-activity that is required by the work-units is:

- 5021 a) the ST;
- 5022 b) the functional specification;
- 5023 c) the TOE design.

5024 The evaluation evidence for this sub-activity that is used if included in the ST for the TOE is:

- 5025 a) the security architecture description;
- 5026 b) the implementation representation;
- 5027 c) the TSF internals description;
- 5028 d) the operational user guidance;

#### 5029 **11.4.4.3 Application notes**

5030 The functional specification describes the interfaces to the TSF (the TSFI) in a structured manner.  
5031 Because of the dependency on Evaluation of sub-activity (ADV\_TDS.1), the evaluator is expected to  
5032 have identified the TSF prior to beginning work on this sub-activity. Without firm knowledge of  
5033 what comprises the TSF, it is not possible to assess the completeness of the TSFI.

5034 In performing the various work units included in this family, the evaluator is asked to make  
5035 assessments of accuracy and completeness of several factors (the TSFI itself, as well as the  
5036 individual components (parameters, actions, error messages, etc.) of the TSFI). In doing this  
5037 analysis, the evaluator is expected to use the documentation provided for the evaluation. This  
5038 includes the ST, the TOE design, and may include other documentation such as the operational user  
5039 guidance, security architecture description, and implementation representation. The  
5040 documentation should be examined in an iterative fashion. The evaluator may read, for example, in

the TOE design how a certain function is implemented, but see no way to invoke that function from the interface. This might cause the evaluator to question the completeness of a particular TSFI description, or whether an interface has been left out of the functional specification altogether. Describing analysis activities of this sort in the ETR is a key method in providing rationale that the work units have been performed appropriately.

It should be recognised that there exist functional requirements whose functionality is manifested wholly or in part architecturally, rather than through a specific mechanism. An example of this is the implementation of mechanisms implementing the Residual information protection (FDP\_RIP) requirements. Such mechanisms typically are implemented to ensure a behaviour isn't present, which is difficult to test and typically is verified through analysis. In the cases where such functional requirements are included in the ST, it is expected that the evaluator recognise that there may be SFRs of this type that have no interfaces, and that this should not be considered a deficiency in the functional specification.

#### 11.4.4.4 Action ADV\_FSP.4.1E

##### 11.4.4.4.1 General

ISO/IEC 15408-3 ADV\_FSP.4.1C: *The functional specification shall completely represent the TSF.*

##### 11.4.4.4.2 Work unit ADV\_FSP.4-1

The evaluator **shall examine** the functional specification to determine that the TSF is fully represented.

The identification of the TSFI is a necessary prerequisite to all other activities in this sub-activity. The TSF must be identified (done as part of the TOE design (ADV\_TDS) work units) in order to identify the TSFI. This activity can be done at a high level to ensure that no large groups of interfaces have been missed (network protocols, hardware interfaces, configuration files), or at a low level as the evaluation of the functional specification proceeds.

In making an assessment for this work unit, the evaluator determines that all portions of the TSF are addressed in terms of the interfaces listed in the functional specification. All portions of the TSF should have a corresponding interface description, or if there are no corresponding interfaces for a portion of the TSF, the evaluator determines that that is acceptable.

ISO/IEC 15408-3 ADV\_FSP.4.2C: *The functional specification shall describe the purpose and method of use for all TSFI.*

##### 11.4.4.4.3 Work unit ADV\_FSP.4-2

The evaluator **shall examine** the functional specification to determine that it states the purpose of each TSFI.

The purpose of a TSFI is a general statement summarising the functionality provided by the interface. It is not intended to be a complete statement of the actions and results related to the interface, but rather a statement to help the reader understand in general what the interface is intended to be used for. The evaluator should not only determine that the purpose exists, but also that it accurately reflects the TSFI by taking into account other information about the interface, such as the description of actions and error messages.

##### 11.4.4.4.4 Work unit ADV\_FSP.4-3

The evaluator **shall examine** the functional specification to determine that the method of use for each TSFI is given.

5083 The method of use for a TSFI summarises how the interface is manipulated in order to invoke the  
5084 actions and obtain the results associated with the TSFI. The evaluator should be able to determine,  
5085 from reading this material in the functional specification, how to use each interface. This does not  
5086 necessarily mean that there needs to be a separate method of use for each TSFI, as it may be  
5087 possible to describe in general how kernel calls are invoked, for instance, and then identify each  
5088 interface using that general style. Different types of interfaces will require different method of use  
5089 specifications. APIs, network protocol interfaces, system configuration parameters, and hardware  
5090 bus interfaces all have very different methods of use, and this should be taken into account by the  
5091 developer when developing the functional specification, as well as by the evaluator evaluating the  
5092 functional specification.

5093 For administrative interfaces whose functionality is documented as being inaccessible to untrusted  
5094 users, the evaluator ensures that the method of making the functions inaccessible is described in  
5095 the functional specification. It should be noted that this inaccessibility needs to be tested by the  
5096 developer in their test suite.

5097 The evaluator should not only determine that the set of method of use descriptions exist, but also  
5098 that they accurately cover each TSFI.

#### 5099 11.4.4.4.5 Work unit ADV\_FSP.4-4

5100 The evaluator **shall examine** the functional specification to determine the completeness of the  
5101 TSFI

5102 The evaluator shall use the design documentation to identify the possible types of interfaces. The  
5103 evaluator shall search the design documentation and the guidance documentation for potential  
5104 TSFI not contained in the developer's documentation, thus indicating that the set of TSFI defined  
5105 by the developer is incomplete. The evaluator **shall examine** the arguments presented by the  
5106 developer that the TSFI is complete and check down to the lowest level of design or with the  
5107 implementation representation that no additional TSFI exist.

5108 ISO/IEC 15408-3 ADV\_FSP.4.3C: *The functional specification shall identify and describe all*  
5109 *parameters associated with each TSFI.*

#### 5110 11.4.4.4.6 Work unit ADV\_FSP.4-5

5111 The evaluator **shall examine** the presentation of the TSFI to determine that it completely identifies  
5112 all parameters associated with every TSFI.

5113 The evaluator examines the functional specification to ensure that all of the parameters are  
5114 described for each TSFI. Parameters are explicit inputs or outputs to an interface that control the  
5115 behaviour of that interface. For examples, parameters are the arguments supplied to an API; the  
5116 various fields in packet for a given network protocol; the individual key values in the Windows  
5117 Registry; the signals across a set of pins on a chip; etc.

5118 In order to determine that all of the parameters are present in the TSFI, the evaluator should  
5119 examine the rest of the interface description (actions, error messages, etc.) to determine if the  
5120 effects of the parameter are accounted for in the description. The evaluator should also check other  
5121 evidence provided for the evaluation (e.g., TOE design, security architecture description,  
5122 operational user guidance, implementation representation) to see if behaviour or additional  
5123 parameters are described there but not in the functional specification.

#### 5124 11.4.4.4.7 Work unit ADV\_FSP.4-6

5125 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
5126 accurately describes all parameters associated with every TSFI.

5127 Once all of the parameters have been identified, the evaluator needs to ensure that they are  
 5128 accurately described, and that the description of the parameters is complete. A parameter  
 5129 description tells what the parameter is in some meaningful way. For instance, the interface *foo(i)*  
 5130 could be described as having "parameter i which is an integer"; this is not an acceptable parameter  
 5131 description. A description such as "parameter i is an integer that indicates the number of users  
 5132 currently logged in to the system" is much more acceptable.

5133 In order to determine that the description of the parameters is complete, the evaluator should  
 5134 examine the rest of the interface description (purpose, method of use, actions, error messages, etc.)  
 5135 to determine if the descriptions of the parameter(s) are accounted for in the description. The  
 5136 evaluator should also check other evidence provided (e.g., TOE design, architectural design,  
 5137 operational user guidance, implementation representation) to see if behaviour or additional  
 5138 parameters are described there but not in the functional specification.

5139 ISO/IEC 15408-3 ADV\_FSP.4.4C: *The functional specification shall describe all actions associated*  
 5140 *with each TSFI.*

#### 5141 11.4.4.4.8 Work unit ADV\_FSP.4-7

5142 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
 5143 accurately describes all actions associated with every TSFI.

5144 The evaluator checks to ensure that all of the actions are described. actions available through an  
 5145 interface describe what the interface does (as opposed to the TOE design, which describes how the  
 5146 actions are provided by the TSFI).

5147 Actions of an interface describe functionality that can be invoked through the interface, and can be  
 5148 categorised as *regular* actions, and *SFR-related* actions. Regular actions are descriptions of what  
 5149 the interface does. The amount of information provided for this description is dependant on the  
 5150 complexity of the interface. The SFR-related actions are those that are visible at any external  
 5151 interface (for instance, audit activity caused by the invocation of an interface (assuming audit  
 5152 requirements are included in the ST) should be described, even though the result of that action is  
 5153 generally not visible through the invoked interface). Depending on the parameters of an interface,  
 5154 there may be many different actions able to be invoked through the interface (for instance, an API  
 5155 might have the first parameter be a "subcommand", and the following parameters be specific to  
 5156 that subcommand. The IOCTL API in some Unix systems is an example of such an interface).

5157 In order to determine that the description of the actions of a TSFI is complete, the evaluator should  
 5158 review the rest of the interface description (parameter descriptions, error messages, etc.) to  
 5159 determine if the actions described are accounted for. The evaluator should also analyse other  
 5160 evidence provided for the evaluation (e.g., TOE design, security architecture description,  
 5161 operational user guidance, implementation representation) to see if there is evidence of actions  
 5162 that are described there but not in the functional specification.

5163 ISO/IEC 15408-3 ADV\_FSP.4.5C: *The functional specification shall describe all direct error messages*  
 5164 *that may result from an invocation of each TSFI.*

#### 5165 11.4.4.4.9 Work unit ADV\_FSP.4-8

5166 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
 5167 accurately describes all error messages resulting from an invocation of each TSFI.

5168 Errors can take many forms, depending on the interface being described. For an API, the interface  
 5169 itself may return an error code; set a global error condition, or set a certain parameter with an  
 5170 error code. For a configuration file, an incorrectly configured parameter may cause an error  
 5171 message to be written to a log file. For a hardware PCI card, an error condition may raise a signal  
 5172 on the bus, or trigger an exception condition to the CPU.

5173 Errors (and the associated error messages) come about through the invocation of an interface. The  
 5174 processing that occurs in response to the interface invocation may encounter error conditions,  
 5175 which trigger (through an implementation-specific mechanism) an error message to be generated.  
 5176 In some instances this may be a return value from the interface itself; in other instances a global  
 5177 value may be set and checked after the invocation of an interface. It is likely that a TOE will have a  
 5178 number of low-level error messages that may result from fundamental resource conditions, such as  
 5179 "disk full" or "resource locked". While these error messages may map to a large number of TSFI,  
 5180 they could be used to detect instances where detail from an interface description has been omitted.  
 5181 For instance, a TSFI that produces a "disk full" message, but has no obvious description of why that  
 5182 TSFI should cause an access to the disk in its description of actions, might cause the evaluator to  
 5183 examine other evidence (Security Architecture (ADV\_ARC), TOE design (TOE\_TDS)) related that  
 5184 TSFI to determine if the description is complete and accurate.

5185 The evaluator determines that, for each TSFI, the exact set of error messages that can be returned  
 5186 on invoking that interface can be determined. The evaluator reviews the evidence provided for the  
 5187 interface to determine if the set of errors seems complete. They cross-check this information with  
 5188 other evidence provided for the evaluation (e.g., TOE design, security architecture description,  
 5189 operational user guidance, implementation representation) to ensure that there are no errors  
 5190 steaming from processing mentioned that are not included in the functional specification.

#### 5191 11.4.4.4.10 Work unit ADV\_FSP.4-9

5192 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
 5193 accurately describes the meaning of all error messages resulting from an invocation of each TSFI.

5194 In order to determine accuracy, the evaluator must be able to understand meaning of the error. For  
 5195 example, if an interface returns a numeric code of 0, 1, or 2, the evaluator would not be able to  
 5196 understand the error if the functional specification only listed: "possible errors resulting from  
 5197 invocation of the *foo()* interface are 0, 1, or 2". Instead the evaluator checks to ensure that the  
 5198 errors are described such as: "possible errors resulting from invocation of the *foo()* interface are 0  
 5199 (processing successful), 1 (file not found), or 2 (incorrect filename specification)".

5200 In order to determine that the description of the errors due to invoking a TSFI is complete, the  
 5201 evaluator examines the rest of the interface description (parameter descriptions, actions, etc.) to  
 5202 determine if potential error conditions that might be caused by using such an interface are  
 5203 accounted for. The evaluator also checks other evidence provided for the evaluation (e.g. TOE  
 5204 design, security architecture description, operational user guidance, implementation  
 5205 representation) to see if error processing related to the TSFI is described there but is not described  
 5206 in the functional specification.

5207 ISO/IEC 15408-3 ADV\_FSP.4.6C: *The tracing shall demonstrate that the SFRs trace to TSFIs in the*  
 5208 *functional specification.*

#### 5209 11.4.4.4.11 Work unit ADV\_FSP.4-10

5210 The evaluator **shall check** that the tracing links the SFRs to the corresponding TSFIs.

5211 The tracing is provided by the developer to serve as a guide to which SFRs are related to which  
 5212 TSFIs. This tracing can be as simple as a table; it is used as input to the evaluator for use in the  
 5213 following work units, in which the evaluator verifies its completeness and accuracy.

#### 5214 11.4.4.5 Action ADV\_FSP.4.2E

##### 5215 11.4.4.5.1 Work unit ADV\_FSP.4-11

5216 The evaluator **shall examine** the functional specification to determine that it is a complete  
 5217 instantiation of the SFRs.

5218 To ensure that all SFRs are covered by the functional specification, as well as the test coverage  
 5219 analysis, the evaluator may build upon the developer's tracing (see ADV\_FSP.4-10 a map between  
 5220 the TOE security functional requirements and the TSFI. Note that this map may have to be at a level  
 5221 of detail below the component or even element level of the requirements, because of operations  
 5222 (assignments, refinements, selections) performed on the functional requirement by the ST author.

5223 For example, the FDP\_ACC.1 component contains an element with assignments. If the ST contained,  
 5224 for instance, ten rules in the FDP\_ACC.1 assignment, and these ten rules were covered by three  
 5225 different TSFI, it would be inadequate for the evaluator to map FDP\_ACC.1 to TSFI A, B, and C and  
 5226 claim they had completed the work unit. Instead, the evaluator would map FDP\_ACC.1 (rule 1) to  
 5227 TSFI A; FDP\_ACC.1 (rule 2) to TSFI B; etc. It might also be the case that the interface is a wrapper  
 5228 interface (e.g., IOCTL), in which case the mapping would need to be specific to certain set of  
 5229 parameters for a given interface.

5230 The evaluator must recognise that for requirements that have little or no manifestation at the TSF  
 5231 boundary (e.g., FDP\_RIP) it is not expected that they completely map those requirements to the  
 5232 TSFI. The analysis for those requirements will be performed in the analysis for the TOE design  
 5233 (ADV\_TDS) when included in the ST. It is also important to note that since the parameters, actions,  
 5234 and error messages associated with TSFIs must be fully specified, the evaluator should be able to  
 5235 determine if all aspects of an SFR appear to be implemented at the interface level.

#### 5236 11.4.4.5.2 Work unit ADV\_FSP.4-12

5237 The evaluator *shall examine* the functional specification to determine that it is an accurate  
 5238 instantiation of the SFRs.

5239 For each functional requirement in the ST that results in effects visible at the TSF boundary, the  
 5240 information in the associated TSFI for that requirement specifies the required functionality  
 5241 described by the requirement. For example, if the ST contains a requirement for access control lists,  
 5242 and the only TSFI that map to that requirement specify functionality for Unix-style protection bits,  
 5243 then the functional specification is not accurate with respect to the requirements.

5244 The evaluator must recognise that for requirements that have little or no manifestation at the TSF  
 5245 boundary (e.g., FDP\_RIP) it is not expected that the evaluator completely map those requirements  
 5246 to the TSFI. The analysis for those requirements will be performed in the analysis for the TOE  
 5247 design (ADV\_TDS) when included in the ST.

#### 5248 11.4.5 Evaluation of sub-activity (ADV\_FSP.5)

##### 5249 11.4.5.1 Objectives

5250 The objective of this sub-activity is to determine whether the developer has completely described  
 5251 all of the TSFI in a manner such that the evaluator is able to determine whether the TSFI are  
 5252 completely and accurately described, and appears to implement the security functional  
 5253 requirements of the ST. The completeness of the interfaces is judged based upon the  
 5254 implementation representation.

##### 5255 11.4.5.2 Input

5256 The evaluation evidence for this sub-activity that is required by the work-units is:

- 5257 a) the ST;
- 5258 b) the functional specification;
- 5259 c) the TOE design;

## ISO/IEC 18045:2008(E)

5260 d) the implementation representation.

5261 The evaluation evidence for this sub-activity that is used if included in the ST for the TOE is:

5262 a) the security architecture description;

5263 b) the TSF internals description;

5264 c) the formal security policy model;

5265 d) the operational user guidance;

### 5266 11.4.5.3 Action ADV\_FSP.5.1E

#### 5267 11.4.5.3.1 General

5268 ISO/IEC 15408-3 ADV\_FSP.5.1C: *The functional specification shall completely represent the TSF.*

#### 5269 11.4.5.3.2 Work unit ADV\_FSP.5-1

5270 The evaluator **shall examine** the functional specification to determine that the TSF is fully  
5271 represented.

5272 The identification of the TSFI is a necessary prerequisite to all other activities in this sub-activity.  
5273 The TSF must be identified (done as part of the TOE design (TOE\_TDS) work units) in order to  
5274 identify the TSFI. This activity can be done at a high level to ensure that no large groups of  
5275 interfaces have been missed (network protocols, hardware interfaces, configuration files), or at a  
5276 low level as the evaluation of the functional specification proceeds.

5277 In making an assessment for this work unit, the evaluator determines that all portions of the TSF  
5278 are addressed in terms of the interfaces listed in the functional specification. All portions of the TSF  
5279 should have a corresponding interface description, or if there are no corresponding interfaces for a  
5280 portion of the TSF, the evaluator determines that that is acceptable.

5281 ISO/IEC 15408-3 ADV\_FSP.5.2C: *The functional specification shall describe the TSFI using a semi-*  
5282 *formal style.*

#### 5283 11.4.5.3.3 Work unit ADV\_FSP.5-2

5284 The evaluator **shall examine** the functional specification to determine that it is presented using a  
5285 semiformal style.

5286 A semi-formal presentation is characterised by a standardised format with a well-defined syntax  
5287 that reduces ambiguity that may occur in informal presentations. Since the intent of the semi-  
5288 formal format is to enhance the reader's ability to understand the presentation, use of certain  
5289 structured presentation methods (pseudo-code, flow charts, block diagrams) are appropriate,  
5290 though not required.

5291 For the purposes of this activity, the evaluator should ensure that the interface descriptions are  
5292 formatted in a structured, consistent manner and use common terminology. A semiformal  
5293 presentation of the interfaces also implies that the level of detail of the presentation for the  
5294 interfaces is largely consistent across all TSFI. For the functional specification, it is acceptable to  
5295 refer to external specifications for portions of the interface as long as those external specifications  
5296 are themselves semiformal.



5297 ISO/IEC 15408-3 ADV\_FSP.5.3C: *The functional specification shall describe the purpose and method*  
 5298 *of use for all TSFI.*

#### 5299 11.4.5.3.4 Work unit ADV\_FSP.5-3

5300 The evaluator **shall examine** the functional specification to determine that it states the purpose of  
 5301 each TSFI.

5302 The purpose of a TSFI is a general statement summarising the functionality provided by the  
 5303 interface. It is not intended to be a complete statement of the actions and results related to the  
 5304 interface, but rather a statement to help the reader understand in general what the interface is  
 5305 intended to be used for. The evaluator should not only determine that the purpose exists, but also  
 5306 that it accurately reflects the TSFI by taking into account other information about the interface,  
 5307 such as the description of actions and error messages.

#### 5308 Work unit ADV\_FSP.5-4

5309 The evaluator **shall examine** the functional specification to determine that the method of use for  
 5310 each TSFI is given.

5311 The method of use for a TSFI summarises how the interface is manipulated in order to invoke the  
 5312 actions and obtain the results associated with the TSFI. The evaluator should be able to determine,  
 5313 from reading this material in the functional specification, how to use each interface. This does not  
 5314 necessarily mean that there needs to be a separate method of use for each TSFI, as it may be  
 5315 possible to describe in general how kernel calls are invoked, for instance, and then identify each  
 5316 interface using that general style. Different types of interfaces will require different method of use  
 5317 specifications. APIs, network protocol interfaces, system configuration parameters, and hardware  
 5318 bus interfaces all have very different methods of use, and this should be taken into account by the  
 5319 developer when developing the functional specification, as well as by the evaluator evaluating the  
 5320 functional specification.

5321 For administrative interfaces whose functionality is documented as being inaccessible to untrusted  
 5322 users, the evaluator ensures that the method of making the functions inaccessible is described in  
 5323 the functional specification. It should be noted that this inaccessibility needs to be tested by the  
 5324 developer in their test suite.

5325 The evaluator should not only determine that the set of method of use descriptions exist, but also  
 5326 that they accurately cover each TSFI.

#### 5327 11.4.5.3.5 Work unit ADV\_FSP.5-5

5328 The evaluator **shall examine** the functional specification to determine the completeness of the  
 5329 TSFI

5330 The evaluator shall use the design documentation to identify the possible types of interfaces. The  
 5331 evaluator shall search the design documentation and the guidance documentation for potential  
 5332 TSFI not contained in the developer's documentation, thus indicating that the set of TSFI defined  
 5333 by the developer is incomplete. The evaluator **shall examine** the arguments presented by the  
 5334 developer that the TSFI is complete and check down to the lowest level of design or with the  
 5335 implementation representation that no additional TSFI exist.

5336 ISO/IEC 15408-3 ADV\_FSP.5.4C: *The functional specification shall identify and describe all*  
 5337 *parameters associated with each TSFI.*

#### 5338 11.4.5.3.6 Work unit ADV\_FSP.5-6

5339 The evaluator **shall examine** the presentation of the TSFI to determine that it completely identifies  
 5340 all parameters associated with every TSFI.

5341 The evaluator examines the functional specification to ensure that all of the parameters are  
 5342 described for each TSFI. Parameters are explicit inputs or outputs to an interface that control the  
 5343 behaviour of that interface. For examples, parameters are the arguments supplied to an API; the  
 5344 various fields in packet for a given network protocol; the individual key values in the Windows  
 5345 Registry; the signals across a set of pins on a chip; etc.

5346 In order to determine that all of the parameters are present in the TSFI, the evaluator should  
 5347 examine the rest of the interface description (actions, error messages, etc.) to determine if the  
 5348 effects of the parameter are accounted for in the description. The evaluator should also check other  
 5349 evidence provided for the evaluation (e.g., TOE design, security architecture description,  
 5350 operational user guidance, implementation representation) to see if behaviour or additional  
 5351 parameters are described there but not in the functional specification.

#### 5352 11.4.5.3.7 Work unit ADV\_FSP.5-7

5353 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
 5354 accurately describes all parameters associated with every TSFI.

5355 Once all of the parameters have been identified, the evaluator needs to ensure that they are  
 5356 accurately described, and that the description of the parameters is complete. A parameter  
 5357 description tells what the parameter is in some meaningful way. For instance, the interface *foo(i)*  
 5358 could be described as having “parameter i which is an integer”; this is not an acceptable parameter  
 5359 description. A description such as “parameter i is an integer that indicates the number of users  
 5360 currently logged in to the system”. is much more acceptable.

5361 In order to determine that the description of the parameters is complete, the evaluator should  
 5362 examine the rest of the interface description (purpose, method of use, actions, error messages, etc.)  
 5363 to determine if the descriptions of the parameter(s) are accounted for in the description. The  
 5364 evaluator should also check other evidence provided (e.g., TOE design, architectural design,  
 5365 operational user guidance, implementation representation) to see if behaviour or additional  
 5366 parameters are described there but not in the functional specification.

5367 ISO/IEC 15408-3 ADV\_FSP.5.5C: *The functional specification shall describe all actions associated*  
 5368 *with each TSFI.*

#### 5369 11.4.5.3.8 Work unit ADV\_FSP.5-8

5370 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
 5371 accurately describes all actions associated with every TSFI.

5372 The evaluator checks to ensure that all of the actions are described. actions available through an  
 5373 interface describe what the interface does (as opposed to the TOE design, which describes how the  
 5374 actions are provided by the TSF).

5375 actions of an interface describe functionality that can be invoked through the interface, and can be  
 5376 categorised as *regular* actions, and *SFR-related* actions. Regular actions are descriptions of what  
 5377 the interface does. The amount of information provided for this description is dependant on the  
 5378 complexity of the interface. The SFR-related actions are those that are visible at any external  
 5379 interface (for instance, audit activity caused by the invocation of an interface (assuming audit  
 5380 requirements are included in the ST) should be described, even though the result of that action is  
 5381 generally not visible through the invoked interface). Depending on the parameters of an interface,  
 5382 there may be many different actions able to be invoked through the interface (for instance, an API  
 5383 might have the first parameter be a “subcommand”, and the following parameters be specific to  
 5384 that subcommand. The IOCTL API in some Unix systems is an example of such an interface).

5385 In order to determine that the description of the actions of a TSFI is complete, the evaluator should  
 5386 review the rest of the interface description (parameter descriptions, error messages, etc.) to  
 5387 determine if the actions described are accounted for. The evaluator should also analyse other

5388 evidence provided for the evaluation (e.g., TOE design, security architecture description,  
5389 operational user guidance, implementation representation) to see if there is evidence of actions  
5390 that are described there but not in the functional specification.

5391 ISO/IEC 15408-3 ADV\_FSP.5.6C: *The functional specification shall describe all direct error messages*  
5392 *that may result from an invocation of each TSFI.*

#### 5393 11.4.5.3.9 Work unit ADV\_FSP.5-9

5394 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
5395 accurately describes all error messages resulting from an invocation of each TSFI.

5396 Errors can take many forms, depending on the interface being described. For an API, the interface  
5397 itself may return an error code; set a global error condition, or set a certain parameter with an  
5398 error code. For a configuration file, an incorrectly configured parameter may cause an error  
5399 message to be written to a log file. For a hardware PCI card, an error condition may raise a signal  
5400 on the bus, or trigger an exception condition to the CPU.

5401 Errors (and the associated error messages) come about through the invocation of an interface. The  
5402 processing that occurs in response to the interface invocation may encounter error conditions,  
5403 which trigger (through an implementation-specific mechanism) an error message to be generated.  
5404 In some instances this may be a return value from the interface itself; in other instances a global  
5405 value may be set and checked after the invocation of an interface. It is likely that a TOE will have a  
5406 number of low-level error messages that may result from fundamental resource conditions, such as  
5407 “disk full” or “resource locked”. While these error messages may map to a large number of TSFI,  
5408 they could be used to detect instances where detail from an interface description has been omitted.  
5409 For instance, a TSFI that produces a “disk full” message, but has no obvious description of why that  
5410 TSFI should cause an access to the disk in its description of actions, might cause the evaluator to  
5411 examine other evidence (ADV\_ARC, ADV\_TDS) related that TSFI to determine if the description is  
5412 complete and accurate.

5413 The evaluator determines that, for each TSFI, the exact set of error messages that can be returned  
5414 on invoking that interface can be determined. The evaluator reviews the evidence provided for the  
5415 interface to determine if the set of errors seems complete. They cross-check this information with  
5416 other evidence provided for the evaluation (e.g., TOE design, security architecture description,  
5417 operational user guidance, implementation representation) to ensure that there are no errors  
5418 stemming from processing mentioned that are not included in the functional specification.

#### 5419 11.4.5.3.10 Work unit ADV\_FSP.5-10

5420 The evaluator **shall examine** the presentation of the TSFI to determine that it completely and  
5421 accurately describes the meaning of all error messages resulting from an invocation of each TSFI.

5422 In order to determine accuracy, the evaluator must be able to understand meaning of the error. For  
5423 example, if an interface returns a numeric code of 0, 1, or 2, the evaluator would not be able to  
5424 understand the error if the functional specification only listed: “possible errors resulting from  
5425 invocation of the *foo()* interface are 0, 1, or 2”. Instead the evaluator checks to ensure that the  
5426 errors are described such as: “possible errors resulting from invocation of the *foo()* interface are 0  
5427 (processing successful), 1 (file not found), or 2 (incorrect filename specification)”.

5428 In order to determine that the description of the errors due to invoking a TSFI is complete, the  
5429 evaluator examines the rest of the interface description (parameter descriptions, actions, etc.) to  
5430 determine if potential error conditions that might be caused by using such an interface are  
5431 accounted for. The evaluator also checks other evidence provided for the evaluation (e.g., TOE  
5432 design, security architecture description, operational user guidance, implementation  
5433 representation) to see if error processing related to the TSFI is described there but is not described  
5434 in the functional specification.

## ISO/IEC 18045:2008(E)

5435 ISO/IEC 15408-3 ADV\_FSP.5.7C: *The functional specification shall describe all error messages that*  
5436 *do not result from an invocation of a TSFI.*

### 5437 11.4.5.3.11 Work unit ADV\_FSP.5-11

5438 The evaluator **shall examine** the functional specification to determine that it completely and  
5439 accurately describes all error messages that do not result from an invocation of any TSFI.

5440 This work unit complements work unit ADV\_FSP.5-9, which describes those error messages that  
5441 result from an invocation of the TSFI. Taken together, these work units cover all error messages  
5442 that might be generated by the TSF.

5443 The evaluator assesses the completeness and accuracy of the functional specification by comparing  
5444 its contents to instances of error message generation within the implementation representation.  
5445 Most of these error messages will have already been covered by work unit ADV\_FSP.5-9.

5446 The error messages related to this work unit are typically those that are not expected to be  
5447 generated, but are constructed as a matter of good programming practises. For example, a case  
5448 statement that defines actions resulting from each of a list of cases may end with a final *else*  
5449 statement to apply to anything that might not be expected; this practise ensures the TSF does not  
5450 get into an undefined state. However, it is not expected that the path of execution would ever get to  
5451 this *else* statement; therefore, any error message generation within this *else* statement would never  
5452 be generated. Although it would not get generated, it must still be included in the functional  
5453 specification.

5454 ISO/IEC 15408-3 ADV\_FSP.5.8C: *The functional specification shall provide a rationale for each error*  
5455 *message contained in the TSF implementation yet does not result from an invocation of a TSFI.*

### 5456 11.4.5.3.12 Work unit ADV\_FSP.5-12

5457 The evaluator **shall examine** the functional specification to determine that it provides a rationale  
5458 for each error message contained in the TSF implementation yet does not result from an invocation  
5459 of a TSFI.

5460 The evaluator ensures that every error message found under work unit ADV\_FSP.5-11 contains a  
5461 rationale describing why it cannot be invoked from the TSFI.

5462 As was described in the previous work unit, this rationale might be as straightforward as the fact  
5463 that the error message in question is provided for completeness of execution logic and that it is  
5464 never expected to be generated. The evaluator ensures that the rationale for each such error  
5465 message is logical.

5466 ISO/IEC 15408-3 ADV\_FSP.5.9C: *The tracing shall demonstrate that the SFRs trace to TSFIs in the*  
5467 *functional specification.*

### 5468 11.4.5.3.13 Work unit ADV\_FSP.5-13

5469 The evaluator **shall check** that the tracing links the SFRs to the corresponding TSFIs.

5470 The tracing is provided by the developer to serve as a guide to which SFRs are related to which  
5471 TSFIs. This tracing can be as simple as a table; it is used as input to the evaluator for use in the  
5472 following work units, in which the evaluator verifies its completeness and accuracy.

5473 **11.4.5.4 Action ADV\_FSP.5.2E**5474 **11.4.5.4.1 Work unit ADV\_FSP.5-14**

5475 The evaluator *shall examine* the functional specification to determine that it is a complete  
5476 instantiation of the SFRs.

5477 To ensure that all SFRs are covered by the functional specification, as well as the test coverage  
5478 analysis, the evaluator may build upon the developer's tracing (see ADV\_FSP.5-13 a map between  
5479 the TOE security functional requirements and the TSFI. Note that this map may have to be at a level  
5480 of detail below the component or even element level of the requirements, because of operations  
5481 (assignments, refinements, selections) performed on the functional requirement by the ST author.

5482 For example, the FDP\_ACC.1 component contains an element with assignments. If the ST contained,  
5483 for instance, ten rules in the FDP\_ACC.1 assignment, and these ten rules were covered by three  
5484 different TSFI, it would be inadequate for the evaluator to map FDP\_ACC.1 to TSFI A, B, and C and  
5485 claim they had completed the work unit. Instead, the evaluator would map FDP\_ACC.1 (rule 1) to  
5486 TSFI A; FDP\_ACC.1 (rule 2) to TSFI B; etc. It might also be the case that the interface is a wrapper  
5487 interface (e.g., IOCTL), in which case the mapping would need to be specific to certain set of  
5488 parameters for a given interface.

5489 The evaluator must recognise that for requirements that have little or no manifestation at the TSF  
5490 boundary (e.g., FDP\_RIP) it is not expected that they completely map those requirements to the  
5491 TSFI. The analysis for those requirements will be performed in the analysis for the TOE design  
5492 (ADV\_TDS) when included in the ST. It is also important to note that since the parameters, actions,  
5493 and error messages associated with TSFIs must be fully specified, the evaluator should be able to  
5494 determine if all aspects of an SFR appear to be implemented at the interface level.

5495 **11.4.5.4.2 Work unit ADV\_FSP.5-15**

5496 The evaluator *shall examine* the functional specification to determine that it is an accurate  
5497 instantiation of the SFRs.

5498 For each functional requirement in the ST that results in effects visible at the TSF boundary, the  
5499 information in the associated TSFI for that requirement specifies the required functionality  
5500 described by the requirement. For example, if the ST contains a requirement for access control lists,  
5501 and the only TSFI that map to that requirement specify functionality for Unix-style protection bits,  
5502 then the functional specification is not accurate with respect to the requirements.

5503 The evaluator must recognise that for requirements that have little or no manifestation at the TSF  
5504 boundary (e.g., FDP\_RIP) it is not expected that the evaluator completely map those requirements  
5505 to the TSFI. The analysis for those requirements will be performed in the analysis for the TOE  
5506 design (ADV\_TDS) when included in the ST.

5507 **11.4.6 Evaluation of sub-activity (ADV\_FSP.6)**

5508 There is no general guidance; the scheme should be consulted for guidance on this sub-activity.

5509 **11.5 Implementation representation (ADV\_IMP)**5510 **11.5.1 Evaluation of sub-activity (ADV\_IMP.1)**5511 **11.5.1.1 Objectives**

5512 The objective of this sub-activity is to determine that the implementation representation made  
5513 available by the developer is suitable for use in other analysis activities; *suitability* is judged by its  
5514 conformance to the requirements for this component.

## ISO/IEC 18045:2008(E)

### 5515 11.5.1.2 Input

5516 The evaluation evidence for this sub-activity is:

- 5517 a) the implementation representation;
- 5518 b) the documentation of the development tools, as resulting from ALC\_TAT ;
- 5519 c) TOE design description.

### 5520 11.5.1.3 Application notes

5521 The entire implementation representation is made available to ensure that analysis activities are  
5522 not curtailed due to lack of information. This does not, however, imply that all of the representation  
5523 is examined when the analysis activities are being performed. This is likely impractical in almost all  
5524 cases, in addition to the fact that it most likely will not result in a higher-assurance TOE vs. targeted  
5525 sampling of the implementation representation. For this sub-activity, this is even truer. It would  
5526 not be productive for the evaluator to spend large amounts of time verifying the requirements for  
5527 one portion of the implementation representation, and then use a different portion of the  
5528 implementation representation in performing analysis for other work units. Therefore, the  
5529 evaluator is encouraged to select the sample of the implementation representation from the areas  
5530 of the TOE that will be of most interest during the analysis performed during work units from  
5531 other families (e.g. ATE\_IND, AVA\_VAN and ADV\_INT).

### 5532 11.5.1.4 Action ADV\_IMP.1.1E

5533 ISO/IEC 15408-3 ADV\_IMP.1.1C: *The implementation representation shall define the TSF to a level of*  
5534 *detail such that the TSF can be generated without further design decisions.*

#### 5535 11.5.1.4.1 Work unit ADV\_IMP.1-1

5536 The evaluator **shall check** that the implementation representation defines the TSF to a level of  
5537 detail such that the TSF can be generated without further design decisions.

5538 Source code or hardware diagrams and/or IC hardware design language code or layout data that  
5539 are used to build the actual hardware are examples of parts of an implementation representation.  
5540 The evaluator samples the implementation representation to gain confidence that it is at the  
5541 appropriate level and not, for instance, a pseudo-code level which requires additional design  
5542 decisions to be made. The evaluator is encouraged to perform a quick check when first looking at  
5543 the implementation representation to assure themselves that the developer has supplied all the  
5544 required information. However, the evaluator is also encouraged to perform the bulk of this check  
5545 while working on other work units that call for examining the implementation; this will ensure the  
5546 sample examined for this work unit is relevant.

5547 ISO/IEC 15408-3 ADV\_IMP.1.2C: *The implementation representation shall be in the form used by the*  
5548 *development personnel.*

#### 5549 11.5.1.4.2 Work unit ADV\_IMP.1-2

5550 The evaluator **shall check** that the implementation representation is in the form used by  
5551 development personnel.

5552 The implementation representation is manipulated by the developer in a form that is suitable for  
5553 transformation to the actual implementation. For instance, the developer may work with files  
5554 containing source code, which is eventually compiled to become part of the TSF. The developer  
5555 makes available the implementation representation in the form they use, so that the evaluator may

5556 use automated techniques in the analysis. This also increases the confidence that the  
 5557 implementation representation examined is actually the one used in the production of the TSF (as  
 5558 opposed to the case where it is supplied in an alternate presentation format, such as a word  
 5559 processor document). It should be noted that other forms of the implementation representation  
 5560 may also be used by the developer; these forms are supplied as well. The overall goal is to supply  
 5561 the evaluator with the information that will maximise the evaluator's analysis efforts.

5562 The evaluator samples the implementation representation to gain confidence that it is the version  
 5563 that is usable by the developer. The sample is such that the evaluator has assurance that all areas of  
 5564 the implementation representation are in conformance with the requirement; however, a complete  
 5565 examination of the entire implementation representation is unnecessary.

5566 Conventions in some forms of the implementation representation may make it difficult or  
 5567 impossible to determine from just the implementation representation itself what the actual result  
 5568 of the compilation or run-time interpretation will be. For example, compiler directives for C  
 5569 language compilers will cause the compiler to exclude or include entire portions of the code.

5570 Some forms of the implementation representation may require additional information because  
 5571 they introduce significant barriers to understanding and analysis. Examples include shrouded  
 5572 source code or source code that has been obfuscated in other ways such that it prevents  
 5573 understanding and/or analysis. These forms of implementation representation typically result  
 5574 from by taking a version of the implementation representation that is used by the TOE developer  
 5575 and running a shrouding or obfuscation program on it. While the shrouded representation is what  
 5576 is compiled and may be closer to the implementation (in terms of structure) than the original, un-  
 5577 shrouded representation, supplying such obfuscated code may cause significantly more time to be  
 5578 spent in analysis tasks involving the representation. When such forms of representation are  
 5579 created, the components require details on the shrouding tools/algorithms used so that the un-  
 5580 shrouded representation can be supplied, and the additional information can be used to gain  
 5581 confidence that the shrouding process does not compromise any security mechanisms.

5582 The evaluator samples the implementation representation to gain confidence that all of the  
 5583 information needed to interpret the implementation representation has been supplied. Note that  
 5584 the tools are among those referenced by Tools and techniques (ALC.TAT) components. The  
 5585 evaluator is encouraged to perform a quick check when first looking at the implementation  
 5586 representation to assure themselves that the developer is on the right track. However, the  
 5587 evaluator is also encouraged to perform the bulk of this check while working on other work units  
 5588 that call for examining the implementation; this will ensure the sample examined for this work unit  
 5589 is relevant.

5590 ISO/IEC 15408-3 ADV\_IMP.1.3C: *The mapping between the TOE design description and the sample of*  
 5591 *the implementation representation shall demonstrate their correspondence.*

#### 5592 11.5.1.4.3 Work unit ADV\_IMP.1-3

5593 The evaluator **shall examine** the mapping between the TOE design description and the sample of  
 5594 the implementation representation to determine that it is accurate.

5595 The evaluator augments the determination of existence (specified in work unit ADV\_IMP.1-1) by  
 5596 verifying the accuracy of a portion of the implementation representation and the TOE design  
 5597 description. For parts of the TOE design description that are interesting, the evaluator would verify  
 5598 the implementation representation accurately reflects the description provided in the TOE design  
 5599 description.

5600 For example, the TOE design description might identify a login module that is used to identify and  
 5601 authenticate users. If user authentication is sufficiently significant, the evaluator would verify that  
 5602 the corresponding code in fact implements that service as described in the TOE design description.  
 5603 It might also be worthwhile to verify that the code accepts the parameters as described in the  
 5604 functional specification.

## ISO/IEC 18045:2008(E)

5605 It is worth pointing out the developer must choose whether to perform the mapping for the entire  
5606 implementation representation, thereby guaranteeing that the chosen sample will be covered, or  
5607 waiting for the sample to be chosen before performing the mapping. The first option is likely more  
5608 work, but may be completed before the evaluation begins. The second option is less work, but will  
5609 produce a suspension of evaluation activity while the necessary evidence is being produced.

### 5610 11.5.2 Evaluation of sub-activity (ADV\_IMP.2)

#### 5611 11.5.2.1 Objectives

5612 The objective of this sub-activity is to determine that the implementation representation made  
5613 available by the developer is suitable for use in other analysis activities; suitability is judged by its  
5614 conformance to the requirements for this component.

#### 5615 11.5.2.2 Input

5616 The evaluation evidence for this sub-activity is:

- 5617 a) the implementation representation;
- 5618 b) the documentation of the development tools, as resulting from ALC\_TAT;
- 5619 c) the TOE design description.

#### 5620 11.5.2.3 Application notes

5621 The entire implementation representation is made available to ensure that analysis activities are  
5622 not curtailed due to lack of information. This does not, however, imply that all of the representation  
5623 is examined in detail when the analysis activities are being performed. This is likely impractical in  
5624 almost all cases, in addition to the fact that it most likely will not result in a higher-assurance TOE.

5625 The new aspect for ADV\_IMP.2 in comparison to ADV\_IMP.1 is that the developer needs to  
5626 demonstrate and the evaluator will confirm that the complete implementation representation is  
5627 mapped to the TOE design description. This does, however, not imply that all other work units  
5628 need an examination of the complete implementation representation. Aspects like appropriate  
5629 level of detail and form of the implementation representation can be covered by sampling as for  
5630 ADV\_IMP.1.

#### 5631 11.5.2.4 Action ADV\_IMP.2.1E

5632 ISO/IEC 15408-3 ADV\_IMP.2.1C *The implementation representation shall define the TSF to a level of*  
5633 *detail such that the TSF can be generated without further design decisions.*

##### 5634 11.5.2.4.1 Work unit ADV\_IMP.2-1

5635 The evaluator **shall check** that the implementation representation defines the TSF to a level of  
5636 detail such that the TSF can be generated without further design decisions.

5637 Source code or hardware diagrams and/or IC hardware design language code or layout data that  
5638 are used to build the actual hardware are examples of parts of an implementation representation.  
5639 The evaluator samples the implementation representation to gain confidence that it is at the  
5640 appropriate level and not, for instance, a pseudo-code level which requires additional design  
5641 decisions to be made. The evaluator is encouraged to perform a quick check when first looking at  
5642 the implementation representation to assure themselves that the developer is on the right track.  
5643 However, the evaluator is also encourage to perform the bulk of this check while working on other



5644 work units that call for examining the implementation; this will ensure the sample examined for  
5645 this work unit is relevant.

5646 If the evaluator has the possibility to actually execute or witness the "built" procedure used to  
5647 transfer the implementation representation into the actual implementation, and to compare the  
5648 result to the TOE as delivered, this may provide an easier and at the same time more reliable check  
5649 for this work unit (and possibly also for the following one).

5650 ISO/IEC 15408-3 ADV\_IMP.2.2C *The implementation representation shall be in the form used by the*  
5651 *development personnel.*

#### 5652 **11.5.2.4.2 Work unit ADV\_IMP.2-2**

5653 The evaluator **shall check** that the implementation representation is in the form used by  
5654 development personnel.

5655 The implementation representation is manipulated by the developer in a form that is suitable for  
5656 transformation to the actual implementation. For instance, the developer may work with files  
5657 containing source code, which is eventually compiled to become part of the TSF. The developer  
5658 makes available the implementation representation in the form they use, so that the evaluator may  
5659 use automated techniques in the analysis. This also increases the confidence that the  
5660 implementation representation examined is actually the one used in the production of the TSF (as  
5661 opposed to the case where it is supplied in an alternate presentation format, such as a word  
5662 processor document). It should be noted that other forms of the implementation representation  
5663 may also be used by the developer; these forms are supplied as well. The overall goal is to supply  
5664 the evaluator with the information that will maximise the evaluator's analysis efforts.

5665 The evaluator samples the implementation representation to gain confidence that it is the version  
5666 that is usable by the developer. The sample is such that the evaluator has assurance that all areas of  
5667 the implementation representation are in conformance with the requirement; however, a complete  
5668 examination of the entire implementation representation is unnecessary.

5669 Conventions in some forms of the implementation representation may make it difficult or  
5670 impossible to determine from just the implementation representation itself what the actual result  
5671 of the compilation or run-time interpretation will be. For example, compiler directives for C  
5672 language compilers will cause the compiler to exclude or include entire portions of the code.

5673 Some forms of the implementation representation may require additional information because  
5674 they introduce significant barriers to understanding and analysis. Examples include shrouded  
5675 source code or source code that has been obfuscated in other ways such that it prevents  
5676 understanding and/or analysis. These forms of implementation representation typically result  
5677 from by taking a version of the implementation representation that is used by the TOE developer  
5678 and running a shrouding or obfuscation program on it. While the shrouded representation is what  
5679 is compiled and may be closer to the implementation (in terms of structure) than the original, un-  
5680 shrouded representation, supplying such obfuscated code may cause significantly more time to be  
5681 spent in analysis tasks involving the representation. When such forms of representation are  
5682 created, the components require details on the shrouding tools/algorithms used so that the un-  
5683 shrouded representation can be supplied, and the additional information can be used to gain  
5684 confidence that the shrouding process does not compromise any security mechanisms.

5685 The evaluator samples the implementation representation to gain confidence that all of the  
5686 information needed to interpret the implementation representation has been supplied. Note that  
5687 the tools are among those referenced by Tools and techniques (ALC\_TAT) components. The  
5688 evaluator is encouraged to perform a quick check when first looking at the implementation  
5689 representation to assure themselves that the developer is on the right track. However, the  
5690 evaluator is also encouraged to perform the bulk of this check while working on other work units  
5691 that call for examining the implementation; this will ensure the sample examined for this work unit  
5692 is relevant.

## ISO/IEC 18045:2008(E)

5693 ISO/IEC 15408-3 ADV\_IMP.2.3C *The mapping between the TOE design description and the entire*  
5694 *implementation representation shall demonstrate their correspondence.*

### 5695 11.5.2.4.3 Work unit ADV\_IMP.2-3

5696 The evaluator **shall examine** the mapping between the TOE design description and the entire  
5697 implementation representation to determine that it is accurate.

5698 The evaluator augments the determination of existence (specified in work unit ADV\_IMP.2-1) by  
5699 verifying the accuracy of the implementation representation and the TOE design description. For  
5700 those parts of TOE design description that are interesting, the evaluator would verify the  
5701 implementation representation accurately reflects the description provided in the TOE design  
5702 description.

5703 For example, the TOE design description might identify a login module that is used to identify and  
5704 authenticate users. If user authentication is sufficiently significant, the evaluator would verify that  
5705 the corresponding code in fact implements that service as described in the TOE design description.  
5706 It might also be worthwhile to verify that the code accepts the parameters as described in the  
5707 functional specification.

5708 Usually it will be expected that the evaluator considers at least the functionality required by the  
5709 SFRs chosen in the ST and aspects described in the security architecture description as  
5710 "interesting" in the sense discussed above. Note however that not all aspects of the security  
5711 architecture are necessarily traceable to specific parts of the implementation representation.

5712 It is worth pointing out the developer must perform the mapping for the entire implementation  
5713 representation, thereby guaranteeing that the chosen sample will be covered.

### 5714 11.5.2.4.4 Work unit ADV\_IMP.2-4

5715 The evaluator **shall examine** the mapping between the TOE design description and the entire  
5716 implementation representation to determine that it is complete.

5717 Note that the completeness here is relevant in both directions: The complete TOE design needs to  
5718 be covered by the implementation representation and all parts of the implementation  
5719 representation needs to be mapped to a corresponding part of the TOE design.

5720 In order to confirm that the entire implementation representation is covered by the mapping the  
5721 evaluator will not need to examine the content of every part of the implementation representation.  
5722 If (in the case of a software TOE) the mapping is for example described by mapping each source  
5723 code file to a module in the TOE design description, it will be sufficient if this mapping is plausible  
5724 from the role of the source code file the evaluator can conclude from information like the naming of  
5725 the source code files, their grouping in subdirectories or their grouping in "built" procedures. Note,  
5726 that aspects of accuracy are covered by the preceding work unit.

5727 In order to confirm that the entire design description is covered by the implementation, the  
5728 evaluator may either use a similar argument as in the other direction, i. e. that all modules  
5729 contained in the TOE design description are mapped to parts of the implementation representation  
5730 in a plausible way. In addition, if the evaluator has established in the preceding work unit that all  
5731 SFRs and all applicable parts of the security architecture description are traceable to the  
5732 implementation representation this may be seen as sufficient evidence that the mapping is  
5733 complete.

5734 **11.6 TSF internals (ADV\_INT)**5735 **11.6.1 Evaluation of sub-activity (ADV\_INT.1)**5736 **11.6.1.1 Objectives**

5737 The objective of this sub-activity is to determine whether the defined subset of the TSF is designed  
 5738 and structured such that the likelihood of flaws is reduced and that maintenance can be more  
 5739 readily performed without the introduction of flaws.

5740 **11.6.1.2 Input**

5741 The evaluation evidence for this sub-activity is:

- 5742 a) the ST;
- 5743 b) the TOE design description;
- 5744 c) the implementation representation (if ADV\_IMP is part of the claimed assurance);
- 5745 d) the TSF internals description and justification;
- 5746 e) the documentation of the coding standards, as resulting from ALC\_TAT.

5747 **11.6.1.3 Application notes**

5748 The role of the internals description is to provide evidence of the structure of the design and  
 5749 implementation of the TSF.

5750 The structure of the design has two aspects: the constituent parts of the TSF and the procedures  
 5751 used to design the TSF. In cases where the TSF is designed in a manner consistent with the design  
 5752 represented by the TOE design (see ADV\_TDS), the assessment of the TSF design is obvious. In  
 5753 cases where the design procedures (see ALC\_TAT) are being followed, the assessment of the TSF  
 5754 design procedures is similarly obvious.

5755 In cases where the TSF is implemented using procedure-based software, this structure is assessed  
 5756 on the basis of its modularity; the modules identified in the internals description are the same as  
 5757 the modules identified in the TOE design (TOE design (TOE\_TDS)). A module consists of one or  
 5758 more source code files that cannot be decomposed into smaller compilable units.

5759 The use of the assignment in this component levies stricter constraints on the subset of the TSF  
 5760 that is explicitly identified in the assignment ADV\_INT.1.1D than on the remainder of the TSF.  
 5761 While the entire TSF is to be designed using good engineering principles and result in a well-  
 5762 structured TSF, only the specified subset is specifically analysed for this characteristic. The  
 5763 evaluator determines that the developer's application of coding standards result in a TSF that is  
 5764 understandable.

5765 The primary goal of this component is to ensure the TSF subset's implementation representation is  
 5766 understandable to facilitate maintenance and analysis (of both the developer and evaluator).

5767 **11.6.1.4 Action ADV\_INT.1.1E**

5768 ISO/IEC 15408-3 ADV\_INT.1.1C: *The justification shall explain the characteristics used to judge the*  
 5769 *meaning of "well-structured".*

## ISO/IEC 18045:2008(E)

### 5770 11.6.1.4.1 Work unit ADV\_INT.1-1

5771 The evaluator **shall examine** the justification to determine that it identifies the basis for  
5772 determining whether the TSF is well-structured.

5773 The evaluator verifies that the criteria for determining the characteristic of being well-structured  
5774 are clearly defined in the justification. Acceptable criteria typically originate from industry  
5775 standards for the technology discipline. For example, procedural software that executes linearly is  
5776 traditionally viewed as well-structured if it adheres to software engineering programming  
5777 practises, such as those defined in the IEEE Standard (*IEEE Std 610.12-1990*). For example, it would  
5778 identify the criteria for the procedural software portions of the TSF subset:

5779 a) the process used for modular decomposition

5780 b) coding standards used in the development of the implementation

5781 c) a description of the maximum acceptable level of intermodule coupling exhibited by  
5782 the TSF subset

5783 d) a description of the minimum acceptable level of cohesion exhibited the modules of  
5784 the TSF subset

5785 For other types of technologies used in the TOE - such as non-procedural software (e.g. object-  
5786 oriented programming), widespread commodity hardware (e.g. PC microprocessors), and special-  
5787 purpose hardware (e.g. smart-card processors) - the evaluator should seek guidance from the  
5788 evaluation authority for determining the adequacy of criteria for being "well-structured".

5789 ISO/IEC 15408-3 ADV\_INT.1.2C: *The TSF internals description shall demonstrate that the assigned*  
5790 *subset of the TSF is well-structured.*

### 5791 11.6.1.4.2 Work unit ADV\_INT.1-2

5792 The evaluator **shall check** the TSF internals description to determine that it identifies the Assigned  
5793 subset of the TSF.

5794 This subset may be identified in terms of the internals of the TSF at any layer of abstraction. For  
5795 example, it may be in terms of the structural elements of the TSF as identified in the TOE design  
5796 (e.g. the audit subsystem), or in terms of the implementation (e.g. *encrypt.c* and *decrypt.c* files, or  
5797 the 6227 IC chip).

5798 It is insufficient to identify this subset in terms of the claimed SFRs (e.g. the portion of the TSF that  
5799 provide anonymity as defined in FPR\_ANO.2) because this does not indicate where to focus the  
5800 analysis.

### 5801 11.6.1.4.3 Work unit ADV\_INT.1-3

5802 The evaluator **shall examine** the TSF internals description to determine that it demonstrates that  
5803 the assigned TSF subset is well-structured.

5804 The evaluator examines the internals description to ensure that it provides a sound explanation of  
5805 how the TSF subset meets the criteria from ADV\_INT.1-1

5806 For example, it would explain how the procedural software portions of the TSF subset meets the  
5807 following:

- 5808 a) that there is a one-to-one correspondence between the modules identified in the TSF  
5809 subset and the modules described in the TOE design (ADV\_TDS)
- 5810 b) how the TSF design is a reflection of the modular decomposition process
- 5811 c) a justification for all instances where the coding standards were not used or met
- 5812 d) a justification for any coupling or cohesion outside the acceptable bounds
- 5813 **11.6.1.5 Action ADV\_INT.1.2E**
- 5814 **11.6.1.5.1 Work unit ADV\_INT.1-4**
- 5815 The evaluator *shall determine* that the TOE design for the assigned TSF subset is well-structured.
- 5816 The evaluator examines a sample of the TOE design to verify the accuracy of the justification. For  
5817 example, a sample of the TOE design is analysed to determine its adherence to the design  
5818 standards, etc. As with all areas where the evaluator performs activities on a subset the evaluator  
5819 provides a justification of the sample size and scope
- 5820 The description of the TOE's decomposition into subsystems and modules will make the argument  
5821 that the TSF subset is well-structured self-evident. Verification that the procedures for structuring  
5822 the TSF (as examined in ALC\_TAT) are being followed will make it self-evident that the TSF subset  
5823 is well-structured.
- 5824 **11.6.1.5.2 Work unit ADV\_INT.1-5**
- 5825 The evaluator *shall determine* that the assigned TSF subset is well-structured.
- 5826 If ADV\_IMP is not part of the claimed assurance, then this work unit is not applicable and is  
5827 therefore considered to be satisfied.
- 5828 The evaluator examines a sample of the TSF subset to verify the accuracy of the internals  
5829 description. For example, a sample of the procedural software portions of the TSF subset is  
5830 analysed to determine its cohesion and coupling, its adherence to the coding standards, etc. As with  
5831 all areas where the evaluator performs activities on a subset the evaluator provides a justification  
5832 of the sample size and scope.
- 5833 **11.6.2 Evaluation of sub-activity (ADV\_INT.2)**
- 5834 **11.6.2.1 Objectives**
- 5835 The objective of this sub-activity is to determine whether the TSF is designed and structured such  
5836 that the likelihood of flaws is reduced and that maintenance can be more readily performed  
5837 without the introduction of flaws.
- 5838 **11.6.2.2 Input**
- 5839 The evaluation evidence for this sub-activity is:
- 5840 a) the modular design description;
- 5841 b) the implementation representation (if ADV\_IMP is part of the claimed assurance));
- 5842 c) the TSF internals description;

## ISO/IEC 18045:2008(E)

5843 d) the documentation of the coding standards, as resulting from ALC\_TAT.

### 5844 11.6.2.3 Application notes

5845 The role of the internals description is to provide evidence of the structure of the design and  
5846 implementation of the TSF.

5847 The structure of the design has two aspects: the constituent parts of the TSF and the procedures  
5848 used to design the TSF. In cases where the TSF is designed in a manner consistent with the design  
5849 represented by the TOE design (see ADV\_TDS), the assessment of the TSF design is obvious. In  
5850 cases where the design procedures (see ALC\_TAT) are being followed, the assessment of the TSF  
5851 design procedures is similarly obvious.

5852 In cases where the TSF is implemented using procedure-based software, this structure is assessed  
5853 on the basis of its modularity; the modules identified in the internals description are the same as  
5854 the modules identified in the TOE design (TOE design (ADV\_TDS)). A module consists of one or  
5855 more source code files that cannot be decomposed into smaller compilable units.

5856 The primary goal of this component is to ensure the TSF's implementation representation is  
5857 understandable to facilitate maintenance and analysis (of both the developer and evaluator).

### 5858 11.6.2.4 Action ADV\_INT.2.1E

5859 ISO/IEC 15408-3 ADV\_INT.2.1C: *The justification shall describe the characteristics used to judge the*  
5860 *meaning of "well-structured".*

#### 5861 11.6.2.4.1 Work unit ADV\_INT.2-1

5862 The evaluator **shall examine** the justification to determine that it identifies the basis for  
5863 determining whether the TSF is well-structured.

5864 The evaluator verifies that the criteria for determining the characteristic of being well-structured  
5865 are clearly defined in the justification. Acceptable criteria typically originate from industry  
5866 standards for the technology discipline. For example, procedural software that executes linearly is  
5867 traditionally viewed as well-structured if it adheres to software engineering programming  
5868 practises, such as those defined in the IEEE Standard (*IEEE Std 610.12-1990*). For example, it would  
5869 identify the criteria for the procedural software portions of the TSF:

5870 a) the process used for modular decomposition

5871 b) coding standards used in the development of the implementation

5872 c) a description of the maximum acceptable level of intermodule coupling exhibited by  
5873 the TSF

5874 d) a description of the minimum acceptable level of cohesion exhibited the modules of  
5875 the TSF

5876 For other types of technologies used in the TOE - such as non-procedural software (e.g. object-  
5877 oriented programming), widespread commodity hardware (e.g. PC microprocessors), and special-  
5878 purpose hardware (e.g. smart-card processors) - the evaluation authority should be consulted for  
5879 determining the adequacy of criteria for being "well-structured".

5880 ISO/IEC 15408-3 ADV\_INT.2.2C: *The TSF internals description shall demonstrate that the entire TSF*  
5881 *is well-structured.*

5882 **11.6.2.4.2 Work unit ADV\_INT.2-2**

5883 The evaluator *shall examine* the TSF internals description to determine that it demonstrates that  
5884 the TSF is well-structured.

5885 The evaluator examines the internals description to ensure that it provides a sound explanation of  
5886 how the TSF meets the criteria from ADV\_INT.2-1

5887 For example, it would explain how the procedural software portions of the TSF meet the following:

5888 a) that there is a one-to-one correspondence between the modules identified in the TSF  
5889 and the modules described in the TOE design (ADV\_TDS)

5890 b) how the TSF design is a reflection of the modular decomposition process

5891 c) a justification for all instances where the coding standards were not used or met

5892 d) a justification for any coupling or cohesion outside the acceptable bounds

5893 **11.6.2.5 Action ADV\_INT.2.2E**

5894 **11.6.2.5.1 Work unit ADV\_INT.2-3**

5895 The evaluator *shall determine* that the TOE design is well-structured.

5896 The evaluator examines the TOE design of a sample of the TSF to verify the accuracy of the  
5897 justification. For example, a sample of the TOE design is analysed to determine its adherence to the  
5898 design standards, etc. As with all areas where the evaluator performs activities on a subset the  
5899 evaluator provides a justification of the sample size and scope

5900 The description of the TOE's decomposition into subsystems and modules will make the argument  
5901 that the TSF subset is well-structured self-evident. Verification that the procedures for structuring  
5902 the TSF (as examined in ALC\_TAT) are being followed will make it self-evident that the TSF subset  
5903 is well-structured.

5904 **11.6.2.5.2 Work unit ADV\_INT.2-4**

5905 The evaluator *shall determine* that the TSF is well-structured.

5906 If ADV\_IMP is not part of the claimed assurance, then this work unit is not applicable and is  
5907 therefore considered to be satisfied.

5908 The evaluator examines a sample of the TSF to verify the accuracy of the internals description. For  
5909 example, a sample of the procedural software portions of the TSF is analysed to determine its  
5910 cohesion and coupling, its adherence to the coding standards, etc. As with all areas where the  
5911 evaluator performs activities on a subset the evaluator provides a justification of the sample size  
5912 and scope.

5913 **11.6.3 Evaluation of sub-activity (ADV\_INT.3)**

5914 **11.6.3.1 Objectives**

5915 The objective of this sub-activity is to determine whether the TSF is designed and structured such  
5916 that the likelihood of flaws is reduced and that maintenance can be more readily performed  
5917 without the introduction of flaws.

5918 **11.6.3.2 Input**

5919 The evaluation evidence for this sub-activity is:

- 5920 a) the modular design description;
- 5921 b) the implementation representation (if ADV\_IMP is part of the claimed assurance);
- 5922 c) the TSF internals description;
- 5923 d) the documentation of the coding standards, as resulting from ALC\_TAT.

5924 **11.6.3.3 Application notes**

5925 The role of the internals description is to provide evidence of the structure of the design and  
5926 implementation of the TSF.

5927 The structure of the design has two aspects: the constituent parts of the TSF and the procedures  
5928 used to design the TSF. In cases where the TSF is designed in a manner consistent with the design  
5929 represented by the TOE design (see ADV\_TDS), the assessment of the TSF design is obvious. In  
5930 cases where the design procedures (see ALC\_TAT) are being followed, the assessment of the TSF  
5931 design procedures is similarly obvious.

5932 In cases where the TSF is implemented using procedure-based software, this structure is assessed  
5933 on the basis of its modularity; the modules identified in the internals description are the same as  
5934 the modules identified in the TOE design (TOE design (ADV\_TDS)). A module consists of one or  
5935 more source code files that cannot be decomposed into smaller compilable units.

5936 The primary goal of this component is to ensure the TSF's implementation representation is  
5937 understandable to facilitate maintenance and analysis (of both the developer and evaluator).

5938 **11.6.3.4 Action ADV\_INT.3.1E**

5939 ADV\_INT.3.1C *The justification shall describe the characteristics used to judge the meaning of*  
5940 *"well-structured" and "complex".*

5941 **11.6.3.4.1 Work unit ADV\_INT.3-1**

5942 The evaluator **shall examine** the justification to determine that it identifies the basis for  
5943 determining whether the TSF is "well-structured" and "not overly complex".

5944 The evaluator verifies that the criteria for determining the characteristic of being "well-structured"  
5945 and "complex" are clearly defined in the justification. Acceptable criteria typically originate from  
5946 industry standards for the technology discipline. For example, procedural software that executes  
5947 linearly is traditionally viewed as well-structured if it adheres to software engineering  
5948 programming practises, such as those defined in the IEEE Standard (IEEE Std 610.12-1990). For  
5949 example, it would identify the criteria for the procedural software portions of the TSF:

- 5950 a) the process used for modular decomposition
- 5951 b) coding standards used in the development of the implementation
- 5952 c) a description of the maximum acceptable level of intermodule coupling exhibited by  
5953 the TSF



5954 d) a description of the minimum acceptable level of cohesion exhibited the modules of  
5955 the TSF

5956 Complexity can for example be measured in the number of decision points and logical paths of  
5957 execution that code takes. Software engineering literature cites complexity as a negative  
5958 characteristic of software because it impedes understanding of the logic and flow of the code.  
5959 Another impediment to the understanding of code is the presence of code that is unnecessary, in  
5960 that it is unused or redundant.

5961 Design complexity minimisation is a key characteristic of a reference validation mechanism, the  
5962 purpose of which is to arrive at a TSF that is easily understood so that it can be completely  
5963 analysed.

5964 See also CC 3.1, Part 3, Annex A.3 for additional information on TSF internals.

5965 The consideration in that annex and those made in the preceding paragraphs of this work unit are  
5966 mainly derived from common knowledge about procedural software. For other types of  
5967 technologies used in the TOE - such as non-procedural software (e.g. object-oriented  
5968 programming), widespread commodity hardware (e.g. PC microprocessors), and special-purpose  
5969 hardware (e.g. smart-card processors) - the evaluation authority should be consulted for  
5970 determining the adequacy of criteria for being "well-structured" and "not overly complex".

5971 The evaluator is reminded to be open for plausible definitions given by the developer. If, for  
5972 example, a smart card developer can justify that the metrics used by him to measure complexity  
5973 are an industry standard in their field, this should usually be sufficient for acceptance of such  
5974 metrics.

5975 ISO/IEC 15408-3 ADV\_INT.3.2C: *The TSF internals description shall demonstrate that the entire TSF*  
5976 *is well-structured and is not overly complex.*

#### 5977 **11.6.3.4.2 Work unit ADV\_INT.3-2**

5978 The evaluator ***shall examine*** the TSF internals description to determine that it demonstrates that  
5979 the TSF is well-structured and not overly complex.

5980 The evaluator examines the internals description to ensure that it provides a sound explanation of  
5981 how the TSF meets the criteria from ADV\_INT.3-1

5982 For example, it would explain how the procedural software portions of the TSF meet the following:

5983 a) that there is a one-to-one correspondence between the modules identified in the TSF  
5984 and the modules described in the TOE design (ADV\_TDS)

5985 b) how the TSF design is a reflection of the modular decomposition process

5986 c) a justification for all instances where the coding standards were not used or met

5987 d) a justification for any coupling or cohesion outside the acceptable bounds

5988 e) how the modular decomposition process reduces complexity

## ISO/IEC 18045:2008(E)

### 5989 11.6.3.5 Action ADV\_INT.3.2E

#### 5990 11.6.3.5.1 Work unit ADV\_INT.3-3

5991 The evaluator **shall determine** that the entire TOE design is well-structured and not overly  
5992 complex.

5993 The evaluator examines the TOE design description of the TSF to verify the accuracy of the  
5994 justification. For example, a sample of the TOE design is analysed to determine its adherence to the  
5995 design standards, etc. As with all areas where the evaluator performs activities on a subset the  
5996 evaluator provides a justification of the sample size and scope

5997 The description of the TOE's decomposition into subsystems and modules will make the argument  
5998 that the TSF is well-structured self-evident. Verification that the procedures for structuring the TSF  
5999 (as examined in ALC\_TAT) are being followed will make it self-evident that the TSF is well-  
6000 structured.

6001 Using the metrics defined by the developer for measuring the complexity of the design will show if  
6002 the metrics is met. If the metrics is only defined for the implementation representation and not for  
6003 the TOE design (note that adequateness of the metrics was considered already in work unit  
6004 ADV\_INT.3-1), there may be no need for using the metrics in this work unit, the complexity-issue is  
6005 then covered by the next work unit.

#### 6006 11.6.3.5.2 Work unit ADV\_INT.3-4

6007 The evaluator **shall determine** that the entire TSF is well-structured and not overly complex.

6008 If ADV\_IMP is not part of the claimed assurance, then this work unit is not applicable and is  
6009 therefore considered to be satisfied.

6010 The evaluator examines a sample of the TSF to verify the accuracy of the internals description. For  
6011 example, a sample of the procedural software portions of the TSF is analysed to determine its  
6012 cohesion and coupling, its adherence to the coding standards, etc. As with all areas where the  
6013 evaluator performs activities on a subset the evaluator provides a justification of the sample size  
6014 and scope.

6015 Similarly the evaluator applies the metric for complexity as defined by the developer and examined  
6016 in work unit ADV\_INT.3-1 to either a sample of the implementation representation or the complete  
6017 implementation representation (this may depend on the metric) and verifies that the metric is in  
6018 fact met. The evaluator may only restrict their application of the metrics to a sample if the  
6019 developer has provided the results of the application of the metrics for the entire TSF and the  
6020 sampling serves as means to convince the evaluator that the application as done by the developer  
6021 was correct (similar to the evaluator's sampling of functional testing already done by the  
6022 developer).

### 6023 11.7 Security policy modelling (ADV\_SPM)

#### 6024 11.7.1 Evaluation of sub-activity (ADV\_SPM.1)

##### 6025 11.7.1.1 Objectives

6026 The objectives of this sub-activity are to determine whether the formal security policy model of the  
6027 TSF clearly and consistently describes the rules and characteristics of the security policies, and  
6028 whether the elements correspond to the TSFIs.

6029 The evaluation evidence for this sub-activity is:

6030 a) the ST;

- 6031 the functional specification;
- 6032 formal security policy model (ADV\_SPM.1.1D);
- 6033 formal proof of correspondence between the model and any formal functional specification  
6034 (ADV\_SPM.1.3D);
- 6035 demonstration of correspondence between the model and the functional specification  
6036 (ADV\_SPM.1.4D).
- 6037 **11.7.1.2 Application notes**
- 6038 This activity applies to cases where the developer has provided a formal security policy model of  
6039 the TOE.
- 6040 A formal TOE security policy model is a representation of the rules (synonymously termed  
6041 "principles") of security policies and characteristics of the TSF behaviour in mathematical terms.  
6042 Their formal counterparts are called security properties and security features, respectively. The  
6043 representation includes but is not limited to algebraic specifications, finite state machines and logic  
6044 formalisms strong enough to formally infer the properties from the features. The formal TSP model  
6045 is accompanied by an informal interpretation explaining how the rules and characteristics are  
6046 mapped to the respective properties and features.
- 6047 The creation of a formal security policy model helps to identify and eliminate ambiguous,  
6048 inconsistent, contradictory, or unenforceable security policy elements. Once the TOE has been built,  
6049 the formal model serves the evaluation effort by contributing to the evaluator's judgement of how  
6050 well the developer has understood the security functionality being implemented and whether  
6051 there are inconsistencies between the security requirements and the TOE design. The confidence in  
6052 the model is accompanied by a proof that it contains no inconsistencies.
- 6053 A formal security model is a precise formal presentation of the important aspects of security and  
6054 their relationship to the behaviour of the TOE; it identifies the set of rules (principles) that defines  
6055 the TOE security policy and the set of practises (characteristics) that regulates how the TSF  
6056 manages, protects, and otherwise controls the system resources. The model includes the set of  
6057 restrictions and properties that specify how information and computing resources are prevented  
6058 from being used to violate the SFRs, accompanied by a persuasive set of engineering arguments  
6059 showing that these restrictions and properties play a key role in the enforcement of the SFRs. It  
6060 consists both of the formalisms that express the security functionality, as well as ancillary text to  
6061 explain the model and to provide it with context. The security behaviour of the TSF is modelled  
6062 both in terms of external behaviour (i.e. how the TSF interacts with the rest of the TOE and with its  
6063 operational environment), as well as its internal behaviour.
- 6064 The Security Policy Model of the TOE is informally abstracted from its realisation by considering  
6065 the proposed security requirements of the ST. The informal abstraction is taken to be successful if  
6066 the TOE's principles turn out to be enforced by its characteristics. The purpose of formal methods  
6067 lies within the enhancement of the rigour of enforcement. Informal arguments are always prone to  
6068 fallacies; especially if relationships among subjects, objects and operations get more and more  
6069 complexinvolvedcomplex. In order to minimise the risk of insecure state arrivals the rules and  
6070 characteristics of the security policy model are mapped to respective properties and features  
6071 within some formal system, whose rigour and strength can afterwards be used to obtain the  
6072 security properties by means of theorems and formal proof.
- 6073 While the term "formal security policy model" is used in academic circles, the CC's approach has no  
6074 fixed definition of "security"; it would equate to whatever SFRs are being claimed. Therefore, the  
6075 formal security policy model is merely a formal representation of the set of SFRs being claimed.
- 6076 The term security policy has traditionally been associated with only access control policies,  
6077 whether label-based (mandatory access control) or user-based (discretionary access control).

## ISO/IEC 18045:2008(E)

6078 However, a security policy is not limited to access control; there are also audit policies,  
6079 identification policies, authentication policies, encryption policies, management policies, and any  
6080 other security policies that are enforced by the TOE, as described in the PP/ST. ADV\_SPM.1.1D  
6081 contains an assignment for identifying these policies that are formally modelled.

6082 It is recognized that not all policies can be formally modelled for all TOEs. This is because either a  
6083 given policy can not be formally modelled in the otherwise well suited framework, or because the  
6084 nature of the TOE renders impossible the modelling of policies that would otherwise be possible to  
6085 model.

### 6086 11.7.1.3 Action ADV\_SPM.1.1E

6087 ISO/IEC 15408-3 ADV\_SPM.1.1C *The model shall be in a formal style, supported by explanatory text*  
6088 *as required, and identify the security policies of the TSF that are modelled.*

#### 6089 11.7.1.3.1 Work unit ADV\_SPM.1-1

6090 The evaluator **shall examine** the TOE security policy model to determine that it is written in a  
6091 formal style.

6092 The evaluator identifies the formal framework upon which the TOE security policy model is based  
6093 and ensures that it is founded on well established mathematical concepts. They also identify the  
6094 security properties and features addressed in the application notes and ensure the formalization of  
6095 at least one security policy.

6096 For guidance on formal methods refer to ISO/IEC 15408-3

#### 6097 11.7.1.3.2 Work unit ADV\_SPM.1-2

6098 The evaluator **shall examine** the TOE security policy model to determine that it contains all  
6099 necessary informal explanatory text.

6100 Supporting narrative descriptions are necessary for all parts of the model (for example, to make  
6101 clear the meaning of any formal notation and how they are used) including the security properties  
6102 and features.

#### 6103 11.7.1.3.3 Work unit ADV\_SPM.1-3

6104 The evaluator **shall examine** the TOE security policy model to determine that all security policies  
6105 of the TSF are identified that are modelled.

6106 The evaluator determines whether the SPM identifies the security policies for which a model is  
6107 provided, identifying the relevant portions of the statement of SFRs that comprise each of the  
6108 modelled policies.

6109 The evaluator determines whether the list of security policies identified by the SPM is consistent  
6110 with the assignment of ADV\_SPM.1.1D in the ST.

6111 The evaluator determines whether for each security policy identified by the SPM a model is in fact  
6112 provided.

6113 ISO/IEC 15408-3 ADV\_SPM.1.2C *For all policies that are modelled, the model shall define security for*  
6114 *the TOE and provide a formal proof that the TOE cannot reach a state that is not secure.*

#### 6115 11.7.1.3.4 Work unit ADV\_SPM.1-4

6116 The evaluator **shall examine** the principles and characteristics of the security policies to determine  
6117 that the modelled security behaviour of the TOE is clearly articulated.

6118 The security policies are expressed in terms of security principles (rules) which are modelled by  
 6119 security properties and define the secure state of the TOE. For example, a model based on state  
 6120 transitions could describe the security policies in terms of principles of its states, identify its initial  
 6121 state, and define what it means to be a secure state.

6122 The evaluator determines that the security policies are reflected within their formal counterparts  
 6123 of the TSP model.

6124 The TOE security behaviour is expressed in terms of security characteristics (i.e. portions of TOE  
 6125 security functionality managing, protecting, and otherwise controlling the system resources  
 6126 including attributes and conditions of the TOE) which are modelled by security features. For  
 6127 example, a model based on state transitions could describe the characteristics as possible actions  
 6128 in each secure state in a level of detail sufficient to decide into which state the TOE will be  
 6129 transformed by that action.

6130 Together the security principles and characteristics describe the entire security posture of the TOE.

6131 In the context of a formal TOE security policy model the security behaviour is considered to be  
 6132 clearly articulated only if an adequate mapping from principles and characteristics to their  
 6133 respective formal counterparts properties and features has been given. The mapping is considered  
 6134 to be adequate if the level of abstraction from the TOE's realization is detailed enough to allow for  
 6135 correct identification of all security objectives and the relation to the security environment.

6136 The above condition for clear articulation is necessary but not sufficient. An informal  
 6137 interpretation of all formal concepts (including attributes, predicates and variables, if available)  
 6138 must be provided in order to make clear their intended meaning.

#### 6139 11.7.1.3.5 Work unit ADV\_SPM.1-5

6140 The evaluator **shall examine** the TOE security policy model rationale to determine that it formally  
 6141 proves that the security features enforce the security properties.

6142 To determine the enforcement, the evaluator considers the security properties and the security  
 6143 features and verifies that the arguments used in the proof are valid. The proof of correspondence  
 6144 between the security properties and the security features shall be formal.

6145 The validity of the security properties shall mean that the TOE is in a secure state. By this, the  
 6146 evaluator confirms by means of the rationale that the TOE never reaches an insecure state.

#### 6147 11.7.1.3.6 Work unit ADV\_SPM.1-6

6148 The evaluator **shall examine** the TOE security policy model rationale to determine that it proves  
 6149 the internal consistency of the TOE security policy model.

6150 The proof shall show the absence of contradictions within the TOE security policy model. In  
 6151 determining the absence of contradictions, the evaluator verifies that the arguments used in the  
 6152 proof are valid.

6153 Since the TOE security policy model is formal, the proof of its internal consistency shall be formal.  
 6154 It is recognized that a complete formal proof of the internal consistency of the TOE security policy  
 6155 model usually is not possible due to the fundamental nature of formal frameworks. Generally, it is  
 6156 sufficient to generate evidence using formal proofs based on the specific TOE security policy model  
 6157 that prove the internal consistency by means of a combination with generic arguments of the  
 6158 formal framework.

6159 ISO/IEC 15408-3 ADV\_SPM.1.3C *The correspondence between the model and the functional*  
 6160 *specification shall be at the correct formal level.*

6161 **11.7.1.3.7 Work unit ADV\_SPM.1-7**

6162 The evaluator *shall examine* the correspondence between the model and the functional  
6163 specification to determine that a semiformal demonstration of correspondence between the model  
6164 and any semiformal functional specification is provided.

6165 This work unit is only applicable to a semiformal presentation of the functional specification, which  
6166 is required by ADV\_FSP.5.2C.

6167 A semiformal correspondence is one that results from a structured approach with a substantial  
6168 degree of rigor (in terms of completeness and correctness), but is not as rigorous as a  
6169 mathematical proof. Such a semiformal correspondence limits the subjective interpretations of its  
6170 terms, and so it provides less ambiguity than would exist in an informal correspondence.

6171 For guidance on semiformal methods refer to Annex 3.1.1 'Semiformal and formal methods'.

6172 **11.7.1.3.8 Work unit ADV\_SPM.1-8**

6173 The evaluator *shall examine* the correspondence between the model and the functional  
6174 specification to determine that a formal proof of correspondence between the model and any  
6175 formal functional specification is provided.

6176 This work unit is only applicable to a formal presentation of the functional specification, which is  
6177 required by ADV\_FSP.6.2D.

6178 There should be a formal proof of correspondence between the model and any formal functional  
6179 specification.

6180 The formal proof of correspondence removes all subjective interpretations of its terms by enlisting  
6181 well-established mathematical concepts to define the syntax and semantics of the formal notation  
6182 and uses rules that support logical reasoning. The security features within the TOE (which are  
6183 identified in the formal TSP model) are expressed in a formal specification language and shown to  
6184 be satisfied by the formal specification.

6185 For guidance on formal methods refer to ISO/IEC 15408-3.

6186 ISO/IEC 15408-3 ADV\_SPM.1.4C *The correspondence shall show that the functional specification is*  
6187 *consistent and complete with respect to the model.*

6188 **11.7.1.3.9 Work unit ADV\_SPM.1-9**

6189 The evaluator *shall examine* the correspondence to determine that the behaviour at the TSF  
6190 interfaces (as articulated in the functional specification) is complete with respect to the behaviour  
6191 modelled by the security features.

6192 The term "correspondence" here means both the formal proof of correspondence between the  
6193 formal SPM and any formal FSP required by ADV\_SPM.1.2D and the demonstration of  
6194 correspondence between the formal SPM and the FSP required by ADV\_SPM.1.3D.

6195 In determining completeness of the correspondence, the evaluator considers the description of  
6196 TSFI behaviour and maps adequate portions (characteristics) to corresponding features of the TSP  
6197 model. The demonstration should show that all characteristics belonging to policies that are  
6198 required to be modelled have an associated feature description in the TOE security policy model,  
6199 and that each feature of the TSP model does occur in the mapping.

6200 Abstention from formally modelling TSFI behaviour always calls for justification on the developer's  
6201 side (also confer the application notes above).

6202 **11.7.1.3.10 Work unit ADV\_SPM.1-10**

6203 The evaluator *shall examine* the correspondence to determine that the behaviour at the TSF  
 6204 interfaces (as articulated in the functional specification) is consistent with respect to the behaviour  
 6205 modelled by the security features.

6206 The term “correspondence” here means both the formal proof of correspondence between the  
 6207 formal SPM and any formal FSP required by ADV\_SPM.1.3D and the demonstration of  
 6208 correspondence between the SPM and the FSP required by ADV\_SPM.1.4D.

6209 The meaning of consistency reflects the conventional understanding in contrast to the internal  
 6210 consistency concept of work unit ADV\_SPM.1-6.

6211 In determining consistency, the evaluator resumes the mapping of TSFI behaviour to security  
 6212 features established in the preceding work unit and verifies that the correspondence shows that  
 6213 each security feature of the TSP model accurately reflects the corresponding TSFI behaviour.

6214 For example, if TSFI behaviour dealt with access management on the granularity of single  
 6215 individuals, then a TSP model describing the security behaviour of the TOE in terms of groups of  
 6216 users would not be consistent. Likewise, if TSFI behaviour dealt with access management for  
 6217 groups of users, then a TSP model describing the security behaviour of the TOE in terms of  
 6218 individual users would also not be consistent.

6219 As another example, if remote untrusted users had to pass more stringent authentication  
 6220 procedures than administrators whose only point of access were within a physically-protected  
 6221 area, then this difference in authentication procedures had to be reflected in the security features.

6222 **11.8 TOE design (ADV\_TDS)**6223 **11.8.1 Evaluation of sub-activity (ADV\_TDS.1)**6224 **11.8.1.1 Input**

6225 The evaluation evidence for this sub-activity is:

- 6226 a) the ST;
- 6227 b) the functional specification;
- 6228 c) security architecture description;
- 6229 d) the TOE design.

6230 **11.8.1.2 Action ADV\_TDS.1.1E**

6231 ISO/IEC 15408-3 ADV\_TDS.1.1C: *The design shall describe the structure of the TOE in terms of*  
 6232 *subsystems.*

6233 **11.8.1.2.1 Work unit ADV\_TDS.1-1**

6234 The evaluator *shall examine* the TOE design to determine that the structure of the entire TOE is  
 6235 described in terms of subsystems.

6236 The evaluator ensures that all of the subsystems of the TOE are identified. This description of the  
 6237 TOE will be used as input to work unit ADV\_TDS.1-2, where the parts of the TOE that make up the  
 6238 TSF are identified. That is, this requirement is on the entire TOE rather than on only the TSF.

## ISO/IEC 18045:2008(E)

6239 The TOE (and TSF) may be described in multiple layers of abstraction (i.e. subsystems and  
6240 modules). Depending upon the complexity of the TOE, its design may be described in terms of  
6241 subsystems and modules, as described in ISO/IEC 15408-3 Annex A, ADV\_TDS: Subsystems and  
6242 Modules. At this level of assurance, the decomposition only need be at the “subsystem” level.

6243 In performing this activity, the evaluator examines other evidence presented for the TOE (e.g., ST,  
6244 operator user guidance) to determine that the description of the TOE in such evidence is consistent  
6245 with the description contained in the TOE design.

6246 ISO/IEC 15408-3 ADV\_TDS.1.2C: *The design shall identify all subsystems of the TSF.*

### 6247 11.8.1.2.2 Work unit ADV\_TDS.1-2

6248 The evaluator **shall examine** the TOE design to determine that all subsystems of the TSF are  
6249 identified.

6250 In work unit ADV\_TDS.1-1 all of the subsystems of the TOE were identified, and a determination  
6251 made that the non-TSF subsystems were correctly characterised. Building on that work, the  
6252 subsystems that were not characterised as non-TSF subsystems should be precisely identified. The  
6253 evaluator determines that, of the hardware and software installed and configured according to the  
6254 Preparative procedures (AGD\_PRE) guidance, each subsystem has been accounted for as either one  
6255 that is part of the TSF, or one that is not.

6256 If TSFs are defined in terms of sub-TSFs for multi assurance the evaluator shall examine that the  
6257 combination of all sub-TSF is consistent and does not omit relevant information for each sub-TSF  
6258 considering the relevant decomposition level.

6259 ISO/IEC 15408-3 ADV\_TDS.1.3C: *The design shall describe the behaviour of each SFR-supporting or*  
6260 *SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.*

### 6261 11.8.1.2.3 Work unit ADV\_TDS.1-3

6262 The evaluator **shall examine** the TOE design to determine that each SFR-supporting or SFR-non-  
6263 interfering subsystem of the TSF is described such that the evaluator can determine that the  
6264 subsystem is SFR-supporting or SFR-non-interfering.

6265 SFR-supporting and SFR-non-interfering subsystems do not need to be described in detail as to  
6266 how they function in the system. However, the evaluator makes a determination, based on the  
6267 evidence provided by the developer, that the subsystems that do not have high-level descriptions  
6268 are SFR-supporting or SFR-non-interfering. Note that if the developer provides a uniform level of  
6269 detailed documentation then this work unit will be largely satisfied, since the point of categorising  
6270 the subsystems is to allow the developer to provide less information for SFR-supporting and SFR-  
6271 non-interfering subsystems than for SFR-enforcing subsystems.

6272 An SFR-supporting subsystem is one that is depended on by an SFR-enforcing subsystem in order  
6273 to implement an SFR, but does not play as direct a role as an SFR-enforcing subsystem. An SFR-  
6274 non-interfering subsystem is one that is not depended upon, in either a supporting or enforcing  
6275 role, to implement an SFR.

6276 ISO/IEC 15408-3 ADV\_TDS.1.4C: *The design shall summarise the SFR-enforcing behaviour of the*  
6277 *SFR-enforcing subsystems.*

### 6278 11.8.1.2.4 Work unit ADV\_TDS.1-4

6279 The evaluator **shall examine** the TOE design to determine that it provides a complete, accurate,  
6280 and high-level summary of the SFR-enforcing behaviour of the SFR-enforcing subsystems.



6281 The developer may designate subsystems as SFR-enforcing, SFR-supporting, and SFR non-  
 6282 interfering, but these “tags” are used only to describe the amount and type of information the  
 6283 developer must provide, and can be used to limit the amount of information the developer has to  
 6284 develop if their engineering process does not produce the documentation required. Whether the  
 6285 subsystems have been categorised by the developer or not, it is the evaluator’s responsibility to  
 6286 determine that the subsystems have the appropriate information for their role (SFR-enforcing, etc.)  
 6287 in the TOE, and to obtain the appropriate information from the developer should the developer fail  
 6288 to provide the required information for a particular subsystem.

6289 SFR-enforcing behaviour refers to how a subsystem provides the functionality that implements an  
 6290 SFR. The goal of evaluator’s assessment is to give the evaluator with an understanding of the way  
 6291 each SFR-enforcing subsystem works. The information provided for the behaviour summary does  
 6292 not have to be as detailed as that provided by the behaviour description. For example, data  
 6293 structures or data items will likely not need to be described in detail. It is the evaluator’s  
 6294 determination, however, with respect to what “high-level” means for a particular TOE, and the  
 6295 evaluator obtains enough information from the developer (even if it turns out to be equivalent to  
 6296 information provided for subsystem behaviour) to make a sound verdict for this work unit.

6297 The evaluator is cautioned, however, that “perfect” assurance is not a goal nor required by this  
 6298 work unit, so judgement will have to be exercised in determine the amount and composition of the  
 6299 evidence required to make a verdict on this work unit.

6300 To determine completeness and accuracy, the evaluator examines other information available (e.g.,  
 6301 functional specification, security architecture description). Summaries of functionality in these  
 6302 documents should be consistent with what is provided for evidence for this work unit.

6303 ISO/IEC 15408-3 ADV\_TDS.1.5C: *The design shall provide a description of the interactions among*  
 6304 *SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other*  
 6305 *subsystems of the TSF.*

#### 6306 11.8.1.2.5 Work unit ADV\_TDS.1-5

6307 The evaluator **shall examine** the TOE design to determine that interactions between the  
 6308 subsystems of the TSF are described.

6309 The goal of describing the interactions between the SFR-enforcing subsystems and other  
 6310 subsystems is to help provide the reader a better understanding of how the TSF performs its  
 6311 functions. These interactions do not need to be characterised at the implementation level (e.g.,  
 6312 parameters passed from one routine in a subsystem to a routine in a different subsystem; global  
 6313 variables; hardware signals (e.g., interrupts) from a hardware subsystem to an interrupt-handling  
 6314 subsystem), but the data elements identified for a particular subsystem that are going to be used  
 6315 by another subsystem need to be covered in this discussion. Any control relationships between  
 6316 subsystems (e.g., a subsystem responsible for configuring a rule base for a firewall system and the  
 6317 subsystem that actually implements these rules) should also be described.

6318 The evaluators need to use their own judgement in assessing the completeness of the description.  
 6319 If the reason for an interaction is unclear, or if there are SFR-related interactions (discovered, for  
 6320 instance, in examining the descriptions of subsystem behaviour) that do not appear to be described,  
 6321 the evaluator ensures that this information is provided by the developer. However, if the evaluator  
 6322 can determine that interactions among a particular set of subsystems, while incompletely  
 6323 described by the developer, will not aid in understanding the overall functionality nor security  
 6324 functionality provided by the TSF, then the evaluator may choose to consider the description  
 6325 sufficient, and not pursue completeness for its own sake.

6326 ISO/IEC 15408-3 ADV\_TDS.1.6C: *The mapping shall demonstrate that all TSFIs trace to the*  
 6327 *behaviour described in the TOE design that they invoke.*

6328 **11.8.1.2.6 Work unit ADV\_TDS.1-6**

6329 The evaluator *shall examine* the TOE design to determine that it contains a complete and accurate  
6330 mapping from the TSFI described in the functional specification to the subsystems of the TSF  
6331 described in the TOE design.

6332 The subsystems described in the TOE design provide a description of how the TSF works at a  
6333 detailed level for SFR-enforcing portions of the TSF, and at a higher level for other portions of the  
6334 TSF. The TSFI provide a description of how the implementation is exercised. The evidence from the  
6335 developer identifies the subsystem that is initially involved when an operation is requested at the  
6336 TSFI, and identify the various subsystems that are primarily responsible for implementing the  
6337 functionality. Note that a complete "call tree" for each TSFI is not required for this work unit.

6338 The evaluator assesses the completeness of the mapping by ensuring that all of the TSFI map to at  
6339 least one subsystem. The verification of accuracy is more complex.

6340 The first aspect of accuracy is that each TSFI is mapped to a subsystem at the TSF boundary. This  
6341 determination can be made by reviewing the subsystem description and interactions, and from this  
6342 information determining its place in the architecture. The next aspect of accuracy is that the  
6343 mapping makes sense. For instance, mapping a TSFI dealing with access control to a subsystem  
6344 that checks passwords is not accurate. The evaluator should again use judgement in making this  
6345 determination. The goal is that this information aids the evaluator in understanding the system and  
6346 implementation of the SFRs, and ways in which entities at the TSF boundary can interact with the  
6347 TSF. The bulk of the assessment of whether the SFRs are described accurately by the subsystems is  
6348 performed in other work units.

6349 **11.8.1.3 Action ADV\_TDS.1.2E**

6350 **11.8.1.3.1 Work unit ADV\_TDS.1-7**

6351 The evaluator *shall examine* the TOE security functional requirements and the TOE design, to  
6352 determine that all ST security functional requirements are covered by the TOE design.

6353 The evaluator may construct a map between the TOE security functional requirements and the TOE  
6354 design. This map will likely be from a functional requirement to a set of subsystems. Note that this  
6355 map may have to be at a level of detail below the component or even element level of the  
6356 requirements, because of operations (assignments, refinements, selections) performed on the  
6357 functional requirement by the ST author.

6358 For example, the FDP\_ACC.1 Subset access control component contains an element with  
6359 assignments. If the ST contained, for instance, ten rules in the FDP\_ACC.1 Subset access control  
6360 assignment, and these ten rules were implemented in specific places within fifteen modules, it  
6361 would be inadequate for the evaluator to map FDP\_ACC.1 Subset access control to one subsystem  
6362 and claim the work unit had been completed. Instead, the evaluator would map FDP\_ACC.1 Subset  
6363 access control (rule 1) to subsystem A, behaviours x, y, and z; FDP\_ACC.1 Subset access control  
6364 (rule 2) to subsystem A, behaviours x, p, and q; etc.

6365 **11.8.1.3.2 Work unit ADV\_TDS.1-8**

6366 The evaluator *shall examine* the TOE design to determine that it is an accurate instantiation of all  
6367 security functional requirements.

6368 The evaluator ensures that each security requirement listed in the TOE security functional  
6369 requirements subclause of the ST has a corresponding design description in the TOE design that  
6370 accurately details how the TSF meets that requirement. This requires that the evaluator identify a  
6371 collection of subsystems that are responsible for implementing a given functional requirement, and  
6372 then examine those subsystems to understand how the requirement is implemented. Finally, the  
6373 evaluator would assess whether the requirement was accurately implemented.

6374 As an example, if the ST requirements specified a role-based access control mechanism, the  
 6375 evaluator would first identify the subsystems that contribute to this mechanism's implementation.  
 6376 This could be done by in-depth knowledge or understanding of the TOE design or by work done in  
 6377 the previous work unit. Note that this trace is only to identify the subsystems, and is not the  
 6378 complete analysis.

6379 The next step would be to understand what mechanism the subsystems implemented. For instance,  
 6380 if the design described an implementation of access control based on UNIX-style protection bits,  
 6381 the design would not be an accurate instantiation of those access control requirements present in  
 6382 the ST example used above. If the evaluator could not determine that the mechanism was  
 6383 accurately implemented because of a lack of detail, the evaluator would have to assess whether all  
 6384 of the SFR-enforcing subsystems have been identified, or if adequate detail had been provided for  
 6385 those subsystems.

#### 6386 **11.8.2 Evaluation of sub-activity (ADV\_TDS.2)**

##### 6387 **11.8.2.1 Input**

6388 The evaluation evidence for this sub-activity is:

- 6389 a) the ST;
- 6390 b) the functional specification;
- 6391 c) security architecture description;
- 6392 d) the TOE design.

##### 6393 **11.8.2.2 Action ADV\_TDS.2.1E**

6394 ISO/IEC 15408-3 ADV\_TDS.2.1C: *The design shall describe the structure of the TOE in terms of*  
 6395 *subsystems.*

##### 6396 **11.8.2.2.1 Work unit ADV\_TDS.2-1**

6397 The evaluator **shall examine** the TOE design to determine that the structure of the entire TOE is  
 6398 described in terms of subsystems.

6399 The evaluator ensures that all of the subsystems of the TOE are identified. This description of the  
 6400 TOE will be used as input to work unit ADV\_TDS.2-2, where the parts of the TOE that make up the  
 6401 TSF are identified. That is, this requirement is on the entire TOE rather than on only the TSF.

6402 The TOE (and TSF) may be described in multiple layers of abstraction (i.e. subsystems and  
 6403 modules). Depending upon the complexity of the TOE, its design may be described in terms of  
 6404 subsystems and modules, as described in ISO/IEC 15408-3, Annex A.4, ADV\_TDS: Subsystems and  
 6405 Modules. At this level of assurance, the decomposition only need be at the "subsystem" level.

6406 In performing this activity, the evaluator examines other evidence presented for the TOE (e.g., ST,  
 6407 operator user guidance) to determine that the description of the TOE in such evidence is consistent  
 6408 with the description contained in the TOE design.

6409 ISO/IEC 15408-3 ADV\_TDS.2.2C: *The design shall identify all subsystems of the TSF.*

6410 **11.8.2.2.2 Work unit ADV\_TDS.2-2**

6411 The evaluator ***shall examine*** the TOE design to determine that all subsystems of the TSF are  
6412 identified.

6413 In work unit ADV\_TDS.2-1 all of the subsystems of the TOE were identified, and a determination  
6414 made that the non-TSF subsystems were correctly characterised. Building on that work, the  
6415 subsystems that were not characterised as non-TSF subsystems should be precisely identified. The  
6416 evaluator determines that, of the hardware and software installed and configured according to the  
6417 Preparative procedures (AGD\_PRE) guidance, each subsystem has been accounted for as either one  
6418 that is part of the TSF, or one that is not.

6419 ISO/IEC 15408-3 ADV\_TDS.2.3C: *The design shall describe the behaviour of each SFR non-interfering*  
6420 *subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.*

6421 **11.8.2.2.3 Work unit ADV\_TDS.2-3**

6422 The evaluator ***shall examine*** the TOE design to determine that each SFR-non-interfering  
6423 subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-  
6424 non-interfering.

6425 SFR-non-interfering subsystems do not need to be described in detail as to how they function in  
6426 the system. However, the evaluator makes a determination, based on the evidence provided by the  
6427 developer, that the subsystems that do not have detailed descriptions are SFR-non-interfering.  
6428 Note that if the developer provides a uniform level of detailed documentation then this work unit  
6429 will be largely satisfied, since the point of categorising the subsystems is to allow the developer to  
6430 provide less information for SFR-non-interfering subsystems than for SFR-enforcing and SFR-  
6431 supporting subsystems.

6432 An SFR-non-interfering subsystem is one on which the SFR-enforcing and SFR-supporting  
6433 subsystems have no dependence; that is, they play no role in implementing SFR functionality.

6434 ISO/IEC 15408-3 ADV\_TDS.2.4C: *The design shall describe the SFR-enforcing behaviour of the SFR-*  
6435 *enforcing subsystems.*

6436 **11.8.2.2.4 Work unit ADV\_TDS.2-4**

6437 The evaluator ***shall examine*** the TOE design to determine that it provides a complete, accurate,  
6438 and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

6439 The developer may designate subsystems as SFR-enforcing, SFR-supporting, and SFR non-  
6440 interfering, but these “tags” are used only to describe the amount and type of information the  
6441 developer must provide, and can be used to limit the amount of information the developer has to  
6442 develop if their engineering process does not produce the documentation required. Whether the  
6443 subsystems have been categorised by the developer or not, it is the evaluator's responsibility to  
6444 determine that the subsystems have the appropriate information for their role (SFR-enforcing, etc.)  
6445 in the TOE, and to obtain the appropriate information from the developer should the developer fail  
6446 to provide the required information for a particular subsystem.

6447 SFR-enforcing behaviour refers to *how* a subsystem provides the functionality that implements an  
6448 SFR. While not at the level of an algorithmic description, a detailed description of behaviour  
6449 typically discusses how the functionality is provided in terms of what key data and data structures  
6450 are, what control relationships exist within a subsystem, and how these elements work together to  
6451 provide the SFR-enforcing behaviour. Such a description also references SFR-supporting behaviour,  
6452 which the evaluator should consider in performing subsequent work units.

6453 To determine completeness and accuracy, the evaluator examines other information available (e.g.,  
 6454 functional specification, security architecture description). Descriptions of functionality in these  
 6455 documents should be consistent with what is provided for evidence for this work unit.

6456 ISO/IEC 15408-3 ADV\_TDS.2.5C: *The design shall summarise the SFR-supporting and SFR-non-*  
 6457 *interfering behaviour of the SFR-enforcing subsystems.*

#### 6458 11.8.2.2.5 Work unit ADV\_TDS.2-5

6459 The evaluator **shall examine** the TOE design to determine that it provides a complete and accurate  
 6460 high-level summary of the SFR-supporting and SFR-non-interfering behaviour of the SFR-enforcing  
 6461 subsystems.

6462 The developer may designate subsystems as SFR-enforcing, SFR-supporting, and SFR non-  
 6463 interfering, but these “tags” are used only to describe the amount and type of information the  
 6464 developer must provide, and can be used to limit the amount of information the developer has to  
 6465 develop if their engineering process does not produce the documentation required. Whether the  
 6466 subsystems have been categorised by the developer or not, it is the evaluator’s responsibility to  
 6467 determine that the subsystems have the appropriate information for their role (SFR-enforcing, etc.)  
 6468 in the TOE, and to obtain the appropriate information from the developer should the developer fail  
 6469 to provide the required information for a particular subsystem.

6470 In contrast to the previous work unit, this work unit calls for the evaluator to assess the  
 6471 information provided for SFR-enforcing subsystems that is SFR-supporting or SFR-non-interfering.  
 6472 The goal of this assessment is two-fold. First, it should provide the evaluator greater understanding  
 6473 of the way each subsystem works. Second, this assessment will help the evaluator to determine  
 6474 that all SFR-enforcing behaviour exhibited by a SFR-enforcing subsystem has been described.  
 6475 Unlike the previous work unit, the information provided for the SFR-supporting or SFR-non-  
 6476 interfering behaviour does not have to be as detailed as that provided by the SFR-enforcing  
 6477 behaviour. For example, data structures or data items that do not pertain to SFR-enforcing  
 6478 functionality will likely not need to be described in detail, if at all. It is the evaluator’s  
 6479 determination, however, with respect to what “high-level” means for a particular TOE, and the  
 6480 evaluator obtains enough information from the developer (even if it turns out to be equivalent to  
 6481 information provided for the parts of the subsystem that are SFR-enforcing) to make a sound  
 6482 verdict for this work unit.

6483 The evaluator is cautioned, however, that “perfect” assurance is not a goal nor required by this  
 6484 work unit, so judgement will have to be exercised in determine the amount and composition of the  
 6485 evidence required to make a verdict on this work unit.

6486 To determine completeness and accuracy, the evaluator examines other information available (e.g.,  
 6487 functional specification, security architecture description). Summaries of functionality in these  
 6488 documents should be consistent with what is provided for evidence for this work unit. In particular,  
 6489 the functional specification should be used to determine that the behaviour required to implement  
 6490 the TSF Interfaces described by the functional specification are completely described by the  
 6491 subsystem, since the behaviour will either be SFR-enforcing, SFR-supporting or SFR-non-  
 6492 interfering.

6493 ISO/IEC 15408-3 ADV\_TDS.2.6C: *The design shall summarise the behaviour of the SFR-supporting*  
 6494 *subsystems.*

#### 6495 11.8.2.2.6 Work unit ADV\_TDS.2-6

6496 The evaluator **shall examine** the TOE design to determine that it provides a complete and accurate  
 6497 high-level summary of the behaviour of the SFR-supporting subsystems.

6498 The developer may designate subsystems as SFR-enforcing, SFR-supporting, and SFR non-  
 6499 interfering, but these “tags” are used only to describe the amount and type of information the

## ISO/IEC 18045:2008(E)

6500 developer must provide, and can be used to limit the amount of information the developer has to  
6501 develop if their engineering process does not produce the documentation required. Whether the  
6502 subsystems have been categorised by the developer or not, it is the evaluator's responsibility to  
6503 determine that the subsystems have the appropriate information for their role (SFR-enforcing, etc.)  
6504 in the TOE, and to obtain the appropriate information from the developer should the developer fail  
6505 to provide the required information for a particular subsystem.

6506 In contrast to the previous two work units, this work unit calls for the developer to provide (and  
6507 the evaluator to assess) information about SFR supporting subsystems. Such subsystems should be  
6508 referenced by the descriptions of the SFR-enforcing subsystems, as well as by the descriptions of  
6509 interactions in work unit ADV\_TDS.2-7. The goal of evaluator's assessment, like that for the  
6510 previous work unit, is two-fold. First, it should provide the evaluator with an understanding of the  
6511 way each SFR-supporting subsystem works. Second, the evaluator determines that the behaviour is  
6512 summarized in enough detail so that the way in which the subsystem supports the SFR-enforcing  
6513 behaviour is clear, and that the behaviour is not itself SFR-enforcing. The information provided for  
6514 SFR-supporting subsystem's behaviour does not have to be as detailed as that provided by the SFR-  
6515 enforcing behaviour. For example, data structures or data items that do not pertain to SFR-  
6516 enforcing functionality will likely not need to be described in detail, if at all. It is the evaluator's  
6517 determination, however, with respect to what "high-level" means for a particular TOE, and the  
6518 evaluator obtains enough information from the developer (even if it turns out to be equivalent to  
6519 information provided for the parts of the subsystem that are SFR-enforcing) to make a sound  
6520 verdict for this work unit.

6521 The evaluator is cautioned, however, that "perfect" assurance is not a goal nor required by this  
6522 work unit, so judgement will have to be exercised in determine the amount and composition of the  
6523 evidence required to make a verdict on this work unit.

6524 To determine completeness and accuracy, the evaluator examines other information available (e.g.,  
6525 functional specification, security architecture description). Summaries of functionality in these  
6526 documents should be consistent with what is provided for evidence for this work unit.

6527 ISO/IEC 15408-3 ADV\_TDS.2.7C: *The design shall provide a description of the interactions among all*  
6528 *subsystems of the TSF.*

### 6529 11.8.2.2.7 Work unit ADV\_TDS.2-7

6530 The evaluator **shall examine** the TOE design to determine that interactions between the  
6531 subsystems of the TSF are described.

6532 The goal of describing the interactions between the subsystems is to help provide the reader a  
6533 better understanding of how the TSF performs its functions. These interactions do not need to be  
6534 characterised at the implementation level (e.g., parameters passed from one routine in a subsystem  
6535 to a routine in a different subsystem; global variables; hardware signals (e.g., interrupts) from a  
6536 hardware subsystem to an interrupt-handling subsystem), but the data elements identified for a  
6537 particular subsystem that are going to be used by another subsystem need to be covered in this  
6538 discussion. Any control relationships between subsystems (e.g., a subsystem responsible for  
6539 configuring a rule base for a firewall system and the subsystem that actually implements these  
6540 rules) should also be described.

6541 It should be noted while the developer should characterise all interactions between subsystems,  
6542 the evaluators need to use their own judgement in assessing the completeness of the description. If  
6543 the reason for an interaction is unclear, or if there are SFR-related interactions (discovered, for  
6544 instance, in examining the descriptions of subsystem behaviour) that do not appear to be described,  
6545 the evaluator ensures that this information is provided by the developer. However, if the evaluator  
6546 can determine that interactions among a particular set of subsystems, while incompletely  
6547 described by the developer, will not aid in understanding the overall functionality nor security  
6548 functionality provided by the TSF, then the evaluator may choose to consider the description  
6549 sufficient, and not pursue completeness for its own sake.

6550 ISO/IEC 15408-3 ADV\_TDS.2.8C: *The mapping shall demonstrate that all TSFIs trace to the*  
 6551 *behaviour described in the TOE design that they invoke.*

#### 6552 11.8.2.2.8 Work unit ADV\_TDS.2-8

6553 The evaluator ***shall examine*** the TOE design to determine that it contains a complete and accurate  
 6554 mapping from the TSFI described in the functional specification to the subsystems of the TSF  
 6555 described in the TOE design.

6556 The subsystems described in the TOE design provide a description of how the TSF works at a  
 6557 detailed level for SFR-enforcing portions of the TSF, and at a higher level for other portions of the  
 6558 TSF. The TSFI provide a description of how the implementation is exercised. The evidence from the  
 6559 developer identifies the subsystem that is initially involved when an operation is requested at the  
 6560 TSFI, and identify the various subsystems that are primarily responsible for implementing the  
 6561 functionality. Note that a complete “call tree” for each TSFI is not required for this work unit.

6562 The evaluator assesses the completeness of the mapping by ensuring that all of the TSFI map to at  
 6563 least one subsystem. The verification of accuracy is more complex.

6564 The first aspect of accuracy is that each TSFI is mapped to a subsystem at the TSF boundary. This  
 6565 determination can be made by reviewing the subsystem description and interactions, and from this  
 6566 information determining its place in the architecture. The next aspect of accuracy is that the  
 6567 mapping makes sense. For instance, mapping a TSFI dealing with access control to a subsystem  
 6568 that checks passwords is not accurate. The evaluator should again use judgement in making this  
 6569 determination. The goal is that this information aids the evaluator in understanding the system and  
 6570 implementation of the SFRs, and ways in which entities at the TSF boundary can interact with the  
 6571 TSF. The bulk of the assessment of whether the SFRs are described accurately by the subsystems is  
 6572 performed in other work units.

#### 6573 11.8.2.3 Action ADV\_TDS.2.2E

##### 6574 11.8.2.3.1 Work unit ADV\_TDS.2-9

6575 The evaluator ***shall examine*** the TOE security functional requirements and the TOE design, to  
 6576 determine that all ST security functional requirements are covered by the TOE design.

6577 The evaluator may construct a map between the TOE security functional requirements and the TOE  
 6578 design. This map will likely be from a functional requirement to a set of subsystems. Note that this  
 6579 map may have to be at a level of detail below the component or even element level of the  
 6580 requirements, because of operations (assignments, refinements, selections) performed on the  
 6581 functional requirement by the ST author.

6582 For example, the FDP\_ACC.1 Subset access control component contains an element with  
 6583 assignments. If the ST contained, for instance, ten rules in the FDP\_ACC.1 Subset access control  
 6584 assignment, and these ten rules were implemented in specific places within fifteen modules, it  
 6585 would be inadequate for the evaluator to map FDP\_ACC.1 Subset access control to one subsystem  
 6586 and claim the work unit had been completed. Instead, the evaluator would map FDP\_ACC.1 Subset  
 6587 access control (rule 1) to subsystem A, behaviours x, y, and z; FDP\_ACC.1 Subset access control  
 6588 (rule 2) to subsystem A, behaviours x, p, and q; etc.

##### 6589 11.8.2.3.2 Work unit ADV\_TDS.2-10

6590 The evaluator ***shall examine*** the TOE design to determine that it is an accurate instantiation of all  
 6591 security functional requirements.

6592 The evaluator ensures that each security requirement listed in the TOE security functional  
 6593 requirements subclause of the ST has a corresponding design description in the TOE design that  
 6594 accurately details how the TSF meets that requirement. This requires that the evaluator identify a

6595 collection of subsystems that are responsible for implementing a given functional requirement, and  
6596 then examine those subsystems to understand how the requirement is implemented. Finally, the  
6597 evaluator would assess whether the requirement was accurately implemented.

6598 As an example, if the ST requirements specified a role-based access control mechanism, the  
6599 evaluator would first identify the subsystems that contribute to this mechanism's implementation.  
6600 This could be done by in-depth knowledge or understanding of the TOE design or by work done in  
6601 the previous work unit. Note that this trace is only to identify the subsystems, and is not the  
6602 complete analysis.

6603 The next step would be to understand what mechanism the subsystems implemented. For instance,  
6604 if the design described an implementation of access control based on UNIX-style protection bits,  
6605 the design would not be an accurate instantiation of those access control requirements present in  
6606 the ST example used above. If the evaluator could not determine that the mechanism was  
6607 accurately implemented because of a lack of detail, the evaluator would have to assess whether all  
6608 of the SFR-enforcing subsystems have been identified, or if adequate detail had been provided for  
6609 those subsystems.

### 6610 **11.8.3 Evaluation of sub-activity (ADV\_TDS.3)**

#### 6611 **11.8.3.1 Objectives**

6612 The objective of this sub-activity is to determine whether the TOE design provides a description of  
6613 the TOE in terms of subsystems sufficient to determine the TSF boundary, and provides a  
6614 description of the TSF internals in terms of modules (and optionally higher-level abstractions). It  
6615 provides a detailed description of the SFR-enforcing modules and enough information about the  
6616 SFR-supporting and SFR-non-interfering modules for the evaluator to determine that the SFRs are  
6617 completely and accurately implemented; as such, the TOE design provides an explanation of the  
6618 implementation representation.

#### 6619 **11.8.3.2 Input**

6620 The evaluation evidence for this sub-activity is:

- 6621 a) the ST;
- 6622 b) the functional specification;
- 6623 c) security architecture description;
- 6624 d) the TOE design.

#### 6625 **11.8.3.3 Application notes**

6626 There are three types of activity that the evaluator must undertake with respect to the TOE design.  
6627 First, the evaluator determines that the TSF boundary has been adequately described. Second, the  
6628 evaluator determines that the developer has provided documentation that conforms to the content  
6629 and presentation requirements for this subsystem, and that is consistent with other documentation  
6630 provided for the TOE. Finally, the evaluator must analyse the design information provided for the  
6631 SFR-enforcing modules (at a detailed level) and the SFR-supporting and SFR-non-interfering  
6632 modules (at a less detailed level) to understand how the system is implemented, and with that  
6633 knowledge ensure that the TSFI in the functional specification are adequately described, and that  
6634 the test information adequately tests the TSF (done in the Class ATE: Tests work units).

6635 It is important to note that while the developer is obligated to provide a complete description of  
6636 the TSF (although SFR-enforcing modules will have more detail than the SFR-supporting or SFR-



non-interfering modules), the evaluator is expected to use their judgement in performing their analysis. While the evaluator is expected to look at every module, the detail to which they examine each module may vary. The evaluator analyses each module in order to gain enough understanding to determine the effect of the functionality of the module on the security of the system, and the depth to which they need to analyse the module may vary depending on the module's role in the system. An important aspect of this analysis is that the evaluator should use the other documentation provided (TSS, functional specification, security architecture description, and the TSF internal document) in order to determine that the functionality that is described is correct, and that the implicit designation of SFR-supporting or SFR-non-interfering modules (see below) is supported by their role in the system architecture.

The developer may designate modules as SFR-enforcing, SFR-supporting, and SFR non-interfering, but these "tags" are used only to describe the amount and type of information the developer must provide, and can be used to limit the amount of information the developer has to develop if their engineering process does not produce the documentation required. Whether the modules have been categorised by the developer or not, it is the evaluator's responsibility to determine that the modules have the appropriate information for their role (SFR-enforcing, etc.) in the TOE, and to obtain the appropriate information from the developer should the developer fail to provide the required information for a particular module.

#### 11.8.3.4 Action ADV\_TDS.3.1E

ISO/IEC 15408-3 ADV\_TDS.3.1C: *The design shall describe the structure of the TOE in terms of subsystems.*

##### 11.8.3.4.1 Work unit ADV\_TDS.3-1

The evaluator **shall examine** the TOE design to determine that the structure of the entire TOE is described in terms of subsystems.

The evaluator ensures that all of the subsystems of the TOE are identified. This description of the TOE will be used as input to work unit ADV\_TDS.3-2, where the parts of the TOE that make up the TSF are identified. That is, this requirement is on the entire TOE rather than on only the TSF.

The TOE (and TSF) may be described in multiple layers of abstraction (i.e. subsystems and modules). Depending upon the complexity of the TOE, its design may be described in terms of subsystems and modules, as described in ISO/IEC 15408-3 Annex A.4, ADV\_TDS: Subsystems and Modules. For a very simple TOE that can be described solely at the "module" level (see ADV\_TDS.3-2), this work unit is not applicable and therefore considered to be satisfied.

In performing this activity, the evaluator examines other evidence presented for the TOE (e.g., ST, operator user guidance) to determine that the description of the TOE in such evidence is consistent with the description contained in the TOE design.

ISO/IEC 15408-3 ADV\_TDS.3.2C: *The design shall describe the TSF in terms of modules.*

##### 11.8.3.4.2 Work unit ADV\_TDS.3-2

The evaluator **shall examine** the TOE design to determine that the entire TSF is described in terms of modules.

The evaluator will examine the modules for specific properties in other work units; in this work unit the evaluator determines that the modular description covers the entire TSF, and not just a portion of the TSF. The evaluator uses other evidence provided for the evaluation (e.g., functional specification, security architecture description) in making this determination. For example, if the functional specification contains interfaces to functionality that does not appear to be described in the TOE design description, it may be the case that a portion of the TSF has not been included appropriately. Making this determination will likely be an iterative process, where as more analysis

## ISO/IEC 18045:2008(E)

6683 is done on the other evidence, more confidence can be gained with respect to the completeness of  
6684 the documentation.

6685 Unlike subsystems, modules describe the implementation in a level of detail that can serve as a  
6686 guide to reviewing the implementation representation. A description of a module should be such  
6687 that one could create an implementation of the module from the description, and the resulting  
6688 implementation would be 1) identical to the actual TSF implementation in terms of the interfaces  
6689 presented, 2) identical in the use of interfaces that are mentioned in the design, and 3) functionally  
6690 equivalent to the description of the purpose of the TSF module. For instance, RFC 793 provides a  
6691 high-level description of the TCP protocol. It is necessarily implementation independent. While it  
6692 provides a wealth of detail, it is **not** a suitable design description because it is not specific to an  
6693 implementation. An actual implementation can add to the protocol specified in the RFC, and  
6694 implementation choices (for instance, the use of global data vs. local data in various parts of the  
6695 implementation) may have an impact on the analysis that is performed. The design description of  
6696 the TCP module would list the interfaces presented by the implementation (rather than just those  
6697 defined in RFC 793), as well as an algorithm description of the processing associated with the  
6698 modules implementing TCP (assuming it was part of the TSF).

6699 ISO/IEC 15408-3 ADV\_TDS.3.3C: *The design shall identify all subsystems of the TSF.*

### 6700 11.8.3.4.3 Work unit ADV\_TDS.3-3

6701 The evaluator **shall examine** the TOE design to determine that all subsystems of the TSF are  
6702 identified.

6703 If the design is presented solely in terms of modules, then subsystems in these requirements are  
6704 equivalent to modules and the activity should be performed at the module level.

6705 In work unit ADV\_TDS.3-1 all of the subsystems of the TOE were identified, and a determination  
6706 made that the non-TSF subsystems were correctly characterised. Building on that work, the  
6707 subsystems that were not characterised as non-TSF subsystems should be precisely identified. The  
6708 evaluator determines that, of the hardware and software installed and configured according to the  
6709 Preparative procedures (AGD\_PRE) guidance, each subsystem has been accounted for as either one  
6710 that is part of the TSF, or one that is not.

6711 ISO/IEC 15408-3 ADV\_TDS.3.4C: *The design shall provide a description of each subsystem of the TSF.*

### 6712 11.8.3.4.4 Work unit ADV\_TDS.3-4

6713 The evaluator **shall examine** the TOE design to determine that each subsystem of the TSF  
6714 describes its role in the enforcement of SFRs described in the ST.

6715 If the design is presented solely in terms of modules, then this work unit will be considered  
6716 satisfied by the assessment done in subsequent work units; no explicit action on the part of the  
6717 evaluator is necessary in this case.

6718 On systems that are complex enough to warrant a subsystem-level description of the TSF in  
6719 addition to the modular description, the goal of the subsystem-level description is to give the  
6720 evaluator context for the modular description that follows. Therefore, the evaluator ensures that  
6721 the subsystem-level description contains a description of how the security functional requirements  
6722 are achieved in the design, but at a level of abstraction above the modular description. This  
6723 description should discuss the mechanisms used at a level that is aligned with the module  
6724 description; this will provide the evaluators the road map needed to intelligently assess the  
6725 information contained in the module description. A well-written set of subsystem descriptions will  
6726 help guide the evaluator in determining the modules that are most important to examine, thus  
6727 focusing the evaluation activity on the portions of the TSF that have the most relevance with  
6728 respect to the enforcement of the SFRs.

6729 The evaluator ensures that all subsystems of the TSF have a description. While the description  
 6730 should focus on the role that the subsystem plays in enforcing or supporting the implementation of  
 6731 the SFRs, enough information must be present so that a context for understanding the SFR-related  
 6732 functionality is provided.

#### 6733 11.8.3.4.5 Work unit ADV\_TDS.3-5

6734 The evaluator *shall examine* the TOE design to determine that each SFR-non-interfering  
 6735 subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-  
 6736 non-interfering.

6737 If the design is presented solely in terms of modules, then this work unit will be considered  
 6738 satisfied by the assessment done in subsequent work units; no explicit action on the part of the  
 6739 evaluator is necessary in this case.

6740 An SFR-non-interfering subsystem is one on which the SFR-enforcing and SFR-supporting  
 6741 subsystems have no dependence; that is, they play no role in implementing SFR functionality.

6742 The evaluator ensures that all subsystems of the TSF have a description. While the description  
 6743 should focus on the role that the subsystem do not plays in enforcing or supporting the  
 6744 implementation of the SFRs, enough information must be present so that a context for  
 6745 understanding the SFR-non-interfering functionality is provided.

6746 ISO/IEC 15408-3 ADV\_TDS.3.5C: *The design shall provide a description of the interactions among all*  
 6747 *subsystems of the TSF.*

#### 6748 11.8.3.4.6 Work unit ADV\_TDS.3-6

6749 The evaluator *shall examine* the TOE design to determine that interactions between the  
 6750 subsystems of the TSF are described.

6751 If the design is presented solely in terms of modules, then this work unit will be considered  
 6752 satisfied by the assessment done in subsequent work units; no explicit action on the part of the  
 6753 evaluator is necessary in this case.

6754 On systems that are complex enough to warrant a subsystem-level description of the TSF in  
 6755 addition to the modular description, the goal of describing the interactions between the  
 6756 subsystems is to help provide the reader a better understanding of how the TSF performs its  
 6757 functions. These interactions do not need to be characterised at the implementation level (e.g.,  
 6758 parameters passed from one routine in a subsystem to a routine in a different subsystem; global  
 6759 variables; hardware signals (e.g., interrupts) from a hardware subsystem to an interrupt-handling  
 6760 subsystem), but the data elements identified for a particular subsystem that are going to be used  
 6761 by another subsystem should be covered in this discussion. Any control relationships between  
 6762 subsystems (e.g., a subsystem responsible for configuring a rule base for a firewall system and the  
 6763 subsystem that actually implements these rules) should also be described.

6764 It should be noted while the developer should characterise all interactions between subsystems,  
 6765 the evaluators need to use their own judgement in assessing the completeness of the description. If  
 6766 the reason for an interaction is unclear, or if there are SFR-related interactions (discovered, for  
 6767 instance, in examining the module-level documentation) that do not appear to be described, the  
 6768 evaluator ensures that this information is provided by the developer. However, if the evaluator can  
 6769 determine that interactions among a particular set of subsystems, while incompletely described by  
 6770 the developer, and a complete description will not aid in understanding the overall functionality  
 6771 nor security functionality provided by the TSF, then the evaluator may choose to consider the  
 6772 description sufficient, and not pursue completeness for its own sake.

6773 ISO/IEC 15408-3 ADV\_TDS.3.6C: *The design shall provide a mapping from the subsystems of the TSF*  
 6774 *to the modules of the TSF.*

## ISO/IEC 18045:2008(E)

### 6775 11.8.3.4.7 Work unit ADV\_TDS.3-7

6776 The evaluator **shall examine** the TOE design to determine that the mapping between the  
6777 subsystems of the TSF and the modules of the TSF is complete.

6778 If the design is presented solely in terms of modules, then this work unit is considered satisfied.

6779 For TOEs that are complex enough to warrant a subsystem-level description of the TSF in addition  
6780 to the modular description, the developer provides a simple mapping showing how the modules of  
6781 the TSF are allocated to the subsystems. This will provide the evaluator a guide in performing their  
6782 module-level assessment. To determine completeness, the evaluator examines each mapping and  
6783 determines that all subsystems map to at least one module, and that all modules map to exactly one  
6784 subsystem.

### 6785 11.8.3.4.8 Work unit ADV\_TDS.3-8

6786 The evaluator **shall examine** the TOE design to determine that the mapping between the  
6787 subsystems of the TSF and the modules of the TSF is accurate.

6788 If the design is presented solely in terms of modules, then this work unit is considered satisfied.

6789 For TOEs that are complex enough to warrant a subsystem-level description of the TSF in addition  
6790 to the modular description, the developer provides a simple mapping showing how the modules of  
6791 the TSF are allocated to the subsystems. This will provide the evaluator a guide in performing their  
6792 module-level assessment. The evaluator may choose to check the accuracy of the mapping in  
6793 conjunction with performing other work units. An "inaccurate" mapping is one where the module  
6794 is mistakenly associated with a subsystem where its functions are not used within the subsystem.  
6795 Because the mapping is intended to be a guide supporting more detailed analysis, the evaluator is  
6796 cautioned to apply appropriate effort to this work unit. Expending extensive evaluator resources  
6797 verifying the accuracy of the mapping is not necessary. Inaccuracies that lead to mis-  
6798 understandings related to the design that are uncovered as part of this or other work units are the  
6799 ones that should be associated with this work unit and corrected.

6800 ISO/IEC 15408-3 ADV\_TDS.3.7C: *The design shall describe each SFR-enforcing module in terms of its*  
6801 *purpose and relationship with other modules.*

### 6802 11.8.3.4.9 Work unit ADV\_TDS.3-9

6803 The evaluator **shall examine** the TOE design to determine that the description of the purpose of  
6804 each SFR-enforcing module and relationship with other modules is complete and accurate.

6805 The developer may designate modules as SFR-enforcing, SFR-supporting, and SFR non-interfering,  
6806 but these "tags" are used only to describe the amount and type of information the developer must  
6807 provide, and can be used to limit the amount of information the developer has to develop if their  
6808 engineering process does not produce the documentation required. Whether the modules have  
6809 been categorised by the developer or not, it is the evaluator's responsibility to determine that the  
6810 modules have the appropriate information for their role (SFR-enforcing, etc.) in the TOE, and to  
6811 obtain the appropriate information from the developer should the developer fail to provide the  
6812 required information for a particular module.

6813 The purpose of a module provides a description indicating what function the module is fulfilling. A  
6814 word of caution to evaluator is in order. The focus of this work unit should be to provide the  
6815 evaluator an understanding of how the module works so that determinations can be made about  
6816 the soundness of the implementation of the SFRs, as well as to support architectural analysis  
6817 performed for ADV\_ARC component. As long as the evaluator has a sound understanding of the  
6818 module's operation, and its relationship to other modules and the TOE as a whole, the evaluator  
6819 should consider the objective of the work achieved and not engage in a documentation exercise for

6820 the developer (by requiring, for example, a complete algorithmic description for a self-evident  
6821 implementation representation).

6822 Because the modules are at such a low level, it may be difficult to determine completeness and  
6823 accuracy impacts from other documentation, such as operational user guidance, the functional  
6824 specification, the TSF internals, or the security architecture description. However, the evaluator  
6825 uses the information present in those documents to the extent possible to help ensure that the  
6826 purpose is accurately and completely described. This analysis can be aided by the analysis  
6827 performed for the work units for the ADV\_TDS.3.10C element, which maps the TSFI in the  
6828 functional specification to the modules of the TSF.

6829 ISO/IEC 15408-3 ADV\_TDS.3.8C: *The design shall describe each SFR-enforcing module in terms of its*  
6830 *SFR-related interfaces, return values from those interfaces, interaction with other modules and called*  
6831 *SFR-related interfaces to other SFR-enforcing modules.*

#### 6832 11.8.3.4.10 Work unit ADV\_TDS.3-10

6833 The evaluator **shall examine** the TOE design to determine that the description of the interfaces  
6834 presented by each SFR-enforcing module contain an accurate and complete description of the SFR-  
6835 related parameters, the calling conventions for each interface, and any values returned directly by  
6836 the interface.

6837 The SFR-related interfaces of a module are those interfaces used by other modules as a means to  
6838 invoke the SFR-related operations provided, and to provide inputs to or receive outputs from the  
6839 module. The purpose in the specification of these interfaces is to permit the exercise of them  
6840 during testing. Inter-module interfaces that are not SFR-related need not be specified or described,  
6841 since they are not a factor in testing. Likewise, other internal interfaces that are not a factor in  
6842 traversing SFR-related paths of execution (such as those internal paths that are fixed) need not be  
6843 specified or described, since they are not a factor in testing.

6844 SFR-related interfaces are described in terms of how they are invoked, and any values that are  
6845 returned. This description would include a list of SFR-related parameters, and descriptions of these  
6846 parameters. Note that global data would also be considered parameters if used by the module  
6847 (either as inputs or outputs) when invoked. If a parameter were expected to take on a set of values  
6848 (e.g., a "flag" parameter), the complete set of values the parameter could take on that would have  
6849 an effect on module processing would be specified. Likewise, parameters representing data  
6850 structures are described such that each field of the data structure is identified and described. Note  
6851 that different programming languages may have additional "interfaces" that would be non-obvious;  
6852 an example would be operator/function overloading in C++. This "implicit interface" in the class  
6853 description would also be described as part of the low-level TOE design. Note that although a  
6854 module could present only one interface, it is more common that a module presents a small set of  
6855 related interfaces.

6856 In terms of the assessment of parameters (inputs and outputs) to a module, any use of global data  
6857 must also be considered. A module "uses" global data if it either reads or writes the data. In order  
6858 to assure the description of such parameters (if used) is complete, the evaluator uses other  
6859 information provided about the module in the TOE design (interfaces, algorithmic description, etc.),  
6860 as well as the description of the particular set of global data assessed in work unit ADV\_TDS.3-10.  
6861 For instance, the evaluator could first determine the processing the module performs by examining  
6862 its function and interfaces presented (particularly the parameters of the interfaces). They could  
6863 then check to see if the processing appears to "touch" any of the global data areas identified in the  
6864 TOE design. The evaluator then determines that, for each global data area that appears to be  
6865 "touched", that global data area is listed as a means of input or output by the module the evaluator  
6866 is examining.

6867 Invocation conventions are a programming-reference-type description that one could use to  
6868 correctly invoke a module's interface if one were writing a program to make use of the module's

## ISO/IEC 18045:2008(E)

6869 functionality through that interface. This includes necessary inputs and outputs, including any set-  
6870 up that may need to be performed with respect to global variables.

6871 Values returned through the interface refer to values that are either passed through parameters or  
6872 messages; values that the function call itself returns in the style of a "C" program function call; or  
6873 values passed through global means (such as certain error routines in \*ix-style operating systems).

6874 In order to assure the description is complete, the evaluator uses other information provided about  
6875 the module in the TOE design (e.g., algorithmic description, global data used) to ensure that it  
6876 appears all data necessary for performing the functions of the module is presented to the module,  
6877 and that any values that other modules expect the module under examination to provide are  
6878 identified as being returned by the module. The evaluator determines accuracy by ensuring that  
6879 the description of the processing matches the information listed as being passed to or from an  
6880 interface.

6881 ISO/IEC 15408-3 ADV\_TDS.3.9C: *The design shall describe each SFR-supporting or SFR-non-*  
6882 *interfering module in terms of its purpose and interaction with other modules.*

### 6883 11.8.3.4.11 Work unit ADV\_TDS.3-11

6884 The evaluator **shall examine** the TOE design to determine that SFR-supporting and SFR-non-  
6885 interfering modules are correctly categorised.

6886 In the cases where the developer has provided different amounts of information for different  
6887 modules, an implicit categorisation has been done. That is, modules (for instance) with detail  
6888 presented on their SFR-related interfaces (see ADV\_TDS.3.10C) are candidate SFR-enforcing  
6889 modules, although examination by the evaluator may lead to a determination that some set of them  
6890 are SFR-supporting or SFR-non-interfering. Those with only a description of their purpose and  
6891 interaction with other modules (for instance) are "implicitly categorised" as SFR-supporting or  
6892 SFR-non-interfering.

6893 In these cases, a key focus of the evaluator for this work unit is attempting to determine from the  
6894 evidence provided for each module implicitly categorised as SFR-supporting or SFR-non-  
6895 interfering and the evaluation information about other modules (in the TOE design, the functional  
6896 specification, the security architecture description, and the operational user guidance), whether  
6897 the module is indeed SFR-supporting or SFR-non-interfering. At this level of assurance some error  
6898 should be tolerated; the evaluator does not have to be absolutely sure that a given module is SFR-  
6899 supporting or SFR-non-interfering, even though it is labelled as such. However, if the evidence  
6900 provided indicates that a SFR-supporting or SFR-non-interfering module is SFR-enforcing, the  
6901 evaluator requests additional information from the developer in order to resolve the apparent  
6902 inconsistency. For instance, suppose the documentation for Module A (an SFR-enforcing module)  
6903 indicates that it calls Module B to perform an access check on a certain type of construct. When the  
6904 evaluator examines the information associated with Module B, they find that all the developer has  
6905 provided is a purpose and a set of interactions (thus implicitly categorising Module B as SFR-  
6906 supporting or SFR-non-interfering). On examining the purpose and interactions from Module A, the  
6907 evaluator finds no mention of Module B performing any access checks, and Module A is not listed  
6908 as a module with which Module B interacts. At this point the evaluator should approach the  
6909 developer to resolve the discrepancies between the information provided in Module A and that in  
6910 Module B.

6911 Another example would be where the evaluator examines the mapping of the TSFI to the modules  
6912 as provided by ADV\_TDS.3.2D. This examination shows that Module C is associated with an SFR  
6913 requiring identification of the user. Again, when the evaluator examines the information associated  
6914 with Module C, they find that all the developer has provided is a purpose and a set of interactions  
6915 (thus implicitly categorising Module C as SFR-supporting or SFR-non-interfering). Examining the  
6916 purpose and interactions presented for Module C, the evaluator is unable to determine why Module  
6917 C, listed as mapping to a TSFI concerned with user identification, would not be classified as SFR-  
6918 enforcing. Again, the evaluator should approach the developer to resolve this discrepancy.

A final example is from the opposite point of view. As before, the developer has provided information associated with Module D consisting of a purpose and a set of interactions (thus implicitly categorising Module D as SFR-supporting or SFR-non-interfering). The evaluator examines all of the evidence provided, including the purpose and interactions for Module D. The purpose appears to give a meaningful description of Module D's function in the TOE, the interactions are consistent with that description, and there is nothing to indicate that Module D is SFR-enforcing. In this case, the evaluator should not demand more information about Module D "just to be sure" it is correctly categorised. The developer has met their obligations and the resulting assurance the evaluator has in the implicit categorisation of Module D is (by definition) appropriate for this assurance level.

#### 11.8.3.4.12 Work unit ADV\_TDS.3-12

The evaluator *shall examine* the TOE design to determine that the description of the purpose of each SFR-supporting or SFR-non-interfering module is complete and accurate.

The description of the purpose of a module indicates what function the module is fulfilling. From the description, the evaluator should be able to obtain a general idea of the module's role. In order to assure the description is complete, the evaluator uses the information provided about the module's interactions with other modules to assess whether the reasons for the module being called are consistent with the module's purpose. If the interaction description contains functionality that is not apparent from, or in conflict with, the module's purpose, the evaluator needs to determine whether the problem is one of accuracy or of completeness. The evaluator should be wary of purposes that are too short, since meaningful analysis based on a one-sentence purpose is likely to be impossible.

Because the modules are at such a low level, it may be difficult to determine completeness and accuracy impacts from other documentation, such as administrative guidance, the functional specification, the security architecture description, or the TSF internals document. However, the evaluator uses the information present in those documents to the extent possible to help ensure that the function is accurately and completely described. This analysis can be aided by the analysis performed for the work units for the ADV\_TDS.3.10C element, which maps the TSFI in the functional specification to the modules of the TSF.

#### 11.8.3.4.13 Work unit ADV\_TDS.3-13

The evaluator *shall examine* the TOE design to determine that the description of a SFR-supporting or SFR-non-interfering module's interaction with other modules is complete and accurate.

It is important to note that, in terms of the Part 3 requirement and this work unit, the term *interaction* is intended to convey less rigour than *interface*. An interaction does not need to be characterised at the implementation level (e.g., parameters passed from one routine in a module to a routine in a different module; global variables; hardware signals (e.g., interrupts) from a hardware subsystem to an interrupt-handling subsystem), but the data elements identified for a particular module that are going to be used by another module should be covered in this discussion. Any control relationships between modules (e.g., a module responsible for configuring a rule base for a firewall system and the module that actually implements these rules) should also be described.

Because the modules are at such a low level, it may be difficult to determine completeness and accuracy impacts from other documentation, such as operational user guidance, the functional specification, the security architecture description, or the TSF internals document. However, the evaluator uses the information present in those documents to the extent possible to help ensure that the function is accurately and completely described. This analysis can be aided by the analysis performed for the work units for the ADV\_TDS.3.10C element, which maps the TSFI in the functional specification to the modules of the TSF.

## ISO/IEC 18045:2008(E)

6967 A module's interaction with other modules goes beyond just a call-tree-type document. The  
6968 interaction is described from a functional perspective of why a module interacts with other  
6969 modules. The module's purpose describes what functions the module provides to other modules;  
6970 the interactions should describe what the module depends on from other modules in order to  
6971 accomplish this function.

6972 ISO/IEC 15408-3 ADV\_TDS.3.10C: *The mapping shall demonstrate that all TSFIs trace to the*  
6973 *behaviour described in the TOE design that they invoke.*

### 6974 11.8.3.4.14 Work unit ADV\_TDS.3-14

6975 The evaluator **shall examine** the TOE design to determine that it contains a complete and accurate  
6976 mapping from the TSFI described in the functional specification to the modules of the TSF  
6977 described in the TOE design.

6978 The modules described in the TOE design provide a description of the implementation of the TSF.  
6979 The TSFI provide a description of how the implementation is exercised. The evidence from the  
6980 developer identifies the module that is initially invoked when an operation is requested at the TSFI,  
6981 and identifies the chain of modules invoked up to the module that is primarily responsible for  
6982 implementing the functionality. However, a complete call tree for each TSFI is not required for this  
6983 work unit. The cases in which more than one module would have to be identified are where there  
6984 are "entry point" modules or wrapper modules that have no functionality other than conditioning  
6985 inputs or de-multiplexing an input. Mapping to one of these modules would not provide any useful  
6986 information to the evaluator.

6987 The evaluator assesses the completeness of the mapping by ensuring that all of the TSFI map to at  
6988 least one module. The verification of accuracy is more complex.

6989 The first aspect of accuracy is that each TSFI is mapped to a module at the TSF boundary. This  
6990 determination can be made by reviewing the module description and its interfaces/interactions.  
6991 The next aspect of accuracy is that each TSFI identifies a chain of modules between the initial  
6992 module identified and a module that is primarily responsible for implementing the function  
6993 presented at the TSF. Note that this may be the initial module, or there may be several modules,  
6994 depending on how much pre-conditioning of the inputs is done. It should be noted that one  
6995 indicator of a pre-conditioning module is that it is invoked for a large number of the TSFI, where  
6996 the TSFI are all of similar type (e.g., system call). The final aspect of accuracy is that the mapping  
6997 makes sense. For instance, mapping a TSFI dealing with access control to a module that checks  
6998 passwords is not accurate. The evaluator should again use judgement in making this determination.  
6999 The goal is that this information aids the evaluator in understanding the system and  
7000 implementation of the SFRs, and ways in which entities at the TSF boundary can interact with the  
7001 TSF. The bulk of the assessment of whether the SFRs are described accurately by the modules is  
7002 performed in other work units.

### 7003 11.8.3.5 Action ADV\_TDS.3.2E

#### 7004 11.8.3.5.1 Work unit ADV\_TDS.3-15

7005 The evaluator **shall examine** the TOE security functional requirements and the TOE design, to  
7006 determine that all ST security functional requirements are covered by the TOE design.

7007 The evaluator may construct a map between the TOE security functional requirements and the TOE  
7008 design. This map will likely be from a functional requirement to a set of subsystems, and later to  
7009 modules. Note that this map may have to be at a level of detail below the component or even  
7010 element level of the requirements, because of operations (assignments, refinements, selections)  
7011 performed on the functional requirement by the ST author.

7012 For example, the FDP\_ACC.1 Subset access control FDP\_ACC.1 Subset access control component  
7013 contains an element with assignments. If the ST contained, for instance, ten rules in the FDP\_ACC.1



7014 Subset access control assignment, and these ten rules were implemented in specific places within  
 7015 fifteen modules, it would be inadequate for the evaluator to map FDP\_ACC.1 Subset access control  
 7016 to one subsystem and claim the work unit had been completed. Instead, the evaluator would map  
 7017 FDP\_ACC.1 Subset access control (rule 1) to modules x, y, and z of subsystem A; FDP\_ACC.1 Subset  
 7018 access control (rule 2) to modules x, p, and q of subsystem A; etc.

#### 7019 11.8.3.5.2 Work unit ADV\_TDS.3-16

7020 The evaluator *shall examine* the TOE design to determine that it is an accurate instantiation of all  
 7021 security functional requirements.

7022 The evaluator may construct a map between the TOE security functional requirements and the TOE  
 7023 design. This map will likely be from a functional requirement to a set of subsystems. Note that this  
 7024 map may have to be at a level of detail below the component or even element level of the  
 7025 requirements, because of operations (assignments, refinements, selections) performed on the  
 7026 functional requirement by the ST author.

7027 As an example, if the ST requirements specified a role-based access control mechanism, the  
 7028 evaluator would first identify the subsystems, and modules that contribute to this mechanism's  
 7029 implementation. This could be done by in-depth knowledge or understanding of the TOE design or  
 7030 by work done in the previous work unit. Note that this trace is only to identify the subsystems, and  
 7031 modules, and is not the complete analysis.

7032 The next step would be to understand what mechanism the subsystems, and modules implemented.  
 7033 For instance, if the design described an implementation of access control based on UNIX-style  
 7034 protection bits, the design would not be an accurate instantiation of those access control  
 7035 requirements present in the ST example used above. If the evaluator could not determine that the  
 7036 mechanism was accurately implemented because of a lack of detail, the evaluator would have to  
 7037 assess whether all of the SFR-enforcing subsystems and modules have been identified, or if  
 7038 adequate detail had been provided for those subsystems and modules.

### 7039 11.8.4 Evaluation of sub-activity (ADV\_TDS.4)

#### 7040 11.8.4.1 Objectives

7041 The objective of this sub-activity is to determine whether the TOE design provides a description of  
 7042 the TOE in terms of subsystems sufficient to determine the TSF boundary, and provides a  
 7043 description of the TSF internals in terms of modules (and optionally higher-level abstractions). It  
 7044 provides a detailed description of the SFR-enforcing and SFR-supporting modules and enough  
 7045 information about the SFR-non-interfering modules for the evaluator to determine that the SFRs  
 7046 are completely and accurately implemented; as such, the TOE design provides an explanation of the  
 7047 implementation representation.

#### 7048 11.8.4.2 Input

7049 The evaluation evidence for this sub-activity is:

- 7050 a) the ST;
- 7051 b) the functional specification;
- 7052 c) security architecture description;
- 7053 d) the TOE design.

## ISO/IEC 18045:2008(E)

### 7054 11.8.4.3 Application notes

7055 There are three types of activity that the evaluator must undertake with respect to the TOE design.  
7056 First, the evaluator determines that the TSF boundary has been adequately described. Second, the  
7057 evaluator determines that the developer has provided documentation that conforms to the content  
7058 and presentation requirements this subsystem, and that is consistent with other documentation  
7059 provided for the TOE. Finally, the evaluator must analyse the design information provided for the  
7060 SFR-enforcing modules (at a detailed level) and the SFR-supporting and SFR-non-interfering  
7061 modules (at a less detailed level) to understand how the system is implemented, and with that  
7062 knowledge ensure that the TSFI in the functional specification are adequately described, and that  
7063 the test information adequately tests the TSF (done in the Class ATE: Tests work units).

### 7064 11.8.4.4 Action ADV\_TDS.4.1E

7065 ISO/IEC 15408-3 ADV\_TDS.4.1C: *The design shall describe the structure of the TOE in terms of*  
7066 *subsystems.*

#### 7067 11.8.4.4.1 Work unit ADV\_TDS.4-1

7068 The evaluator **shall examine** the TOE design to determine that the structure of the entire TOE is  
7069 described in terms of subsystems.

7070 The evaluator ensures that all of the subsystems of the TOE are identified. This description of the  
7071 TOE will be used as input to work unit ADV\_TDS.4-4, where the parts of the TOE that make up the  
7072 TSF are identified. That is, this requirement is on the entire TOE rather than on only the TSF.

7073 The TOE (and TSF) may be described in multiple layers of abstraction (i.e. subsystems and  
7074 modules). Depending upon the complexity of the TOE, its design may be described in terms of  
7075 subsystems and modules, as described in ISO/IEC 15408-3 Annex A.4, ADV\_TDS: Subsystems and  
7076 Modules. For a very simple TOE that can be described solely at the "module" level (see ADV\_TDS.4-  
7077 2), this work unit is not applicable and therefore considered to be satisfied.

7078 In performing this activity, the evaluator examines other evidence presented for the TOE (e.g., ST,  
7079 operator user guidance) to determine that the description of the TOE in such evidence is consistent  
7080 with the description contained in the TOE design.

7081 ISO/IEC 15408-3 ADV\_TDS.4.2C: *The design shall describe the TSF in terms of modules, designating*  
7082 *each module as SFR-enforcing, SFR-supporting, or SFR-non-interfering.*

#### 7083 11.8.4.4.2 Work unit ADV\_TDS.4-2

7084 The evaluator **shall examine** the TOE design to determine that the entire TSF is described in terms  
7085 of modules.

7086 The evaluator will examine the modules for specific properties in other work units; in this work  
7087 unit the evaluator determines that the modular description covers the entire TSF, and not just a  
7088 portion of the TSF. The evaluator uses other evidence provided for the evaluation (e.g., functional  
7089 specification, architectural description) in making this determination. For example, if the functional  
7090 specification contains interfaces to functionality that does not appear to be described in the TOE  
7091 design description, it may be the case that a portion of the TSF has not been included appropriately.  
7092 Making this determination will likely be an iterative process, whereas more analysis is done on the  
7093 other evidence, more confidence can be gained with respect to the completeness of the  
7094 documentation.

7095 Unlike subsystems, modules describe the implementation in a level of detail that can serve as a  
7096 guide to reviewing the implementation representation. A description of a module should be such  
7097 that one could create an implementation of the module from the description, and the resulting  
7098 implementation would be 1) identical to the actual TSF implementation in terms of the interfaces

7099 presented, 2) identical in the use of interfaces that are mentioned in the design, and 3) functionally  
 7100 equivalent to the description of the purpose of the TSF module. For instance, RFC 793 provides a  
 7101 high-level description of the TCP protocol. It is necessarily implementation independent. While it  
 7102 provides a wealth of detail, it is **not** a suitable design description because it is not specific to an  
 7103 implementation. An actual implementation can add to the protocol specified in the RFC, and  
 7104 implementation choices (for instance, the use of global data vs. local data in various parts of the  
 7105 implementation) may have an impact on the analysis that is performed. The design description of  
 7106 the TCP module would list the interfaces presented by the implementation (rather than just those  
 7107 defined in RFC 793), as well as an algorithm description of the processing associated with the  
 7108 modules implementing TCP (assuming it was part of the TSF).

#### 7109 11.8.4.4.3 Work unit ADV\_TDS.4-3

7110 The evaluator **shall check** the TOE design to determine that the TSF modules are identified as  
 7111 either SFR-enforcing, SFR-supporting, or SFR-non-interfering.

7112 The purpose of designating each module (according to the role a particular module plays in the  
 7113 enforcement of the SFRs) is to allow developers to provide less information about the parts of the  
 7114 TSF that have little role in security. It is always permissible for the developer to provide more  
 7115 information or detail than the requirements demand, as might occur when the information has  
 7116 been gathered outside the evaluation context. In such cases the developer must still designate the  
 7117 modules as either SFR-enforcing, SFR-supporting, or SFR-non-interfering.

7118 The accuracy of these designations is continuously reviewed as the evaluation progresses. The  
 7119 concern is the mis-designation of modules as being less important (and hence, having less  
 7120 information) than is really the case. While blatant mis-designations may be immediately apparent  
 7121 (e.g., designating an authentication module as anything but SFR-enforcing when User identification  
 7122 (FIA\_UID) is one of the SFRs being claimed), other mis-designations might not be discovered until  
 7123 the TSF is better understood. The evaluator must therefore keep in mind that these designations  
 7124 are the developer's initial best effort, but are subject to change. Further guidance is provided under  
 7125 work unit ADV\_TDS.4-17, which examines the accuracy of these designations.

7126 ISO/IEC 15408-3 ADV\_TDS.4.3C: *The design shall identify all subsystems of the TSF.*

#### 7127 11.8.4.4.4 Work unit ADV\_TDS.4-4

7128 The evaluator **shall examine** the TOE design to determine that all subsystems of the TSF are  
 7129 identified.

7130 If the design is presented solely in terms of modules, then subsystems in these requirements are  
 7131 equivalent to modules and the activity should be performed at the module level.

7132 In work unit ADV\_TDS.4-1 all of the subsystems of the TOE were identified, and a determination  
 7133 made that the non-TSF subsystems were correctly characterised. Building on that work, the  
 7134 subsystems that were not characterised as non-TSF subsystems should be precisely identified. The  
 7135 evaluator determines that, of the hardware and software installed and configured according to the  
 7136 Preparative procedures (AGD\_PRE) guidance, each subsystem has been accounted for as either one  
 7137 that is part of the TSF, or one that is not.

7138 ISO/IEC 15408-3 ADV\_TDS.4.4C: *The design shall provide a semiformal description of each  
 7139 subsystem of the TSF, supported by informal, explanatory text where appropriate.*

#### 7140 11.8.4.4.5 Work unit ADV\_TDS.4-5

7141 The evaluator **shall examine** the TDS documentation to determine that the semiformal notation  
 7142 used for describing the subsystems, modules and their interfaces is defined or referenced.

7143 A semiformal notation can be either defined by the sponsor or a corresponding standard be  
7144 referenced. The evaluator should provide a mapping of security functions and their interfaces  
7145 outlining in what part of the documentation a function or interface is semiformal described and  
7146 what notation is used. The evaluator examines all semiformal notations used to make sure that  
7147 they are of a semiformal style and to justify the appropriateness of the manner how the semiformal  
7148 notations are used for the TOE.

7149 The evaluator is reminded that a semi-formal presentation is characterised by a standardised  
7150 format with a well-defined syntax that reduces ambiguity that may occur in informal presentations.  
7151 The syntax of all semiformal notations used in the functional specification shall be defined or a  
7152 corresponding standard be referenced. The evaluator verifies that the semiformal notations used  
7153 for expressing the functional specification are capable of expressing features relevant to security.  
7154 In order to determine this, the evaluator can refer to the SFR and compare the TSF security  
7155 features stated in the ST and those described in the FSP using the semiformal notations.

#### 7156 11.8.4.4.6 Work unit ADV\_TDS.4-6

7157 The evaluator **shall examine** the TOE design to determine that each subsystem of the TSF  
7158 describes its role in the enforcement of SFRs described in the ST.

7159 If the design is presented solely in terms of modules, then this work unit will be considered  
7160 satisfied by the assessment done in subsequent work units; no explicit action on the part of the  
7161 evaluator is necessary in this case.

7162 On systems that are complex enough to warrant a subsystem-level description of the TSF in  
7163 addition to the modular description, the goal of the subsystem-level description is to give the  
7164 evaluator context for the modular description that follows. Therefore, the evaluator ensures that  
7165 the subsystem-level description contains a description of how the security functional requirements  
7166 are achieved in the design, but at a level of abstraction above the modular description. This  
7167 description should discuss the mechanisms used at a level that is aligned with the module  
7168 description; this will provide the evaluators the road map needed to intelligently assess the  
7169 information contained in the module description. A well-written set of subsystem descriptions will  
7170 help guide the evaluator in determining the modules that are most important to examine, thus  
7171 focusing the evaluation activity on the portions of the TSF that have the most relevance with  
7172 respect to the enforcement of the SFRs.

7173 The evaluator ensures that all subsystems of the TSF have a description. While the description  
7174 should focus on the role that the subsystem plays in enforcing or supporting the implementation of  
7175 the SFRs, enough information must be present so that a context for understanding the SFR-related  
7176 functionality is provided.

#### 7177 11.8.4.4.7 Work unit ADV\_TDS.4-7

7178 The evaluator **shall examine** the TOE design to determine that each SFR-non-interfering  
7179 subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-  
7180 non-interfering.

7181 If the design is presented solely in terms of modules, then this work unit will be considered  
7182 satisfied by the assessment done in subsequent work units; no explicit action on the part of the  
7183 evaluator is necessary in this case.

7184 An SFR-non-interfering subsystem is one on which the SFR-enforcing and SFR-supporting  
7185 subsystems have no dependence; that is, they play no role in implementing SFR functionality.

7186 The evaluator ensures that all subsystems of the TSF have a description. While the description  
7187 should focus on the role that the subsystem do not plays in enforcing or supporting the  
7188 implementation of the SFRs, enough information must be present so that a context for  
7189 understanding the SFR-non-interfering functionality is provided.

7190 ISO/IEC 15408-3 ADV\_TDS.4.5C: *The design shall provide a description of the interactions among all*  
 7191 *subsystems of the TSF.*

#### 7192 **11.8.4.4.8 Work unit ADV\_TDS.4-8**

7193 The evaluator ***shall examine*** the TOE design to determine that interactions between the  
 7194 subsystems of the TSF are described.

7195 If the design is presented solely in terms of modules, then this work unit will be considered  
 7196 satisfied by the assessment done in subsequent work units; no explicit action on the part of the  
 7197 evaluator is necessary in this case.

7198 On systems that are complex enough to warrant a subsystem-level description of the TSF in  
 7199 addition to the modular description, the goal of describing the interactions between the  
 7200 subsystems is to help provide the reader a better understanding of how the TSF performs its  
 7201 functions. These interactions do not need to be characterised at the implementation level (e.g.,  
 7202 parameters passed from one routine in a subsystem to a routine in a different subsystem; global  
 7203 variables; hardware signals (e.g., interrupts) from a hardware subsystem to an interrupt-handling  
 7204 subsystem), but the data elements identified for a particular subsystem that are going to be used  
 7205 by another subsystem need to be covered in this discussion. Any control relationships between  
 7206 subsystems (e.g., a subsystem responsible for configuring a rule base for a firewall system and the  
 7207 subsystem that actually implements these rules) should also be described.

7208 It should be noted while the developer should characterise all interactions between subsystems,  
 7209 the evaluators need to use their own judgement in assessing the completeness of the description. If  
 7210 the reason for an interaction is unclear, or if there are SFR-related interactions (discovered, for  
 7211 instance, in examining the module-level documentation) that do not appear to be described, the  
 7212 evaluator ensures that this information is provided by the developer. However, if the evaluator can  
 7213 determine that interactions among a particular set of subsystems, while incompletely described by  
 7214 the developer, and a complete description will not aid in understanding the overall functionality  
 7215 nor security functionality provided by the TSF, then the evaluator may choose to consider the  
 7216 description sufficient, and not pursue completeness for its own sake.

7217 ISO/IEC 15408-3 ADV\_TDS.4.6C: *The design shall provide a mapping from the subsystems of the TSF*  
 7218 *to the modules of the TSF.*

#### 7219 **11.8.4.4.9 Work unit ADV\_TDS.4-9**

7220 The evaluator ***shall examine*** the TOE design to determine that the mapping between the  
 7221 subsystems of the TSF and the modules of the TSF is complete.

7222 If the design is presented solely in terms of modules, then this work unit is considered satisfied.

7223 For TOEs that are complex enough to warrant a subsystem-level description of the TSF in addition  
 7224 to the modular description, the developer provides a simple mapping showing how the modules of  
 7225 the TSF are allocated to the subsystems. This will provide the evaluator a guide in performing their  
 7226 module-level assessment. To determine completeness, the evaluator examines each mapping and  
 7227 determines that all subsystems map to at least one module, and that all modules map to exactly one  
 7228 subsystem.

#### 7229 **11.8.4.4.10 Work unit ADV\_TDS.4-10**

7230 The evaluator ***shall examine*** the TOE design to determine that the mapping between the  
 7231 subsystems of the TSF to the modules of the TSF is accurate.

7232 If the design is presented solely in terms of modules, then this work unit is considered satisfied.

7233 For TOEs that are complex enough to warrant a subsystem-level description of the TSF in addition  
 7234 to the modular description, the developer provides a simple mapping showing how the modules of  
 7235 the TSF are allocated to the subsystems. This will provide the evaluator a guide in performing their  
 7236 module-level assessment. The evaluator may choose to check the accuracy of the mapping in  
 7237 conjunction with performing other work units. An “inaccurate” mapping is one where the module  
 7238 is mistakenly associated with a subsystem where its functions are not used within the subsystem.  
 7239 Because the mapping is intended to be a guide supporting more detailed analysis, the evaluator is  
 7240 cautioned to apply appropriate effort to this work unit. Expending extensive evaluator resources  
 7241 verifying the accuracy of the mapping is not necessary. Inaccuracies that lead to mis-  
 7242 understandings related to the design that are uncovered as part of this or other work units are the  
 7243 ones that should be associated with this work unit and corrected.

7244 ISO/IEC 15408-3 ADV\_TDS.4.7C: *The design shall describe each SFR-enforcing and SFR-supporting*  
 7245 *module in terms of its purpose and relationship with other modules.*

#### 7246 11.8.4.4.11 Work unit ADV\_TDS.4-11

7247 The evaluator **shall examine** the TOE design to determine that the description of the purpose of  
 7248 each SFR-enforcing and SFR-supporting module, and relationship with other modules is complete  
 7249 and accurate.

7250 The developer may designate modules as SFR-enforcing, SFR-supporting, and SFR non-interfering,  
 7251 but these “tags” are used only to describe the amount and type of information the developer must  
 7252 provide, and can be used to limit the amount of information the developer has to develop if their  
 7253 engineering process does not produce the documentation required. Whether the modules have  
 7254 been categorised by the developer or not, it is the evaluator’s responsibility to determine that the  
 7255 modules have the appropriate information for their role (SFR-enforcing, etc.) in the TOE, and to  
 7256 obtain the appropriate information from the developer should the developer fail to provide the  
 7257 required information for a particular module.

7258 The purpose of a module provides a description indicating what function the module is fulfilling. A  
 7259 word of caution to evaluator is in order. The focus of this work unit should be to provide the  
 7260 evaluator an understanding of how the module works so that determinations can be made about  
 7261 the soundness of the implementation of the SFRs, as well as to support architectural analysis  
 7262 performed for ADV\_ARC subsystems. As long as the evaluator has a sound understanding of the  
 7263 module’s operation, and its relationship to other modules and the TOE as a whole, the evaluator  
 7264 should consider the objective of the work achieved and not engage in a documentation exercise for  
 7265 the developer (by requiring, for example, a complete algorithmic description for a self-evident  
 7266 implementation representation).

7267 Because the modules are at such a low level, it may be difficult determine completeness and  
 7268 accuracy impacts from other documentation, such as operational user guidance, the functional  
 7269 specification, the TSF internals, or the security architecture description. However, the evaluator  
 7270 uses the information present in those documents to the extent possible to help ensure that the  
 7271 purpose is accurately and completely described. This analysis can be aided by the analysis  
 7272 performed for the work units for the ADV\_TDS.4.10C element, which maps the TSFI in the  
 7273 functional specification to the modules of the TSF.

7274 ISO/IEC 15408-3 ADV\_TDS.4.8C: *The design shall describe each SFR-enforcing and SFR-supporting*  
 7275 *module in terms of its SFR-related interfaces, return values from those interfaces, interaction with*  
 7276 *other modules and called SFR-related interfaces to other SFR-enforcing or SFR-supporting modules.*

#### 7277 11.8.4.4.12 Work unit ADV\_TDS.4-12

7278 The evaluator **shall examine** the TOE design to determine that the description of the interfaces  
 7279 presented by each SFR-enforcing and SFR-supporting module contain an accurate and complete  
 7280 description of the SFR-related parameters, the invocation conventions for each interface, and any  
 7281 values returned directly by the interface.

7282 The SFR-related interfaces of a module are those interfaces used by other modules as a means to  
 7283 invoke the SFR-related operations provided, and to provide inputs to or receive outputs from the  
 7284 module. The purpose in the specification of these interfaces is to permit the exercise of them  
 7285 during testing. Inter-module interfaces that are not SFR-related need not be specified or described,  
 7286 since they are not a factor in testing. Likewise, other internal interfaces that are not a factor in  
 7287 traversing SFR-related paths of execution (such as those internal paths that are fixed).

7288 SFR-related interfaces of SFR-supporting modules are all interfaces of SFR-supporting modules  
 7289 that are called directly or indirectly from SFR-enforcing modules. Those interfaces need to be  
 7290 described with all the parameter used in such a call. This allows the evaluator to understand the  
 7291 purpose of the call to the SFR-supporting module in the context of operation of the SFR-enforcing  
 7292 modules.

7293 SFR-related interfaces are described in terms of how they are invoked, and any values that are  
 7294 returned. This description would include a list of parameters, and descriptions of these parameters.  
 7295 Note that global data would also be considered parameters if used by the module (either as inputs  
 7296 or outputs) when invoked. If a parameter were expected to take on a set of values (e.g., a "flag"  
 7297 parameter), the complete set of values the parameter could take on that would have an effect on  
 7298 module processing would be specified. Likewise, parameters representing data structures are  
 7299 described such that each field of the data structure is identified and described. Note that different  
 7300 programming languages may have additional "interfaces" that would be non-obvious; an example  
 7301 would be operator/function overloading in C++. This "implicit interface" in the class description  
 7302 would also be described as part of the low-level TOE design. Note that although a module could  
 7303 present only one interface, it is more common that a module presents a small set of related  
 7304 interfaces.

7305 In terms of the assessment of parameters (inputs and outputs) to a module, any use of global data  
 7306 must also be considered. A module "uses" global data if it either reads or writes the data. In order  
 7307 to assure the description of such parameters (if used) is complete, the evaluator uses other  
 7308 information provided about the module in the TOE design (interfaces, algorithmic description, etc.),  
 7309 as well as the description of the particular set of global data assessed in work unit ADV\_TDS.4-12.  
 7310 For instance, the evaluator could first determine the processing the module performs by examining  
 7311 its function and interfaces presented (particularly the parameters of the interfaces). They could  
 7312 then check to see if the processing appears to "touch" any of the global data areas identified in the  
 7313 TDS design. The evaluator then determines that, for each global data area that appears to be  
 7314 "touched", that global data area is listed as a means of input or output by the module the evaluator  
 7315 is examining.

7316 Invocation conventions are a programming-reference-type description that one could use to  
 7317 correctly invoke a module's interface if one were writing a program to make use of the module's  
 7318 functionality through that interface. This includes necessary inputs and outputs, including any set-  
 7319 up that may need to be performed with respect to global variables.

7320 Values returned through the interface refer to values that are either passed through parameters or  
 7321 messages; values that the function call itself returns in the style of a "C" program function call; or  
 7322 values passed through global means (such as certain error routines in \*ix-style operating systems).

7323 In order to assure the description is complete, the evaluator uses other information provided about  
 7324 the module in the TOE design (e.g., algorithmic description, global data used) to ensure that it  
 7325 appears all data necessary for performing the functions of the module is presented to the module,  
 7326 and that any values that other modules expect the module under examination to provide are  
 7327 identified as being returned by the module. The evaluator determines accuracy by ensuring that  
 7328 the description of the processing matches the information listed as being passed to or from an  
 7329 interface.

7330 ISO/IEC 15408-3 ADV\_TDS.4.9C: *The design shall describe each SFR-non-interfering module in terms*  
 7331 *of its purpose and interaction with other modules.*

7332 **11.8.4.4.13 Work unit ADV\_TDS.4-13**

7333 The evaluator **shall examine** the TOE design to determine that SFR-non-interfering modules are  
7334 correctly categorised.

7335 As mentioned in work unit ADV\_TDS.4-2, less information is required about modules that are SFR-  
7336 non-interfering. A key focus of the evaluator for this work unit is attempting to determine from the  
7337 evidence provided for each module implicitly categorised as SFR-non-interfering and the  
7338 evaluation (information about other modules in the TOE design, the functional specification, the  
7339 security architecture description, the operational user guidance, the TSF internals document, and  
7340 perhaps even the implementation representation) whether the module is indeed SFR-non-  
7341 interfering. At this level of assurance some error should be tolerated; the evaluator does not have  
7342 to be absolutely sure that a given module is SFR-non-interfering, even though it is labelled as such.  
7343 However, if the evidence provided indicates that a SFR-non-interfering module is SFR-enforcing or  
7344 SFR-supporting, the evaluator requests additional information from the developer in order to  
7345 resolve the apparent inconsistency. For example, suppose the documentation for Module A (an  
7346 SFR-enforcing module) indicates that it calls Module B to perform an access check on a certain type  
7347 of construct. When the evaluator examines the information associated with Module B, it is  
7348 discovered that the only information the developer has provided is a purpose and a set of  
7349 interactions (thus implicitly categorising Module B as SFR-supporting or SFR-non-interfering). On  
7350 examining the purpose and interactions from Module A, the evaluator finds no mention of Module  
7351 B performing any access checks, and Module A is not listed as a module with which Module B  
7352 interacts. At this point the evaluator should approach the developer to resolve the discrepancies  
7353 between the information provided in Module A and that in Module B.

7354 Another example would be where the evaluator examines the mapping of the TSFI to the modules  
7355 as provided by ADV\_TDS.4.2D. This examination shows that Module C is associated with an SFR  
7356 requiring identification of the user. Again, when the evaluator examines the information associated  
7357 with Module C, they find that all the developer has provided is a purpose and a set of interactions  
7358 (thus implicitly categorising Module C as SFR-non-interfering). Examining the purpose and  
7359 interactions presented for Module C, the evaluator is unable to determine why Module C, listed as  
7360 mapping to a TSFI concerned with user identification, would not be classified as SFR-enforcing or  
7361 SFR-supporting. Again, the evaluator should approach the developer to resolve this discrepancy.

7362 A final example illustrates the opposite situation. As before, the developer has provided  
7363 information associated with Module D consisting of a purpose and a set of interactions (thus  
7364 implicitly categorising Module D as SFR-non-interfering). The evaluator examines all of the  
7365 evidence provided, including the purpose and interactions for Module D. The purpose appears to  
7366 give a meaningful description of Module D's function in the TOE, the interactions are consistent  
7367 with that description, and there is nothing to indicate that Module D is SFR-enforcing or SFR-  
7368 supporting. In this case, the evaluator should not demand more information about Module D "just  
7369 to be sure" it is correctly categorised. The developer has met the obligations and the resulting  
7370 assurance the evaluator has in the implicit categorisation of Module D is (by definition)  
7371 appropriate for this assurance level.

7372 **11.8.4.4.14 Work unit ADV\_TDS.4-14**

7373 The evaluator **shall examine** the TOE design to determine that the description of the purpose of  
7374 each SFR-non-interfering module is complete and accurate.

7375 The description of the purpose of a module indicates what function the module is fulfilling. From  
7376 the description, the evaluator should be able to obtain a general idea of the module's role. In order  
7377 to assure the description is complete, the evaluator uses the information provided about the  
7378 module's interactions with other modules to assess whether the reasons for the module being  
7379 called are consistent with the module's purpose. If the interaction description contains  
7380 functionality that is not apparent from, or in conflict with, the module's purpose, the evaluator  
7381 needs to determine whether the problem is one of accuracy or of completeness. The evaluator



7382 should be wary of purposes that are too short, since meaningful analysis based on a one-sentence  
7383 purpose is likely to be impossible.

7384 Because the modules are at such a low level, it may be difficult to determine completeness and  
7385 accuracy impacts from other documentation, such as operational user guidance, the functional  
7386 specification, the security architecture description, or the TSF internals document. However, the  
7387 evaluator uses the information present in those documents to the extent possible to help ensure  
7388 that the function is accurately and completely described. This analysis can be aided by the analysis  
7389 performed for the work units for the ADV\_TDS.4.10C element, which maps the TSFI in the  
7390 functional specification to the modules of the TSF.

#### 7391 11.8.4.4.15 Work unit ADV\_TDS.4-15

7392 The evaluator *shall examine* the TOE design to determine that the description of a SFR-non-  
7393 interfering module's interaction with other modules is complete and accurate.

7394 It is important to note that, in terms of the Part 3 requirement and this work unit, the term  
7395 *interaction* is intended to convey less rigour than *interface*. An interaction does not need to be  
7396 characterised at the implementation level (e.g., parameters passed from one routine in a module to  
7397 a routine in a different module; global variables; hardware signals (e.g., interrupts) from a  
7398 hardware subsystem to an interrupt-handling subsystem), but the data elements identified for a  
7399 particular module that are going to be used by another module should be covered in this discussion.  
7400 Any control relationships between modules (e.g., a module responsible for configuring a rule base  
7401 for a firewall system and the module that actually implements these rules) should also be  
7402 described.

7403 A module's interaction with other modules can be captured in many ways. The intent for the TOE  
7404 design is to allow the evaluator to understand (in part through analysis of module interactions) the  
7405 role of the SFR-supporting and SFR-non-interfering modules in the overall TOE design.  
7406 Understanding of this role will aid the evaluator in performing work unit ADV\_TDS.4-8.

7407 A module's interaction with other modules goes beyond just a call-tree-type document. The  
7408 interaction is described from a functional perspective of why a module interacts with other  
7409 modules. The module's purpose describes what functions the module provides to other modules;  
7410 the interactions should describe what the module depends on from other modules in order to  
7411 accomplish this function.

7412 Because the modules are at such a low level, it may be difficult to determine completeness and  
7413 accuracy impacts from other documentation, such as operational user guidance, the functional  
7414 specification, the security architecture description, or the TSF internals document. However, the  
7415 evaluator uses the information present in those documents to the extent possible to help ensure  
7416 that the interactions are accurately and completely described.

7417 ISO/IEC 15408-3 ADV\_TDS.4.10C: *The mapping shall demonstrate that all TSFIs trace to the*  
7418 *behaviour described in the TOE design that they invoke.*

#### 7419 11.8.4.4.16 Work unit ADV\_TDS.4-16

7420 The evaluator *shall examine* the TOE design to determine that it contains a complete and accurate  
7421 mapping from the TSFI described in the functional specification to the modules of the TSF  
7422 described in the TOE design.

7423 The modules described in the TOE design provide a description of the implementation of the TSF.  
7424 The TSFI provide a description of how the implementation is exercised. The evidence from the  
7425 developer identifies the module that is initially invoked when an operation is requested at the TSFI,  
7426 and identify the chain of modules invoked up to the module that is primarily responsible for  
7427 implementing the functionality. However, a complete call tree for each TSFI is not required for this  
7428 work unit. The cases in which more than one module would have to be identified are where there

## ISO/IEC 18045:2008(E)

7429 are “entry point” modules or wrapper modules that have no functionality other than conditioning  
7430 inputs or de-multiplexing an input. Mapping to one of these modules would not provide any useful  
7431 information to the evaluator.

7432 The evaluator assesses the completeness of the mapping by ensuring that all of the TSFI map to at  
7433 least one module. The verification of accuracy is more complex.

7434 The first aspect of accuracy is that each TSFI is mapped to a module at the TSF boundary. This  
7435 determination can be made by reviewing the module description and its interfaces/interactions.  
7436 The next aspect of accuracy is that each TSFI identifies a chain of modules between the initial  
7437 module identified and a module that is primarily responsible for implementing the function  
7438 presented at the TSF. Note that this may be the initial module, or there may be several modules,  
7439 depending on how much pre-conditioning of the inputs is done. It should be noted that one  
7440 indicator of a pre-conditioning module is that it is invoked for a large number of the TSFI, where  
7441 the TSFI are all of similar type (e.g., system call). The final aspect of accuracy is that the mapping  
7442 makes sense. For instance, mapping a TSFI dealing with access control to a module that checks  
7443 passwords is not accurate. The evaluator should again use judgement in making this determination.  
7444 The goal is that this information aids the evaluator in understanding the system and  
7445 implementation of the SFRs, and ways in which entities at the TSF boundary can interact with the  
7446 TSF. The bulk of the assessment of whether the SFRs are described accurately by the modules is  
7447 performed in other work units.

### 7448 11.8.4.5 Action ADV\_TDS.4.2E

#### 7449 11.8.4.5.1 Work unit ADV\_TDS.4-17

7450 The evaluator **shall examine** the TOE security functional requirements and the TOE design, to  
7451 determine that all ST security functional requirements are covered by the TOE design.

7452 The evaluator may construct a map between the TOE security functional requirements and the TOE  
7453 design. This map will likely be from a functional requirement to a set of subsystems, and later to  
7454 modules. Note that this map may have to be at a level of detail below the component or even  
7455 element level of the requirements, because of operations (assignments, refinements, selections)  
7456 performed on the functional requirement by the ST author.

7457 For example, the FDP\_ACC.1 Subset access control component contains an element with  
7458 assignments. If the ST contained, for instance, ten rules in the FDP\_ACC.1 Subset access control  
7459 assignment, and these ten rules were implemented in specific places within fifteen modules, it  
7460 would be inadequate for the evaluator to map FDP\_ACC.1 Subset access control to one subsystem  
7461 and claim the work unit had been completed. Instead, the evaluator would map FDP\_ACC.1 Subset  
7462 access control (rule 1) to modules x, y and z of subsystem A; FDP\_ACC.1 Subset access control (rule  
7463 2) to x, p, and q of subsystem A; etc.

#### 7464 11.8.4.5.2 Work unit ADV\_TDS.4-18

7465 The evaluator **shall examine** the TOE design to determine that it is an accurate instantiation of all  
7466 security functional requirements.

7467 The evaluator may construct a map between the TOE security functional requirements and the TOE  
7468 design. This map will likely be from a functional requirement to a set of subsystems. Note that this  
7469 map may have to be at a level of detail below the component or even element level of the  
7470 requirements, because of operations (assignments, refinements, selections) performed on the  
7471 functional requirement by the ST author.

7472 As an example, if the ST requirements specified a role-based access control mechanism, the  
7473 evaluator would first identify the subsystems, and modules that contribute to this mechanism's  
7474 implementation. This could be done by in-depth knowledge or understanding of the TOE design or

7475 by work done in the previous work unit. Note that this trace is only to identify the subsystems, and  
7476 modules, and is not the complete analysis.

7477 The next step would be to understand what mechanism the subsystems, and modules implemented.  
7478 For instance, if the design described an implementation of access control based on UNIX-style  
7479 protection bits, the design would not be an accurate instantiation of those access control  
7480 requirements present in the ST example used above. If the evaluator could not determine that the  
7481 mechanism was accurately implemented because of a lack of detail, the evaluator would have to  
7482 assess whether all of the SFR-enforcing subsystems and modules have been identified, or if  
7483 adequate detail had been provided for those subsystems and modules.

#### 7484 **11.8.5 Evaluation of sub-activity (ADV\_TDS.5)**

##### 7485 **11.8.5.1 Objectives**

7486 The objectives of this sub-activity are to determine whether the TOE design provides a description  
7487 of the TOE in terms of subsystems sufficient to determine the TSF boundary, and provides a  
7488 description of the TSF internals in terms of modules (and optionally higher-level abstractions). It  
7489 provides enough information about the modules for the evaluator to determine that the SFRs are  
7490 completely and accurately implemented; as such, the TOE design provides an explanation of the  
7491 implementation representation.

##### 7492 **11.8.5.2 Input**

7493 The evaluation evidence for this sub-activity is:

- 7494 a) the ST;
- 7495 b) the functional specification;
- 7496 c) security architecture description;
- 7497 d) the TOE design.

##### 7498 **11.8.5.3 Application notes**

7499 There are three types of activity that the evaluator must undertake with respect to the TOE design.  
7500 First, the evaluator determines that the TSF boundary has been adequately described. Second, the  
7501 evaluator determines that the developer has provided documentation that conforms to the content  
7502 and presentation requirements this subsystem, and that is consistent with other documentation  
7503 provided for the TOE. Finally, the evaluator must analyse the design information provided for the  
7504 modules (at a detailed level) to understand how the system is implemented, and with that  
7505 knowledge ensure that the TSFI in the functional specification are adequately described, and that  
7506 the test information adequately tests the TSF (done in the Class ATE: Tests work units).

##### 7507 **11.8.5.4 Action ADV\_TDS.5.1E**

7508 ADV\_TDS.5.1C *The design shall describe the structure of the TOE in terms of subsystems.*

##### 7509 **11.8.5.4.1 Work unit ADV\_TDS.5-1**

7510 The evaluator **shall examine** the TOE design to determine that the structure of the entire TOE is  
7511 described in terms of subsystems.

## ISO/IEC 18045:2008(E)

7512 The evaluator ensures that all of the subsystems of the TOE are identified. This description of the  
7513 TOE will be used as input to work unit ADV\_TDS.5-4, where the parts of the TOE that make up the  
7514 TSF are identified. That is, this requirement is on the entire TOE rather than on only the TSF.

7515 The TOE (and TSF) may be described in multiple layers of abstraction (i.e. subsystems and  
7516 modules). Depending upon the complexity of the TOE, its design may be described in terms of  
7517 subsystems and modules, as described in CC Part 3 Annex A.4, ADV\_TDS: Subsystems and Modules.  
7518 For a very simple TOE that can be described solely at the "module" level (see ADV\_TDS.5-2), this  
7519 work unit is not applicable and therefore considered to be satisfied.

7520 In performing this activity, the evaluator examines other evidence presented for the TOE (e.g., ST,  
7521 operator user guidance) to determine that the description of the TOE in such evidence is consistent  
7522 with the description contained in the TOE design.

7523 ADV\_TDS.5.2C *The design shall describe the TSF in terms of modules, designating each module as*  
7524 *SFR-enforcing, SFR-supporting, or SFR-non-interfering.*

### 7525 11.8.5.4.2 Work unit ADV\_TDS.5-2

7526 The evaluator **shall examine** the TOE design to determine that the entire TSF is described in terms  
7527 of modules.

7528 The evaluator will examine the modules for specific properties in other work units; in this work  
7529 unit the evaluator determines that the modular description covers the entire TSF, and not just a  
7530 portion of the TSF. The evaluator uses other evidence provided for the evaluation (e.g., functional  
7531 specification, architectural description) in making this determination. For example, if the functional  
7532 specification contains interfaces to functionality that does not appear to be described in the TOE  
7533 design description, it may be the case that a portion of the TSF has not been included appropriately.  
7534 Making this determination will likely be an iterative process, where as more analysis is done on the  
7535 other evidence, more confidence can be gained with respect to the completeness of the  
7536 documentation.

7537 Unlike subsystems, modules describe the implementation in a level of detail that can serve as a  
7538 guide to reviewing the implementation representation. A description of a module should be such  
7539 that one could create an implementation of the module from the description, and the resulting  
7540 implementation would be 1) identical to the actual TSF implementation in terms of the interfaces  
7541 presented, 2) identical in the use of interfaces that are mentioned in the design, and 3) functionally  
7542 equivalent to the description of the purpose of the TSF module. For instance, RFC 793 provides a  
7543 high-level description of the TCP protocol. It is necessarily implementation independent. While it  
7544 provides a wealth of detail, it is **not** a suitable design description because it is not specific to an  
7545 implementation. An actual implementation can add to the protocol specified in the RFC, and  
7546 implementation choices (for instance, the use of global data vs. local data in various parts of the  
7547 implementation) may have an impact on the analysis that is performed. The design description of  
7548 the TCP module would list the interfaces presented by the implementation (rather than just those  
7549 defined in RFC 793), as well as an algorithm description of the processing associated with the  
7550 modules implementing TCP (assuming it was part of the TSF).

### 7551 11.8.5.4.3 Work unit ADV\_TDS.5-3

7552 The evaluator **shall check** the TOE design to determine that the TSF modules are identified as  
7553 either SFR-enforcing, SFR-supporting, or SFR-non-interfering.

7554 The purpose of designating each module (according to the role a particular module plays in the  
7555 enforcement of the SFRs) is to allow developers to provide less information about the parts of the  
7556 TSF that have little role in security. It is always permissible for the developer to provide more  
7557 information or detail than the requirements demand, as might occur when the information has  
7558 been gathered outside the evaluation context. In such cases the developer must still designate the  
7559 modules as either SFR-enforcing, SFR-supporting, or SFR-non-interfering.

7560 The accuracy of these designations is continuously reviewed as the evaluation progresses. The  
 7561 concern is the mis-designation of modules as being less important (and hence, having less  
 7562 information) than is really the case. While blatant mis-designations may be immediately apparent  
 7563 (e.g., designating an authentication module as anything but SFR-enforcing when User identification  
 7564 (FIA\_UID) is one of the SFRs being claimed), other mis-designations might not be discovered until  
 7565 the TSF is better understood. The evaluator must therefore keep in mind that these designations  
 7566 are the developer's initial best effort, but are subject to change. Further guidance is provided under  
 7567 work unit ADV\_TDS.5-16, which examines the accuracy of these designations.

7568 *ADV\_TDS.5.3C The design shall identify all subsystems of the TSF.*

#### 7569 **11.8.5.4.4 Work unit ADV\_TDS.5-4**

7570 The evaluator **shall examine** the TOE design to determine that all subsystems of the TSF are  
 7571 identified.

7572 If the design is presented solely in terms of modules, then subsystems in these requirements are  
 7573 equivalent to modules and the activity should be performed at the module level.

7574 In work unit ADV\_TDS.5-1 all of the subsystems of the TOE were identified, and a determination  
 7575 made that the non-TSF subsystems were correctly characterised. Building on that work, the  
 7576 subsystems that were not characterised as non-TSF subsystems should be precisely identified. The  
 7577 evaluator determines that, of the hardware and software installed and configured according to the  
 7578 Preparative procedures (AGD\_PRE) guidance, each subsystem has been accounted for as either one  
 7579 that is part of the TSF, or one that is not.

7580 *ADV\_TDS.5.4C The design shall provide a semiformal description of each subsystem of the TSF,*  
 7581 *supported by informal, explanatory text where appropriate.*

#### 7582 **11.8.5.4.5 Work unit ADV\_TDS.5-5**

7583 The evaluator **shall examine** the TDS documentation to determine that the semiformal notation  
 7584 used for describing the subsystems, modules and their interfaces is defined or referenced.

7585 A semiformal notation can be either defined by the sponsor or a corresponding standard be  
 7586 referenced. The evaluator should provide a mapping of security functions and their interfaces  
 7587 outlining in what part of the documentation a function or interface is semiformal described and  
 7588 what notation is used. The evaluator examines all semiformal notations used to make sure that  
 7589 they are of a semiformal style and to justify the appropriateness of the manner how the semiformal  
 7590 notations are used for the TOE.

7591 The evaluator is reminded that a semi-formal presentation is characterised by a standardised  
 7592 format with a well-defined syntax that reduces ambiguity that may occur in informal presentations.  
 7593 The syntax of all semiformal notations used in the functional specification shall be defined or a  
 7594 corresponding standard be referenced. The evaluator verifies that the semiformal notations used  
 7595 for expressing the functional specification are capable of expressing features relevant to security.  
 7596 In order to determine this, the evaluator can refer to the SFR and compare the TSF security  
 7597 features stated in the ST and those described in the FSP using the semiformal notations.

7598 Note that ADV\_TDS.5.7C requires the module description to be semiformal. This work unit  
 7599 therefore applies also to that description.

#### 7600 **11.8.5.4.6 Work unit ADV\_TDS.5-6**

7601 The evaluator **shall examine** the TOE design to determine that each subsystem of the TSF  
 7602 describes its role in the enforcement of SFRs described in the ST.

## ISO/IEC 18045:2008(E)

7603 If the design is presented solely in terms of modules, then this work unit will be considered  
7604 satisfied by the assessment done in subsequent work units; no explicit action on the part of the  
7605 evaluator is necessary in this case.

7606 On systems that are complex enough to warrant a subsystem-level description of the TSF in  
7607 addition to the modular description, the goal of the subsystem-level description is to give the  
7608 evaluator context for the modular description that follows. Therefore, the evaluator ensures that  
7609 the subsystem-level description contains a description of how the security functional requirements  
7610 are achieved in the design, but at a level of abstraction above the modular description. This  
7611 description should discuss the mechanisms used at a level that is aligned with the module  
7612 description; this will provide the evaluators the road map needed to intelligently assess the  
7613 information contained in the module description. A well-written set of subsystem descriptions will  
7614 help guide the evaluator in determining the modules that are most important to examine, thus  
7615 focusing the evaluation activity on the portions of the TSF that have the most relevance with  
7616 respect to the enforcement of the SFRs.

7617 The evaluator ensures that all subsystems of the TSF have a description. While the description  
7618 should focus on the role that the subsystem plays in enforcing or supporting the implementation of  
7619 the SFRs, enough information must be present so that a context for understanding the SFR-related  
7620 functionality is provided.

### 7621 11.8.5.4.7 Work unit ADV\_TDS.5-7

7622 The evaluator **shall examine** the TOE design to determine that each SFR-non-interfering  
7623 subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-  
7624 non-interfering.

7625 If the design is presented solely in terms of modules, then this work unit will be considered  
7626 satisfied by the assessment done in subsequent work units; no explicit action on the part of the  
7627 evaluator is necessary in this case.

7628 An SFR-non-interfering subsystem is one on which the SFR-enforcing and SFR-supporting  
7629 subsystems have no dependence; that is, they play no role in implementing SFR functionality.

7630 The evaluator ensures that all subsystems of the TSF have a description. While the description  
7631 should focus on the role that the subsystem do not plays in enforcing or supporting the  
7632 implementation of the SFRs, enough information must be present so that a context for  
7633 understanding the SFR-non-interfering functionality is provided.

7634 ADV\_TDS.5.5C *The design shall provide a description of the interactions among all subsystems of*  
7635 *the TSF.*

### 7636 11.8.5.4.8 Work unit ADV\_TDS.5-8

7637 The evaluator **shall examine** the TOE design to determine that interactions between the  
7638 subsystems of the TSF are described.

7639 If the design is presented solely in terms of modules, then this work unit will be considered  
7640 satisfied by the assessment done in subsequent work units; no explicit action on the part of the  
7641 evaluator is necessary in this case.

7642 On systems that are complex enough to warrant a subsystem-level description of the TSF in  
7643 addition to the modular description, the goal of describing the interactions between the  
7644 subsystems is to help provide the reader a better understanding of how the TSF performs its  
7645 functions. These interactions do not need to be characterised at the implementation level (e.g.,  
7646 parameters passed from one routine in a subsystem to a routine in a different subsystem; global  
7647 variables; hardware signals (e.g., interrupts) from a hardware subsystem to an interrupt-handling  
7648 subsystem), but the data elements identified for a particular subsystem that are going to be used

7649 by another subsystem need to be covered in this discussion. Any control relationships between  
 7650 subsystems (e.g., a subsystem responsible for configuring a rule base for a firewall system and the  
 7651 subsystem that actually implements these rules) should also be described.

7652 It should be noted while the developer should characterise all interactions between subsystems,  
 7653 the evaluators need to use their own judgement in assessing the completeness of the description. If  
 7654 the reason for an interaction is unclear, or if there are SFR-related interactions (discovered, for  
 7655 instance, in examining the module-level documentation) that do not appear to be described, the  
 7656 evaluator ensures that this information is provided by the developer. However, if the evaluator can  
 7657 determine that interactions among a particular set of subsystems, while incompletely described by  
 7658 the developer, and a complete description will not aid in understanding the overall functionality  
 7659 nor security functionality provided by the TSF, then the evaluator may choose to consider the  
 7660 description sufficient, and not pursue completeness for its own sake.

7661 ADV\_TDS.5.6C *The design shall provide a mapping from the subsystems of the TSF to the modules*  
 7662 *of the TSF.*

#### 7663 11.8.5.4.9 Work unit ADV\_TDS.5-9

7664 The evaluator **shall examine** the TOE design to determine that the mapping between the  
 7665 subsystems of the TSF and the modules of the TSF is complete.

7666 If the design is presented solely in terms of modules, then this work unit is considered satisfied.

7667 For TOEs that are complex enough to warrant a subsystem-level description of the TSF in addition  
 7668 to the modular description, the developer provides a simple mapping showing how the modules of  
 7669 the TSF are allocated to the subsystems. This will provide the evaluator a guide in performing their  
 7670 module-level assessment. To determine completeness, the evaluator examines each mapping and  
 7671 determines that all subsystems map to at least one module, and that all modules map to exactly one  
 7672 subsystem.

#### 7673 11.8.5.4.10 Work unit ADV\_TDS.5-10

7674 The evaluator **shall examine** the TOE design to determine that the mapping between the  
 7675 subsystems of the TSF to the modules of the TSF is accurate.

7676 If the design is presented solely in terms of modules, then this work unit is considered satisfied.

7677 For TOEs that are complex enough to warrant a subsystem-level description of the TSF in addition  
 7678 to the modular description, the developer provides a simple mapping showing how the modules of  
 7679 the TSF are allocated to the subsystems. This will provide the evaluator a guide in performing their  
 7680 module-level assessment. The evaluator may choose to check the accuracy of the mapping in  
 7681 conjunction with performing other work units. An "inaccurate" mapping is one where the module  
 7682 is mistakenly associated with a subsystem where its functions are not used within the subsystem.  
 7683 Because the mapping is intended to be a guide supporting more detailed analysis, the evaluator is  
 7684 cautioned to apply appropriate effort to this work unit. Expending extensive evaluator resources  
 7685 verifying the accuracy of the mapping is not necessary. Inaccuracies that lead to mis-  
 7686 understandings related to the design that are uncovered as part of this or other work units are the  
 7687 ones that should be associated with this work unit and corrected.

7688 ADV\_TDS.5.7C *The design shall provide a semiformal description of each module in terms of its*  
 7689 *purpose, interaction, interfaces, return values from those interfaces, and called interfaces to other*  
 7690 *modules, supported by informal, explanatory text where appropriate.*

#### 7691 11.8.5.4.11 Work unit ADV\_TDS.5-11

7692 The evaluator **shall examine** the TOE design to determine that the semiformal description of the  
 7693 purpose of each module, and its relationship with other modules is complete and accurate.

## ISO/IEC 18045:2008(E)

7694 The developer may designate modules as SFR-enforcing, SFR-supporting, and SFR non-interfering,  
7695 but these “tags” are used only to describe the amount and type of information the developer must  
7696 provide, and can be used to limit the amount of information the developer has to develop if their  
7697 engineering process does not produce the documentation required. Whether the modules have  
7698 been categorised by the developer or not, it is the evaluator’s responsibility to determine that the  
7699 modules have the appropriate information for their role (SFR-enforcing, etc.) in the TOE, and to  
7700 obtain the appropriate information from the developer should the developer fail to provide the  
7701 required information for a particular module.

7702 The purpose of a module provides a description indicating what function the module is fulfilling. A  
7703 word of caution to the evaluator is in order. The focus of this work unit should be to provide the  
7704 evaluator an understanding of how the module works so that determinations can be made about  
7705 the soundness of the implementation of the SFRs, as well as to support architectural analysis  
7706 performed for ADV\_ARC subsystems. As long as the evaluator has a sound understanding of the  
7707 module’s operation, and its relationship to other modules and the TOE as a whole, the evaluator  
7708 should consider the objective of the work achieved and not engage in a documentation exercise for  
7709 the developer (by requiring, for example, a complete algorithmic description for a self-evident  
7710 implementation representation).

7711 Because the modules are at such a low level, it may be difficult determine completeness and  
7712 accuracy impacts from other documentation, such as operational user guidance, the functional  
7713 specification, the TSF internals, or the security architecture description. However, the evaluator  
7714 uses the information present in those documents to the extent possible to help ensure that the  
7715 purpose is accurately and completely described. This analysis can be aided by the analysis  
7716 performed for the work units for the ADV\_TDS.5.8C element, which maps the TSFI in the functional  
7717 specification to the modules of the TSF.

### 7718 11.8.5.4.12 Work unit ADV\_TDS.5-12

7719 The evaluator *shall examine* the TOE design to determine that the semiformal description of the  
7720 interfaces presented by each module contain an accurate and complete description of the related  
7721 parameters, the invocation conventions for each interface, and any values returned directly by the  
7722 interface.

7723 The interfaces of a module are those interfaces used by other modules as a means to invoke the  
7724 operations provided, and to provide inputs to or receive outputs from the module. The purpose in  
7725 the specification of these interfaces is to permit the exercise of them during testing. Inter-module  
7726 interfaces that are not SFR-related need not be specified or described, since they are not a factor in  
7727 testing. Likewise, other internal interfaces that are not a factor in traversing SFR-related paths of  
7728 execution (such as those internal paths that are fixed).

7729 SFR-related interfaces are all interfaces that are called directly or indirectly from SFR-enforcing  
7730 modules. Those interfaces need to be described with all the parameter used in such a call. This  
7731 allows the evaluator to understand the purpose of the call in the context of operation of the SFR-  
7732 enforcing modules.

7733 SFR-related interfaces are described in terms of how they are invoked, and any values that are  
7734 returned. This description would include a list of parameters, and descriptions of these parameters.  
7735 Note that global data would also be considered parameters if used by the module (either as inputs  
7736 or outputs) when invoked. If a parameter were expected to take on a set of values (e.g., a “flag”  
7737 parameter), the complete set of values the parameter could take on, that would have an effect on  
7738 module processing, would be specified. Likewise, parameters representing data structures are  
7739 described such that each field of the data structure is identified and described. Note that different  
7740 programming languages may have additional “interfaces” that would be non-obvious; an example  
7741 would be operator/function overloading in C++. This “implicit interface” in the class description  
7742 would also be described as part of the low-level TOE design. Note that although a module could  
7743 present only one interface, it is more common that a module presents a small set of related  
7744 interfaces.



7745 In terms of the assessment of parameters (inputs and outputs) to a module, any use of global data  
 7746 must also be considered. A module “uses” global data if it either reads or writes the data. In order  
 7747 to assure the description of such parameters (if used) is complete, the evaluator uses other  
 7748 information provided about the module in the TOE design (interfaces, algorithmic description, etc.),  
 7749 as well as the description of the particular set of global data assessed in work unit ADV\_TDS.5-10.  
 7750 For instance, the evaluator could first determine the processing the module performs by examining  
 7751 its function and interfaces presented (particularly the parameters of the interfaces). They could  
 7752 then check to see if the processing appears to “touch” any of the global data areas identified in the  
 7753 TDS design. The evaluator then determines that, for each global data area that appears to be  
 7754 “touched”, that global data area is listed as a means of input or output by the module the evaluator  
 7755 is examining.

7756 Invocation conventions are a programming-reference-type description that one could use to  
 7757 correctly invoke a module's interface if one were writing a program to make use of the module's  
 7758 functionality through that interface. This includes necessary inputs and outputs, including any set-  
 7759 up that may need to be performed with respect to global variables.

7760 Values returned through the interface refer to values that are either passed through parameters or  
 7761 messages; values that the function call itself returns in the style of a “C” program function call; or  
 7762 values passed through global means (such as certain error routines in \*ix-style operating systems).

7763 In order to assure the description is complete, the evaluator uses other information provided about  
 7764 the module in the TOE design (e.g., algorithmic description, global data used) to ensure that it  
 7765 appears all data necessary for performing the functions of the module is presented to the module,  
 7766 and that any values that other modules expect the module under examination to provide are  
 7767 identified as being returned by the module. The evaluator determines accuracy by ensuring that  
 7768 the description of the processing matches the information listed as being passed to or from an  
 7769 interface.

7770 ADV\_TDS.5.8C *The mapping shall demonstrate that all TSFIs trace to the behaviour described in*  
 7771 *the TOE design that they invoke.*

#### 7772 11.8.5.4.13 Work unit ADV\_TDS.5-13

7773 The evaluator **shall examine** the TOE design to determine that it contains a complete and accurate  
 7774 mapping from the TSFI described in the functional specification to the modules of the TSF  
 7775 described in the TOE design.

7776 The modules described in the TOE design provide a description of the implementation of the TSF.  
 7777 The TSFI provide a description of how the implementation is exercised. The evidence from the  
 7778 developer identifies the module that is initially invoked when an operation is requested at the TSFI,  
 7779 and identify the chain of modules invoked up to the module that is primarily responsible for  
 7780 implementing the functionality. However, a complete call tree for each TSFI is not required for this  
 7781 work unit. The cases in which more than one module would have to be identified are where there  
 7782 are “entry point” modules or wrapper modules that have no functionality other than conditioning  
 7783 inputs or de-multiplexing an input. Mapping to one of these modules would not provide any useful  
 7784 information to the evaluator.

7785 The evaluator assesses the completeness of the mapping by ensuring that all of the TSFI map to at  
 7786 least one module. The verification of accuracy is more complex.

7787 The first aspect of accuracy is that each TSFI is mapped to a module at the TSF boundary. This  
 7788 determination can be made by reviewing the module description and its interfaces/interactions.  
 7789 The next aspect of accuracy is that each TSFI identifies a chain of modules between the initial  
 7790 module identified and a module that is primarily responsible for implementing the function  
 7791 presented at the TSF. Note that this may be the initial module, or there may be several modules,  
 7792 depending on how much pre-conditioning of the inputs is done. It should be noted that one  
 7793 indicator of a pre-conditioning module is that it is invoked for a large number of the TSFI, where

7794 the TSFI are all of similar type (e.g., system call). The final aspect of accuracy is that the mapping  
7795 makes sense. For instance, mapping a TSFI dealing with access control to a module that checks  
7796 passwords is not accurate. The evaluator should again use judgement in making this determination.  
7797 The goal is that this information aids the evaluator in understanding the system and  
7798 implementation of the SFRs, and ways in which entities at the TSF boundary can interact with the  
7799 TSF. The bulk of the assessment of whether the SFRs are described accurately by the modules is  
7800 performed in other work units.

#### 7801 **11.8.5.4.14 Work unit ADV\_TDS.5-14**

7802 The evaluator shall examine the TOE security functional requirements and the TOE design, to  
7803 determine that all ST security functional requirements are covered by the TOE design. The  
7804 evaluator may construct a map between the TOE security functional requirements and the TOE  
7805 design. This map will likely be from a functional requirement to a set of subsystems, and later to  
7806 modules. Note that this map may have to be at a level of detail below the component or even  
7807 element level of the requirements, because of operations (assignments, refinements, selections)  
7808 performed on the functional requirement by the ST author.

7809 For example, the FDP\_ACC.1 Subset access control component contains an element with  
7810 assignments. If the ST contained, for instance, ten rules in the FDP\_ACC.1 Subset access control  
7811 assignment, and these ten rules were implemented in specific places within fifteen modules, it  
7812 would be inadequate for the evaluator to map FDP\_ACC.1 Subset access control to one subsystem  
7813 and claim the work unit had been completed. Instead, the evaluator would map FDP\_ACC.1 Subset  
7814 access control (rule 1) to modules x, y and z of subsystem A; FDP\_ACC.1 Subset access control (rule  
7815 2) to x, p, and q of subsystem A; etc.

#### 7816 **11.8.5.4.15 Work unit ADV\_TDS.5-15**

7817 The evaluator shall examine the TOE design to determine that it is an accurate instantiation of all  
7818 security functional requirements.

7819 The evaluator may construct a map between the TOE security functional requirements and the TOE  
7820 design. This map will likely be from a functional requirement to a set of subsystems and modules.  
7821 Note that this map may have to be at a level of detail below the component or even element level of  
7822 the requirements, because of operations (assignments, refinements, selections) performed on the  
7823 functional requirement by the ST author.

7824 As an example, if the ST requirements specified a role-based access control mechanism, the  
7825 evaluator would first identify the subsystems, and modules that contribute to this mechanism's  
7826 implementation. This could be done by in-depth knowledge or understanding of the TOE design or  
7827 by work done in the previous work unit. Note that this trace is only to identify the subsystems, and  
7828 modules, and is not the complete analysis.

7829 The next step would be to understand what mechanism the subsystems, and modules implemented.  
7830 For instance, if the design described an implementation of access control based on UNIX-style  
7831 protection bits, the design would not be an accurate instantiation of those access control  
7832 requirements present in the ST example used above. If the evaluator could not determine that the  
7833 mechanism was accurately implemented because of a lack of detail, the evaluator would have to  
7834 assess whether all of the SFR-enforcing subsystems and modules have been identified, or if  
7835 adequate detail had been provided for those subsystems and modules.

#### 7836 **11.8.6 Evaluation of sub-activity (ADV\_TDS.6)**

7837 There is no general guidance; the scheme should be consulted for guidance on this sub-activity.

## 11.9 Composite design compliance (ADV\_COMP)

The composite-specific work units defined in this chapter are intended to be integrated as refinements to the evaluation activities of the ADV class listed in the following table. The other activities of ADV class do not require composite-specific work units.

| CC assurance family | Evaluation activity | Evaluation work unit         | Composite-specific work unit |
|---------------------|---------------------|------------------------------|------------------------------|
| ADV_ARC             | ADV_ARC.1.1E        | ADV_ARC.1.1C/<br>ADV_ARC.1-1 | ADV_COMP.1-1                 |
| ADV_IMP             | ADV_IMP.1.1E        | ADV_IMP.1.1C/<br>ADV_IMP.1-1 | ADV_COMP.1-1                 |
| ADV_TDS             | ADV_TDS.1.2E        | ADV_TDS.1-7                  | ADV_COMP.1-1                 |

NB: If the level of the assurance requirement chosen is higher than those identified in this table, the composite-specific work unit is also applicable.

### 11.9.1 Evaluation of sub-activity (ADV\_COMP.1)

#### 11.9.1.1 Objectives

The aim of this activity is to determine whether the requirements on the application, imposed by the underlying platform, are fulfilled in the composite product.

#### 11.9.1.2 Application notes

The requirements on the application, imposed by the underlying platform, can be formulated in the relevant certification report (e.g. in form of constraints and recommendations), user guidance and ETR\_COMP (in form of observations and recommendations) for the platform. The developer of the composite product shall regard each of these sources, if available and implement the composite product in such a way that the applicable requirements are fulfilled.

The TSF of the composite product is represented at various levels of abstraction in the families of the development class ADV. Experiential, the appropriate levels of design representation for examining, whether the requirements of the platform are fulfilled by the composite product, are the TOE design (ADV\_TDS), security architecture (ADV\_ARC) and the implementation (ADV\_IMP). In case, these design representation levels are not available (e.g. due to the assurance package chosen is EAL1), the current activity is not applicable (see the next paragraph for the reason)

Due to the definition of the composite TOE the interface between the underlying platform and the application is the internal one, hence, a functional specification (ADV\_FSP) as representation level is not appropriate for analysing the design compliance.

Security architecture ADV\_ARC as assurance family is dedicated to ensure that integrative security services like domain separation, self-protection and non-bypassability properly work. It is impossible and not the sense of the composite evaluation to have an insight into the architectural internals of the underlying platform (it is a matter of the platform evaluation). What the Composite Evaluator has to do in the context of ADV\_ARC is

- a) to determine whether the application uses services of the underlying platform within its own Composite-ST to provide domain separation, self-protection, non-bypassability and protected start-up; if no, there is no further composite activities for ADV\_ARC; if yes, then

## ISO/IEC 18045:2008(E)

- 7872           b) the evaluator has to determine, whether the application uses these platform-services  
7873           in an appropriate/secure way
- 7874       Since consistency of the composite product security policy has already been considered in the  
7875       context of the Security Target in the assurance family ASE\_COMP there is no necessity to consider  
7876       non-contradictoriness of the security policy model (ADV\_SPM) of the composite TOE and the  
7877       security policy model of the underlying platform.
- 7878       **11.9.1.3 Action ADV\_COMP.1.1E**
- 7879       The evaluator shall confirm that the rationale for design compliance is complete, coherent, and  
7880       internally consistent.
- 7881       *ADV\_COMP.1.1C The design compliance justification shall provide a rationale for design compliance –*  
7882       *on an appropriate representation level – of how the requirements on the application, imposed by the*  
7883       *underlying platform, are fulfilled in the composite product.*
- 7884       **11.9.1.3.1 Work unit ADV\_COMP.1-1**
- 7885       The evaluator shall examine the rationale for design compliance to determine that all applicable  
7886       requirements on the application, imposed by the underlying platform, are fulfilled by the  
7887       composite product.
- 7888       In order to perform this work unit the evaluator shall use the rationale for design compliance as  
7889       well as the TSF representation on the ADV\_TDS, ADV\_ARC and ADV\_IMP levels on the one side and  
7890       the input of the platform developer in form of the certification report, guidance and ETR\_COMP on  
7891       the other side. The evaluator shall analyse which platform requirements are applicable for the  
7892       current composite product, based on the identified RP\_SFR-MECH and RP\_SFR-SERV. The  
7893       evaluator shall compare each of the applicable requirements with the actual specification and/or  
7894       implementation of the composite product and determine, for each requirement, whether it is  
7895       fulfilled. As result, the evaluator confirms or disproves the rationale for design compliance.
- 7896       For example, platform guidance may require the application to perform a special start-up  
7897       sequence testing the current state of the platform and initialising its self-protection mechanisms.  
7898       Such information might be found in the description of secure architecture ADV\_ARC of the  
7899       composite TOE; see also the Application Note above.
- 7900       A second example, platform guidance may require the application to perform a DFA check on the  
7901       DES operation, while the application is implementing BAC in an e-passport MRTD. The ADV\_ARC  
7902       will explain whether the platform guidance is followed up or not, and in case that the  
7903       requirements in the platform guidance are not followed a corresponding reasoning will be  
7904       provided. The arguments of the developer explain why a non-compliance will not introduce  
7905       vulnerabilities.
- 7906       The appropriate representation level (ADV\_TDS, ADV\_ARC and/or ADV\_IMP), what the analysis is  
7907       being performed on, can be chosen and mixed flexibly depending on the concrete composite TOE  
7908       and the requirement in question. Where it is not self-explaining, the evaluator shall justify why the  
7909       representation level chosen is appropriate.
- 7910       The evaluator activities in the context of this work unit can be spread over different single  
7911       evaluation aspects (e.g. over ADV\_TDS and ADV\_IMP). In this case the evaluator performs the  
7912       partial activity in the context of the corresponding single evaluation aspect. Then the notation for  
7913       this work unit shall be ADV\_COMP.1-1-TDS, ADV\_COMP.1-1-ARC and ADV\_COMP.1-1-IMP,  
7914       respectively.
- 7915       If the assurance package chosen does not contain the families ADV\_TDS, ADV\_ARC or ADV\_IMP (e.g.  
7916       EAL1), this work unit is not applicable (cf. Application Note above).

7917 The result of this work unit shall be integrated to the result of ADV\_TDS.1-2E/ ADV\_TDS.1-7,  
 7918 ADV\_ARC.1.1E/ ADV\_ARC.1.1C/ ADV\_ARC.1-1, ADV\_IMP.1.1E/ ADV\_IMP.1.1C/ ADV\_IMP.1-1 (or  
 7919 the equivalent higher components if a higher assurance level is selected).

## 7920 **12 Class AGD: Guidance documents**

### 7921 **12.1 Introduction**

7922 The purpose of the guidance document activity is to judge the adequacy of the documentation  
 7923 describing how the user can handle the TOE in a secure manner. Such documentation should take  
 7924 into account the various types of users (e.g. those who accept, install, administrate or operate the  
 7925 TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

7926 The guidance documents class is subdivided into two families which are concerned firstly with the  
 7927 preparative procedures (all that has to be done to transform the delivered TOE into its evaluated  
 7928 configuration in the environment as described in the ST, i.e. accepting and installing the TOE) and  
 7929 secondly with the operational user guidance (all that has to be done during the operation of the  
 7930 TOE in its evaluated configuration, i.e. operation and administration).

### 7931 **12.2 Application notes**

7932 The guidance documents activity applies to those functions and interfaces which are related to the  
 7933 security of the TOE. The secure configuration of the TOE is described in the ST.

### 7934 **12.3 Operational user guidance (AGD\_OPE)**

#### 7935 **12.3.1 Evaluation of sub-activity (AGD\_OPE.1)**

##### 7936 **12.3.1.1 Objectives**

7937 The objectives of this sub-activity are to determine whether the user guidance describes for each  
 7938 user role the security functionality and interfaces provided by the TSF, provides instructions and  
 7939 guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation,  
 7940 facilitates prevention and detection of insecure TOE states, or whether it is misleading or  
 7941 unreasonable.

##### 7942 **12.3.1.2 Input**

7943 The evaluation evidence for this sub-activity is:

- 7944 a) the ST;
- 7945 b) the functional specification;
- 7946 c) the TOE design, if applicable;
- 7947 d) the user guidance;

##### 7948 **12.3.1.3 Action AGD\_OPE.1.1E**

7949 ISO/IEC 15408-3 AGD\_OPE.1.1C: *The operational user guidance shall describe, for each user role, the*  
 7950 *user-accessible functions and privileges that should be controlled in a secure processing environment,*  
 7951 *including appropriate warnings.*

7952 **12.3.1.3.1 Work unit AGD\_OPE.1-1**

7953 The evaluator **shall examine** the operational user guidance to determine that it describes, for each  
7954 user role, the user-accessible functions and privileges that should be controlled in a secure  
7955 processing environment, including appropriate warnings.

7956 The configuration of the TOE may allow different user roles to have dissimilar privileges in making  
7957 use of the different functions of the TOE. This means that some users are authorised to perform  
7958 certain functions, while other users may not be so authorised. These functions and privileges  
7959 should be described, for each user role, by the user guidance.

7960 The user guidance identifies, for each user role, the functions and privileges that must be  
7961 controlled, the types of commands required for them, and the reasons for such commands. The  
7962 user guidance should contain warnings regarding the use of these functions and privileges.  
7963 Warnings should address expected effects, possible side effects, and possible interactions with  
7964 other functions and privileges.

7965 ISO/IEC 15408-3 AGD\_OPE.1.2C: *The operational user guidance shall describe, for each user role,*  
7966 *how to use the available interfaces provided by the TOE in a secure manner.*

7967 **12.3.1.3.2 Work unit AGD\_OPE.1-2**

7968 The evaluator **shall examine** the operational user guidance to determine that it describes, for each  
7969 user role, the secure use of the available interfaces provided by the TOE.

7970 The user guidance should provide advice regarding effective use of the TSF (e.g. reviewing  
7971 password composition practises, suggested frequency of user file backups, discussion on the effects  
7972 of changing user access privileges).

7973 ISO/IEC 15408-3 AGD\_OPE.1.3C: *The operational user guidance shall describe, for each user role, the*  
7974 *available functions and interfaces, in particular all security parameters under the control of the user,*  
7975 *indicating secure values as appropriate.*

7976 **12.3.1.3.3 Work unit AGD\_OPE.1-3**

7977 The evaluator **shall examine** the operational user guidance to determine that it describes, for each  
7978 user role, the available security functionality and interfaces, in particular all security parameters  
7979 under the control of the user, indicating secure values as appropriate.

7980 The user guidance should contain an overview of the security functionality that is visible at the  
7981 user interfaces.

7982 The user guidance should identify and describe the purpose, behaviour, and interrelationships of  
7983 the security interfaces and functionality.

7984 For each user-accessible interface, the user guidance should:

7985 a) describe the method(s) by which the interface is invoked (e.g. command-line,  
7986 programming-language system call, menu selection, command button);

7987 b) describe the parameters to be set by the user, their particular purposes, valid and  
7988 default values, and secure and insecure use settings of such parameters, both  
7989 individually or in combination;

7990 c) describe the immediate TSF response, message, or code returned.

7991 The evaluator should consider the functional specification and the ST to determine that the TSF  
 7992 described in these documents is consistent to the operational user guidance. The evaluator has to  
 7993 ensure that the operational user guidance is complete to allow the secure use through the TSFI  
 7994 available to all types of human users. The evaluator may, as an aid, prepare an informal mapping  
 7995 between the guidance and these documents. Any omissions in this mapping may indicate  
 7996 incompleteness.

7997 ISO/IEC 15408-3 AGD\_OPE.1.4C: *The operational user guidance shall, for each user role, clearly*  
 7998 *present each type of security-relevant event relative to the user-accessible functions that need to be*  
 7999 *performed, including changing the security characteristics of entities under the control of the TSF.*

#### 8000 12.3.1.3.4 Work unit AGD\_OPE.1-4

8001 The evaluator **shall examine** the operational user guidance to determine that it describes, for each  
 8002 user role, each type of security-relevant event relative to the user functions that need to be  
 8003 performed, including changing the security characteristics of entities under the control of the TSF  
 8004 and operation following failure or operational error.

8005 All types of security-relevant events are detailed for each user role, such that each user knows  
 8006 what events may occur and what action (if any) they may have to take in order to maintain security.  
 8007 Security-relevant events that may occur during operation of the TOE (e.g. audit trail overflow,  
 8008 system crash, updates to user records, such as when a user account is removed when the user  
 8009 leaves the organisation) are adequately defined to allow user intervention to maintain secure  
 8010 operation.

8011 ISO/IEC 15408-3 AGD\_OPE.1.5C: *The operational user guidance shall identify all possible modes of*  
 8012 *operation of the TOE (including operation following failure or operational error), their consequences*  
 8013 *and implications for maintaining secure operation.*

#### 8014 12.3.1.3.5 Work unit AGD\_OPE.1-5

8015 The evaluator **shall examine** the operational user guidance and other evaluation evidence to  
 8016 determine that the guidance identifies all possible modes of operation of the TOE (including, if  
 8017 applicable, operation following failure or operational error), their consequences and implications  
 8018 for maintaining secure operation.

8019 Other evaluation evidence, particularly the functional specification, provide an information source  
 8020 that the evaluator should use to determine that the guidance contains sufficient guidance  
 8021 information.

8022 If test documentation is included in the assurance package, then the information provided in this  
 8023 evidence can also be used to determine that the guidance contains sufficient guidance  
 8024 documentation. The detail provided in the test steps can be used to confirm that the guidance  
 8025 provided is sufficient for the use and administration of the TOE.

8026 The evaluator should focus on a single human visible TSFI at a time, comparing the guidance for  
 8027 securely using the TSFI with other evaluation evidence, to determine that the guidance related to  
 8028 the TSFI is sufficient for the secure usage (i.e. consistent with the SFRs) of that TSFI. The evaluator  
 8029 should also consider the relationships between interfaces, searching for potential conflicts.

8030 ISO/IEC 15408-3 AGD\_OPE.1.6C: *The operational user guidance shall, for each user role, describe the*  
 8031 *security measures to be followed in order to fulfil the security objectives for the operational*  
 8032 *environment as described in the ST.*

8033 **12.3.1.3.6 Work unit AGD\_OPE.1-6**

8034 The evaluator **shall examine** the operational user guidance to determine that it describes, for each  
8035 user role, the security measures to be followed in order to fulfil the security objectives for the  
8036 operational environment as described in the ST.

8037 The evaluator analyses the security objectives for the operational environment in the ST and  
8038 determines that for each user role, the relevant security measures are described appropriately in  
8039 the user guidance.

8040 The security measures described in the user guidance should include all relevant external  
8041 procedural, physical, personnel and connectivity measures.

8042 Note that those measures relevant for secure installation of the TOE are examined in Preparative  
8043 procedures (AGD\_PRE).

8044 ISO/IEC 15408-3 AGD\_OPE.1.7C: *The operational user guidance shall be clear and reasonable.*

8045 **12.3.1.3.7 Work unit AGD\_OPE.1-7**

8046 The evaluator **shall examine** the operational user guidance to determine that it is clear.

8047 The guidance is unclear if it can reasonably be misconstrued by an administrator or user, and used  
8048 in a way detrimental to the TOE, or to the security provided by the TOE.

8049 **12.3.1.3.8 Work unit AGD\_OPE.1-8**

8050 The evaluator **shall examine** the operational user guidance to determine that it is reasonable.

8051 The guidance is unreasonable if it makes demands on the TOE's usage or operational environment  
8052 that are inconsistent with the ST or unduly onerous to maintain security.

8053 **12.4 Preparative procedures (AGD\_PRE)**

8054 **12.4.1 Evaluation of sub-activity (AGD\_PRE.1)**

8055 **12.4.1.1 Objectives**

8056 The objective of this sub-activity is to determine whether the procedures and steps for the secure  
8057 preparation of the TOE have been documented and result in a secure configuration.

8058 **12.4.1.2 Input**

8059 The evaluation evidence for this sub-activity is:

- 8060 a) the ST;
- 8061 b) the TOE including its preparative procedures;
- 8062 c) the description of developer's delivery procedures, if applicable;

8063 **12.4.1.3 Application notes**

8064 The preparative procedures refer to all acceptance and installation procedures, that are necessary  
8065 to progress the TOE to the secure configuration as described in the ST.



8066 **12.4.1.4 Action AGD\_PRE.1.1E**

8067 ISO/IEC 15408-3 AGD\_PRE.1.1C: *The preparative procedures shall describe all the steps necessary*  
8068 *for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.*

8069 **12.4.1.4.1 Work unit AGD\_PRE.1-1**

8070 The evaluator **shall examine** the provided acceptance procedures to determine that they describe  
8071 the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery  
8072 procedures.

8073 If it is not anticipated by the developer's delivery procedures that acceptance procedures will or  
8074 can be applied, this work unit is not applicable, and is therefore considered to be satisfied.

8075 The acceptance procedures should include as a minimum, that the user has to check that all parts  
8076 of the TOE as indicated in the ST have been delivered in the correct version.

8077 The acceptance procedures should reflect the steps the user has to perform in order to accept the  
8078 delivered TOE that are implied by the developer's delivery procedures.

8079 The acceptance procedures should provide detailed information about the following, if applicable:

8080 a) making sure that the delivered TOE is the complete evaluated instance;

8081 b) detecting modification/masquerading of the delivered TOE.

8082 ISO/IEC 15408-3 AGD\_PRE.1.2C: *The preparative procedures shall describe all the steps necessary*  
8083 *for secure installation of the TOE and for the secure preparation of the operational environment in*  
8084 *accordance with the security objectives for the operational environment as described in the ST.*

8085 **12.4.1.4.2 Work unit AGD\_PRE.1-2**

8086 The evaluator **shall examine** the provided installation procedures to determine that they describe  
8087 the steps necessary for secure installation of the TOE and the secure preparation of the operational  
8088 environment in accordance with the security objectives in the ST.

8089 If it is not anticipated that installation procedures will or can be applied (e.g. because the TOE may  
8090 already be delivered in an operational state), this work unit is not applicable, and is therefore  
8091 considered to be satisfied.

8092 The installation procedures should provide detailed information about the following, if applicable:

8093 a) minimum system requirements for secure installation;

8094 b) requirements for the operational environment in accordance with the security  
8095 objectives provided by the ST;

8096 c) the steps the user has to perform in order to get to an operational TOE being  
8097 commensurate with its evaluated configuration. Such a description shall include - for  
8098 each step - a clear scheme for the decision on the next step depended on success,  
8099 failure or problems at the current step;

8100 d) changing the installation specific security characteristics of entities under the control  
8101 of the TSF (for example parameters, settings, passwords);

8102 e) handling exceptions and problems.

8103 **12.4.1.5 Action AGD\_PRE.1.2E**

8104 **12.4.1.5.1 Work unit AGD\_PRE.1-3**

8105 The evaluator *shall perform* all user procedures necessary to prepare the TOE to determine that  
8106 the TOE and its operational environment can be prepared securely using only the supplied  
8107 preparative procedures.

8108 Preparation requires the evaluator to advance the TOE from a deliverable state to the state in  
8109 which it is operational, including acceptance and installation of the TOE, and enforcing the SFRs  
8110 consistent with the security objectives for the TOE specified in the ST.

8111 The evaluator should follow only the developer's procedures and may perform the activities that  
8112 customers are usually expected to perform to accept and install the TOE, using the supplied  
8113 preparative procedures only. Any difficulties encountered during such an exercise may be  
8114 indicative of incomplete, unclear or unreasonable guidance.

8115 This work unit may be performed in conjunction with the evaluation activities under Independent  
8116 testing (ATE\_IND).

8117 If it is known that the TOE will be used as a dependent component for a composed TOE evaluation,  
8118 then the evaluator should ensure that the operational environment is satisfied by the base  
8119 component used in the composed TOE.

8120 **13 Class ALC: Life-cycle support**

8121 **13.1 Introduction**

8122 The purpose of the life-cycle support activity is to determine the adequacy of the security  
8123 procedures that the developer uses during the development and maintenance of the TOE. These  
8124 procedures include the life-cycle model used by the developer, the configuration management, the  
8125 security measures used throughout TOE development, the tools used by the developer throughout  
8126 the life-cycle of the TOE, the handling of security flaws, and the delivery activity.

8127 Poorly controlled development and maintenance of the TOE can result in vulnerabilities in the  
8128 implementation. Conformance to a defined life-cycle model can help to improve controls in this  
8129 area. A measurable life-cycle model used for the TOE can remove ambiguity in assessing the  
8130 development progress of the TOE.

8131 The purpose of the configuration management activity is to assist the consumer in identifying the  
8132 evaluated TOE, to ensure that configuration items are uniquely identified, and the adequacy of the  
8133 procedures that are used by the developer to control and track changes that are made to the TOE.  
8134 This includes details on what changes are tracked, how potential changes are incorporated, and the  
8135 degree to which automation is used to reduce the scope for error.

8136 Developer security procedures are intended to protect the TOE and its associated design  
8137 information from interference or disclosure. Interference in the development process may allow  
8138 the deliberate introduction of vulnerabilities. Disclosure of design information may allow  
8139 vulnerabilities to be more easily exploited. The adequacy of the procedures will depend on the  
8140 nature of the TOE and the development process.

8141 The use of well-defined development tools and the application of implementation standards by the  
8142 developer and by third parties involved in the development process help to ensure that  
8143 vulnerabilities are not inadvertently introduced during refinement.

8144 The flaw remediation activity is intended to track security flaws, to identify corrective actions, and  
8145 to distribute the corrective action information to TOE users.

8146 The purpose of the delivery activity is to judge the adequacy of the documentation of the  
8147 procedures used to ensure that the TOE is delivered to the consumer without modification.

8148 Appropriate detailed comment/changes are invited.

8149 **ALC\_COMP**

8150 Appropriate detailed comment/changes are invited.

8151

## 8152 **13.2 CM capabilities (ALC\_CMC)**

### 8153 **13.2.1 Evaluation of sub-activity (ALC\_CMC.1)**

#### 8154 **13.2.1.1 Objectives**

8155 The objectives of this sub-activity are to determine whether the developer has clearly identified the  
8156 TOE.

#### 8157 **13.2.1.2 Input**

8158 The evaluation evidence for this sub-activity is:

8159 a) the ST;

8160 b) the TOE suitable for testing.

#### 8161 **13.2.1.3 Action ALC\_CMC.1.1E**

8162 ISO/IEC 15408-3 ALC\_CMC.1.1C: *The TOE shall be labelled with its unique reference.*

##### 8163 **13.2.1.3.1 Work unit ALC\_CMC.1-1**

8164 The evaluator **shall check** that the TOE provided for evaluation is labelled with its reference.

8165 The evaluator should ensure that the TOE contains the unique reference which is stated in the ST.  
8166 This could be achieved through labelled packaging or media, or by a label displayed by the  
8167 operational TOE. This is to ensure that it would be possible for consumers to identify the TOE (e.g.  
8168 at the point of purchase or use).

8169 The TOE may provide a method by which it can be easily identified. For example, a software TOE  
8170 may display its name and version number during the start up routine, or in response to a command  
8171 line entry. A hardware or firmware TOE may be identified by a part number physically stamped on  
8172 the TOE.

8173 Alternatively, the unique reference provided for the TOE may be the combination of the unique  
8174 reference of each component from which the TOE is comprised (e.g. in the case of a composed TOE).

##### 8175 **13.2.1.3.2 Work unit ALC\_CMC.1-2**

8176 The evaluator **shall check** that the TOE references used are consistent.

8177 If the TOE is labelled more than once then the labels have to be consistent. For example, it should  
8178 be possible to relate any labelled guidance documentation supplied as part of the TOE to the  
8179 evaluated operational TOE. This ensures that consumers can be confident that they have purchased  
8180 the evaluated version of the TOE, that they have installed this version, and that they have the  
8181 correct version of the guidance to operate the TOE in accordance with its ST.

8182 The evaluator also verifies that the TOE reference is consistent with the ST.

8183 If this work unit is applied to a composed TOE, the following will apply. The composed IT TOE will  
8184 not be labelled with its unique (composite) reference, but only the individual components will be  
8185 labelled with their appropriate TOE reference. It would require further development for the IT TOE  
8186 to be labelled, i.e. during start-up and/or operation, with the composite reference. If the composed  
8187 TOE is delivered as the constituent component TOEs, then the TOE items delivered will not contain  
8188 the composite reference. However, the composed TOE ST will include the unique reference for the  
8189 composed TOE and will identify the components comprising the composed TOE through which the  
8190 consumers will be able to determine whether they have the appropriate items.

#### 8191 **13.2.2 Evaluation of sub-activity (ALC\_CMC.2)**

##### 8192 **13.2.2.1 Objectives**

8193 The objectives of this sub-activity are to determine whether the developer uses a CM system that  
8194 uniquely identifies all configuration items.

##### 8195 **13.2.2.2 Input**

8196 The evaluation evidence for this sub-activity is:

- 8197 a) the ST;
- 8198 b) the TOE suitable for testing;
- 8199 c) the configuration management documentation.

##### 8200 **13.2.2.3 Application notes**

8201 This component contains an implicit evaluator action to determine that the CM system is being  
8202 used. As the requirements here are limited to identification of the TOE and provision of a  
8203 configuration list, this action is already covered by, and limited to, the existing work units. At  
8204 Evaluation of sub-activity (ALC\_CMC.3) the requirements are expanded beyond these two items,  
8205 and more explicit evidence of operation is required.

##### 8206 **13.2.2.4 Action ALC\_CMC.2.1E**

8207 ISO/IEC 15408-3 ALC\_CMC.2.1C: *The TOE shall be labelled with its unique reference.*

##### 8208 **13.2.2.4.1 Work unit ALC\_CMC.2-1**

8209 The evaluator **shall check** that the TOE provided for evaluation is labelled with its reference.

8210 The evaluator should ensure that the TOE contains the unique reference which is stated in the ST.  
8211 This could be achieved through labelled packaging or media, or by a label displayed by the  
8212 operational TOE. This is to ensure that it would be possible for consumers to identify the TOE (e.g.  
8213 at the point of purchase or use).

8214 The TOE may provide a method by which it can be easily identified. For example, a software TOE  
8215 may display its name and version number during the start up routine, or in response to a command  
8216 line entry. A hardware or firmware TOE may be identified by a part number physically stamped on  
8217 the TOE.

8218 Alternatively, the unique reference provided for the TOE may be the combination of the unique  
8219 reference of each component from which the TOE is comprised (e.g. in the case of a composed TOE).

#### 8220 13.2.2.4.2 Work unit ALC\_CMC.2-2

8221 The evaluator **shall check** that the TOE references used are consistent.

8222 If the TOE is labelled more than once then the labels have to be consistent. For example, it should  
8223 be possible to relate any labelled guidance documentation supplied as part of the TOE to the  
8224 evaluated operational TOE. This ensures that consumers can be confident that they have purchased  
8225 the evaluated version of the TOE, that they have installed this version, and that they have the  
8226 correct version of the guidance to operate the TOE in accordance with its ST.

8227 The evaluator also verifies that the TOE reference is consistent with the ST.

8228 If this work unit is applied to a composed TOE, the following will apply. The composed IT TOE will  
8229 not be labelled with its unique (composite) reference, but only the individual components will be  
8230 labelled with their appropriate TOE reference. It would require further development for the IT TOE  
8231 to be labelled, i.e. during start-up and/or operation, with the composite reference. If the composed  
8232 TOE is delivered as the constituent component TOEs, then the TOE items delivered will not contain  
8233 the composite reference. However, the composed TOE ST will include the unique reference for the  
8234 composed TOE and will identify the components comprising the composed TOE through which the  
8235 consumers will be able to determine whether they have the appropriate items.

8236 ISO/IEC 15408-3 ALC\_CMC.2.2C: *The CM documentation shall describe the method used to uniquely*  
8237 *identify the configuration items.*

#### 8238 13.2.2.4.3 Work unit ALC\_CMC.2-3

8239 The evaluator **shall examine** the method of identifying configuration items to determine that it  
8240 describes how configuration items are uniquely identified.

8241 Procedures should describe how the status of each configuration item can be tracked throughout  
8242 the life-cycle of the TOE. The procedures may be detailed in the CM plan or throughout the CM  
8243 documentation. The information included should describe:

8244 a) the method how each configuration item is uniquely identified, such that it is possible  
8245 to track versions of the same configuration item;

8246 b) the method how configuration items are assigned unique identifiers and how they are  
8247 entered into the CM system;

8248 c) the method to be used to identify superseded versions of a configuration item.

8249 ISO/IEC 15408-3 ALC\_CMC.2.3C: *The CM system shall uniquely identify all configuration items.*

#### 8250 13.2.2.4.4 Work unit ALC\_CMC.2-4

8251 The evaluator **shall examine** the configuration items to determine that they are identified in a way  
8252 that is consistent with the CM documentation.

## ISO/IEC 18045:2008(E)

8253 Assurance that the CM system uniquely identifies all configuration items is gained by examining  
8254 the identifiers for the configuration items. For both configuration items that comprise the TOE, and  
8255 drafts of configuration items that are submitted by the developer as evaluation evidence, the  
8256 evaluator confirms that each configuration item possesses a unique identifier in a manner  
8257 consistent with the unique identification method that is described in the CM documentation.

### 8258 13.2.3 Evaluation of sub-activity (ALC\_CMC.3)

#### 8259 13.2.3.1 Objectives

8260 The objectives of this sub-activity are to determine whether the developer uses a CM system that  
8261 uniquely identifies all configuration items, and whether the ability to modify these items is  
8262 properly controlled.

#### 8263 13.2.3.2 Input

8264 The evaluation evidence for this sub-activity is:

- 8265 a) the ST;
- 8266 b) the TOE suitable for testing;
- 8267 c) the configuration management documentation.

#### 8268 13.2.3.3 Action ALC\_CMC.3.1E

8269 ISO/IEC 15408-3 ALC\_CMC.3.1C: *The TOE shall be labelled with its unique reference.*

##### 8270 13.2.3.3.1 Work unit ALC\_CMC.3-1

8271 The evaluator **shall check** that the TOE provided for evaluation is labelled with its reference.

8272 The evaluator should ensure that the TOE contains the unique reference which is stated in the ST.  
8273 This could be achieved through labelled packaging or media, or by a label displayed by the  
8274 operational TOE. This is to ensure that it would be possible for consumers to identify the TOE (e.g.  
8275 at the point of purchase or use).

8276 The TOE may provide a method by which it can be easily identified. For example, a software TOE  
8277 may display its name and version number during the start up routine, or in response to a command  
8278 line entry. A hardware or firmware TOE may be identified by a part number physically stamped on  
8279 the TOE.

8280 Alternatively, the unique reference provided for the TOE may be the combination of the unique  
8281 reference of each component from which the TOE is comprised (e.g. in the case of a composed TOE).

##### 8282 13.2.3.3.2 Work unit ALC\_CMC.3-2

8283 The evaluator **shall check** that the TOE references used are consistent.

8284 If the TOE is labelled more than once then the labels have to be consistent. For example, it should  
8285 be possible to relate any labelled guidance documentation supplied as part of the TOE to the  
8286 evaluated operational TOE. This ensures that consumers can be confident that they have purchased  
8287 the evaluated version of the TOE, that they have installed this version, and that they have the  
8288 correct version of the guidance to operate the TOE in accordance with its ST.

8289 The evaluator also verifies that the TOE reference is consistent with the ST.

8290 If this work unit is applied to a composed TOE, the following will apply. The composed IT TOE will  
 8291 not be labelled with its unique (composite) reference, but only the individual components will be  
 8292 labelled with their appropriate TOE reference. It would require further development for the IT TOE  
 8293 to be labelled, i.e. during start-up and/or operation, with the composite reference. If the composed  
 8294 TOE is delivered as the constituent component TOEs, then the TOE items delivered will not contain  
 8295 the composite reference. However, the composed TOE ST will include the unique reference for the  
 8296 composed TOE and will identify the components comprising the composed TOE through which the  
 8297 consumers will be able to determine whether they have the appropriate items.

8298 ISO/IEC 15408-3 ALC\_CMC.3.2C: *The CM documentation shall describe the method used to uniquely*  
 8299 *identify the configuration items.*

#### 8300 13.2.3.3.3 Work unit ALC\_CMC.3-3

8301 The evaluator **shall examine** the method of identifying configuration items to determine that it  
 8302 describes how configuration items are uniquely identified.

8303 Procedures should describe how the status of each configuration item can be tracked throughout  
 8304 the life-cycle of the TOE. The procedures may be detailed in the CM plan or throughout the CM  
 8305 documentation. The information included should describe:

8306 a) the method how each configuration item is uniquely identified, such that it is possible  
 8307 to track versions of the same configuration item;

8308 b) the method how configuration items are assigned unique identifiers and how they are  
 8309 entered into the CM system;

8310 c) the method to be used to identify superseded versions of a configuration item.

8311 ISO/IEC 15408-3 ALC\_CMC.3.3C: *The CM system shall uniquely identify all configuration items.*

#### 8312 13.2.3.3.4 Work unit ALC\_CMC.3-4

8313 The evaluator **shall examine** the configuration items to determine that they are identified in a way  
 8314 that is consistent with the CM documentation.

8315 Assurance that the CM system uniquely identifies all configuration items is gained by examining  
 8316 the identifiers for the configuration items. For both configuration items that comprise the TOE, and  
 8317 drafts of configuration items that are submitted by the developer as evaluation evidence, the  
 8318 evaluator confirms that each configuration item possesses a unique identifier in a manner  
 8319 consistent with the unique identification method that is described in the CM documentation.

8320 ISO/IEC 15408-3 ALC\_CMC.3.4C: *The CM system shall provide measures such that only authorised*  
 8321 *changes are made to the configuration items.*

#### 8322 13.2.3.3.5 Work unit ALC\_CMC.3-5

8323 The evaluator **shall examine** the CM access control measures described in the CM plan to  
 8324 determine that they are effective in preventing unauthorised access to the configuration items.

8325 The evaluator may use a number of methods to determine that the CM access control measures are  
 8326 effective. For example, the evaluator may exercise the access control measures to ensure that the  
 8327 procedures could not be bypassed. The evaluator may use the outputs generated by the CM system  
 8328 procedures required by ALC\_CMC.3.8C. The evaluator may also witness a demonstration of the CM  
 8329 system to ensure that the access control measures employed are operating effectively.

## ISO/IEC 18045:2008(E)

- 8330 ISO/IEC 15408-3 ALC\_CMC.3.5C: *The CM documentation shall include a CM plan.*
- 8331 **13.2.3.3.6 Work unit ALC\_CMC.3-6**
- 8332 The evaluator ***shall check*** that the CM documentation provided includes a CM plan.
- 8333 The CM plan needs not to be a connected document, but it is recommended that there is a single  
8334 document that describes where the various parts of the CM plan can be found. If the CM plan is no  
8335 single document, the list in the following work unit gives hints regarding which context is expected.
- 8336 ISO/IEC 15408-3 ALC\_CMC.3.6C: *The CM plan shall describe how the CM system is used for the*  
8337 *development of the TOE.*
- 8338 **13.2.3.3.7 Work unit ALC\_CMC.3-7**
- 8339 The evaluator ***shall examine*** the CM plan to determine that it describes how the CM system is used  
8340 for the development of the TOE.
- 8341 The descriptions contained in a CM plan include, if applicable:
- 8342 a) all activities performed in the TOE development that are subject to configuration  
8343 management procedures (e.g. creation, modification or deletion of a configuration  
8344 item, data-backup, archiving);
  - 8345 b) which means (e.g. CM tools, forms) have to be made available;
  - 8346 c) the usage of the CM tools: the necessary details for a user of the CM system to be able  
8347 to operate the CM tools correctly in order to maintain the integrity of the TOE;
  - 8348 d) which other objects (development components, tools, assessment environments, etc)  
8349 are taken under CM control;
  - 8350 e) the roles and responsibilities of individuals required to perform operations on  
8351 individual configuration items (different roles may be identified for different types of  
8352 configuration items (e.g. design documentation or source code));
  - 8353 f) how CM instances (e.g. change control boards, interface control working groups) are  
8354 introduced and staffed;
  - 8355 g) the description of the change management, including the process of verifying that the  
8356 proposed change is necessary and the consequence would be acceptable;
  - 8357 h) the procedures that are used to ensure that only authorised individuals can make  
8358 changes to configuration items;
  - 8359 i) the procedures that are used to ensure that concurrency problems do not occur as a  
8360 result of simultaneous changes to configuration items;
  - 8361 j) the evidence that is generated as a result of application of the procedures. For  
8362 example, for a change to a configuration item, the CM system might record a  
8363 description of the change, accountability for the change, identification of all  
8364 configuration items affected, status (e.g. pending or completed), and date and time of



|      |                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------|
| 8365 | the change. This might be recorded in an audit trail of changes made or change                                      |
| 8366 | control records;                                                                                                    |
| 8367 | k) the approach to version control and unique referencing of TOE versions (e.g. covering                            |
| 8368 | the release of patches in operating systems, and the subsequent detection of their                                  |
| 8369 | application).                                                                                                       |
| 8370 | ISO/IEC 15408-3 ALC_CMC.3.7C: <i>The evidence shall demonstrate that all configuration items are</i>                |
| 8371 | <i>being maintained under the CM system.</i>                                                                        |
| 8372 | <b>13.2.3.3.8 Work unit ALC_CMC.3-8</b>                                                                             |
| 8373 | The evaluator <b><i>shall check</i></b> that the configuration items identified in the configuration list are being |
| 8374 | maintained by the CM system.                                                                                        |
| 8375 | The CM system employed by the developer should maintain the integrity of the TOE. The evaluator                     |
| 8376 | should check that for each type of configuration item (e.g. design documents or source code                         |
| 8377 | modules) contained in the configuration list there are examples of the evidence generated by the                    |
| 8378 | procedures described in the CM plan. In this case, the approach to sampling will depend upon the                    |
| 8379 | level of granularity used in the CM system to control CM items. Where, for example, 10,000 source                   |
| 8380 | code modules are identified in the configuration list, a different sampling strategy needs to be                    |
| 8381 | applied compared to the case in which there are only 5, or even 1. The emphasis of this activity                    |
| 8382 | should be on ensuring that the CM system is being operated correctly, rather than on the detection                  |
| 8383 | of any minor error.                                                                                                 |
| 8384 | For guidance on sampling see A.2, Sampling.                                                                         |
| 8385 | ISO/IEC 15408-3 ALC_CMC.3.8C: <i>The evidence shall demonstrate that the CM system is being</i>                     |
| 8386 | <i>operated in accordance with the CM plan.</i>                                                                     |
| 8387 | <b>13.2.3.3.9 Work unit ALC_CMC.3-9</b>                                                                             |
| 8388 | The evaluator <b><i>shall check</i></b> the CM documentation to ascertain that it includes the CM system            |
| 8389 | records identified by the CM plan.                                                                                  |
| 8390 | The output produced by the CM system should provide the evidence that the evaluator needs to be                     |
| 8391 | confident that the CM plan is being applied, and also that all configuration items are being                        |
| 8392 | maintained by the CM system as required by ALC_CMC.3.7C. Example output could include change                        |
| 8393 | control forms, or configuration item access approval forms.                                                         |
| 8394 | <b>13.2.3.3.10 Work unit ALC_CMC.3-10</b>                                                                           |
| 8395 | The evaluator <b><i>shall examine</i></b> the evidence to determine that the CM system is being operated in         |
| 8396 | accordance with the CM plan.                                                                                        |
| 8397 | The evaluator should select and examine a sample of evidence covering each type of CM-relevant                      |
| 8398 | operation that has been performed on a configuration item (e.g. creation, modification, deletion,                   |
| 8399 | reversion to an earlier version) to confirm that all operations of the CM system have been carried                  |
| 8400 | out in line with documented procedures. The evaluator confirms that the evidence includes all the                   |
| 8401 | information identified for that operation in the CM plan. Examination of the evidence may require                   |
| 8402 | access to a CM tool that is used. The evaluator may choose to sample the evidence.                                  |
| 8403 | For guidance on sampling see A.2, Sampling.                                                                         |
| 8404 | Further confidence in the correct operation of the CM system and the effective maintenance of                       |
| 8405 | configuration items may be established by means of interviews with selected development staff. In                   |
| 8406 | conducting such interviews, the evaluator aims to gain a deeper understanding of how the CM                         |

8407 system is used in practise as well as to confirm that the CM procedures are being applied as  
8408 described in the CM documentation. Note that such interviews should complement rather than  
8409 replace the examination of documentary evidence, and may not be necessary if the documentary  
8410 evidence alone satisfies the requirement. However, given the wide scope of the CM plan it is  
8411 possible that some aspects (e.g. roles and responsibilities) may not be clear from the CM plan and  
8412 records alone. This is one case where clarification may be necessary through interviews.

8413 It is expected that the evaluator will visit the development site in support of this activity.

8414 For guidance on site visits see A.4, Site Visits.

#### 8415 **13.2.4 Evaluation of sub-activity (ALC\_CMC.4)**

##### 8416 **13.2.4.1 Objectives**

8417 The objectives of this sub-activity are to determine whether the developer has clearly identified the  
8418 TOE and its associated configuration items, and whether the ability to modify these items is  
8419 properly controlled by automated tools, thus making the CM system less susceptible to human  
8420 error or negligence.

##### 8421 **13.2.4.2 Input**

8422 The evaluation evidence for this sub-activity is:

8423 a) the ST;

8424 b) the TOE suitable for testing;

8425 c) the configuration management documentation.

##### 8426 **13.2.4.3 Action ALC\_CMC.4.1E**

8427 ISO/IEC 15408-3 ALC\_CMC.4.1C: *The TOE shall be labelled with its unique reference.*

##### 8428 **13.2.4.3.1 Work unit ALC\_CMC.4-1**

8429 The evaluator **shall check** that the TOE provided for evaluation is labelled with its reference.

8430 The evaluator should ensure that the TOE contains the unique reference which is stated in the ST.  
8431 This could be achieved through labelled packaging or media, or by a label displayed by the  
8432 operational TOE. This is to ensure that it would be possible for consumers to identify the TOE (e.g.  
8433 at the point of purchase or use).

8434 The TOE may provide a method by which it can be easily identified. For example, a software TOE  
8435 may display its name and version number during the start up routine, or in response to a command  
8436 line entry. A hardware or firmware TOE may be identified by a part number physically stamped on  
8437 the TOE.

8438 Alternatively, the unique reference provided for the TOE may be the combination of the unique  
8439 reference of each component from which the TOE is comprised (e.g. in the case of a composed TOE).

##### 8440 **13.2.4.3.2 Work unit ALC\_CMC.4-2**

8441 The evaluator **shall check** that the TOE references used are consistent.

8442 If the TOE is labelled more than once then the labels have to be consistent. For example, it should  
 8443 be possible to relate any labelled guidance documentation supplied as part of the TOE to the  
 8444 evaluated operational TOE. This ensures that consumers can be confident that they have purchased  
 8445 the evaluated version of the TOE, that they have installed this version, and that they have the  
 8446 correct version of the guidance to operate the TOE in accordance with its ST.

8447 The evaluator also verifies that the TOE reference is consistent with the ST.

8448 If this work unit is applied to a composed TOE, the following will apply. The composed TOE will not  
 8449 be labelled with its unique (composite) reference, but only the individual components will be  
 8450 labelled with their appropriate TOE reference. It would require further development for the  
 8451 composed TOE to be labelled, i.e. during start-up and/or operation, with the composite reference. If  
 8452 the composed TOE is delivered as the constituent component TOEs, then the TOE items delivered  
 8453 will not contain the composite reference. However, the composed TOE ST will include the unique  
 8454 reference for the composed TOE and will identify the components comprising the composed TOE  
 8455 through which the consumers will be able to determine whether they have the appropriate items.

8456 ISO/IEC 15408-3 ALC\_CMC.4.2C: *The CM documentation shall describe the method used to uniquely*  
 8457 *identify the configuration items.*

#### 8458 **13.2.4.3.3 Work unit ALC\_CMC.4-3**

8459 The evaluator ***shall examine*** the method of identifying configuration items to determine that it  
 8460 describes how configuration items are uniquely identified.

8461 Procedures should describe how the status of each configuration item can be tracked throughout  
 8462 the life-cycle of the TOE. The procedures may be detailed in the CM plan or throughout the CM  
 8463 documentation. The information included should describe:

8464 a) the method how each configuration item is uniquely identified, such that it is possible  
 8465 to track versions of the same configuration item;

8466 b) the method how configuration items are assigned unique identifiers and how they are  
 8467 entered into the CM system;

8468 c) the method to be used to identify superseded versions of a configuration item.

8469 ISO/IEC 15408-3 ALC\_CMC.4.3C: *The CM system shall uniquely identify all configuration items.*

#### 8470 **13.2.4.3.4 Work unit ALC\_CMC.4-4**

8471 The evaluator ***shall examine*** the configuration items to determine that they are identified in a way  
 8472 that is consistent with the CM documentation.

8473 Assurance that the CM system uniquely identifies all configuration items is gained by examining  
 8474 the identifiers for the configuration items. For configuration items identified under ALC\_CMS, the  
 8475 evaluator confirms that each configuration item possesses a unique identifier in a manner  
 8476 consistent with the unique identification method that is described in the CM documentation.

8477 ISO/IEC 15408-3 ALC\_CMC.4.4C: *The CM system shall provide automated measures such that only*  
 8478 *authorised changes are made to the configuration items.*

8479 **13.2.4.3.5 Work unit ALC\_CMC.4-5**

8480 The evaluator **shall examine** the CM access control measures described in the CM plan (cf.  
8481 ALC\_CMC.4.6C) to determine that they are automated and effective in preventing unauthorised  
8482 access to the configuration items.

8483 The evaluator may use a number of methods to determine that the CM access control measures are  
8484 effective. For example, the evaluator may exercise the access control measures to ensure that the  
8485 procedures could not be bypassed. The evaluator may use the outputs generated by the CM system  
8486 procedures required by ALC\_CMC.4.10C. The evaluator may also witness a demonstration of the  
8487 CM system to ensure that the access control measures employed are operating effectively.

8488 ISO/IEC 15408-3 ALC\_CMC.4.5C: *The CM system shall support the production of the TOE by*  
8489 *automated means.*

8490 **13.2.4.3.6 Work unit ALC\_CMC.4-6**

8491 The evaluator **shall check** the CM plan (cf.ALC\_CMC.4.6C) for automated procedures for supporting  
8492 the production of the TOE.

8493 The term “production” applies to those processes adopted by the developer to progress the TOE  
8494 from the implementation representation to a state acceptable for delivery to the end customer.

8495 The evaluator verifies the existence of automated production support procedures within the CM  
8496 plan.

8497 The following are examples for automated means supporting the production of the TOE:

- 8498 • a “make” tool (as provided with many software development tools) in the case of a  
8499 software TOE;
- 8500 • a tool ensuring automatically (for example by means of bar codes) that only parts are  
8501 combined which indeed belong together in the case of a hardware TOE.

8502 **13.2.4.3.7 Work unit ALC\_CMC.4-7**

8503 The evaluator **shall examine** the TOE production support procedures to determine that they are  
8504 effective in ensuring that a TOE is generated that reflects its implementation representation.

8505 The production support procedures should describe which tools have to be used to produce the  
8506 final TOE from the implementation representation in a clearly defined way. The conventions,  
8507 directives, or other necessary constructs are described under ALC\_TAT.

8508 The evaluator determines that by following the production support procedures the correct  
8509 configuration items would be used to generate the TOE. For example, in a software TOE this may  
8510 include checking that the automated production procedures ensure that all source files and related  
8511 libraries are included in the compiled object code. Moreover, the procedures should ensure that  
8512 compiler options and comparable other options are defined uniquely. For a hardware TOE, this  
8513 work unit may include checking that the automatic production procedures ensure that the  
8514 belonging parts are built together and no parts are missing.

8515 The customer can then be confident that the version of the TOE delivered for installation is derived  
8516 from the implementation representation in an unambiguous way and implements the SFRs as  
8517 described in the ST.

8518 The evaluator should bear in mind that the CM system need not necessarily possess the capability  
8519 to produce the TOE, but should provide support for the process that will help reduce the  
8520 probability of human error.

8521 ISO/IEC 15408-3 ALC\_CMC.4.6C: *The CM documentation shall include a CM plan.*

8522 **13.2.4.3.8 Work unit ALC\_CMC.4-8**

8523 The evaluator **shall check** that the CM documentation provided includes a CM plan.

8524 The CM plan does not need to be contained within a single document, but it is recommended that  
8525 there is a separate document that describes where the various parts of the CM plan can be found. If  
8526 the CM plan is provided by a set of documents, the list in the following work unit gives guidance  
8527 regarding the required content.

8528 ISO/IEC 15408-3 ALC\_CMC.4.7C: *The CM plan shall describe how the CM system is used for the*  
8529 *development of the TOE.*

8530 **13.2.4.3.9 Work unit ALC\_CMC.4-9**

8531 The evaluator **shall examine** the CM plan to determine that it describes how the CM system is used  
8532 for the development of the TOE.

8533 The descriptions contained in a CM plan include, if applicable:

8534 a) all activities performed in the TOE development that are subject to configuration  
8535 management procedures (e.g. creation, modification or deletion of a configuration  
8536 item, data-backup, archiving);

8537 b) which means (e.g. CM tools, forms) have to be made available;

8538 c) the usage of the CM tools: the necessary details for a user of the CM system to be able  
8539 to operate the CM tools correctly in order to maintain the integrity of the TOE;

8540 d) the production support procedures;

8541 e) which other objects (development components, tools, assessment environments, etc)  
8542 are taken under CM control;

8543 f) the roles and responsibilities of individuals required to perform operations on  
8544 individual configuration items (different roles may be identified for different types of  
8545 configuration items (e.g. design documentation or source code));

8546 g) how CM instances (e.g. change control boards, interface control working groups) are  
8547 introduced and staffed;

8548 h) the description of the change management;

8549 i) the procedures that are used to ensure that only authorised individuals can make  
8550 changes to configuration items;

8551 j) the procedures that are used to ensure that concurrency problems do not occur as a  
8552 result of simultaneous changes to configuration items;

## ISO/IEC 18045:2008(E)

- 8553 k) the evidence that is generated as a result of application of the procedures. For  
8554 example, for a change to a configuration item, the CM system might record a  
8555 description of the change, accountability for the change, identification of all  
8556 configuration items affected, status (e.g. pending or completed), and date and time of  
8557 the change. This might be recorded in an audit trail of changes made or change  
8558 control records;
- 8559 l) the approach to version control and unique referencing of TOE versions (e.g. covering  
8560 the release of patches in operating systems, and the subsequent detection of their  
8561 application).
- 8562 ISO/IEC 15408-3 ALC\_CMC.4.8C: *The CM plan shall describe the procedures used to accept modified*  
8563 *or newly created configuration items as part of the TOE.*
- 8564 **13.2.4.3.10 Work unit ALC\_CMC.4-10**
- 8565 The evaluator ***shall examine*** the CM plan to determine that it describes the procedures used to  
8566 accept modified or newly created configuration items as parts of the TOE.
- 8567 The descriptions of the acceptance procedures in the CM plan should include the developer roles or  
8568 individuals responsible for the acceptance and the criteria to be used for acceptance. In order to  
8569 meet the desired assurance level, the acceptance criteria may include a suite of tests that  
8570 determines whether the required security objective and/or performance objective is met. The  
8571 criteria should take into account all acceptance situations that may occur, in particular:
- 8572 a) accepting an item into the CM system for the first time, in particular inclusion of  
8573 software, firmware and hardware components from other manufacturers into the  
8574 TOE ("integration");
- 8575 b) moving configuration items to the next life-cycle phase at each stage of the  
8576 construction of the TOE (e.g. module, subsystem, system);
- 8577 c) subsequent to transports between different development sites.
- 8578 If this work unit is applied to a dependent component that is going to be integrated in a composed  
8579 TOE, the CM plan should consider the control of base components obtained by the dependent TOE  
8580 developer.
- 8581 When obtaining the components the evaluators are to verify the following:
- 8582 a) Transfer of each base component from the base component developer to the  
8583 integrator (dependent TOE developer) was performed in accordance with the base  
8584 component TOE's secure delivery procedures, as reported in the base component  
8585 TOE certification report.
- 8586 b) The component received has the same identifiers as those stated in the ST and  
8587 Certification Report for the component TOE.
- 8588 c) All additional material required by a developer for composition (integration) is  
8589 provided. This is to include the necessary extract of the component TOE's functional  
8590 specification.
- 8591 ISO/IEC 15408-3 ALC\_CMC.4.9C: *The evidence shall demonstrate that all configuration items are*  
8592 *being maintained under the CM system.*

8593 **13.2.4.3.11 Work unit ALC\_CMC.4-11**

8594 The evaluator **shall check** that the configuration items identified in the configuration list are being  
8595 maintained by the CM system.

8596 The CM system employed by the developer should maintain the integrity of the TOE. The evaluator  
8597 should check that for each type of configuration item (e.g. design documents or source code  
8598 modules) contained in the configuration list there are examples of the evidence generated by the  
8599 procedures described in the CM plan. In this case, the approach to sampling will depend upon the  
8600 level of granularity used in the CM system to control CM items. Where, for example, 10,000 source  
8601 code modules are identified in the configuration list, a different sampling strategy needs to be  
8602 applied compared to the case in which there are only 5, or even 1. The emphasis of this activity  
8603 should be on ensuring that the CM system is being operated correctly, rather than on the detection  
8604 of any minor error.

8605 For guidance on sampling see A.2, Sampling.

8606 ISO/IEC 15408-3 ALC\_CMC.4.10C: *The evidence shall demonstrate that the CM system is being*  
8607 *operated in accordance with the CM plan.*

8608 **13.2.4.3.12 Work unit ALC\_CMC.4-12**

8609 The evaluator **shall check** the CM documentation to ascertain that it includes the CM system  
8610 records identified by the CM plan.

8611 The output produced by the CM system should provide the evidence that the evaluator needs to be  
8612 confident that the CM plan is being applied, and also that all configuration items are being  
8613 maintained by the CM system as required by ALC\_CMC.4.9C. Example output could include change  
8614 control forms, or configuration item access approval forms.

8615 **13.2.4.3.13 Work unit ALC\_CMC.4-13**

8616 The evaluator **shall examine** the evidence to determine that the CM system is being operated in  
8617 accordance with the CM plan.

8618 The evaluator should select and examine a sample of evidence covering each type of CM-relevant  
8619 operation that has been performed on a configuration item (e.g. creation, modification, deletion,  
8620 reversion to an earlier version) to confirm that all operations of the CM system have been carried  
8621 out in line with documented procedures. The evaluator confirms that the evidence includes all the  
8622 information identified for that operation in the CM plan. Examination of the evidence may require  
8623 access to a CM tool that is used. The evaluator may choose to sample the evidence.

8624 For guidance on sampling see A.2, Sampling.

8625 Further confidence in the correct operation of the CM system and the effective maintenance of  
8626 configuration items may be established by means of interviews with selected development staff. In  
8627 conducting such interviews, the evaluator aims to gain a deeper understanding of how the CM  
8628 system is used in practise as well as to confirm that the CM procedures are being applied as  
8629 described in the CM documentation. Note that such interviews should complement rather than  
8630 replace the examination of documentary evidence, and may not be necessary if the documentary  
8631 evidence alone satisfies the requirement. However, given the wide scope of the CM plan it is  
8632 possible that some aspects (e.g. roles and responsibilities) may not be clear from the CM plan and  
8633 records alone. This is one case where clarification may be necessary through interviews.

8634 It is expected that the evaluator will visit the development site in support of this activity.

8635 For guidance on site visits see A.4, Site Visits.

**13.2.5 Evaluation of sub-activity (ALC\_CMC.5)**

**13.2.5.1 Objectives**

The objectives of this sub-activity are to determine whether the developer has clearly identified the TOE and its associated configuration items, and whether the ability to modify these items is properly controlled by automated tools, thus making the CM system less susceptible to human error or negligence.

**13.2.5.2 Input**

The evaluation evidence for this sub-activity is:

- a) the ST;
- b) the TOE suitable for testing;
- c) the configuration management documentation.

**13.2.5.3 Action ALC\_CMC.5.1E**

ISO/IEC 15408-3 ALC\_CMC.5.1C: *The TOE shall be labelled with its unique reference.*

**13.2.5.3.1 Work unit ALC\_CMC.5-1**

The evaluator **shall check** that the TOE provided for evaluation is labelled with its reference.

The evaluator should ensure that the TOE contains the unique reference which is stated in the ST. This could be achieved through labelled packaging or media, or by a label displayed by the operational TOE. This is to ensure that it would be possible for consumers to identify the TOE (e.g. at the point of purchase or use).

The TOE may provide a method by which it can be easily identified. For example, a software TOE may display its name and version number during the start up routine, or in response to a command line entry. A hardware or firmware TOE may be identified by a part number physically stamped on the TOE.

Alternatively, the unique reference provided for the TOE may be the combination of the unique reference of each component from which the TOE is comprised (e.g. in the case of a composed TOE).

**13.2.5.3.2 Work unit ALC\_CMC.5-2**

The evaluator **shall check** that the TOE references used are consistent.

If the TOE is labelled more than once then the labels have to be consistent. For example, it should be possible to relate any labelled guidance documentation supplied as part of the TOE to the evaluated operational TOE. This ensures that consumers can be confident that they have purchased the evaluated version of the TOE, that they have installed this version, and that they have the correct version of the guidance to operate the TOE in accordance with its ST.

The evaluator also verifies that the TOE reference is consistent with the ST.

If this work unit is applied to a composed TOE, the following will apply. The composed IT TOE will not be labelled with its unique (composite) reference, but only the individual components will be labelled with their appropriate TOE reference. It would require further development for the IT TOE to be labelled, i.e. during start-up and/or operation, with the composite reference. If the composed



8673 TOE is delivered as the constituent component TOEs, then the TOE items delivered will not contain  
8674 the composite reference. However, the composed TOE ST will include the unique reference for the  
8675 composed TOE and will identify the components comprising the composed TOE through which the  
8676 consumers will be able to determine whether they have the appropriate items.

8677 ISO/IEC 15408-3 ALC\_CMC.5.2C: *The CM documentation shall describe the method used to uniquely*  
8678 *identify the configuration items.*

#### 8679 13.2.5.3.3 Work unit ALC\_CMC.5-3

8680 The evaluator **shall examine** the method of identifying configuration items to determine that it  
8681 describes how configuration items are uniquely identified.

8682 Procedures should describe how the status of each configuration item can be tracked throughout  
8683 the life-cycle of the TOE. The procedures may be detailed in the CM plan or throughout the CM  
8684 documentation. The information included should describe:

- 8685 a) the method how each configuration item is uniquely identified, such that it is possible  
8686 to track versions of the same configuration item;
- 8687 b) the method how configuration items are assigned unique identifiers and how they are  
8688 entered into the CM system;
- 8689 c) the method to be used to identify superseded versions of a configuration item.

8690 ISO/IEC 15408-3 ALC\_CMC.5.3C: *The CM documentation shall justify that the acceptance procedures*  
8691 *provide for an adequate and appropriate review of changes to all configuration items.*

#### 8692 13.2.5.3.4 Work unit ALC\_CMC.5-4

8693 The evaluator **shall examine** the CM documentation to determine that it justifies that the  
8694 acceptance procedures provide for an adequate and appropriate review of changes to all  
8695 configuration items.

8696 The CM documentation should make it sufficiently clear that by following the acceptance  
8697 procedures only parts of adequate quality are incorporated into the TOE.

8698 ISO/IEC 15408-3 ALC\_CMC.5.4C: *The CM system shall uniquely identify all configuration items.*

#### 8699 13.2.5.3.5 Work unit ALC\_CMC.5-5

8700 The evaluator **shall examine** the configuration items to determine that they are identified in a way  
8701 that is consistent with the CM documentation.

8702 Assurance that the CM system uniquely identifies all configuration items is gained by examining  
8703 the identifiers for the configuration items. For both configuration items that comprise the TOE, and  
8704 drafts of configuration items that are submitted by the developer as evaluation evidence, the  
8705 evaluator confirms that each configuration item possesses a unique identifier in a manner  
8706 consistent with the unique identification method that is described in the CM documentation.

8707 ISO/IEC 15408-3 ALC\_CMC.5.5C: *The CM system shall provide automated measures such that only*  
8708 *authorised changes are made to the configuration items.*

## ISO/IEC 18045:2008(E)

### 8709 13.2.5.3.6 Work unit ALC\_CMC.5-6

8710 The evaluator **shall examine** the CM access control measures described in the CM plan (cf.  
8711 ALC\_CMC.5.12C) to determine that they are automated and effective in preventing unauthorised  
8712 access to the configuration items.

8713 The evaluator may use a number of methods to determine that the CM access control measures are  
8714 effective. For example, the evaluator may exercise the access control measures to ensure that the  
8715 procedures could not be bypassed. The evaluator may use the outputs generated by the CM system  
8716 procedures required by ALC\_CMC.5.16C. The evaluator may also witness a demonstration of the  
8717 CM system to ensure that the access control measures employed are operating effectively.

8718 ISO/IEC 15408-3 ALC\_CMC.5.6C: *The CM system shall support the production of the TOE by*  
8719 *automated means.*

### 8720 13.2.5.3.7 Work unit ALC\_CMC.5-7

8721 The evaluator **shall check** the CM plan (cf. ALC\_CMC.5.12C) for automated procedures for  
8722 supporting the production of the TOE.

8723 The term “production” applies to those processes adopted by the developer to progress the TOE  
8724 from the implementation representation to a state acceptable for delivery to the end customer.

8725 The evaluator verifies the existence of automated production support procedures within the CM  
8726 plan.

8727 The following are examples for automated means supporting the production of the TOE:

- 8728 • a “make” tool (as provided with many software development tools) in the case of a  
8729 software TOE;
- 8730 • a tool ensuring automatically (for example by means of bar codes) that only parts are  
8731 combined which indeed belong together in the case of a hardware TOE.

### 8732 13.2.5.3.8 Work unit ALC\_CMC.5-8

8733 The evaluator **shall examine** the TOE production support procedures to determine that they are  
8734 effective in ensuring that a TOE is generated that reflects its implementation representation.

8735 The production support procedures should describe which tools have to be used to produce the  
8736 final TOE from the implementation representation in a clearly defined way. The conventions,  
8737 directives, or other necessary constructs are described under ALC\_TAT.

8738 The evaluator determines that by following the production support procedures the correct  
8739 configuration items would be used to generate the TOE. For example, in a software TOE this may  
8740 include checking that the automated production procedures ensure that all source files and related  
8741 libraries are included in the compiled object code. Moreover, the procedures should ensure that  
8742 compiler options and comparable other options are defined uniquely. For a hardware TOE, this  
8743 work unit may include checking that the automatic production procedures ensure that the  
8744 belonging parts are built together and no parts are missing.

8745 The customer can then be confident that the version of the TOE delivered for installation is derived  
8746 from the implementation representation in an unambiguous way and implements the SFRs as  
8747 described in the ST.

8748 The evaluator should bear in mind that the CM system need not necessarily possess the capability  
8749 to produce the TOE, but should provide support for the process that will help reduce the  
8750 probability of human error.

8751 ISO/IEC 15408-3 ALC\_CMC.5.7C: *The CM system shall ensure that the person responsible for*  
8752 *accepting a configuration item into CM is not the person who developed it.*

8753 **13.2.5.3.9 Work unit ALC\_CMC.5-9**

8754 The evaluator **shall examine** the CM system to determine that it ensures that the person  
8755 responsible for accepting a configuration item is not the person who developed it.

8756 The acceptance procedures describe who is responsible for accepting a configuration item. From  
8757 these descriptions, the evaluator should be able to determine that the person who developed a  
8758 configuration item is in no case responsible for its acceptance.

8759 ISO/IEC 15408-3 ALC\_CMC.5.8C: *The CM system shall identify the configuration items that comprise*  
8760 *the TSF.*

8761 **13.2.5.3.10 Work unit ALC\_CMC.5-10**

8762 The evaluator **shall examine** the CM system to determine that it identifies the configuration items  
8763 that comprise the TSF.

8764 The CM documentation should describe how the CM system identifies the configuration items that  
8765 comprise the TSF. The evaluator should select a sample of configuration items covering each type  
8766 of items, particularly containing TSF and non-TSF items, and check that they are correctly classified  
8767 by the CM system.

8768 For guidance on sampling see A.2, Sampling.

8769 ISO/IEC 15408-3 ALC\_CMC.5.9C: *The CM system shall support the audit of all changes to the TOE by*  
8770 *automated means, including the originator, date, and time in the audit trail.*

8771 **13.2.5.3.11 Work unit ALC\_CMC.5-11**

8772 The evaluator **shall examine** the CM system to determine that it supports the audit of all changes  
8773 to the TOE by automated means, including the originator, date, and time in the audit trail.

8774 The evaluator should inspect a sample of audit trails and check, if they contain the minimum  
8775 information.

8776 ISO/IEC 15408-3 ALC\_CMC.5.10C: *The CM system shall provide an automated means to identify all*  
8777 *other configuration items that are affected by the change of a given configuration item.*

8778 **13.2.5.3.12 Work unit ALC\_CMC.5-12**

8779 The evaluator **shall examine** the CM system to determine that it provides an automated means to  
8780 identify all other configuration items that are affected by the change of a given configuration item.

8781 The CM documentation should describe how the CM system identifies all other configuration items  
8782 that are affected by the change of a given configuration item. The evaluator should select a sample  
8783 of configuration items, covering all types of items, and exercise the automated means to determine  
8784 that it identifies all items that are affected by the change of the selected item.

8785 For guidance on sampling see A.2, Sampling.

## ISO/IEC 18045:2008(E)

8786 ISO/IEC 15408-3 ALC\_CMC.5.11C: *The CM system shall be able to identify the version of the*  
8787 *implementation representation from which the TOE is generated.*

### 8788 13.2.5.3.13 Work unit ALC\_CMC.5-13

8789 The evaluator **shall examine** the CM system to determine that it is able to identify the version of  
8790 the implementation representation from which the TOE is generated.

8791 The CM documentation should describe how the CM system identifies the version of the  
8792 implementation representation from which the TOE is generated. The evaluator should select a  
8793 sample of the parts used to produce the TOE and should apply the CM system to verify that it  
8794 identifies the corresponding implementation representation in the correct version.

8795 For guidance on sampling see A.2, Sampling.

8796 ISO/IEC 15408-3 ALC\_CMC.5.12C: *The CM documentation shall include a CM plan.*

### 8797 13.2.5.3.14 Work unit ALC\_CMC.5-14

8798 The evaluator **shall check** that the CM documentation provided includes a CM plan.

8799 The CM plan needs not to be a connected document, but it is recommended that there is a single  
8800 document that describes where the various parts of the CM plan can be found. If the CM plan is no  
8801 single document, the list in the following work unit gives hints regarding which context is expected.

8802 ISO/IEC 15408-3 ALC\_CMC.5.13C: *The CM plan shall describe how the CM system is used for the*  
8803 *development of the TOE.*

### 8804 13.2.5.3.15 Work unit ALC\_CMC.5-15

8805 The evaluator **shall examine** the CM plan to determine that it describes how the CM system is used  
8806 for the development of the TOE.

8807 The descriptions contained in a CM plan include, if applicable:

8808 a) all activities performed in the TOE development that are subject to configuration  
8809 management procedures (e.g. creation, modification or deletion of a configuration  
8810 item, data-backup, archiving);

8811 b) which means (e.g. CM tools, forms) have to be made available;

8812 c) the usage of the CM tools: the necessary details for a user of the CM system to be able  
8813 to operate the CM tools correctly in order to maintain the integrity of the TOE;

8814 d) the production support procedures;

8815 e) which other objects (development components, tools, assessment environments, etc)  
8816 are taken under CM control;

8817 f) the roles and responsibilities of individuals required to perform operations on  
8818 individual configuration items (different roles may be identified for different types of  
8819 configuration items (e.g. design documentation or source code));

8820 g) how CM instances (e.g. change control boards, interface control working groups) are  
8821 introduced and staffed;

- 8822 h) the description of the change management;
- 8823 i) the procedures that are used to ensure that only authorised individuals can make  
8824 changes to configuration items;
- 8825 j) the procedures that are used to ensure that concurrency problems do not occur as a  
8826 result of simultaneous changes to configuration items;
- 8827 k) the evidence that is generated as a result of application of the procedures. For  
8828 example, for a change to a configuration item, the CM system might record a  
8829 description of the change, accountability for the change, identification of all  
8830 configuration items affected, status (e.g. pending or completed), and date and time of  
8831 the change. This might be recorded in an audit trail of changes made or change  
8832 control records;
- 8833 l) the approach to version control and unique referencing of TOE versions (e.g. covering  
8834 the release of patches in operating systems, and the subsequent detection of their  
8835 application).
- 8836 ISO/IEC 15408-3 ALC\_CMC.5.14C: *The CM plan shall describe the procedures used to accept modified*  
8837 *or newly created configuration items as part of the TOE.*
- 8838 **13.2.5.3.16 Work unit ALC\_CMC.5-16**
- 8839 The evaluator ***shall examine*** the CM plan to determine that it describes the procedures used to  
8840 accept modified or newly created configuration items as parts of the TOE.
- 8841 The descriptions of the acceptance procedures in the CM plan should include the developer roles or  
8842 individuals responsible for the acceptance and the criteria to be used for acceptance. In order to  
8843 meet the desired assurance level, the acceptance criteria may include a suite of tests that  
8844 determines whether the required security objective and/or performance objective is met. The  
8845 criteria should take into account all acceptance situations that may occur, in particular:
- 8846 a) accepting an item into the CM system for the first time, in particular inclusion of  
8847 software, firmware and hardware components from other manufacturers into the  
8848 TOE ("integration");
- 8849 b) moving configuration items to the next life-cycle phase at each stage of the  
8850 construction of the TOE (e.g. module, subsystem, system);
- 8851 c) subsequent to transports between different development sites.
- 8852 If this work unit is applied to a dependent component that is going to be integrated in a composed  
8853 TOE, the CM plan should consider the control of base components obtained by the dependent TOE  
8854 developer.
- 8855 When obtaining the components the evaluators are to verify the following:
- 8856 a) Transfer of each base component from the base component developer to the  
8857 integrator (dependent TOE developer) was performed in accordance with the base  
8858 component TOE's secure delivery procedures, as reported in the base component  
8859 TOE certification report.

## ISO/IEC 18045:2008(E)

- 8860 b) The component received has the same identifiers as those stated in the ST and  
8861 Certification Report for the component TOE.
- 8862 c) All additional material required by a developer for composition (integration) is  
8863 provided. This is to include the necessary extract of the component TOE's functional  
8864 specification.
- 8865 ISO/IEC 15408-3 ALC\_CMC.5.15C: *The evidence shall demonstrate that all configuration items are*  
8866 *being maintained under the CM system.*
- 8867 **13.2.5.3.17 Work unit ALC\_CMC.5-17**
- 8868 The evaluator **shall check** that the configuration items identified in the configuration list are being  
8869 maintained by the CM system.
- 8870 The CM system employed by the developer should maintain the integrity of the TOE. The evaluator  
8871 should check that for each type of configuration item (e.g. design documents or source code  
8872 modules) contained in the configuration list there are examples of the evidence generated by the  
8873 procedures described in the CM plan. In this case, the approach to sampling will depend upon the  
8874 level of granularity used in the CM system to control CM items. Where, for example, 10,000 source  
8875 code modules are identified in the configuration list, a different sampling strategy needs to be  
8876 applied compared to the case in which there are only 5, or even 1. The emphasis of this activity  
8877 should be on ensuring that the CM system is being operated correctly, rather than on the detection  
8878 of any minor error.
- 8879 For guidance on sampling see A.2, Sampling.
- 8880 ISO/IEC 15408-3 ALC\_CMC.5.16C: *The evidence shall demonstrate that the CM system is being*  
8881 *operated in accordance with the CM plan.*
- 8882 **13.2.5.3.18 Work unit ALC\_CMC.5-18**
- 8883 The evaluator **shall check** the CM documentation to ascertain that it includes the CM system  
8884 records identified by the CM plan.
- 8885 The output produced by the CM system should provide the evidence that the evaluator needs to be  
8886 confident that the CM plan is being applied, and also that all configuration items are being  
8887 maintained by the CM system as required by ALC\_CMC.5.15C. Example output could include change  
8888 control forms, or configuration item access approval forms.
- 8889 **13.2.5.3.19 Work unit ALC\_CMC.5-19**
- 8890 The evaluator **shall examine** the evidence to determine that the CM system is being operated in  
8891 accordance with the CM plan.
- 8892 The evaluator should select and examine a sample of evidence covering each type of CM-relevant  
8893 operation that has been performed on a configuration item (e.g. creation, modification, deletion,  
8894 reversion to an earlier version) to confirm that all operations of the CM system have been carried  
8895 out in line with documented procedures. The evaluator confirms that the evidence includes all the  
8896 information identified for that operation in the CM plan. Examination of the evidence may require  
8897 access to a CM tool that is used. The evaluator may choose to sample the evidence.
- 8898 For guidance on sampling see A.2, Sampling.
- 8899 Further confidence in the correct operation of the CM system and the effective maintenance of  
8900 configuration items may be established by means of interviews with selected development staff. In  
8901 conducting such interviews, the evaluator aims to gain a deeper understanding of how the CM

8902 system is used in practise as well as to confirm that the CM procedures are being applied as  
 8903 described in the CM documentation. Note that such interviews should complement rather than  
 8904 replace the examination of documentary evidence, and may not be necessary if the documentary  
 8905 evidence alone satisfies the requirement. However, given the wide scope of the CM plan it is  
 8906 possible that some aspects (e.g. roles and responsibilities) may not be clear from the CM plan and  
 8907 records alone. This is one case where clarification may be necessary through interviews.

8908 It is expected that the evaluator will visit the development site in support of this activity.

8909 For guidance on site visits see A.4, Site Visits.

#### 8910 **13.2.5.4 Action ALC\_CMC.5.2E**

##### 8911 **13.2.5.4.1 Work unit ALC\_CMC.5-20**

8912 The evaluator *shall examine* the production support procedures to determine that by following  
 8913 these procedures a TOE would be produced like that one provided by the developer for testing  
 8914 activities.

8915 If the TOE is a small software TOE and production consists of compiling and linking, the evaluator  
 8916 might confirm the adequacy of the production support procedures by reapplying them himself.

8917 If the production process of the TOE is more complicated (as for example in the case of a smart  
 8918 card), but has already started, the evaluator should inspect the application of the production  
 8919 support procedures during a visit of the development site. They might compare a copy of the TOE  
 8920 produced in their presence with the samples used for their testing activities.

8921 For guidance on site visits see A.4, Site Visits.

8922 Otherwise the evaluator's determination should be based on the documentary evidence provided  
 8923 by the developer.

8924 This work unit may be performed in conjunction with the evaluation activities under  
 8925 Implementation representation (ADV\_IMP).

### 8926 **13.3 CM scope (ALC\_CMS)**

#### 8927 **13.3.1 Evaluation of sub-activity (ALC\_CMS.1)**

##### 8928 **13.3.1.1 Objectives**

8929 The objective of this sub-activity is to determine whether the developer performs configuration  
 8930 management on the TOE and the evaluation evidence. These configuration items are controlled in  
 8931 accordance with CM capabilities (ALC\_CMC).

##### 8932 **13.3.1.2 Input**

8933 The evaluation evidence for this sub-activity is:

8934 a) the ST;

8935 b) the configuration list.

##### 8936 **13.3.1.3 Action ALC\_CMS.1.1E**

8937 ISO/IEC 15408-3 ALC\_CMS.1.1C: *The configuration list shall include the following: the TOE itself; and*  
 8938 *the evaluation evidence required by the SARs.*

## ISO/IEC 18045:2008(E)

### 8939 13.3.1.3.1 Work unit ALC\_CMS.1-1

8940 The evaluator **shall check** that the configuration list includes the following set of items:

8941 a) the TOE itself;

8942 b) the evaluation evidence required by the SARs in the ST.

8943 ISO/IEC 15408-3 ALC\_CMS.1.2C: *The configuration list shall uniquely identify the configuration items.*

### 8944 13.3.1.3.2 Work unit ALC\_CMS.1-2

8945 The evaluator **shall examine** the configuration list to determine that it uniquely identifies each  
8946 configuration item.

8947 The configuration list contains sufficient information to uniquely identify which version of each  
8948 item has been used (typically a version number). Use of this list will enable the evaluator to check  
8949 that the correct configuration items, and the correct version of each item, have been used during  
8950 the evaluation.

### 8951 13.3.2 Evaluation of sub-activity (ALC\_CMS.2)

#### 8952 13.3.2.1 Objectives

8953 The objective of this sub-activity is to determine whether the configuration list includes the TOE,  
8954 the parts that comprise the TOE, and the evaluation evidence. These configuration items are  
8955 controlled in accordance with CM capabilities (ALC\_CMC).

#### 8956 13.3.2.2 Input

8957 The evaluation evidence for this sub-activity is:

8958 a) the ST;

8959 b) the configuration list.

#### 8960 13.3.2.3 Action ALC\_CMS.2.1E

8961 ISO/IEC 15408-3 ALC\_CMS.2.1C: *The configuration list shall include the following: the TOE itself; the*  
8962 *evaluation evidence required by the SARs; and the parts that comprise the TOE.*

### 8963 13.3.2.3.1 Work unit ALC\_CMS.2-1

8964 The evaluator **shall check** that the configuration list includes the following set of items:

8965 a) the TOE itself;

8966 b) the parts that comprise the TOE;

8967 c) the evaluation evidence required by the SARs.

8968 ISO/IEC 15408-3 ALC\_CMS.2.2C: *The configuration list shall uniquely identify the configuration items.*



8969 **13.3.2.3.2 Work unit ALC\_CMS.2-2**

8970 The evaluator **shall examine** the configuration list to determine that it uniquely identifies each  
8971 configuration item.

8972 The configuration list contains sufficient information to uniquely identify which version of each  
8973 item has been used (typically a version number). Use of this list will enable the evaluator to check  
8974 that the correct configuration items, and the correct version of each item, have been used during  
8975 the evaluation.

8976 ISO/IEC 15408-3 ALC\_CMS.2.3C: *For each TSF relevant configuration item, the configuration list*  
8977 *shall indicate the developer of the item.*

8978 **13.3.2.3.3 Work unit ALC\_CMS.2-3**

8979 The evaluator **shall check** that the configuration list indicates the developer of each TSF relevant  
8980 configuration item.

8981 If only one developer is involved in the development of the TOE, this work unit is not applicable,  
8982 and is therefore considered to be satisfied.

8983 **13.3.3 Evaluation of sub-activity (ALC\_CMS.3)**

8984 **13.3.3.1 Objectives**

8985 The objective of this sub-activity is to determine whether the configuration list includes the TOE,  
8986 the parts that comprise the TOE, the TOE implementation representation, and the evaluation  
8987 evidence. These configuration items are controlled in accordance with CM capabilities (ALC\_CMC).

8988 **13.3.3.2 Input**

8989 The evaluation evidence for this sub-activity is:

- 8990 a) the ST;
- 8991 b) the configuration list.

8992 **13.3.3.3 Action ALC\_CMS.3.1E**

8993 ISO/IEC 15408-3 ALC\_CMS.3.1C: *The configuration list shall include the following: the TOE itself; the*  
8994 *evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation*  
8995 *representation.*

8996 **13.3.3.3.1 Work unit ALC\_CMS.3-1**

8997 The evaluator **shall check** that the configuration list includes the following set of items:

- 8998 a) the TOE itself;
- 8999 b) the parts that comprise the TOE;
- 9000 c) the TOE implementation representation;
- 9001 d) the evaluation evidence required by the SARs in the ST.

## ISO/IEC 18045:2008(E)

9002 ISO/IEC 15408-3 ALC\_CMS.3.2C: *The configuration list shall uniquely identify the configuration items.*

### 9003 13.3.3.3.2 Work unit ALC\_CMS.3-2

9004 The evaluator **shall examine** the configuration list to determine that it uniquely identifies each  
9005 configuration item.

9006 The configuration list contains sufficient information to uniquely identify which version of each  
9007 item has been used (typically a version number). Use of this list will enable the evaluator to check  
9008 that the correct configuration items, and the correct version of each item, have been used during  
9009 the evaluation.

9010 ISO/IEC 15408-3 ALC\_CMS.3.3C: *For each TSF relevant configuration item, the configuration list*  
9011 *shall indicate the developer of the item.*

### 9012 13.3.3.3.3 Work unit ALC\_CMS.3-3

9013 The evaluator **shall check** that the configuration list indicates the developer of each TSF relevant  
9014 configuration item.

9015 If only one developer is involved in the development of the TOE, this work unit is not applicable,  
9016 and is therefore considered to be satisfied.

## 9017 13.3.4 Evaluation of sub-activity (ALC\_CMS.4)

### 9018 13.3.4.1 Objectives

9019 The objective of this sub-activity is to determine whether the configuration list includes the TOE,  
9020 the parts that comprise the TOE, the TOE implementation representation, security flaws, and the  
9021 evaluation evidence. These configuration items are controlled in accordance with CM capabilities  
9022 (ALC\_CMC).

### 9023 13.3.4.2 Input

9024 The evaluation evidence for this sub-activity is:

9025 a) the ST;

9026 b) the configuration list.

### 9027 13.3.4.3 Action ALC\_CMS.4.1E

9028 ISO/IEC 15408-3 ALC\_CMS.4.1C: *The configuration list shall include the following: the TOE itself; the*  
9029 *evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation*  
9030 *representation; and security flaw reports and resolution status.*

### 9031 13.3.4.3.1 Work unit ALC\_CMS.4-1

9032 The evaluator **shall check** that the configuration list includes the following set of items:

9033 a) the TOE itself;

9034 b) the parts that comprise the TOE;

9035 c) the TOE implementation representation;

- 9036 d) the evaluation evidence required by the SARs in the ST;
- 9037 e) the documentation used to record details of reported security flaws associated with  
9038 the implementation (e.g., problem status reports derived from a developer's problem  
9039 database).
- 9040 ISO/IEC 15408-3 ALC\_CMS.4.2C: *The configuration list shall uniquely identify the configuration items.*
- 9041 **13.3.4.3.2 Work unit ALC\_CMS.4-2**
- 9042 The evaluator **shall examine** the configuration list to determine that it uniquely identifies each  
9043 configuration item.
- 9044 The configuration list contains sufficient information to uniquely identify which version of each  
9045 item has been used (typically a version number). Use of this list will enable the evaluator to check  
9046 that the correct configuration items, and the correct version of each item, have been used during  
9047 the evaluation.
- 9048 ISO/IEC 15408-3 ALC\_CMS.4.3C: *For each TSF relevant configuration item, the configuration list*  
9049 *shall indicate the developer of the item.*
- 9050 **13.3.4.3.3 Work unit ALC\_CMS.4-3**
- 9051 The evaluator **shall check** that the configuration list indicates the developer of each TSF relevant  
9052 configuration item.
- 9053 If only one developer is involved in the development of the TOE, this work unit is not applicable,  
9054 and is therefore considered to be satisfied.
- 9055 **13.3.5 Evaluation of sub-activity (ALC\_CMS.5)**
- 9056 **13.3.5.1 Objectives**
- 9057 The objective of this sub-activity is to determine whether the configuration list includes the TOE,  
9058 the parts that comprise the TOE, the TOE implementation representation, security flaws,  
9059 development tools and related information, and the evaluation evidence. These configuration items  
9060 are controlled in accordance with CM capabilities (ALC\_CMC).
- 9061 **13.3.5.2 Input**
- 9062 The evaluation evidence for this sub-activity is:
- 9063 a) the ST;
- 9064 b) the configuration list.
- 9065 **13.3.5.3 Action ALC\_CMS.5.1E**
- 9066 ISO/IEC 15408-3 ALC\_CMS.5.1C: *The configuration list shall include the following: the TOE itself; the*  
9067 *evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation*  
9068 *representation; security flaw reports and resolution status; and development tools and related*  
9069 *information.*
- 9070 **13.3.5.3.1 Work unit ALC\_CMS.5-1**
- 9071 The evaluator **shall check** that the configuration list includes the following set of items:

## ISO/IEC 18045:2008(E)

- 9072 a) the TOE itself;
- 9073 b) the parts that comprise the TOE;
- 9074 c) the TOE implementation representation;
- 9075 d) the evaluation evidence required by the SARs in the ST;
- 9076 e) the documentation used to record details of reported security flaws associated with  
9077 the implementation (e.g., problem status reports derived from a developer's problem  
9078 database);
- 9079 f) all tools (incl. test software, if applicable) involved in the development and  
9080 production of the TOE including the names, versions, configurations and roles of  
9081 each development tool, and related documentation.
- 9082 For a software TOE, "development tools" are usually programming languages and compiler and  
9083 "related documentation" comprises compiler and linker options. For a hardware TOE,  
9084 "development tools" might be hardware design languages, simulation and synthesis tools,  
9085 compilers, and "related documentation" might comprise compiler options again.
- 9086 ISO/IEC 15408-3 ALC\_CMS.5.2C: *The configuration list shall uniquely identify the configuration items.*
- 9087 **13.3.5.3.2 Work unit ALC\_CMS.5-2**
- 9088 The evaluator ***shall examine*** the configuration list to determine that it uniquely identifies each  
9089 configuration item.
- 9090 The configuration list contains sufficient information to uniquely identify which version of each  
9091 item has been used (typically a version number). Use of this list will enable the evaluator to check  
9092 that the correct configuration items, and the correct version of each item, have been used during  
9093 the evaluation.
- 9094 ISO/IEC 15408-3 ALC\_CMS.5.3C: *For each TSF relevant configuration item, the configuration list*  
9095 *shall indicate the developer of the item.*
- 9096 **13.3.5.3.3 Work unit ALC\_CMS.5-3**
- 9097 The evaluator ***shall check*** that the configuration list indicates the developer of each TSF relevant  
9098 configuration item.
- 9099 If only one developer is involved in the development of the TOE, this work unit is not applicable,  
9100 and is therefore considered to be satisfied.
- 9101 **13.4 Delivery (ALC\_DEL)**
- 9102 **13.4.1 Evaluation of sub-activity (ALC\_DEL.1)**
- 9103 **13.4.1.1 Objectives**
- 9104 The objective of this sub-activity is to determine whether the delivery documentation describes all  
9105 procedures used to maintain security of the TOE when distributing the TOE to the user.

9106 **13.4.1.2 Input**

9107 The evaluation evidence for this sub-activity is:

9108 a) the ST;

9109 b) the delivery documentation.

9110 **13.4.1.3 Action ALC\_DEL.1.1E**9111 ISO/IEC 15408-3 ALC\_DEL.1.1C: *The delivery documentation shall describe all procedures that are*  
9112 *necessary to maintain security when distributing versions of the TOE to the consumer.*9113 **13.4.1.3.1 Work unit ALC\_DEL.1-1**9114 The evaluator **shall examine** the delivery documentation to determine that it describes all  
9115 procedures that are necessary to maintain security when distributing versions of the TOE or parts  
9116 of it to the consumer.9117 The delivery documentation describes proper procedures to maintain security of the TOE during  
9118 transfer of the TOE or its component parts and to determine the identification of the TOE.9119 The delivery documentation should cover the entire TOE, but may contain different procedures for  
9120 different parts of the TOE. The evaluation should consider the totality of procedures.9121 The delivery procedures should be applicable across all phases of delivery from the production  
9122 environment to the installation environment (e.g. packaging, storage and distribution). Standard  
9123 commercial practise for packaging and delivery may be acceptable. This includes shrink wrapped  
9124 packaging, a security tape or a sealed envelope. For the distribution, physical (e.g. public mail or a  
9125 private distribution service) or electronic (e.g. electronic mail or downloading off the Internet)  
9126 procedures may be used.9127 Cryptographic checksums or a software signature may be used by the developer to ensure that  
9128 tampering or masquerading can be detected. Tamper proof seals additionally indicate if the  
9129 confidentiality has been broken. For software TOEs, confidentiality might be assured by using  
9130 encryption. If availability is of concern, a secure transportation might be required.

9131 Interpretation of the term "necessary to maintain security" will need to consider:

- 9132 • The nature of the TOE (e.g. whether it is software or hardware).
- 9133 • The overall security level stated for the TOE by the chosen level of the Vulnerability  
9134 Assessment. If the TOE is required to be resistant against attackers of a certain potential  
9135 in its intended environment, this should also apply to the delivery of the TOE. The  
9136 evaluator should determine that a balanced approach has been taken, such that delivery  
9137 does not present a weak point in an otherwise secure development process.
- 9138 • The security objectives provided by the ST. The emphasis in the delivery documentation  
9139 is likely to be on measures related to integrity, as integrity of the TOE is always  
9140 important. However, confidentiality and availability of the delivery will be of concern in  
9141 the delivery of some TOEs; procedures relating to these aspects of the secure delivery  
9142 should also be discussed in the procedures.

9143 **13.4.1.4 Implied evaluator action**9144 ISO/IEC 15408-3 ALC\_DEL.1.2D: *The developer shall use the delivery procedures.*

9145 **13.4.1.4.1 Work unit ALC\_DEL.1-2**

9146 The evaluator *shall examine* aspects of the delivery process to determine that the delivery  
9147 procedures are used.

9148 The approach taken by the evaluator to check the application of delivery procedures will depend  
9149 on the nature of the TOE, and the delivery process itself. In addition to examination of the  
9150 procedures themselves, the evaluator seeks some assurance that they are applied in practise. Some  
9151 possible approaches are:

9152 a) a visit to the distribution site(s) where practical application of the procedures may be  
9153 observed;

9154 b) examination of the TOE at some stage during delivery, or after the user has received it  
9155 (e.g. checking for tamper proof seals);

9156 c) observing that the process is applied in practise when the evaluator obtains the TOE  
9157 through regular channels;

9158 d) questioning end users as to how the TOE was delivered.

9159 For guidance on site visits see A.4, Site Visits.

9160 It may be the case of a newly developed TOE that the delivery procedures have yet to be exercised.  
9161 In these cases, the evaluator has to be satisfied that appropriate procedures and facilities are in  
9162 place for future deliveries and that all personnel involved are aware of their responsibilities. The  
9163 evaluator may request a “dry run” of a delivery if this is practical. If the developer has produced  
9164 other similar products, then an examination of procedures in their use may be useful in providing  
9165 assurance.

9166 **13.5 Development security (ALC\_DVS)**

9167 **13.5.1 Evaluation of sub-activity (ALC\_DVS.1)**

9168 **13.5.1.1 Objectives**

9169 The objective of this sub-activity is to determine whether the developer's security controls on the  
9170 development environment are adequate to provide the confidentiality and integrity of the TOE  
9171 design and implementation that is necessary to ensure that secure operation of the TOE is not  
9172 compromised.

9173 **13.5.1.2 Input**

9174 The evaluation evidence for this sub-activity is:

9175 a) the ST;

9176 b) the development security documentation.

9177 In addition, the evaluator may need to examine other deliverables to determine that the security  
9178 controls are well-defined and followed. Specifically, the evaluator may need to examine the  
9179 developer's configuration management documentation (the input for the Evaluation of sub-activity  
9180 (ALC\_CMC.4) “Production support and acceptance procedures” and the Evaluation of sub-activity  
9181 (ALC\_CMS.4) “Problem tracking CM coverage”). Evidence that the procedures are being applied is  
9182 also required.

9183 **13.5.1.3 Action ALC\_DVS.1.1E**

9184 ISO/IEC 15408-3 ALC\_DVS.1.1C: *The development security documentation shall describe all the*  
 9185 *physical, procedural, personnel, and other security measures that are necessary to protect the*  
 9186 *confidentiality and integrity of the TOE design and implementation in its development environment.*

9187 **13.5.1.3.1 Work unit ALC\_DVS.1-1**

9188 The evaluator ***shall examine*** the development security documentation to determine that it details  
 9189 all security measures used in the development environment that are necessary to protect the  
 9190 confidentiality and integrity of the TOE design and implementation.

9191 The evaluator determines what is necessary by first referring to the ST for any information that  
 9192 may assist in the determination of necessary protection.

9193 If no explicit information is available from the ST the evaluator will need to make a determination  
 9194 of the necessary measures. In cases where the developer's measures are considered less than what  
 9195 is necessary, a clear justification should be provided for the assessment, based on a potential  
 9196 exploitable vulnerability.

9197 The following types of security measures are considered by the evaluator when examining the  
 9198 documentation:

9199 a) physical, for example physical access controls used to prevent unauthorised access to  
 9200 the TOE development environment (during normal working hours and at other  
 9201 times);

9202 b) procedural, for example covering:

- 9203 • granting of access to the development environment or to specific parts of the  
 9204 environment such as development machines
- 9205 • revocation of access rights when a person leaves the development team
- 9206 • transfer of protected material within and out of the development environment and  
 9207 between different development sites in accordance with defined acceptance procedures
- 9208 • admitting and escorting visitors to the development environment
- 9209 • roles and responsibilities in ensuring the continued application of security measures, and  
 9210 the detection of security breaches.

9211 c) personnel, for example any controls or checks made to establish the trustworthiness  
 9212 of new development staff;

9213 d) other security measures, for example the logical protections on any development  
 9214 machines.

9215 The development security documentation should identify the locations at which development  
 9216 occurs, and describe the aspects of development performed, along with the security measures  
 9217 applied at each location and for transports between different locations. For example, development  
 9218 could occur at multiple facilities within a single building, multiple buildings at the same site, or at  
 9219 multiple sites. Transports of parts of the TOE or the unfinished TOE between different  
 9220 development sites are to be covered by Development security (ALC\_DVS), whereas the transport of  
 9221 the finished TOE to the consumer is dealt with in Delivery (ALC\_DEL).

## ISO/IEC 18045:2008(E)

9222 Development includes the production of the TOE.

### 9223 13.5.1.3.2 Work unit ALC\_DVS.1-2

9224 The evaluator *shall examine* the development confidentiality and integrity policies in order to  
9225 determine the sufficiency of the security measures employed.

9226 The evaluator should examine whether the following is included in the policies:

9227 a) what information relating to the TOE development needs to be kept confidential, and  
9228 which members of the development staff are allowed to access such material;

9229 b) what material must be protected from unauthorised modification in order to preserve  
9230 the integrity of the TOE, and which members of the development staff are allowed to  
9231 modify such material.

9232 The evaluator should determine that these policies are described in the development security  
9233 documentation, that the security measures employed are consistent with the policies, and that they  
9234 are complete.

9235 It should be noted that configuration management procedures will help protect the integrity of the  
9236 TOE and the evaluator should avoid overlap with the work-units conducted for the CM capabilities  
9237 (ALC\_CMC). For example, the CM documentation may describe the security procedures necessary  
9238 for controlling the roles or individuals who should have access to the development environment  
9239 and who may modify the TOE.

9240 Whereas the CM capabilities (ALC\_CMC) requirements are fixed, those for the Development  
9241 security (ALC\_DVS), mandating only necessary measures, are dependent on the nature of the TOE,  
9242 and on information that may be provided in the ST. The evaluators would then determine that such  
9243 a policy had been applied under this sub-activity.

### 9244 13.5.1.4 Action ALC\_DVS.1.2E

#### 9245 13.5.1.4.1 Work unit ALC\_DVS.1-3

9246 The evaluator *shall examine* the development security documentation and associated evidence to  
9247 determine that the security measures are being applied.

9248 This work unit requires the evaluator to determine that the security measures described in the  
9249 development security documentation are being followed, such that the integrity of the TOE and the  
9250 confidentiality of associated documentation is being adequately protected. For example, this could  
9251 be determined by examination of the documentary evidence provided. Documentary evidence  
9252 should be supplemented by visiting the development environment. A visit to the development  
9253 environment will allow the evaluator to:

9254 a) observe the application of security measures (e.g. physical measures);

9255 b) examine documentary evidence of application of procedures;

9256 c) interview development staff to check awareness of the development security policies  
9257 and procedures, and their responsibilities.

9258 A development site visit is a useful means of gaining confidence in the measures being used. Any  
9259 decision not to make such a visit should be determined in consultation with the evaluation  
9260 authority.



9261 For guidance on site visits see A.4, Site Visits.

## 9262 13.5.2 Evaluation of sub-activity (ALC\_DVS.2)

### 9263 13.5.2.1 Objectives

9264 The objective of this sub-activity is to determine whether the developer's security controls on the  
9265 development environment are adequate to provide the confidentiality and integrity of the TOE  
9266 design and implementation that is necessary to ensure that secure operation of the TOE is not  
9267 compromised. Additionally, sufficiency of the measures as applied is intended be justified.

### 9268 13.5.2.2 Input

9269 The evaluation evidence for this sub-activity is:

9270 a) the ST;

9271 b) the development security documentation.

9272 In addition, the evaluator may need to examine other deliverables to determine that the security  
9273 controls are well-defined and followed. Specifically, the evaluator may need to examine the  
9274 developer's configuration management documentation (the input for the Evaluation of sub-activity  
9275 (ALC\_CMC.4) "Production support and acceptance procedures" and the Evaluation of sub-activity  
9276 (ALC\_CMS.4) "Problem tracking CM coverage"). Evidence that the procedures are being applied is  
9277 also required.

### 9278 13.5.2.3 Action ALC\_DVS.2.1E

9279 ISO/IEC 15408-3 ALC\_DVS.2.1C: *The development security documentation shall describe all the*  
9280 *physical, procedural, personnel, and other security measures that are necessary to protect the*  
9281 *confidentiality and integrity of the TOE design and implementation in its development environment.*

#### 9282 13.5.2.3.1 Work unit ALC\_DVS.2-1

9283 The evaluator **shall examine** the development security documentation to determine that it details  
9284 all security measures used in the development environment that are necessary to protect the  
9285 confidentiality and integrity of the TOE design and implementation.

9286 The evaluator determines what is necessary by first referring to the ST for any information that  
9287 may assist in the determination of necessary protection.

9288 If no explicit information is available from the ST the evaluator will need to make a determination  
9289 of the necessary measures. In cases where the developer's measures are considered less than what  
9290 is necessary, a clear justification should be provided for the assessment, based on a potential  
9291 exploitable vulnerability.

9292 The following types of security measures are considered by the evaluator when examining the  
9293 documentation:

9294 a) physical, for example physical access controls used to prevent unauthorised access to  
9295 the TOE development environment (during normal working hours and at other  
9296 times);

9297 b) procedural, for example covering:

## ISO/IEC 18045:2008(E)

- 9298 • granting of access to the development environment or to specific parts of the  
9299 environment such as development machines
- 9300 • revocation of access rights when a person leaves the development team
- 9301 • transfer of protected material out of the development environment and between different  
9302 development sites in accordance with defined acceptance procedures
- 9303 • admitting and escorting visitors to the development environment
- 9304 • roles and responsibilities in ensuring the continued application of security measures, and  
9305 the detection of security breaches.
- 9306 c) personnel, for example any controls or checks made to establish the trustworthiness  
9307 of new development staff;
- 9308 d) other security measures, for example the logical protections on any development  
9309 machines.
- 9310 The development security documentation should identify the locations at which development  
9311 occurs, and describe the aspects of development performed, along with the security measures  
9312 applied at each location and for transports between different locations. For example, development  
9313 could occur at multiple facilities within a single building, multiple buildings at the same site, or at  
9314 multiple sites. Transports of parts of the TOE or the unfinished TOE between different  
9315 development sites are to be covered by the Development security (ALC\_DVS), whereas the  
9316 transport of the finished TOE to the consumer is dealt with in the Delivery (ALC\_DEL).
- 9317 Development includes the production of the TOE.
- 9318 ISO/IEC 15408-3 ALC\_DVS.2.2C: *The development security documentation shall justify that the*  
9319 *security measures provide the necessary level of protection to maintain the confidentiality and*  
9320 *integrity of the TOE.*
- 9321 **13.5.2.3.2 Work unit ALC\_DVS.2-2**
- 9322 The evaluator ***shall examine*** the development security documentation to determine that an  
9323 appropriate justification is given why the security measures provide the necessary level of  
9324 protection to maintain the confidentiality and integrity of the TOE.
- 9325 Since attacks on the TOE or its related information are assumed in different design and production  
9326 stages, measures and procedures need to have an appropriate level necessary to prevent those  
9327 attacks or to make them more difficult.
- 9328 Since this level depends on the overall attack potential claimed for the TOE (cf. the Vulnerability  
9329 analysis (AVA\_VAN) component chosen), the development security documentation should justify  
9330 the necessary level of protection to maintain the confidentiality and integrity of the TOE. This level  
9331 has to be achieved by the security measures applied.
- 9332 The concept of protection measures should be consistent, and the justification should include an  
9333 analysis of how the measures are mutually supportive. All aspects of development and production  
9334 on all the different sites with all roles involved up to delivery of the TOE should be analysed.
- 9335 Justification may include an analysis of potential vulnerabilities taking the applied security  
9336 measures into account.
- 9337 There may be a convincing argument showing that e.g.

- 9338 • The technical measures and mechanisms of the developer's infrastructure are sufficient  
9339 for keeping the appropriate security level (e.g. cryptographic mechanisms as well as  
9340 physical protection mechanisms, properties of the CM system (cf. ALC\_CMC.4-5));
  
- 9341 • The system containing the implementation representation of the TOE (including  
9342 concerning guidance documents) provides effective protection against logical attacks e.g.  
9343 by "Trojan" code or viruses. It might be adequate, if the implementation representation is  
9344 kept on an isolated system where only the software necessary to maintain it is installed  
9345 and where no additional software is installed afterwards.
  
- 9346 • Data brought into this system need to be carefully considered to prevent the installation  
9347 of hidden functionality onto the system. The effectiveness of these measures need to be  
9348 tested, e.g. by independently trying to get access to the machine, install some additional  
9349 executable (program, macro etc.) or get some information out of the machine using  
9350 logical attacks.
  
- 9351 • The appropriate organisational (procedural and personal) measures are unconditionally  
9352 enforced.
  
- 9353 **13.5.2.3.3 Work unit ALC\_DVS.2-3**
  
- 9354 The evaluator ***shall examine*** the development confidentiality and integrity policies in order to  
9355 determine the sufficiency of the security measures employed.
  
- 9356 The evaluator should examine whether the following is included in the policies:
  
- 9357     a) what information relating to the TOE development needs to be kept confidential, and  
9358         which members of the development staff are allowed to access such material;
  
- 9359     b) what material must be protected from unauthorised modification in order to preserve  
9360         the integrity of the TOE, and which members of the development staff are allowed to  
9361         modify such material.
  
- 9362 The evaluator should determine that these policies are described in the development security  
9363 documentation, that the security measures employed are consistent with the policies, and that they  
9364 are complete.
  
- 9365 It should be noted that configuration management procedures will help protect the integrity of the  
9366 TOE and the evaluator should avoid overlap with the work-units conducted for the CM capabilities  
9367 (ALC\_CMC). For example, the CM documentation may describe the security procedures necessary  
9368 for controlling the roles or individuals who should have access to the development environment  
9369 and who may modify the TOE.
  
- 9370 Whereas the CM capabilities (ALC\_CMC) requirements are fixed, those for the Development  
9371 security (ALC\_DVS), mandating only necessary measures, are dependent on the nature of the TOE,  
9372 and on information that may be provided in the ST. For example, the ST may identify a security  
9373 objective for the development environment that requires the TOE to be developed by staff that has  
9374 security clearance. The evaluators would then determine that such a policy had been applied under  
9375 this sub-activity.

## ISO/IEC 18045:2008(E)

### 9376 13.5.2.4 Action ALC\_DVS.2.2E

#### 9377 13.5.2.4.1 Work unit ALC\_DVS.2-4

9378 The evaluator **shall examine** the development security documentation and associated evidence to  
9379 determine that the security measures are being applied.

9380 This work unit requires the evaluator to determine that the security measures described in the  
9381 development security documentation are being followed, such that the integrity of the TOE and the  
9382 confidentiality of associated documentation is being adequately protected. For example, this could  
9383 be determined by examination of the documentary evidence provided. Documentary evidence  
9384 should be supplemented by visiting the development environment. A visit to the development  
9385 environment will allow the evaluator to:

9386 a) observe the application of security measures (e.g. physical measures);

9387 b) examine documentary evidence of application of procedures;

9388 c) interview development staff to check awareness of the development security policies  
9389 and procedures, and their responsibilities.

9390 A development site visit is a useful means of gaining confidence in the measures being used. Any  
9391 decision not to make such a visit should be determined in consultation with the evaluation  
9392 authority.

9393 For guidance on site visits see A.4, Site Visits.

### 9394 13.6 Flaw remediation (ALC\_FLR)

#### 9395 13.6.1 Evaluation of sub-activity (ALC\_FLR.1)

##### 9396 13.6.1.1 Objectives

9397 The objective of this sub-activity is to determine whether the developer has established flaw  
9398 remediation procedures that describe the tracking of security flaws, the identification of corrective  
9399 actions, and the distribution of corrective action information to TOE users.

##### 9400 13.6.1.2 Input

9401 The evaluation evidence for this sub-activity is:

9402 a) the flaw remediation procedures documentation.

##### 9403 13.6.1.3 Action ALC\_FLR.1.1E

9404 ISO/IEC 15408-3 ALC\_FLR.1.1C: *The flaw remediation procedures documentation shall describe the*  
9405 *procedures used to track all reported security flaws in each release of the TOE.*

##### 9406 13.6.1.3.1 Work unit ALC\_FLR.1-1

9407 The evaluator **shall examine** the flaw remediation procedures documentation to determine that it  
9408 describes the procedures used to track all reported security flaws in each release of the TOE.

9409 The procedures describe the actions that are taken by the developer from the time each suspected  
9410 security flaw is reported to the time that it is resolved. This includes the flaw's entire time frame,

9411 from initial detection through ascertaining that the flaw is a security flaw, to resolution of the  
9412 security flaw.

9413 If a flaw is discovered not to be security-relevant, there is no need (for the purposes of the Flaw  
9414 remediation (ALC\_FLR) requirements) for the flaw remediation procedures to track it further; only  
9415 that there be an explanation of why the flaw is not security-relevant.

9416 While these requirements do not mandate that there be a publicised means for TOE users to report  
9417 security flaws, they do mandate that all security flaws that are reported be tracked. That is, a  
9418 reported security flaw cannot be ignored simply because it comes from outside the developer's  
9419 organisation.

9420 ISO/IEC 15408-3 ALC\_FLR.1.2C: *The flaw remediation procedures shall require that a description of*  
9421 *the nature and effect of each security flaw be provided, as well as the status of finding a correction to*  
9422 *that flaw.*

#### 9423 **13.6.1.3.2 Work unit ALC\_FLR.1-2**

9424 The evaluator ***shall examine*** the flaw remediation procedures to determine that the application of  
9425 these procedures would produce a description of each security flaw in terms of its nature and  
9426 effects.

9427 The procedures identify the actions that are taken by the developer to describe the nature and  
9428 effects of each security flaw in sufficient detail to be able to reproduce it. The description of the  
9429 nature of a security flaw addresses whether it is an error in the documentation, a flaw in the design  
9430 of the TSF, a flaw in the implementation of the TSF, etc. The description of the security flaw's  
9431 effects identifies the portions of the TSF that are affected and how those portions are affected. For  
9432 example, a security flaw in the implementation might be found that affects the identification and  
9433 authentication enforced by the TSF by permitting authentication with the password "BACK DOOR".

#### 9434 **13.6.1.3.3 Work unit ALC\_FLR.1-3**

9435 The evaluator ***shall examine*** the flaw remediation procedures to determine that the application of  
9436 these procedures would identify the status of finding a correction to each security flaw.

9437 The flaw remediation procedures identify the different stages of security flaws. This differentiation  
9438 includes at least: suspected security flaws that have been reported, suspected security flaws that  
9439 have been confirmed to be security flaws, and security flaws whose solutions have been  
9440 implemented. It is permissible that additional stages (e.g. flaws that have been reported but not yet  
9441 investigated, flaws that are under investigation, security flaws for which a solution has been found  
9442 but not yet implemented) be included.

9443 ISO/IEC 15408-3 ALC\_FLR.1.3C: *The flaw remediation procedures shall require that corrective*  
9444 *actions be identified for each of the security flaws.*

#### 9445 **13.6.1.3.4 Work unit ALC\_FLR.1-4**

9446 The evaluator ***shall check*** the flaw remediation procedures to determine that the application of  
9447 these procedures would identify the corrective action for each security flaw.

9448 *Corrective action* may consist of a repair to the hardware, firmware, or software portions of the  
9449 TOE, a modification of TOE guidance, or both. Corrective action that constitutes modifications to  
9450 TOE guidance (e.g. details of procedural measures to be taken to obviate the security flaw) includes  
9451 both those measures serving as only an interim solution (until the repair is issued) as well as those  
9452 serving as a permanent solution (where it is determined that the procedural measure is the best  
9453 solution).

## ISO/IEC 18045:2008(E)

9454 If the source of the security flaw is a documentation error, the corrective action consists of an  
9455 update of the affected TOE guidance. If the corrective action is a procedural measure, this measure  
9456 will include an update made to the affected TOE guidance to reflect these corrective procedures.

9457 ISO/IEC 15408-3 ALC\_FLR.1.4C: *The flaw remediation procedures documentation shall describe the*  
9458 *methods used to provide flaw information, corrections and guidance on corrective actions to TOE*  
9459 *users.*

### 9460 13.6.1.3.5 Work unit ALC\_FLR.1-5

9461 The evaluator **shall examine** the flaw remediation procedures documentation to determine that it  
9462 describes a means of providing the TOE users with the necessary information on each security flaw.

9463 The *necessary information* about each security flaw consists of its description (not necessarily at  
9464 the same level of detail as that provided as part of work unit ALC\_FLR.1-2), the prescribed  
9465 corrective action, and any associated guidance on implementing the correction.

9466 TOE users may be provided with such information, correction, and documentation updates in any  
9467 of several ways, such as their posting to a website, their being sent to TOE users, or arrangements  
9468 made for the developer to install the correction. In cases where the means of providing this  
9469 information requires action to be initiated by the TOE user, the evaluator examines any TOE  
9470 guidance to ensure that it contains instructions for retrieving the information.

9471 The only metric for assessing the adequacy of the method used for providing the information,  
9472 corrections and guidance is that there be a reasonable expectation that TOE users can obtain or  
9473 receive it. For example, consider the method of dissemination where the requisite data is posted to  
9474 a website for one month, and the TOE users know that this will happen and when this will happen.  
9475 This may not be especially reasonable or effective (as, say, a permanent posting to the website), yet  
9476 it is feasible that the TOE user could obtain the necessary information. On the other hand, if the  
9477 information were posted to the website for only one hour, yet TOE users had no way of knowing  
9478 this or when it would be posted, it is infeasible that they would ever get the necessary information.

### 9479 13.6.2 Evaluation of sub-activity (ALC\_FLR.2)

#### 9480 13.6.2.1 Objectives

9481 The objective of this sub-activity is to determine whether the developer has established flaw  
9482 remediation procedures that describe the tracking of security flaws, the identification of corrective  
9483 actions, and the distribution of corrective action information to TOE users. Additionally, this sub-  
9484 activity determines whether the developer's procedures provide for the corrections of security  
9485 flaws, for the receipt of flaw reports from TOE users, and for assurance that the corrections  
9486 introduce no new security flaws.

9487 In order for the developer to be able to act appropriately upon security flaw reports from TOE  
9488 users, TOE users need to understand how to submit security flaw reports to the developer, and  
9489 developers need to know how to receive these reports. Flaw remediation guidance addressed to  
9490 the TOE user ensures that TOE users are aware of how to communicate with the developer; flaw  
9491 remediation procedures describe the developer's role in such communication

#### 9492 13.6.2.2 Input

9493 The evaluation evidence for this sub-activity is:

9494 a) the flaw remediation procedures documentation;

9495 b) flaw remediation guidance documentation.

9496 **13.6.2.3 Action ALC\_FLR.2.1E**

9497 ISO/IEC 15408-3 ALC\_FLR.2.1C: *The flaw remediation procedures documentation shall describe the*  
 9498 *procedures used to track all reported security flaws in each release of the TOE.*

9499 **13.6.2.3.1 Work unit ALC\_FLR.2-1**

9500 The evaluator **shall examine** the flaw remediation procedures documentation to determine that it  
 9501 describes the procedures used to track all reported security flaws in each release of the TOE.

9502 The procedures describe the actions that are taken by the developer from the time each suspected  
 9503 security flaw is reported to the time that it is resolved. This includes the flaw's entire time frame,  
 9504 from initial detection through ascertaining that the flaw is a security flaw, to resolution of the  
 9505 security flaw.

9506 If a flaw is discovered not to be security-relevant, there is no need (for the purposes of the Flaw  
 9507 remediation (ALC\_FLR) requirements) for the flaw remediation procedures to track it further; only  
 9508 that there be an explanation of why the flaw is not security-relevant.

9509 ISO/IEC 15408-3 ALC\_FLR.2.2C: *The flaw remediation procedures shall require that a description of*  
 9510 *the nature and effect of each security flaw be provided, as well as the status of finding a correction to*  
 9511 *that flaw.*

9512 **13.6.2.3.2 Work unit ALC\_FLR.2-2**

9513 The evaluator **shall examine** the flaw remediation procedures to determine that the application of  
 9514 these procedures would produce a description of each security flaw in terms of its nature and  
 9515 effects.

9516 The procedures identify the actions that are taken by the developer to describe the nature and  
 9517 effects of each security flaw in sufficient detail to be able to reproduce it. The description of the  
 9518 nature of a security flaw addresses whether it is an error in the documentation, a flaw in the design  
 9519 of the TSF, a flaw in the implementation of the TSF, etc. The description of the security flaw's  
 9520 effects identifies the portions of the TSF that are affected and how those portions are affected. For  
 9521 example, a security flaw in the implementation might be found that affects the identification and  
 9522 authentication enforced by the TSF by permitting authentication with the password "BACKDOOR".

9523 **13.6.2.3.3 Work unit ALC\_FLR.2-3**

9524 The evaluator **shall examine** the flaw remediation procedures to determine that the application of  
 9525 these procedures would identify the status of finding a correction to each security flaw.

9526 The flaw remediation procedures identify the different stages of security flaws. This differentiation  
 9527 includes at least: suspected security flaws that have been reported, suspected security flaws that  
 9528 have been confirmed to be security flaws, and security flaws whose solutions have been  
 9529 implemented. It is permissible that additional stages (e.g. flaws that have been reported but not yet  
 9530 investigated, flaws that are under investigation, security flaws for which a solution has been found  
 9531 but not yet implemented) be included.

9532 ISO/IEC 15408-3 ALC\_FLR.2.3C: *The flaw remediation procedures shall require that corrective*  
 9533 *actions be identified for each of the security flaws.*

9534 **13.6.2.3.4 Work unit ALC\_FLR.2-4**

9535 The evaluator **shall check** the flaw remediation procedures to determine that the application of  
 9536 these procedures would identify the corrective action for each security flaw.

## ISO/IEC 18045:2008(E)

9537 *Corrective action* may consist of a repair to the hardware, firmware, or software portions of the  
9538 TOE, a modification of TOE guidance, or both. Corrective action that constitutes modifications to  
9539 TOE guidance (e.g. details of procedural measures to be taken to obviate the security flaw) includes  
9540 both those measures serving as only an interim solution (until the repair is issued) as well as those  
9541 serving as a permanent solution (where it is determined that the procedural measure is the best  
9542 solution).

9543 If the source of the security flaw is a documentation error, the corrective action consists of an  
9544 update of the affected TOE guidance. If the corrective action is a procedural measure, this measure  
9545 will include an update made to the affected TOE guidance to reflect these corrective procedures.

9546 ISO/IEC 15408-3 ALC\_FLR.2.4C: *The flaw remediation procedures documentation shall describe the*  
9547 *methods used to provide flaw information, corrections and guidance on corrective actions to TOE*  
9548 *users.*

### 9549 13.6.2.3.5 Work unit ALC\_FLR.2-5

9550 The evaluator **shall examine** the flaw remediation procedures documentation to determine that it  
9551 describes a means of providing the TOE users with the necessary information on each security flaw.

9552 *The necessary information* about each security flaw consists of its description (not necessarily at  
9553 the same level of detail as that provided as part of work unit ALC\_FLR.2-2), the prescribed  
9554 corrective action, and any associated guidance on implementing the correction.

9555 TOE users may be provided with such information, correction, and documentation updates in any  
9556 of several ways, such as their posting to a website, their being sent to TOE users, or arrangements  
9557 made for the developer to install the correction. In cases where the means of providing this  
9558 information requires action to be initiated by the TOE user, the evaluator examines any TOE  
9559 guidance to ensure that it contains instructions for retrieving the information.

9560 The only metric for assessing the adequacy of the method used for providing the information,  
9561 corrections and guidance is that there be a reasonable expectation that TOE users can obtain or  
9562 receive it. For example, consider the method of dissemination where the requisite data is posted to  
9563 a website for one month, and the TOE users know that this will happen and when this will happen.  
9564 This may not be especially reasonable or effective (as, say, a permanent posting to the website), yet  
9565 it is feasible that the TOE user could obtain the necessary information. On the other hand, if the  
9566 information were posted to the website for only one hour, yet TOE users had no way of knowing  
9567 this or when it would be posted, it is infeasible that they would ever get the necessary information.

9568 ISO/IEC 15408-3 ALC\_FLR.2.5C: *The flaw remediation procedures shall describe a means by which*  
9569 *the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.*

### 9570 13.6.2.3.6 Work unit ALC\_FLR.2-6

9571 The evaluator **shall examine** the flaw remediation procedures to determine that they describe  
9572 procedures for the developer to accept reports of security flaws or requests for corrections to such  
9573 flaws.

9574 The procedures ensure that TOE users have a means by which they can communicate with the TOE  
9575 developer. By having a means of contact with the developer, the user can report security flaws,  
9576 enquire about the status of security flaws, or request corrections to flaws. This means of contact  
9577 may be part of a more general contact facility for reporting non-security related problems.

9578 The use of these procedures is not restricted to TOE users; however, only the TOE users are  
9579 actively supplied with the details of these procedures. Others who might have access to or  
9580 familiarity with the TOE can use the same procedures to submit reports to the developer, who is  
9581 then expected to process them. Any means of submitting reports to the developer, other than those



9582 identified by the developer, are beyond the scope of this work unit; reports generated by other  
9583 means need not be addressed.

9584 ISO/IEC 15408-3 ALC\_FLR.2.6C: *The procedures for processing reported security flaws shall ensure*  
9585 *that any reported flaws are remediated and the remediation procedures issued to TOE users.*

9586 **13.6.2.3.7 Work unit ALC\_FLR.2-7**

9587 The evaluator ***shall examine*** the flaw remediation procedures to determine that the application of  
9588 these procedures would help to ensure every reported flaw is corrected.

9589 The flaw remediation procedures cover not only those security flaws discovered and reported by  
9590 developer personnel, but also those reported by TOE users. The procedures are sufficiently  
9591 detailed so that they describe how it is ensured that each reported security flaw is corrected. The  
9592 procedures contain reasonable steps that show progress leading to the eventual, inevitable  
9593 resolution.

9594 The procedures describe the process that is taken from the point at which the suspected security  
9595 flaw is determined to be a security flaw to the point at which it is resolved.

9596 **13.6.2.3.8 Work unit ALC\_FLR.2-8**

9597 The evaluator ***shall examine*** the flaw remediation procedures to determine that the application of  
9598 these procedures would help to ensure that the TOE users are issued remediation procedures for  
9599 each security flaw.

9600 The procedures describe the process that is taken from the point at which a security flaw is  
9601 resolved to the point at which the remediation procedures are provided. The procedures for  
9602 delivering corrective actions should be consistent with the security objectives; they need not  
9603 necessarily be identical to the procedures used for delivering the TOE, as documented to meet  
9604 ALC\_DEL, if included in the assurance requirements. For example, if the hardware portion of a TOE  
9605 were originally delivered by bonded courier, updates to hardware resulting from flaw remediation  
9606 would likewise be expected to be distributed by bonded courier. Updates unrelated to flaw  
9607 remediation would follow the procedures set forth in the documentation meeting the Delivery  
9608 (ALC\_DEL) requirements.

9609 ISO/IEC 15408-3 ALC\_FLR.2.7C: *The procedures for processing reported security flaws shall provide*  
9610 *safeguards that any corrections to these security flaws do not introduce any new flaws.*

9611 **13.6.2.3.9 Work unit ALC\_FLR.2-9**

9612 The evaluator ***shall examine*** the flaw remediation procedures to determine that the application of  
9613 these procedures would result in safeguards that the potential correction contains no adverse  
9614 effects.

9615 Through analysis, testing, or a combination of the two, the developer may reduce the likelihood  
9616 that adverse effects will be introduced when a security flaw is corrected. The evaluator assesses  
9617 whether the procedures provide detail in how the necessary mix of analysis and testing actions is  
9618 to be determined for a given correction.

9619 The evaluator also determines that, for instances where the source of the security flaw is a  
9620 documentation problem, the procedures include the means of safeguarding against the  
9621 introduction of contradictions with other documentation.

9622 ISO/IEC 15408-3 ALC\_FLR.2.8C: *The flaw remediation guidance shall describe a means by which TOE*  
9623 *users report to the developer any suspected security flaws in the TOE.*

9624 **13.6.2.3.10 Work unit ALC\_FLR.2-10**

9625 The evaluator **shall examine** the flaw remediation guidance to determine that the application of  
9626 these procedures would result in a means for the TOE user to provide reports of suspected security  
9627 flaws or requests for corrections to such flaws.

9628 The guidance ensures that TOE users have a means by which they can communicate with the TOE  
9629 developer. By having a means of contact with the developer, the user can report security flaws,  
9630 enquire about the status of security flaws, or request corrections to flaws.

9631 **13.6.3 Evaluation of sub-activity (ALC\_FLR.3)**

9632 **13.6.3.1 Objectives**

9633 The objective of this sub-activity is to determine whether the developer has established flaw  
9634 remediation procedures that describe the tracking of security flaws, the identification of corrective  
9635 actions, and the distribution of corrective action information to TOE users. Additionally, this sub-  
9636 activity determines whether the developer's procedures provide for the corrections of security  
9637 flaws, for the receipt of flaw reports from TOE users, for assurance that the corrections introduce  
9638 no new security flaws, for the establishment of a point of contact for each TOE user, and for the  
9639 timely issue of corrective actions to TOE users.

9640 In order for the developer to be able to act appropriately upon security flaw reports from TOE  
9641 users, TOE users need to understand how to submit security flaw reports to the developer, and  
9642 developers need to know how to receive these reports. Flaw remediation guidance addressed to  
9643 the TOE user ensures that TOE users are aware of how to communicate with the developer; flaw  
9644 remediation procedures describe the developer's role in such communication.

9645 **13.6.3.2 Input**

9646 The evaluation evidence for this sub-activity is:

- 9647 a) the flaw remediation procedures documentation;
- 9648 b) flaw remediation guidance documentation.

9649 **13.6.3.3 Action ALC\_FLR.3.1E**

9650 ISO/IEC 15408-3 ALC\_FLR.3.1C: *The flaw remediation procedures documentation shall describe the*  
9651 *procedures used to track all reported security flaws in each release of the TOE.*

9652 **13.6.3.3.1 Work unit ALC\_FLR.3-1**

9653 The evaluator **shall examine** the flaw remediation procedures documentation to determine that it  
9654 describes the procedures used to track all reported security flaws in each release of the TOE.

9655 The procedures describe the actions that are taken by the developer from the time each suspected  
9656 security flaw is reported to the time that it is resolved. This includes the flaw's entire time frame,  
9657 from initial detection through ascertaining that the flaw is a security flaw, to resolution of the  
9658 security flaw.

9659 If a flaw is discovered not to be security-relevant, there is no need (for the purposes of the Flaw  
9660 remediation (ALC\_FLR) requirements) for the flaw remediation procedures to track it further; only  
9661 that there be an explanation of why the flaw is not security-relevant.

9662 ISO/IEC 15408-3 ALC\_FLR.3.2C: *The flaw remediation procedures shall require that a description of*  
 9663 *the nature and effect of each security flaw be provided, as well as the status of finding a correction to*  
 9664 *that flaw.*

9665 **13.6.3.3.2 Work unit ALC\_FLR.3-2**

9666 The evaluator ***shall examine*** the flaw remediation procedures to determine that the application of  
 9667 these procedures would produce a description of each security flaw in terms of its nature and  
 9668 effects.

9669 The procedures identify the actions that are taken by the developer to describe the nature and  
 9670 effects of each security flaw in sufficient detail to be able to reproduce it. The description of the  
 9671 nature of a security flaw addresses whether it is an error in the documentation, a flaw in the design  
 9672 of the TSF, a flaw in the implementation of the TSF, etc. The description of the security flaw's  
 9673 effects identifies the portions of the TSF that are affected and how those portions are affected. For  
 9674 example, a security flaw in the implementation might be found that affects the identification and  
 9675 authentication enforced by the TSF by permitting authentication with the password "BACKDOOR".

9676 **13.6.3.3.3 Work unit ALC\_FLR.3-3**

9677 The evaluator ***shall examine*** the flaw remediation procedures to determine that the application of  
 9678 these procedures would identify the status of finding a correction to each security flaw.

9679 The flaw remediation procedures identify the different stages of security flaws. This differentiation  
 9680 includes at least: suspected security flaws that have been reported, suspected security flaws that  
 9681 have been confirmed to be security flaws, and security flaws whose solutions have been  
 9682 implemented. It is permissible that additional stages (e.g. flaws that have been reported but not yet  
 9683 investigated, flaws that are under investigation, security flaws for which a solution has been found  
 9684 but not yet implemented) be included.

9685 ISO/IEC 15408-3 ALC\_FLR.3.3C: *The flaw remediation procedures shall require that corrective*  
 9686 *actions be identified for each of the security flaws.*

9687 **13.6.3.3.4 Work unit ALC\_FLR.3-4**

9688 The evaluator ***shall check*** the flaw remediation procedures to determine that the application of  
 9689 these procedures would identify the corrective action for each security flaw.

9690 *Corrective action* may consist of a repair to the hardware, firmware, or software portions of the  
 9691 TOE, a modification of TOE guidance, or both. Corrective action that constitutes modifications to  
 9692 TOE guidance (e.g. details of procedural measures to be taken to obviate the security flaw) includes  
 9693 both those measures serving as only an interim solution (until the repair is issued) as well as those  
 9694 serving as a permanent solution (where it is determined that the procedural measure is the best  
 9695 solution).

9696 If the source of the security flaw is a documentation error, the corrective action consists of an  
 9697 update of the affected TOE guidance. If the corrective action is a procedural measure, this measure  
 9698 will include an update made to the affected TOE guidance to reflect these corrective procedures.

9699 ISO/IEC 15408-3 ALC\_FLR.3.4C: *The flaw remediation procedures documentation shall describe the*  
 9700 *methods used to provide flaw information, corrections and guidance on corrective actions to TOE*  
 9701 *users.*

9702 **13.6.3.3.5 Work unit ALC\_FLR.3-5**

9703 The evaluator ***shall examine*** the flaw remediation procedures documentation to determine that it  
 9704 describes a means of providing the TOE users with the necessary information on each security flaw.

## ISO/IEC 18045:2008(E)

9705 *The necessary information* about each security flaw consists of its description (not necessarily at  
9706 the same level of detail as that provided as part of work unit ALC\_FLR.3-2), the prescribed  
9707 corrective action, and any associated guidance on implementing the correction.

9708 TOE users may be provided with such information, correction, and documentation updates in any  
9709 of several ways, such as their posting to a website, their being sent to TOE users, or arrangements  
9710 made for the developer to install the correction. In cases where the means of providing this  
9711 information requires action to be initiated by the TOE user, the evaluator examines any TOE  
9712 guidance to ensure that it contains instructions for retrieving the information.

9713 The only metric for assessing the adequacy of the method used for providing the information,  
9714 corrections and guidance is that there be a reasonable expectation that TOE users can obtain or  
9715 receive it. For example, consider the method of dissemination where the requisite data is posted to  
9716 a website for one month, and the TOE users know that this will happen and when this will happen.  
9717 This may not be especially reasonable or effective (as, say, a permanent posting to the website), yet  
9718 it is feasible that the TOE user could obtain the necessary information. On the other hand, if the  
9719 information were posted to the website for only one hour, yet TOE users had no way of knowing  
9720 this or when it would be posted, it is infeasible that they would ever get the necessary information.

9721 For TOE users who register with the developer (see work unit ALC\_FLR.3-12), the passive  
9722 availability of this information is not sufficient. Developers must actively send the information (or a  
9723 notification of its availability) to registered TOE users.

9724 ISO/IEC 15408-3 ALC\_FLR.3.5C: *The flaw remediation procedures shall describe a means by which*  
9725 *the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.*

### 9726 13.6.3.3.6 Work unit ALC\_FLR.3-6

9727 The evaluator **shall examine** the flaw remediation procedures to determine that the application of  
9728 these procedures would result in a means for the developer to receive from TOE user reports of  
9729 suspected security flaws or requests for corrections to such flaws.

9730 The procedures ensure that TOE users have a means by which they can communicate with the TOE  
9731 developer. By having a means of contact with the developer, the user can report security flaws,  
9732 enquire about the status of security flaws, or request corrections to flaws. This means of contact  
9733 may be part of a more general contact facility for reporting non-security related problems.

9734 The use of these procedures is not restricted to TOE users; however, only the TOE users are  
9735 actively supplied with the details of these procedures. Others who might have access to or  
9736 familiarity with the TOE can use the same procedures to submit reports to the developer, who is  
9737 then expected to process them. Any means of submitting reports to the developer, other than those  
9738 identified by the developer, are beyond the scope of this work unit; reports generated by other  
9739 means need not be addressed.

9740 ISO/IEC 15408-3 ALC\_FLR.3.6C: *The flaw remediation procedures shall include a procedure*  
9741 *requiring timely response and the automatic distribution of security flaw reports and the associated*  
9742 *corrections to registered users who might be affected by the security flaw.*

### 9743 13.6.3.3.7 Work unit ALC\_FLR.3-7

9744 The evaluator **shall examine** the flaw remediation procedures to determine that the application of  
9745 these procedures would result in a timely means of providing the registered TOE users who might  
9746 be affected with reports about, and associated corrections to, each security flaw.

9747 The issue of timeliness applies to the issuance of both security flaw reports and the associated  
9748 corrections. However, these need not be issued at the same time. It is recognised that flaw reports  
9749 should be generated and issued as soon as an interim solution is found, even if that solution is as

9750 drastic as turn off the TOE. Likewise, when a more permanent (and less drastic) solution is found, it  
9751 should be issued without undue delay.

9752 It is unnecessary to restrict the recipients of the reports and associated corrections to only those  
9753 TOE users who might be affected by the security flaw; it is permissible that all TOE users be given  
9754 such reports and corrections for all security flaws, provided such is done in a timely manner.

#### 9755 **13.6.3.3.8 Work unit ALC\_FLR.3-8**

9756 The evaluator *shall examine* the flaw remediation procedures to determine that the application of  
9757 these procedures would result in automatic distribution of the reports and associated corrections  
9758 to the registered TOE users who might be affected.

9759 *Automatic distribution* does not mean that human interaction with the distribution method is not  
9760 permitted. In fact, the distribution method could consist entirely of manual procedures, perhaps  
9761 through a closely monitored procedure with prescribed escalation upon the lack of issue of reports  
9762 or corrections.

9763 It is unnecessary to restrict the recipients of the reports and associated corrections to only those  
9764 TOE users who might be affected by the security flaw; it is permissible that all TOE users be given  
9765 such reports and corrections for all security flaws, provided such is done automatically.

9766 ISO/IEC 15408-3 ALC\_FLR.3.7C: *The procedures for processing reported security flaws shall ensure*  
9767 *that any reported flaws are remediated and the remediation procedures issued to TOE users.*

#### 9768 **13.6.3.3.9 Work unit ALC\_FLR.3-9**

9769 The evaluator *shall examine* the flaw remediation procedures to determine that the application of  
9770 these procedures would help to ensure that every reported flaw is corrected.

9771 The flaw remediation procedures cover not only those security flaws discovered and reported by  
9772 developer personnel, but also those reported by TOE users. The procedures are sufficiently  
9773 detailed so that they describe how it is ensured that each reported security flaw is remediated. The  
9774 procedures contain reasonable steps that show progress leading to the eventual, inevitable  
9775 resolution.

9776 The procedures describe the process that is taken from the point at which the suspected security  
9777 flaw is determined to be a security flaw to the point at which it is resolved.

#### 9778 **13.6.3.3.10 Work unit ALC\_FLR.3-10**

9779 The evaluator *shall examine* the flaw remediation procedures to determine that the application of  
9780 these procedures would help to ensure that the TOE users are issued remediation procedures for  
9781 each security flaw.

9782 The procedures describe the process that is taken from the point at which a security flaw is  
9783 resolved to the point at which the remediation procedures are provided. The procedures for  
9784 delivering remediation procedures should be consistent with the security objectives; they need not  
9785 necessarily be identical to the procedures used for delivering the TOE, as documented to meet  
9786 Delivery (ALC\_DEL), if included in the assurance requirements. For example, if the hardware  
9787 portion of a TOE were originally delivered by bonded courier, updates to hardware resulting from  
9788 flaw remediation would likewise be expected to be distributed by bonded courier. Updates  
9789 unrelated to flaw remediation would follow the procedures set forth in the documentation meeting  
9790 the Delivery (ALC\_DEL) requirements.

9791 ISO/IEC 15408-3 ALC\_FLR.3.8C: *The procedures for processing reported security flaws shall provide*  
9792 *safeguards that any corrections to these security flaws do not introduce any new flaws.*

## ISO/IEC 18045:2008(E)

### 9793 13.6.3.3.11 Work unit ALC\_FLR.3-11

9794 The evaluator **shall examine** the flaw remediation procedures to determine that the application of  
9795 these procedures would result in safeguards that the potential correction contains no adverse  
9796 effects.

9797 Through analysis, testing, or a combination of the two, the developer may reduce the likelihood  
9798 that adverse effects will be introduced when a security flaw is corrected. The evaluator assesses  
9799 whether the procedures provide detail in how the necessary mix of analysis and testing actions is  
9800 to be determined for a given correction.

9801 The evaluator also determines that, for instances where the source of the security flaw is a  
9802 documentation problem, the procedures include the means of safeguarding against the  
9803 introduction of contradictions with other documentation.

9804 ISO/IEC 15408-3 ALC\_FLR.3.9C: *The flaw remediation guidance shall describe a means by which TOE*  
9805 *users report to the developer any suspected security flaws in the TOE.*

### 9806 13.6.3.3.12 Work unit ALC\_FLR.3-12

9807 The evaluator **shall examine** the flaw remediation guidance to determine that the application of  
9808 these procedures would result in a means for the TOE user to provide reports of suspected security  
9809 flaws or requests for corrections to such flaws.

9810 The guidance ensures that TOE users have a means by which they can communicate with the TOE  
9811 developer. By having a means of contact with the developer, the user can report security flaws,  
9812 enquire about the status of security flaws, or request corrections to flaws.

9813 ISO/IEC 15408-3 ALC\_FLR.3.10C: *The flaw remediation guidance shall describe a means by which*  
9814 *TOE users may register with the developer, to be eligible to receive security flaw reports and*  
9815 *corrections.*

### 9816 13.6.3.3.13 Work unit ALC\_FLR.3-13

9817 The evaluator **shall examine** the flaw remediation guidance to determine that it describes a means  
9818 of enabling the TOE users to register with the developer.

9819 *Enabling the TOE users to register with the developer* simply means having a way for each TOE user  
9820 to provide the developer with a point of contact; this point of contact is to be used to provide the  
9821 TOE user with information related to security flaws that might affect that TOE user, along with any  
9822 corrections to the security flaw. Registering the TOE user may be accomplished as part of the  
9823 standard procedures that TOE users undergo to identify themselves to the developer, for the  
9824 purposes of registering a software licence, or for obtaining update and other useful information.

9825 There need not be one registered TOE user per installation of the TOE; it would be sufficient if  
9826 there were one registered TOE user for an organisation. For example, a corporate TOE user might  
9827 have a centralised acquisition office for all of its sites. In this case, the acquisition office would be a  
9828 sufficient point of contact for all of that TOE user's sites, so that all of the TOE user's installations of  
9829 the TOE have a registered point of contact.

9830 In either case, it must be possible to associate each TOE that is delivered with an organisation in  
9831 order to ensure that there is a registered user for each TOE. For organisations that have many  
9832 different addresses, this assures that there will be no user who is erroneously presumed to be  
9833 covered by a registered TOE user.

9834 It should be noted that TOE users need not register; they must only be provided with a means of  
9835 doing so. However, users who choose to register must be directly sent the information (or a  
9836 notification of its availability).

9837 ISO/IEC 15408-3 ALC\_FLR.3.11C: *The flaw remediation guidance shall identify the specific points of*  
9838 *contact for all reports and enquiries about security issues involving the TOE.*

9839 **13.6.3.3.14 Work unit ALC\_FLR.3-14**

9840 The evaluator **shall examine** the flaw remediation guidance to determine that it identifies specific  
9841 points of contact for user reports and enquiries about security issues involving the TOE.

9842 The guidance includes a means whereby registered TOE users can interact with the developer to  
9843 report discovered security flaws in the TOE or to make enquiries regarding discovered security  
9844 flaws in the TOE.

9845 **13.7 Life-cycle definition (ALC\_LCD)**

9846 **13.7.1 Evaluation of sub-activity (ALC\_LCD.1)**

9847 **13.7.1.1 Objectives**

9848 The objective of this sub-activity is to determine whether the developer has used a documented  
9849 model of the TOE life-cycle.

9850 **13.7.1.2 Input**

9851 The evaluation evidence for this sub-activity is:

- 9852 a) the ST;
- 9853 b) the life-cycle definition documentation.

9854 **13.7.1.3 Action ALC\_LCD.1.1E**

9855 ISO/IEC 15408-3 ALC\_LCD.1.1C: *The life-cycle definition documentation shall describe the model*  
9856 *used to develop and maintain the TOE.*

9857 **13.7.1.3.1 Work unit ALC\_LCD.1-1**

9858 The evaluator **shall examine** the documented description of the life-cycle model used to determine  
9859 that it covers the development and maintenance process.

9860 The description of the life-cycle model should include:

- 9861 a) information on the life-cycle phases of the TOE and the boundaries between the  
9862 subsequent phases;
- 9863 b) information on the procedures, tools and techniques used by the developer (e.g. for  
9864 design, coding, testing, bug-fixing);
- 9865 c) overall management structure governing the application of the procedures (e.g. an  
9866 identification and description of the individual responsibilities for each of the  
9867 procedures required by the development and maintenance process covered by the  
9868 life-cycle model);
- 9869 d) information on which parts of the TOE are delivered by subcontractors, if  
9870 subcontractors are involved.

## ISO/IEC 18045:2008(E)

9871 Evaluation of sub-activity (ALC\_LCD.1) does not require the model used to conform to any standard  
9872 life-cycle model.

9873 ISO/IEC 15408-3 ALC\_LCD.1.2C: *The life-cycle model shall provide for the necessary control over the*  
9874 *development and maintenance of the TOE.*

### 9875 13.7.1.3.2 Work unit ALC\_LCD.1-2

9876 The evaluator **shall examine** the life-cycle model to determine that use of the procedures, tools  
9877 and techniques described by the life-cycle model will make the necessary positive contribution to  
9878 the development and maintenance of the TOE.

9879 The information provided in the life-cycle model gives the evaluator assurance that the  
9880 development and maintenance procedures adopted would minimise the likelihood of security  
9881 flaws. For example, if the life-cycle model described the review process, but did not make provision  
9882 for recording changes to components, then the evaluator may be less confident that errors will not  
9883 be introduced into the TOE. The evaluator may gain further assurance by comparing the  
9884 description of the model against an understanding of the development process gleaned from  
9885 performing other evaluator actions relating to the TOE development (e.g. those covered under the  
9886 CM capabilities (ALC\_CMC)). Identified deficiencies in the life-cycle model will be of concern if they  
9887 might reasonably be expected to give rise to the introduction of flaws into the TOE, either  
9888 accidentally or deliberately.

9889 ISO/IEC 15408 SERIES does not mandate any particular development approach, and each should be  
9890 judged on merit. For example, spiral, rapid-prototyping and waterfall approaches to design can all  
9891 be used to produce a quality TOE if applied in a controlled environment.

### 9892 13.7.2 Evaluation of sub-activity (ALC\_LCD.2)

#### 9893 13.7.2.1 Objectives

9894 The objective of this sub-activity is to determine whether the developer has used a documented  
9895 and measurable model of the TOE life-cycle.

#### 9896 13.7.2.2 Input

9897 The evaluation evidence for this sub-activity is:

- 9898 a) the ST;
- 9899 b) the life-cycle definition documentation;
- 9900 c) information about the standard used;
- 9901 d) the life-cycle output documentation.

#### 9902 13.7.2.3 Action ALC\_LCD.2.1E

9903 ISO/IEC 15408-3 ALC\_LCD.2.1C: *The life-cycle definition documentation shall describe the model*  
9904 *used to develop and maintain the TOE, including the details of its arithmetic parameters and/or*  
9905 *metrics used to measure the quality of the TOE and/or its development.*



9906 **13.7.2.3.1 Work unit ALC\_LCD.2-1**

9907 The evaluator **shall examine** the documented description of the life-cycle model used to determine  
 9908 that it covers the development and maintenance process, including the details of its arithmetic  
 9909 parameters and/or metrics used to measure the TOE development.

9910 The description of the life-cycle model includes:

- 9911 a) information on the life-cycle phases of the TOE and the boundaries between the  
 9912 subsequent phases;
- 9913 b) information on the procedures, tools and techniques used by the developer (e.g. for  
 9914 design, coding, testing, bug-fixing);
- 9915 c) overall management structure governing the application of the procedures (e.g. an  
 9916 identification and description of the individual responsibilities for each of the  
 9917 procedures required by the development and maintenance process covered by the  
 9918 life-cycle model);
- 9919 d) information on which parts of the TOE are delivered by subcontractors, if  
 9920 subcontractors are involved;
- 9921 e) information on the parameters/metrics that are used to measure the TOE  
 9922 development. Metrics standards typically include guides for measuring and  
 9923 producing reliable products and cover the aspects reliability, quality, performance,  
 9924 complexity and cost. For the evaluation all those metrics are of relevance, which are  
 9925 used to increase quality by decreasing the probability of faults and thereby in turn  
 9926 increase assurance in the security of the TOE.

9927 ISO/IEC 15408-3 ALC\_LCD.2.2C: *The life-cycle model shall provide for the necessary control over the*  
 9928 *development and maintenance of the TOE.*

9929 **13.7.2.3.2 Work unit ALC\_LCD.2-2**

9930 The evaluator **shall examine** the life-cycle model to determine that use of the procedures, tools  
 9931 and techniques described by the life-cycle model will make the necessary positive contribution to  
 9932 the development and maintenance of the TOE.

9933 The information provided in the life-cycle model gives the evaluator assurance that the  
 9934 development and maintenance procedures adopted would minimise the likelihood of security  
 9935 flaws. For example, if the life-cycle model described the review process, but did not make provision  
 9936 for recording changes to components, then the evaluator may be less confident that errors will not  
 9937 be introduced into the TOE. The evaluator may gain further assurance by comparing the  
 9938 description of the model against an understanding of the development process gleaned from  
 9939 performing other evaluator actions relating to the TOE development (e.g. those covered under the  
 9940 CM capabilities (ALC\_CMC)). Identified deficiencies in the life-cycle model will be of concern if they  
 9941 might reasonably be expected to give rise to the introduction of flaws into the TOE, either  
 9942 accidentally or deliberately.

9943 ISO/IEC 15408 series does not mandate any particular development approach, and each should be  
 9944 judged on merit. For example, spiral, rapid-prototyping and waterfall approaches to design can all  
 9945 be used to produce a quality TOE if applied in a controlled environment.

9946 For the metrics/measurements used in the life-cycle model, evidence has to be provided that  
 9947 shows how those metrics/measurements usefully contribute to the minimisation of the likelihood

9948 of flaws. This can be viewed as the overall goal for measurement in an ALC context. As a  
 9949 consequence the metrics/measurements have to be selected based on their capability to achieve  
 9950 that overall goal or contribute to that. In the first place a metric/measure is suitable with respect to  
 9951 ALC if a correlation between the metric/measure and the number of flaws can be stated with a  
 9952 certain degree of reliability. But also a metric/measure useful for management purposes as for  
 9953 planning and monitoring the TOE development are helpful since badly managed projects are  
 9954 endangered to produce bad quality and to introduce flaws.

9955 It may be possible to use metrics for quality improvement, for which this use is not obvious. For  
 9956 example a metric to estimate the expected cost of a product development may help quality, if the  
 9957 developer can show that this is used to provide an adequate budget for development projects and  
 9958 that this helps to avoid quality problems arising from resource shortages.

9959 It is not required that every single step in the life cycle of the TOE is measurable. However the  
 9960 evaluator should see from the description of the measures and procedures that the metrics are  
 9961 appropriate to control the overall quality of the TOE and to minimise possible security flaws by this.

9962 ISO/IEC 15408-3 ALC\_LCD.2.3C: *The life-cycle output documentation shall provide the results of the*  
 9963 *measurements of the TOE development using the measurable life-cycle model.*

#### 9964 **13.7.2.3.3 Work unit ALC\_LCD.2-3**

9965 The evaluator ***shall examine*** the life-cycle output documentation to determine that it provides the  
 9966 results of the measurements of the TOE development using the measurable life-cycle model.

9967 The results of the measurements and the life-cycle progress of the TOE should be in accordance  
 9968 with the life-cycle model.

9969 The output documentation not only includes numeric values of the metrics but also documents  
 9970 actions taken as a result of the measurements and in accordance with the model. For example there  
 9971 may be a requirement that a certain design phase needs to be repeated, if some error rates  
 9972 measured during testing are outside of a defined threshold. In this case the documentation should  
 9973 show that such action was taken, if indeed the thresholds were not met.

9974 If the evaluation is conducted in parallel with the development of the TOE it may be possible that  
 9975 quality measurements have not been used in the past. In this case the evaluator should use the  
 9976 documentation of the planned procedures in order to gain confidence that corrective actions are  
 9977 defined if results of quality measurements deviate from some threshold.

### 9978 **13.8 TOE Development Artifacts (ALC\_TDA)**

#### 9979 **13.8.1 Evaluation of sub-activity (ALC\_TDA.1)**

### 9980 **13.9 ALC\_TDA**

#### 9981 **13.9.1 Evaluation of sub-activity (ALC\_TDA.1)**

##### 9982 **13.9.1.1 Objectives**

9983 The objectives of this sub-activity are to determine whether the developer has recorded the unique  
 9984 identifiers of the implementation representation which has been used to generate the TOE.

##### 9985 **13.9.1.1.1 Input**

9986 The evaluation evidence for this sub-activity is

9987 a) the ST;

- 9988 b) the list of TOE implementation representation identifiers as output from the  
9989 developer action of ISO/IEC 15408-3 ALC\_TDA.1.1D;
- 9990 c) the list of TOE implementation representation element names;
- 9991 d) the timestamp of the list of TOE implementation representation identifiers as output  
9992 from the developer action of ISO/IEC 15408-3 ALC\_TDA.1.2D;
- 9993 e) the (author) origination information of the list of TOE implementation representation  
9994 identifiers;
- 9995 f) the developer documentation describing the following as required in ISO/IEC 15408-  
9996 3 ALC\_TDA.1.6D
- 9997 1) the developer's creation of the list of unique TOE implementation representation  
9998 identifiers as recorded during the TOE generation time;
- 9999 2) the developer's timestamp being applied to the list of unique TOE  
10000 implementation representation identifiers as recorded during the TOE  
10001 generation time;
- 10002 3) the maintenance of the (author) origination information of the list of unique TOE  
10003 implementation representation identifiers as recorded during the TOE  
10004 generation time;
- 10005 4) the maintenance of the integrity of the list of unique TOE implementation  
10006 representation identifiers as recorded during the TOE generation time and its  
10007 associated timestamp and (author) origination information;
- 10008 5) the developer's mechanism to trace from the TOE to the list of unique TOE  
10009 implementation representation identifiers as recorded during the TOE  
10010 generation time;
- 10011 g) the user manual of the developer's development tool which use the TOE  
10012 implementation representation.

10013 **13.9.1.1.2 Action ALC\_TDA.1.1E**

10014 ISO/IEC 15408-3 ALC\_TDA.1.1C: The list of unique TOE implementation representation identifiers  
10015 as recorded during the TOE generation time shall demonstrate the correspondence between the  
10016 TOE implementation representation element identifiers and the TOE implementation  
10017 representation element names.

10018 **13.9.1.1.3 Work unit ALC\_TDA.1-1**

10019 The evaluator *shall examine* the developer documentation describing the developer's creation of  
10020 the list of unique TOE implementation representation identifiers as recorded during the TOE  
10021 generation time to determine that there is a correspondence between the TOE implementation  
10022 representation identifiers and the TOE implementation representation element names. If the  
10023 developer simply uses the unique TOE implementation representation identifiers as the TOE  
10024 implementation representation element names, then the correspondence is trivial. Otherwise, the  
10025 correspondence should have the following effect. If two elements within the TOE implementation

## ISO/IEC 18045:2008(E)

10026 representation share the same name, then either they are the same or they are separately  
10027 identified by two distinct identifiers.

10028 EXAMPLE

10029 If the TOE implementation representation elements are data files residing in a repository such as a  
10030 hard drive or in the cloud, then the TOE implementation representation element names are just  
10031 files names. In that case, it is possible that those two files in the hard drive or in the cloud share the  
10032 same name, but they have different contents. As a result, two distinct identifiers are necessary to  
10033 distinguish them apart. The correspondence between the TOE implementation representation  
10034 element identifiers and the TOE implementation representation element names therefore maps or  
10035 links the two distinct identifiers to the same file name.

10036 **13.9.1.1.4 Action ALC\_TDA.1.2E**

10037 ISO/IEC 15408-3 ALC\_TDA.1.2C: The TOE implementation representation element names shall be  
10038 in the same form as used or referenced by the development tool to generate the TOE.

10039 **13.9.1.1.5 Work unit ALC\_TDA.1-2**

10040 The evaluator *shall examine* the user manual of the developer's development tool used to generate  
10041 the TOE to determine that the development tool accepts the TOE implementation representation  
10042 element names as its input parameters.

10043 EXAMPLE

10044 If the TOE implementation representation elements are data files residing in a repository such as a  
10045 hard drive or in the cloud, then the evaluator only need to discover from the development tool user  
10046 manual that the development tool accepts local or remote file names as its input parameters.

10047 **13.9.1.1.6 Action ALC\_TDA.1.3E**

10048 ISO/IEC 15408-3 ALC\_TDA.1.3C: The timestamp of the list of unique TOE implementation  
10049 representation identifiers as recorded during the TOE generation time shall be consistent with the  
10050 creation time of the TOE.

10051 **13.9.1.1.7 Work unit ALC\_TDA.1-3**

10052 The evaluator *shall check* the timestamp of the list of TOE implementation representation  
10053 identifiers as output from the developer action of ISO/IEC 15408-3 ALC\_TDA.1.2D that it is  
10054 consistent with the creation time of the TOE as referenced in the ST.

10055 This consistence means that the number of days that the timestamp of the list of TOE  
10056 implementation representation identifiers precedes the TOE creation time does not exceed the first  
10057 order of magnitude. It is also not reasonable that the TOE creation time is older than the  
10058 timestamp of the list of TOE implementation representation identifiers.

10059 **13.9.1.1.8 Action ALC\_TDA.1.4E**

10060 ISO/IEC 15408-3 ALC\_TDA.1.4C: The (author) origination information of the list of unique TOE  
10061 implementation representation identifiers as recorded during the TOE generation time shall be  
10062 consistent with the (author) origination information of the TOE.

10063 **13.9.1.1.9 Work unit ALC\_TDA.1-4**

10064 The evaluator *shall check* the (author) origination information of the list of unique TOE  
10065 implementation representation identifiers that it is consistent with the (author) origination  
10066 information of the TOE as referenced in the ST.

10067 This consistence means that the (author) origination of the list of unique TOE implementation  
10068 representation identifiers is related to the (author) origination of the TOE professionally.

10069 EXAMPLE

10070 A reasonable relationship is that the (author) origination of the list of unique TOE implementation  
10071 representation identifiers is an employee, a contractor, a supplier, a subsidiary, or an  
10072 organizational division of, or is identical to the (author) origination of the TOE. However, it is not  
10073 reasonable that the (author) origination of the list of unique TOE implementation representation  
10074 identifiers and the (author) origination of the TOE are not documented as related professionally.

10075 **13.9.1.2 Action ALC\_TDA.1.5E**

10076 **13.9.1.2.1 Work unit ALC\_TDA.1-5**

10077 The evaluator *shall check* the integrity of the list of unique TOE implementation representation  
10078 identifiers as recorded during the TOE generation time and its associated timestamp and (author)  
10079 origination information by examining the developer documentation describing the maintenance of  
10080 this integrity characteristic. It is necessary that the developer documentation explains an  
10081 applicable scenario where none of the following items is freely modified without any proper  
10082 authorization after its initial existence:

- 10083 • the list of unique TOE implementation representation identifiers;
- 10084 • its associated timestamp;
- 10085 • its associated (author) origination information.

10086 EXAMPLE

10087 Applicable scenarios include the following:

- 10088 • these items reside in an access-controlled location and the associated access log/record  
10089 indicates that these items have not been changed since their initial creation;
- 10090 • these items are written in a read only media;
- 10091 • these items are digitally signed and are verifiable with a valid public key.

10092 **13.9.1.3 Action ALC\_TDA.1.6E**

10093 **13.9.1.3.1 Work unit ALC\_TDA.1-6**

10094 The evaluator *shall examine* the developer documentation describing the developer's mechanism  
10095 to trace from the TOE to the list of unique TOE implementation representation identifiers as  
10096 recorded during the TOE generation time to confirm the developer's ability to trace from the TOE  
10097 to the list of unique TOE implementation representation identifiers.

10098 It is necessary that the evaluator follows the developer documentation to find a list of identifiers  
10099 using the TOE as its input and the evaluator checks that this list of identifiers matches the list of  
10100 TOE implementation representation identifiers as output from the developer action of ISO/IEC  
10101 15408-3 ALC\_TDA.1.1D.

10102 EXAMPLE

10103 It is acceptable that the developer uses a tracing mechanism that directly or indirectly writes the  
10104 list of TOE implementation representation identifiers or its representation to the TOE.

## ISO/IEC 18045:2008(E)

10105 Alternatively, it is also acceptable that the developer uses a bill of materials database as a tracing  
10106 mechanism to maintain the correspondence between the TOE and the list of TOE implementation  
10107 representation identifiers.

### 10108 13.9.2 Evaluation of sub-activity (ALC\_TDA.2)

#### 10109 13.9.2.1 Objectives

10110 The objectives of this sub-activity are to determine whether the elements of implementation  
10111 representation maintained under the configuration scope of ALC\_CMS.3 are identifiable using the  
10112 developer's unique identifiers of the implementation representation as recorded during the TOE  
10113 generation time.

#### 10114 13.9.2.2 Input

10115 The evaluation evidence for this sub-activity is

- 10116 a) the ST;
- 10117 b) the list of TOE implementation representation identifiers as output from the  
10118 developer action of ISO/IEC 15408-3 ALC\_TDA.1.1D or ALC\_TDA.2.1D;
- 10119 c) the list of TOE implementation representation element names;
- 10120 d) the timestamp of the list of TOE implementation representation identifiers as output  
10121 from the developer action of ISO/IEC 15408-3 ALC\_TDA.1.2D or ALC\_TDA.2.2D;
- 10122 e) the (author) origination information of the list of TOE implementation representation  
10123 identifiers;
- 10124 f) the developer documentation describing the following as required in ISO/IEC 15408-  
10125 3 ALC\_TDA.1.6D or ALC\_TDA.2.6D
  - 10126 1) the developer's creation of the list of unique TOE implementation representation  
10127 identifiers as recorded during the TOE generation time;
  - 10128 2) the developer's timestamp being applied to the list of unique TOE  
10129 implementation representation identifiers as recorded during the TOE  
10130 generation time;
  - 10131 3) the maintenance of the (author) origination information of the list of unique TOE  
10132 implementation representation identifiers as recorded during the TOE  
10133 generation time;
  - 10134 4) the maintenance of the integrity of the list of unique TOE implementation  
10135 representation identifiers as recorded during the TOE generation time and its  
10136 associated timestamp and (author) origination information;
  - 10137 5) the developer's mechanism to trace from the TOE to the list of unique TOE  
10138 implementation representation identifiers as recorded during the TOE  
10139 generation time;

10140 g) the user manual of the developer's development tool which use the TOE  
10141 implementation representation;

10142 h) the element names of implementation representation (as parts of the configuration  
10143 list) under the configuration scope of ISO/IEC 15408-3 ALC\_CMS.3.

#### 10144 13.9.2.3 Action ALC\_TDA.2.1E

##### 10145 13.9.2.3.1 Work unit ALC\_TDA.2-1

10146 The evaluator *shall examine* the developer documentation describing the developer's creation of  
10147 the list of unique TOE implementation representation identifiers as recorded during the TOE  
10148 generation time to determine that there is a correspondence between the TOE implementation  
10149 representation identifiers and the TOE implementation representation element names. If the  
10150 developer simply uses the unique TOE implementation representation identifiers as the TOE  
10151 implementation representation element names, then the correspondence is trivial. Otherwise, the  
10152 correspondence should have the following effect. If two elements within the TOE implementation  
10153 representation share the same name, then either they are the same or they are separately  
10154 identified by two distinct identifiers.

##### 10155 EXAMPLE

10156 If the TOE implementation representation elements are data files residing in a repository such as a  
10157 hard drive or in the cloud, then the TOE implementation representation element names are just  
10158 files names. In that case, it is possible that those two files in the hard drive or in the cloud share the  
10159 same name, but they have different contents. As a result, two distinct identifiers are necessary to  
10160 distinguish them apart. The correspondence between the TOE implementation representation  
10161 element identifiers and the TOE implementation representation element names therefore maps or  
10162 links the two distinct identifiers to the same file name. Action ALC\_TDA.2.2E

##### 10163 13.9.2.3.2 Work unit ALC\_TDA.2-2

10164 The evaluator *shall examine* the user manual of the developer's development tool used to generate  
10165 the TOE to determine that the development tool accepts the TOE implementation representation  
10166 element names as its input parameters.

##### 10167 EXAMPLE

10168 If the TOE implementation representation elements are data files residing in a repository such as a  
10169 hard drive or in the cloud, then the evaluator only need to discover from the development tool user  
10170 manual that the development tool accepts local or remote file names as its input parameters.  
10171 Action ALC\_TDA.2.3E

##### 10172 13.9.2.3.3 Work unit ALC\_TDA.2-3

10173 The evaluator *shall check* the timestamp of the list of TOE implementation representation  
10174 identifiers as output from the developer action of ISO/IEC 15408-3 ALC\_TDA.1.2D that it is  
10175 consistent with the creation time of the TOE as referenced in the ST.

10176 This consistence means that the number of days that the timestamp of the list of TOE  
10177 implementation representation identifiers precedes the TOE creation time does not exceed the first  
10178 order of magnitude. It is also not reasonable that the TOE creation time is older than the  
10179 timestamp of the list of TOE implementation representation identifiers.

## ISO/IEC 18045:2008(E)

### 10180 13.9.2.4 Action ALC\_TDA.2.4E

#### 10181 13.9.2.4.1 Work unit ALC\_TDA.2-4

10182 The evaluator **shall check** the (author) origination information of the list of unique TOE  
10183 implementation representation identifiers that it is consistent with the (author) origination  
10184 information of the TOE as referenced in the ST.

10185 This consistence means that the (author) origination of the list of unique TOE implementation  
10186 representation identifiers is related to the (author) origination of the TOE professionally.

#### 10187 EXAMPLE

10188 A reasonable relationship is that the (author) origination of the list of unique TOE implementation  
10189 representation identifiers is an employee, a contractor, a supplier, a subsidiary, or an  
10190 organizational division of, or is identical to the (author) origination of the TOE. However, it is not  
10191 reasonable that the (author) origination of the list of unique TOE implementation representation  
10192 identifiers and the (author) origination of the TOE are not documented as related professionally.  
10193 Action ALC\_TDA.2.5E

#### 10194 13.9.2.4.2 Work unit ALC\_TDA.2-5

10195 The evaluator **shall check** the integrity of the list of unique TOE implementation representation  
10196 identifiers as recorded during the TOE generation time and its associated timestamp and (author)  
10197 origination information by examining the developer documentation describing the maintenance of  
10198 this integrity characteristic. It is necessary that the developer documentation explains an  
10199 applicable scenario where none of the following items is freely modified without any proper  
10200 authorization after its initial existence:

- 10201 • the list of unique TOE implementation representation identifiers;
- 10202 • its associated timestamp;
- 10203 • its associated (author) origination information.

10204 Applicable scenarios include the following:

- 10205 • these items reside in an access-controlled location and the associated access log/record  
10206 indicates that these items have not been changed since their initial creation;
- 10207 • these items are written in a read only media;
- 10208 • these items are digitally signed and are verifiable with a valid public key.

### 10209 13.9.2.5 Action ALC\_TDA.2.6E

#### 10210 13.9.2.5.1 Work unit ALC\_TDA.2-6

10211 The evaluator **shall examine** the developer documentation describing the developer's mechanism  
10212 to trace from the TOE to the list of unique TOE implementation representation identifiers as  
10213 recorded during the TOE generation time to confirm the developer's ability to trace from the TOE  
10214 to the list of unique TOE implementation representation identifiers.

10215 It is necessary that the evaluator follows the developer documentation to find a list of identifiers  
10216 using the TOE as its input and the evaluator checks that this list of identifiers matches the list of  
10217 TOE implementation representation identifiers as output from the developer action of ISO/IEC  
10218 15408-3 ALC\_TDA.1.1D.



10219 EXAMPLE

10220 It is acceptable that the developer uses a tracing mechanism that directly or indirectly writes the  
10221 list of TOE implementation representation identifiers or its representation to the TOE.  
10222 Alternatively, it is also acceptable that the developer uses a bill of materials database as a tracing  
10223 mechanism to maintain the correspondence between the TOE and the list of TOE implementation  
10224 representation identifiers. Action ALC\_TDA.2.7E

10225 ISO/IEC 15408-3 ALC\_TDA.2.5C: *The list of identifiers of the elements of implementation*  
10226 *representation under the configuration scope of ALC\_CMS.3 shall match with the list of unique TOE*  
10227 *implementation representation identifiers as recorded during the TOE generation time.*

#### 10228 13.9.2.5.2 Work unit ALC\_TDA.2-7

10229 The evaluator **shall check** that the TOE implementation representation identifiers in the  
10230 correspondence as determined in Work unit ALC\_TDA.1-1 are capable to identify the element  
10231 names of implementation representation (as parts of the configuration list) under the  
10232 configuration scope of ALC\_CMS.3.

#### 10233 13.9.3 Evaluation of sub-activity (ALC\_TDA.3)

##### 10234 13.9.3.1 Objectives

10235 A regenerated TOE copy is a TOE regeneration from another copy of the TOE implementation  
10236 representation according to the developer's unique identifiers of the implementation  
10237 representation as recorded during the TOE generation time. The objectives of this sub-activity are  
10238 to determine that the developer's explanation of the functional differences, if any, between the  
10239 regenerated TOE copy and the original TOE takes into account all visible differences, if any,  
10240 between the regenerated TOE copy and the original TOE.

##### 10241 13.9.3.2 Input

10242 The evaluation evidence for this sub-activity is

- 10243 a) the ST;
- 10244 b) the list of TOE implementation representation identifiers as output from the  
10245 developer action of ISO/IEC 15408-3 ALC\_TDA.1.1D or ALC\_TDA.2.1D or  
10246 ALC\_TDA.3.1D;
- 10247 c) the list of TOE implementation representation element names;
- 10248 d) the timestamp of the list of TOE implementation representation identifiers as output  
10249 from the developer action of ISO/IEC 15408-3 ALC\_TDA.1.2D or ALC\_TDA.2.2D or  
10250 ALC\_TDA.3.2D;
- 10251 e) the (author) origination information of the list of TOE implementation representation  
10252 identifiers;
- 10253 f) the developer documentation describing the following as required in ISO/IEC 15408-  
10254 3 ALC\_TDA.1.6D or ALC\_TDA.2.6D or ALC\_TDA.3.6D
- 10255 1) the developer's creation of the list of unique TOE implementation representation  
10256 identifiers as recorded during the TOE generation time;

## ISO/IEC 18045:2008(E)

- 10257 2) the developer's timestamp being applied to the list of unique TOE  
10258 implementation representation identifiers as recorded during the TOE  
10259 generation time;
- 10260 3) the maintenance of the (author) origination information of the list of unique TOE  
10261 implementation representation identifiers as recorded during the TOE  
10262 generation time;
- 10263 4) the maintenance of the integrity of the list of unique TOE implementation  
10264 representation identifiers as recorded during the TOE generation time and its  
10265 associated timestamp and (author) origination information;
- 10266 5) the developer's mechanism to trace from the TOE to the list of unique TOE  
10267 implementation representation identifiers as recorded during the TOE  
10268 generation time;
- 10269 g) the user manual of the developer's development tool which use the TOE  
10270 implementation representation;
- 10271 h) the element names of implementation representation (as parts of the configuration  
10272 list) under the configuration scope of ISO/IEC 15408-3 ALC\_CMS.3;
- 10273 i) the input for the evaluation of ADV\_IMP.1 sub-activity, which are
- 10274 1) the implementation representation;
- 10275 2) the documentation of the development tools, as resulting from ALC\_TAT;
- 10276 3) TOE design description;
- 10277 j) the developer's explanation of the functional differences, if any, between the  
10278 regenerated TOE copy and the original TOE as output from the developer action of  
10279 ISO/IEC 15408-3 ALC\_TDA.3.9D.
- 10280 **13.9.3.2.1 Action ALC\_TDA.3.1E**
- 10281 The evaluator ***shall confirm*** that the information provided meets all requirements for content and  
10282 presentation of evidence.
- 10283 **13.9.3.2.2 Work unit ALC\_TDA.3-1**
- 10284 The evaluator ***shall examine*** the developer documentation describing the developer's creation of  
10285 the list of unique TOE implementation representation identifiers as recorded during the TOE  
10286 generation time to determine that there is a correspondence between the TOE implementation  
10287 representation identifiers and the TOE implementation representation element names. If the  
10288 developer simply uses the unique TOE implementation representation identifiers as the TOE  
10289 implementation representation element names, then the correspondence is trivial. Otherwise, the  
10290 correspondence should have the following effect. If two elements within the TOE implementation  
10291 representation share the same name, then either they are the same or they are separately  
10292 identified by two distinct identifiers.
- 10293 EXAMPLE

10294 If the TOE implementation representation elements are data files residing in a repository such as a  
 10295 hard drive or in the cloud, then the TOE implementation representation element names are just  
 10296 files names. In that case, it is possible that those two files in the hard drive or in the cloud share the  
 10297 same name, but they have different contents. As a result, two distinct identifiers are necessary to  
 10298 distinguish them apart. The correspondence between the TOE implementation representation  
 10299 element identifiers and the TOE implementation representation element names therefore maps or  
 10300 links the two distinct identifiers to the same file name. Action ISO/IEC 15408-3 ALC\_TDA.3.2E

10301 **13.9.3.2.3 Work unit ALC\_TDA.3-2**

10302 The evaluator *shall examine* the user manual of the developer's development tool used to generate  
 10303 the TOE to determine that the development tool accepts the TOE implementation representation  
 10304 element names as its input parameters.

10305 **EXAMPLE**

10306 If the TOE implementation representation elements are data files residing in a repository such as a  
 10307 hard drive or in the cloud, then the evaluator only need to discover from the development tool user  
 10308 manual that the development tool accepts local or remote file names as its input parameters.  
 10309 Action ALC\_TDA.3.3E

10310 **13.9.3.2.4 Work unit ALC\_TDA.3-3**

10311 The evaluator *shall check* the timestamp of the list of TOE implementation representation  
 10312 identifiers as output from the developer action of ISO/IEC 15408-3 ALC\_TDA.1.2D that it is  
 10313 consistent with the creation time of the TOE as referenced in the ST.

10314 This consistency means that the number of days that the timestamp of the list of TOE  
 10315 implementation representation identifiers precedes the TOE creation time does not exceed the first  
 10316 order of magnitude. It is also not reasonable that the TOE creation time is older than the  
 10317 timestamp of the list of TOE implementation representation identifiers.

10318 Action ISO/IEC 15408-3 ALC\_TDA.3.4E

10319 **13.9.3.2.5 Work unit ALC\_TDA.3-4**

10320 The evaluator *shall check* the (author) origination information of the list of unique TOE  
 10321 implementation representation identifiers that it is consistent with the (author) origination  
 10322 information of the TOE as referenced in the ST.

10323 This consistence means that the (author) origination of the list of unique TOE implementation  
 10324 representation identifiers is related to the (author) origination of the TOE professionally.

10325 **EXAMPLE**

10326 A reasonable relationship is that the (author) origination of the list of unique TOE implementation  
 10327 representation identifiers is an employee, a contractor, a supplier, a subsidiary, or an  
 10328 organizational division of, or is identical to the (author) origination of the TOE. However, it is not  
 10329 reasonable that the (author) origination of the list of unique TOE implementation representation  
 10330 identifiers and the (author) origination of the TOE are not documented as related professionally.

10331 Action ISO/IEC 15408-3 ALC\_TDA.3.5E

10332 **13.9.3.2.6 Work unit ALC\_TDA.3-5**

10333 The evaluator *shall check* the integrity of the list of unique TOE implementation representation  
 10334 identifiers as recorded during the TOE generation time and its associated timestamp and (author)  
 10335 origination information by examining the developer documentation describing the maintenance of

## ISO/IEC 18045:2008(E)

10336 this integrity characteristic. It is necessary that the developer documentation explains an  
10337 applicable scenario where none of the following items is freely modified without any proper  
10338 authorization after its initial existence:

- 10339 • the list of unique TOE implementation representation identifiers;
- 10340 • its associated timestamp;
- 10341 • its associated (author) origination information.

10342 EXAMPLE

10343 Applicable scenarios include the following:

- 10344 • these items reside in an access-controlled location and the associated access log/record  
10345 indicates that these items have not been changed since their initial creation;
- 10346 • these items are written in a read only media;
- 10347 • these items are digitally signed and are verifiable with a valid public key.

10348 Action ISO/IEC 15408-3 ALC\_TDA.3.6E

### 10349 13.9.3.2.7 Work unit ALC\_TDA.3-6

10350 The evaluator *shall examine* the developer documentation describing the developer's mechanism  
10351 to trace from the TOE to the list of unique TOE implementation representation identifiers as  
10352 recorded during the TOE generation time to confirm the developer's ability to trace from the TOE  
10353 to the list of unique TOE implementation representation identifiers.

10354 It is necessary that the evaluator follows the developer documentation to find a list of identifiers  
10355 using the TOE as its input and the evaluator checks that this list of identifiers matches the list of  
10356 TOE implementation representation identifiers as output from the developer action of ISO/IEC  
10357 15408-3 ALC\_TDA.1.1D.

10358 EXAMPLE

10359 It is acceptable that the developer uses a tracing mechanism that directly or indirectly writes the  
10360 list of TOE implementation representation identifiers or its representation to the TOE.  
10361 Alternatively, it is also acceptable that the developer uses a bill of materials database as a tracing  
10362 mechanism to maintain the correspondence between the TOE and the list of TOE implementation  
10363 representation identifiers. Action ALC\_TDA.3.7E

### 10364 13.9.3.2.8 Work unit ALC\_TDA.3-7

10365 It is same as Work unit ALC\_TDA.2-7.

### 10366 13.9.3.3 Action ALC\_TDA.3.8E

10367 ISO/IEC 15408-3 ALC\_TDA.3.6C: The developer's explanation of the functional differences, if any,  
10368 between the regenerated TOE copy and the original TOE shall take into account all visible  
10369 differences, if any, between the regenerated TOE copy and the original TOE.

10370 **13.9.3.3.1 Work unit ALC\_TDA.3-8**

10371 The evaluator **shall check** that the developer's explanation of the functional differences, if any,  
 10372 between the regenerated TOE copy and the original TOE takes into account all visible differences, if  
 10373 any, between the regenerated TOE copy and the original TOE.

10374 If parts of the TOE consist of software such as a collection of binary executable files, then it is  
 10375 possible to observe the corresponding differences between the regenerated TOE copy and the  
 10376 original TOE using a binary file editor/viewer or other applicable software diagnostic or testing  
 10377 tools. If parts of the TOE consist of hardware such as integrated circuits, then it is possible to  
 10378 observe the corresponding differences between the regenerated TOE copy and the original TOE  
 10379 using a microscope or other applicable hardware diagnostic or testing tools. In either case, if there  
 10380 is no visible difference between the regenerated TOE copy and the original TOE, then there is no  
 10381 functional difference for the developer to explain and the evaluator trivially takes all visible  
 10382 differences into account.

10383 **13.10 Tools and techniques (ALC\_TAT)**10384 **13.10.1 Evaluation of sub-activity (ALC\_TAT.1)**10385 **13.10.1.1 Objectives**

10386 The objective of this sub-activity is to determine whether the developer has used well-defined  
 10387 development tools (e.g. programming languages or computer-aided design (CAD) systems) that  
 10388 yield consistent and predictable results.

10389 **13.10.1.2 Input**

10390 The evaluation evidence for this sub-activity is:

- 10391 a) the development tool documentation;
- 10392 b) the subset of the implementation representation.

10393 **13.10.1.3 Application notes**

10394 This work may be performed in parallel with the evaluation activities under Implementation  
 10395 representation (ADV\_IMP), specifically with regard to determining the use of features in the tools  
 10396 that will affect the object code (e.g. compilation options).

10397 **13.10.1.4 Action ALC\_TAT.1.1E**

10398 ISO/IEC 15408-3 ALC\_TAT.1.1C: *Each development tool used for implementation shall be well-*  
 10399 *defined.*

10400 **13.10.1.4.1 Work unit ALC\_TAT.1-1**

10401 The evaluator **shall examine** the development tool documentation provided to determine that  
 10402 each development tools is well-defined.

10403 For example, a well-defined language, compiler or CAD system may be considered to be one that  
 10404 conforms to a recognised standard, such as the ISO standards. A well-defined language is one that  
 10405 has a clear and complete description of its syntax, and a detailed description of the semantics of  
 10406 each construct.

## ISO/IEC 18045:2008(E)

10407 ISO/IEC 15408-3 ALC\_TAT.1.2C: *The documentation of each development tool shall unambiguously*  
10408 *define the meaning of all statements as well as all conventions and directives used in the*  
10409 *implementation.*

### 10410 13.10.1.4.2 Work unit ALC\_TAT.1-2

10411 The evaluator **shall examine** the documentation of each development tool to determine that it  
10412 unambiguously defines the meaning of all statements as well as all conventions and directives used  
10413 in the implementation.

10414 The development tool documentation (e.g. programming language specifications and user  
10415 manuals) should cover all statements used in the implementation representation of the TOE, and  
10416 for each such statement should provide a clear and unambiguous definition of the purpose and  
10417 effect of that statement. This work may be performed in parallel with the evaluator's examination  
10418 of the implementation representation performed during the ADV\_IMP sub-activity. The key test the  
10419 evaluator should apply is whether or not the documentation is sufficiently clear for the evaluator to  
10420 be able to understand the implementation representation. The documentation should not assume  
10421 (for example) that the reader is an expert in the programming language used.

10422 Reference to the use of a documented standard is an acceptable approach to meet this requirement,  
10423 provided that the standard is available to the evaluator. Any differences from the standard should  
10424 be documented.

10425 The critical test is whether the evaluator can understand the TOE source code when performing  
10426 source code analysis covered in the ADV\_IMP sub-activity. However, the following checklist can  
10427 additionally be used in searching for problem areas:

10428 a) In the language definition, phrases such as "the effect of this construct is undefined"  
10429 and terms such as "implementation dependent" or "erroneous" may indicate ill-  
10430 defined areas.

10431 b) Aliasing (allowing the same piece of memory to be referenced in different ways) is a  
10432 common source of ambiguity problems.

10433 c) Exception handling (e.g. what happens after memory exhaustion or stack overflow) is  
10434 often poorly defined.

10435 Most languages in common use, however well designed, will have some problematic constructs. If  
10436 the implementation language is mostly well defined, but some problematic constructs exist, then  
10437 an inconclusive verdict should be assigned, pending examination of the source code.

10438 The implementation standards description should include at least following:

- 10439 • How to implement TOE so as to avoid problematic constructs inherent in the  
10440 programming language used and/or in the development tool
- 10441 • How to implement TOE so as to avoid unwanted behaviour from security perspective (or  
10442 vulnerabilities) introduced by the development tool. Note that sometimes developers face  
10443 the situation that the code generated by the development tool used by the developer does  
10444 not fulfil the desired security property.
- 10445 • How to implement TOE so as to meet the rules imposed by third party developers

10446 Note that information required under ADV\_COMP.1.1C will be a part of the rules when composite  
10447 evaluation approach is selected.

- 10448 It is not sufficient to describe just naming rules which do no harm to the security in the light of  
10449 modern compilers.
- 10450 The evaluator should verify, during the examination of source code, that any use of the problematic  
10451 constructs does not introduce vulnerabilities. The evaluator should also ensure that constructs  
10452 precluded by the documented standard are not used.
- 10453 The development tool documentation should define all conventions and directives used in the  
10454 implementation.
- 10455 ISO/IEC 15408-3 ALC\_TAT.1.3C: *The documentation of each development tool shall unambiguously*  
10456 *define the meaning of all implementation-dependent options.*
- 10457 **13.10.1.4.3 Work unit ALC\_TAT.1-3**
- 10458 The evaluator ***shall examine*** the development tool documentation to determine that it  
10459 unambiguously defines the meaning of all implementation-dependent options.
- 10460 The documentation of software development tools should include definitions of implementation-  
10461 dependent options that may affect the meaning of the executable code, and those that are different  
10462 from the standard language as documented. Where source code is provided to the evaluator,  
10463 information should also be provided on compilation and linking options used.
- 10464 The documentation for hardware design and development tools should describe the use of all  
10465 options that affect the output from the tools (e.g. detailed hardware specifications, or actual  
10466 hardware).
- 10467 **13.10.2 Evaluation of sub-activity (ALC\_TAT.2)**
- 10468 **13.10.2.1 Objectives**
- 10469 The objective of this sub-activity is to determine whether the developer has used well-defined  
10470 development tools (e.g. programming languages or computer-aided design (CAD) systems) that  
10471 yield consistent and predictable results, and whether implementation standards have been applied.
- 10472 **13.10.2.2 Input**
- 10473 The evaluation evidence for this sub-activity is:
- 10474 a) the development tool documentation;
- 10475 b) the implementation standards description;
- 10476 c) the provided implementation representation of the TSF.
- 10477 **13.10.2.3 Application notes**
- 10478 This work may be performed in parallel with the evaluation activities under ADV\_IMP, specifically  
10479 with regard to determining the use of features in the tools that will affect the object code (e.g.  
10480 compilation options).
- 10481 **13.10.2.4 Action ALC\_TAT.2.1E**
- 10482 ISO/IEC 15408-3 ALC\_TAT.2.1C: *Each development tool used for implementation shall be well-*  
10483 *defined.*

## ISO/IEC 18045:2008(E)

### 10484 13.10.2.4.1 Work unit ALC\_TAT.2-1

10485 The evaluator **shall examine** the development tool documentation provided to determine that  
10486 each development tool is well-defined.

10487 For example, a well-defined language, compiler or CAD system may be considered to be one that  
10488 conforms to a recognised standard, such as the ISO standards. A well-defined language is one that  
10489 has a clear and complete description of its syntax, and a detailed description of the semantics of  
10490 each construct.

10491 ISO/IEC 15408-3 ALC\_TAT.2.2C: *The documentation of each development tool shall unambiguously*  
10492 *define the meaning of all statements as well as all conventions and directives used in the*  
10493 *implementation.*

### 10494 13.10.2.4.2 Work unit ALC\_TAT.2-2

10495 The evaluator **shall examine** the documentation of each development tool to determine that it  
10496 unambiguously defines the meaning of all statements as well as all conventions and directives used  
10497 in the implementation.

10498 The development tool documentation (e.g. programming language specifications and user  
10499 manuals) should cover all statements used in the implementation representation of the TOE, and  
10500 for each such statement should provide a clear and unambiguous definition of the purpose and  
10501 effect of that statement. This work may be performed in parallel with the evaluator's examination  
10502 of the implementation representation performed during the ADV\_IMP sub-activity. The key test the  
10503 evaluator should apply is whether or not the documentation is sufficiently clear for the evaluator to  
10504 be able to understand the implementation representation. The documentation should not assume  
10505 (for example) that the reader is an expert in the programming language used.

10506 Reference to the use of a documented standard is an acceptable approach to meet this requirement,  
10507 provided that the standard is available to the evaluator. Any differences from the standard should  
10508 be documented.

10509 The critical test is whether the evaluator can understand the TOE source code when performing  
10510 source code analysis covered in the ADV\_IMP sub-activity. However, the following checklist can  
10511 additionally be used in searching for problem areas:

10512 a) In the language definition, phrases such as "the effect of this construct is undefined"  
10513 and terms such as "implementation dependent" or "erroneous" may indicate ill-  
10514 defined areas.

10515 b) Aliasing (allowing the same piece of memory to be referenced in different ways) is a  
10516 common source of ambiguity problems.

10517 c) Exception handling (e.g. what happens after memory exhaustion or stack overflow) is  
10518 often poorly defined.

10519 Most languages in common use, however well designed, will have some problematic constructs. If  
10520 the implementation language is mostly well defined, but some problematic constructs exist, then  
10521 an inconclusive verdict should be assigned, pending examination of the source code.

10522 The implementation standards description should include at least following:

- 10523 • How to implement TOE so as to avoid problematic constructs inherent in the  
10524 programming language used and/or in the development tool



- 10525 • How to implement TOE so as to avoid unwanted behaviour from security perspective (or  
10526 vulnerabilities) introduced by the development tool. Note that sometimes developers face  
10527 the situation that the code generated by the development tool used by the developer does  
10528 not fulfil the desired security property.
- 10529 • How to implement TOE so as to meet the rules imposed by third party developers
- 10530 Note that information required under ADV\_COMP.1.1C will be a part of the rules when composite  
10531 evaluation approach is selected.
- 10532 It is not sufficient to describe just naming rules which do no harm to the security in the light of  
10533 modern compilers.
- 10534 The evaluator should verify, during the examination of source code, that any use of the problematic  
10535 constructs does not introduce vulnerabilities. The evaluator should also ensure that constructs  
10536 precluded by the documented standard are not used.
- 10537 The development tool documentation should define all conventions and directives used in the  
10538 implementation.
- 10539 ISO/IEC 15408-3 ALC\_TAT.2.3C: *The documentation of each development tool shall unambiguously*  
10540 *define the meaning of all implementation-dependent options.*
- 10541 **13.10.2.4.3 Work unit ALC\_TAT.2-3**
- 10542 The evaluator ***shall examine*** the development tool documentation to determine that it  
10543 unambiguously defines the meaning of all implementation-dependent options.
- 10544 The documentation of software development tools should include definitions of implementation-  
10545 dependent options that may affect the meaning of the executable code, and those that are different  
10546 from the standard language as documented. Where source code is provided to the evaluator,  
10547 information should also be provided on compilation and linking options used.
- 10548 The documentation for hardware design and development tools should describe the use of all  
10549 options that affect the output from the tools (e.g. detailed hardware specifications, or actual  
10550 hardware).
- 10551 **13.10.2.5 Action ALC\_TAT.2.2E**
- 10552 **13.10.2.5.1 Work unit ALC\_TAT.2-4**
- 10553 The evaluator ***shall examine*** aspects of the implementation process to determine that documented  
10554 implementation standards have been applied.
- 10555 This work unit requires the evaluator to analyse the provided implementation representation of  
10556 the TOE to determine whether the documented implementation standards have been applied.
- 10557 The evaluator should verify that constructs excluded by the documented standard are not used.
- 10558 Additionally, the evaluator should verify the developer's procedures which ensure the application  
10559 of the defined standards within the design and implementation process of the TOE. Therefore,  
10560 documentary evidence should be supplemented by visiting the development environment. A visit  
10561 to the development environment will allow the evaluator to:
- 10562 a) observe the application of defined standards;

## ISO/IEC 18045:2008(E)

- 10563 b) examine documentary evidence of application of procedures describing the use of  
10564 defined standards;
- 10565 c) interview development staff to check awareness of the application of defined  
10566 standards and procedures.
- 10567 A development site visit is a useful means of gaining confidence in the procedures being used. Any  
10568 decision not to make such a visit should be determined in consultation with the evaluation  
10569 authority.
- 10570 The evaluator compares the provided implementation representation with the description of the  
10571 applied implementation standards and verifies their use.
- 10572 At this level it is not required that the complete provided implementation representation of the  
10573 TSF is based on implementation standards, but only those parts that are developed by the TOE  
10574 developer himself. The evaluator may consult the configuration list required by the CM scope  
10575 (ALC\_CMS) to get the information which parts are developed by the TOE developer, and which by  
10576 third party developers.
- 10577 If the referenced implementation standards are not applied for at least parts of the provided  
10578 implementation representation, the evaluator action related to this work unit is assigned a fail  
10579 verdict.
- 10580 Note that parts of the TOE which are not TSF relevant do not need to be examined.
- 10581 This work unit may be performed in conjunction with the evaluation activities under ADV\_IMP.
- 10582 **13.10.3 Evaluation of sub-activity (ALC\_TAT.3)**
- 10583 **13.10.3.1 Objectives**
- 10584 The objective of this sub-activity is to determine whether the developer and their subcontractors  
10585 have used well-defined development tools (e.g. programming languages or computer-aided design  
10586 (CAD) systems) that yield consistent and predictable results, and whether implementation  
10587 standards have been applied.
- 10588 **13.10.3.2 Input**
- 10589 The evaluation evidence for this sub-activity is:
- 10590 a) the development tool documentation;
- 10591 b) the implementation standards description;
- 10592 c) the provided implementation representation of the TSF.
- 10593 **13.10.3.3 Application notes**
- 10594 This work may be performed in parallel with the evaluation activities under ADV\_IMP, specifically  
10595 with regard to determining the use of features in the tools that will affect the object code (e.g.  
10596 compilation options).

10597      **13.10.3.4 Action ALC\_TAT.3.1E**

10598      ISO/IEC 15408-3 ALC\_TAT.3.1C: *Each development tool used for implementation shall be well-*  
 10599      *defined.*

10600      **13.10.3.4.1 Work unit ALC\_TAT.3-1**

10601      The evaluator **shall examine** the development tool documentation provided to determine that  
 10602      each development tool is well-defined.

10603      For example, a well-defined language, compiler or CAD system may be considered to be one that  
 10604      conforms to a recognised standard, such as the ISO standards. A well-defined language is one that  
 10605      has a clear and complete description of its syntax, and a detailed description of the semantics of  
 10606      each construct.

10607      At this level, the documentation of development tools used by third party contributors to the TOE  
 10608      has to be included in the evaluator's examination.

10609      ISO/IEC 15408-3 ALC\_TAT.3.2C: *The documentation of each development tool shall unambiguously*  
 10610      *define the meaning of all statements as well as all conventions and directives used in the*  
 10611      *implementation.*

10612      **13.10.3.4.2 Work unit ALC\_TAT.3-2**

10613      The evaluator **shall examine** the documentation of each development tool to determine that it  
 10614      unambiguously defines the meaning of all statements as well as all conventions and directives used  
 10615      in the implementation.

10616      The development tool documentation (e.g. programming language specifications and user  
 10617      manuals) should cover all statements used in the implementation representation of the TOE, and  
 10618      for each such statement should provide a clear and unambiguous definition of the purpose and  
 10619      effect of that statement. This work may be performed in parallel with the evaluator's examination  
 10620      of the implementation representation performed during the ADV\_IMP sub-activity. The key test the  
 10621      evaluator should apply is whether or not the documentation is sufficiently clear for the evaluator to  
 10622      be able to understand the implementation representation. The documentation should not assume  
 10623      (for example) that the reader is an expert in the programming language used.

10624      Reference to the use of a documented standard is an acceptable approach to meet this requirement,  
 10625      provided that the standard is available to the evaluator. Any differences from the standard should  
 10626      be documented.

10627      The critical test is whether the evaluator can understand the TOE source code when performing  
 10628      source code analysis covered in the ADV\_IMP sub-activity. However, the following checklist can  
 10629      additionally be used in searching for problem areas:

10630      a) In the language definition, phrases such as "the effect of this construct is undefined"  
 10631      and terms such as "implementation dependent" or "erroneous" may indicate ill-  
 10632      defined areas.

10633      b) Aliasing (allowing the same piece of memory to be referenced in different ways) is a  
 10634      common source of ambiguity problems.

10635      c) Exception handling (e.g. what happens after memory exhaustion or stack overflow) is  
 10636      often poorly defined.

## ISO/IEC 18045:2008(E)

10637 Most languages in common use, however well designed, will have some problematic constructs. If  
10638 the implementation language is mostly well defined, but some problematic constructs exist, then  
10639 an inconclusive verdict should be assigned, pending examination of the source code.

10640 The implementation standards description should include at least following:

10641 • How to implement TOE so as to avoid problematic constructs inherent in the  
10642 programming language used and/or in the development tool

10643 • How to implement TOE so as to avoid unwanted behaviour from security perspective (or  
10644 vulnerabilities) introduced by the development tool. Note that sometimes developers face  
10645 the situation that the code generated by the development tool used by the developer does  
10646 not fulfil the desired security property.

10647 • How to implement TOE so as to meet the rules imposed by third party developers

10648 Note that information required under ADV\_COMP.1.1C will be a part of the rules when composite  
10649 evaluation approach is selected.

10650 It is not sufficient to describe just naming rules which do no harm to the security in the light of  
10651 modern compilers.

10652 The evaluator should verify, during the examination of source code, that any use of the problematic  
10653 constructs does not introduce vulnerabilities. The evaluator should also ensure that constructs  
10654 precluded by the documented standard are not used.

10655 The development tool documentation should define all conventions and directives used in the  
10656 implementation.

10657 At this level, the documentation of development tools used by third party contributors to the TOE  
10658 has to be included in the evaluator's examination.

10659 ISO/IEC 15408-3 ALC\_TAT.3.3C: *The documentation of each development tool shall unambiguously*  
10660 *define the meaning of all implementation-dependent options.*

### 10661 13.10.3.4.3 Work unit ALC\_TAT.3-3

10662 The evaluator **shall examine** the development tool documentation to determine that it  
10663 unambiguously defines the meaning of all implementation-dependent options.

10664 The documentation of software development tools should include definitions of implementation-  
10665 dependent options that may affect the meaning of the executable code, and those that are different  
10666 from the standard language as documented. Where source code is provided to the evaluator,  
10667 information should also be provided on compilation and linking options used.

10668 The documentation for hardware design and development tools should describe the use of all  
10669 options that affect the output from the tools (e.g. detailed hardware specifications, or actual  
10670 hardware).

10671 At this level, the documentation of development tools used by third party contributors to the TOE  
10672 has to be included in the evaluator's examination.

10673 **13.10.3.5 Action ALC\_TAT.3.2E**10674 **13.10.3.5.1 Work unit ALC\_TAT.3-4**

10675 The evaluator *shall examine* aspects of the implementation process to determine that documented  
10676 implementation standards have been applied.

10677 This work unit requires the evaluator to analyse the provided implementation representation of  
10678 the TOE to determine whether the documented implementation standards have been applied.

10679 The evaluator should verify that constructs excluded by the documented standard are not used.

10680 Additionally, the evaluator should verify the developer's procedures which ensure the application  
10681 of the defined standards within the design and implementation process of the TOE. Therefore,  
10682 documentary evidence should be supplemented by visiting the development environment. A visit  
10683 to the development environment will allow the evaluator to:

10684 a) observe the application of defined standards;

10685 b) examine documentary evidence of application of procedures describing the use of  
10686 defined standards;

10687 c) interview development staff to check awareness of the application of defined  
10688 standards and procedures.

10689 A development site visit is a useful means of gaining confidence in the procedures being used. Any  
10690 decision not to make such a visit should be determined in consultation with the evaluation  
10691 authority.

10692 The evaluator compares the provided implementation representation with the description of the  
10693 applied implementation standards and verifies their use.

10694 At this level it is required that the complete provided implementation representation of the TSF is  
10695 based on implementation standards, including third party contributions. This may require the  
10696 evaluator to visit the sites of contributors. The evaluator may consult the configuration list  
10697 required by the CM scope (ALC\_CMS) to see who has developed which part of the TOE.

10698 Note that parts of the TOE which are not TSF relevant do not need to be examined.

10699 This work unit may be performed in conjunction with the evaluation activities under ADV\_IMP.

10700 **13.11 Integration of composition parts and consistency check of delivery**  
10701 **procedures (ALC\_COMP)**

10702 **13.11.1 General**

10703 The composite-specific work units defined here are intended to be integrated as refinements to the  
10704 evaluation activities of the ALC class listed in the following table. The other activities of ALC class  
10705 do not require composite-specific work units.

| CC assurance family | Evaluation activity | Evaluation work unit | Composite-specific work unit |
|---------------------|---------------------|----------------------|------------------------------|
| ALC_CMS             | ALC_CMS.1.2C        | ALC_CMS.1-2          | ALC_COMP.1-1                 |

**ISO/IEC 18045:2008(E)**

|         |              |              |              |
|---------|--------------|--------------|--------------|
| AGD_PRE | AGD_PRE.1.1C | AGD_PRE.1-1  | ALC_COMP.1-2 |
| ALC_CMC | ALC_CMC.4.8C | ALC_CMC.4-10 | ALC_CMC.4-10 |

10706 NB: If the level of the assurance requirement chosen is higher than those identified in this table, the  
10707 composite-specific work unit is also applicable.

10708 **13.11.2 Evaluation of sub-activity (ALC\_COMP.1)**

10709 **13.11.2.1 Objectives**

10710 The aims of this activity are to determine whether – the correct version of the application is  
10711 installed onto/into the correct version of the underlying platform, and

10712 – the preparative guidance procedures of Platform and Application Developers are compatible with  
10713 the acceptance procedure of the Composite Product Integrator.

10714 **13.11.2.2 Action ALC\_COMP.1.1E**

10715 The evaluator ***shall examine*** the evidence that the evaluated version of the application has been  
10716 installed onto / embedded into the correct, certified version of the underlying platform.

10717 The AGD\_PRE documentation of the platform provided by the platform developer contains  
10718 requirements for the secure acceptance of the platform and security measures to which the  
10719 application developer or product composite integrator has to adhere. The application developer  
10720 has to provide evidence that (if applicable), these requirements are followed up and the required  
10721 security measures are implemented.

10722 The special composite evaluator activity is to check the evidence of the version correctness for  
10723 both parts of the composite product and that the secure acceptance and installation of the platform  
10724 has been performed.

10725 For the underlying platform, the evaluator shall determine that the actual identification of the  
10726 platform is commensurate with the respective data in the platform certificate as part of following  
10727 up on the procedures as specified in the AGD\_PRE of the platform.

10728 For the application, the relevant task is trivial due to the fact that the Composite Product Evaluator  
10729 has to perform this task in the context of the assurance family ALC\_CMS.

10730 Components identification evidence can be supplied in two different ways: technical and  
10731 organisational. A technical evidence of version correctness is being generated by the composite  
10732 product itself: the platform and the application return – in each case – strings containing  
10733 unambiguous version numbers as answers to the respective commands. E.g. it can be the return  
10734 string of a command or the hard copy of the Windows Information (like 'About'); in case of smart  
10735 cards it can be an appropriate ATR.

10736 Technical evidence of version correctness for hardware can also be supplied, if applicable, by  
10737 reading off the unambiguous inscription on its surface. Note that there are no physical indication  
10738 existing on most smart card's microcontrollers.

10739 Technical evidence is recommended to be provided.

10740 An organisational evidence of version correctness is being generated by the Composite Product  
10741 Integrator on the basis of his configuration lists containing unambiguous version information of  
10742 the platform and the application having been composed into the final composite product.

10743 For example, in case of smart cards it can be an acknowledgement statement (e.g. configuration  
10744 list) of the underlying platform manufacturer to the application software manufacturer containing

10745 the evidence for the versions of the platform, any embedded software and its pre-personalisation  
 10746 parameters. Organisational evidence is always possible and, hence, shall be provided. The result of  
 10747 this work unit shall be integrated to the result of ALC\_CMS1.1C/ ALC\_CMS.1-2 (or the equivalent  
 10748 higher components if a higher assurance level is selected).

10749 ALC\_COMP.1.2C

10750 **Editors' Notes**

10751 **Suggestions for text improvements would be welcomed in response to CD3 review**

## 10752 **14 Class ATE: Tests**

### 10753 **14.1 Introduction**

10754 The goal of this activity is to determine whether the TOE behaves as described in the ST and as  
 10755 specified in the evaluation evidence (described in the ADV class). This determination is achieved  
 10756 through some combination of the developer's own functional testing of the TSF (Functional tests  
 10757 (ATE\_FUN)) and independent testing the TSF by the evaluator (Independent testing (ATE\_IND)). At  
 10758 the lowest level of assurance, there is no requirement for developer involvement, so the only  
 10759 testing is conducted by the evaluator, using the limited available information about the TOE.  
 10760 Additional assurance is gained as the developer becomes increasingly involved both in testing and  
 10761 in providing additional information about the TOE, and as the evaluator increases the independent  
 10762 testing activities.

### 10763 **14.2 Application notes**

10764 Testing of the TSF is conducted by the evaluator and, in most cases, by the developer. The  
 10765 evaluator's testing efforts consist not only of creating and running original tests, but also of  
 10766 assessing the adequacy of the developer's tests and re-running a subset of them.

10767 The evaluator analyses the developer's tests to determine the extent to which they are sufficient to  
 10768 demonstrate that TSFI (see Functional specification (ADV\_FSP)) perform as specified, and to  
 10769 understand the developer's approach to testing. Similarly, the evaluator analyses the developer's  
 10770 tests to determine the extent to which they are sufficient to demonstrate the internal behaviour  
 10771 and properties of the TSF.

10772 The evaluator also executes a subset of the developer's tests as documented to gain confidence in  
 10773 the developer's test results: the evaluator will use the results of this analysis as an input to  
 10774 independently testing a subset of the TSF. With respect to this subset, the evaluator takes a testing  
 10775 approach that is different from that of the developer, particularly if the developer's tests have  
 10776 shortcomings.

10777 To determine the adequacy of developer's test documentation or to create new tests, the evaluator  
 10778 needs to understand the desired expected behaviour of the TSF, both internally and as seen at the  
 10779 TSFI, in the context of the SFRs it is to satisfy. The evaluator may choose to divide the TSF and TSFI  
 10780 into subsets according to functional areas of the ST (audit subsystem, audit-related TSFI,  
 10781 authentication module, authentication-related TSFI, etc.) if they were not already divided in the ST,  
 10782 and focus on one subset of the TSF and TSFI at a time, examining the ST requirement and the  
 10783 relevant parts of the development and guidance documentation to gain an understanding of the  
 10784 way the TOE is expected to behave. This reliance upon the development documentation  
 10785 underscores the need for the dependencies on ADV by Coverage (ATE\_COV) and Depth (ATE\_DPT).

10786 ISO/IEC 15408 series has separated coverage and depth from functional tests to increase the  
 10787 flexibility when applying the components of the families. However, the requirements of the families  
 10788 are intended to be applied together to confirm that the TSF operates according to its specification.  
 10789 This tight coupling of families has led to some duplication of evaluator work units across sub-  
 10790 activities. These application notes are used to minimise duplication of text between sub-activities.

**14.2.1 Understanding the expected behaviour of the TOE**

Before the adequacy of test documentation can be accurately evaluated, or before new tests can be created, the evaluator has to understand the desired expected behaviour of a security function in the context of the requirements it is to satisfy.

As mentioned earlier, the evaluator may choose to subset the TSF and TSFI according to SFRs (audit, authentication, etc.) in the ST and focus on one subset at a time. The evaluator examines each ST requirement and the relevant parts of the functional specification and guidance documentation to gain an understanding of the way the related TSFI is expected to behave. Similarly, the evaluator examines the relevant parts of the TOE design and security architecture documentation to gain an understanding of the way the related modules or subsystems of the TSF are expected to behave.

With an understanding of the expected behaviour, the evaluator examines the test plan to gain an understanding of the testing approach. In most cases, the testing approach will entail a TSFI being stimulated and its responses observed. Externally-visible functionality can be tested directly; however, in cases where functionality is not visible external to the TOE (for example, testing the residual information protection functionality), other means will need to be employed.

**14.2.2 Testing vs. alternate approaches to verify the expected behaviour of functionality**

In cases where it is impractical or inadequate to test specific functionality (where it provides no externally-visible TSFI), the test plan should identify the alternate approach to verify expected behaviour. It is the evaluator's responsibility to determine the suitability of the alternate approach. However, the following should be considered when assessing the suitability of alternate approaches:

- a) an analysis of the implementation representation to determine that the required behaviour should be exhibited by the TOE is an acceptable alternate approach. This could mean a code inspection for a software TOE or perhaps a chip mask inspection for a hardware TOE.
- b) it is acceptable to use evidence of developer integration or module testing, even if the claimed assurance requirements do not include availability of lower level descriptions of the TOE modules (e.g. Evaluation of sub-activity (ADV\_TDS.3)) or implementation (Implementation representation (ADV\_IMP)). If evidence of developer integration or module testing is used in verifying the expected behaviour of a security functionality, care should be given to confirm that the testing evidence reflects the current implementation of the TOE. If the subsystems or modules have been changed since testing occurred, evidence that the changes were tracked and addressed by analysis or further testing will usually be required.

It should be emphasised that supplementing the testing effort with alternate approaches should only be undertaken when both the developer and evaluator determine that there exists no other practical means to test the expected behaviour.

**14.2.3 Verifying the adequacy of tests**

Test pre-requisites are necessary to establish the required initial conditions for the test. They may be expressed in terms of parameters that must be set or in terms of test ordering in cases where the completion of one test establishes the necessary pre-requisites for another test. The evaluator must determine that the pre-requisites are complete and appropriate in that they will not bias the observed test results towards the expected test results.

The test steps and expected results specify the actions and parameters to be applied to the TSFI as well as how the expected results should be verified and what they are. The evaluator must



10837 determine that the test steps and expected results are consistent with the descriptions of the TSFI  
 10838 in the functional specification. This means that each characteristic of the TSFI behaviour explicitly  
 10839 described in the functional specification should have tests and expected results to verify that  
 10840 behaviour.

10841 The overall aim of this testing activity is to determine that each subsystem, module, and TSFI has  
 10842 been sufficiently tested against the behavioural claims in the functional specification, TOE design,  
 10843 and architecture description. At the higher assurance levels, testing also includes bounds testing  
 10844 and negative testing. The test procedures will provide insight as to how the TSFIs, modules, and  
 10845 subsystems have been exercised by the developer during testing. The evaluator uses this  
 10846 information when developing additional tests to independently test the TSF.

### 10847 **14.3 Coverage (ATE\_COV)**

#### 10848 **14.3.1 Evaluation of sub-activity (ATE\_COV.1)**

##### 10849 **14.3.1.1 Objectives**

10850 The objective of this sub-activity is to determine whether the developer has tested the TSFIs, and  
 10851 that the developer's test coverage evidence shows correspondence between the tests identified in  
 10852 the test documentation and the TSFIs described in the functional specification.

##### 10853 **14.3.1.2 Input**

10854 The evaluation evidence for this sub-activity is:

- 10855 a) the ST;
- 10856 b) the functional specification;
- 10857 c) the test documentation;
- 10858 d) the test coverage evidence.

##### 10859 **14.3.1.3 Application notes**

10860 The coverage analysis provided by the developer is required to show the correspondence between  
 10861 the tests provided as evaluation evidence and the functional specification. However, the coverage  
 10862 analysis need not demonstrate that all TSFI have been tested, or that all externally-visible  
 10863 interfaces to the TOE have been tested. Such shortcomings are considered by the evaluator during  
 10864 the independent testing (Evaluation of sub-activity (ATE\_IND.2)) sub-activity.

##### 10865 **14.3.1.4 Action ATE\_COV.1.1E**

10866 ISO/IEC 15408-3 ATE\_COV.1.1C: *The evidence of the test coverage shall show the correspondence*  
 10867 *between the tests in the test documentation and the TSFIs in the functional specification.*

##### 10868 **14.3.1.4.1 Work unit ATE\_COV.1-1**

10869 The evaluator **shall examine** the test coverage evidence to determine that the correspondence  
 10870 between the tests identified in the test documentation and the TSFIs described in the functional  
 10871 specification is accurate.

10872 Correspondence may take the form of a table or matrix. The coverage evidence required for this  
 10873 component will reveal the extent of coverage, rather than to show complete coverage. In cases

## ISO/IEC 18045:2008(E)

10874 where coverage is shown to be poor the evaluator should increase the level of independent testing  
10875 to compensate.

### 10876 **14.3.2 Evaluation of sub-activity (ATE\_COV.2)**

#### 10877 **14.3.2.1 Objectives**

10878 The objective of this sub-activity is to determine whether the developer has tested all of the TSFIs,  
10879 and that the developer's test coverage evidence shows correspondence between the tests  
10880 identified in the test documentation and the TSFIs described in the functional specification.

#### 10881 **14.3.2.2 Input**

- 10882 a) the ST;
- 10883 b) the functional specification;
- 10884 c) the test documentation;
- 10885 d) the test coverage analysis.

#### 10886 **14.3.2.3 Action ATE\_COV.2.1E**

10887 ISO/IEC 15408-3 ATE\_COV.2.1C: *The analysis of the test coverage shall demonstrate the*  
10888 *correspondence between the tests in the test documentation and the TSFIs in the functional*  
10889 *specification.*

##### 10890 **14.3.2.3.1 Work unit ATE\_COV.2-1**

10891 The evaluator **shall examine** the test coverage analysis to determine that the correspondence  
10892 between the tests in the test documentation and the interfaces in the functional specification is  
10893 accurate.

10894 A simple cross-table may be sufficient to show test correspondence. The identification of the tests  
10895 and the interfaces presented in the test coverage analysis has to be unambiguous.

10896 The evaluator is reminded that this does not imply that all tests in the test documentation must  
10897 map to interfaces in the functional specification.

##### 10898 **14.3.2.3.2 Work unit ATE\_COV.2-2**

10899 The evaluator **shall examine** the test plan to determine that the testing approach for each interface  
10900 demonstrates the expected behaviour of that interface.

10901 Guidance on this work unit can be found in:

- 10902 a) 14.2.1, Understanding the expected behaviour of the TOE
- 10903 b) 14.2.2, Testing vs. alternate approaches to verify the expected behaviour of  
10904 functionality

##### 10905 **14.3.2.3.3 Work unit ATE\_COV.2-3**

10906 The evaluator **shall examine** the test procedures to determine that the test prerequisites, test  
10907 steps and expected result(s) adequately test each interface.

- 10908 Guidance on this work units, as it pertains to the functional specification, can be found in:
- 10909 a) 14.2.3, Verifying the adequacy of tests
- 10910 ISO/IEC 15408-3 ATE\_COV.2.2C: *The analysis of the test coverage shall demonstrate that all TSFIs in*  
10911 *the functional specification have been tested.*
- 10912 **14.3.2.3.4 Work unit ATE\_COV.2-4**
- 10913 The evaluator **shall examine** the test coverage analysis to determine that the correspondence  
10914 between the interfaces in the functional specification and the tests in the test documentation is  
10915 complete.
- 10916 All TSFIs that are described in the functional specification have to be present in the test coverage  
10917 analysis and mapped to tests in order for completeness to be claimed, although exhaustive  
10918 specification testing of interfaces is not required. Incomplete coverage would be evident if an  
10919 interface was identified in the functional specification and no test was mapped to it.
- 10920 The evaluator is reminded that this does not imply that all tests in the test documentation must  
10921 map to interfaces in the functional specification.
- 10922 **14.3.3 Evaluation of sub-activity (ATE\_COV.3)**
- 10923 **14.3.3.1 Objectives**
- 10924 The objective of this sub-activity is to determine whether the developer has tested all of the TSFIs  
10925 exhaustively, and that the developer's test coverage evidence shows correspondence between the  
10926 tests identified in the test documentation and the TSFIs described in the functional specification.
- 10927 A particular objective of this component is to confirm that all parameters of all of the TSFIs have  
10928 been tested.
- 10929 **14.3.3.2 Input**
- 10930 The evaluation evidence for this sub-activity is:
- 10931 a) the ST;
- 10932 b) the functional specification;
- 10933 c) the test documentation;
- 10934 d) the test coverage analysis.
- 10935 **14.3.3.3 Action ATE\_COV.3.1E**
- 10936 ISO/IEC 15408-3 ATE\_COV.3.1C: *The analysis of the test coverage shall demonstrate the*  
10937 *correspondence between the tests in the test documentation and the TSFIs in the functional*  
10938 *specification.*
- 10939 **14.3.3.3.1 Work unit ATE\_COV.3-1**
- 10940 The evaluator **shall examine** the test coverage analysis to determine that the correspondence  
10941 between the tests in the test documentation and the interfaces in the functional specification is  
10942 accurate.

## ISO/IEC 18045:2008(E)

10943 A simple cross-table may be sufficient to show test correspondence. The identification of the tests  
10944 and the interfaces presented in the test coverage analysis has to be unambiguous.

10945 The evaluator is reminded that this does not imply that all tests in the test documentation must  
10946 map to interfaces in the functional specification.

### 10947 14.3.3.3.2 Work unit ATE\_COV.3-2

10948 The evaluator **shall examine** the test plan to determine that the testing approach for each interface  
10949 demonstrates the expected behaviour of that interface.

10950 Guidance on this work unit can be found in:

10951 a) 15.2.1 Understanding the expected behaviour of the TOE

10952 b) 15.2.2 Testing vs. alternate approaches to verify the expected behaviour of  
10953 functionality

### 10954 14.3.3.3.3 Work unit ATE\_COV.3-3

10955 The evaluator **shall examine** the test procedures to determine that the test prerequisites, test  
10956 steps and expected result(s) adequately test each interface.

10957 Guidance on this work unit, as it pertains to the functional specification, can be found in:

10958 a) 14.2.3 Verifying the adequacy of tests

10959 *ISO/IEC 15408-3 ATE\_COV.3.2C The analysis of the test coverage shall demonstrate that all*  
10960 *TSFIs in the functional specification have been completely tested.*

### 10961 14.3.3.3.4 Work unit ATE\_COV.3-4

10962 The evaluator **shall examine** the test coverage analysis to determine that the correspondence  
10963 between the interfaces in the functional specification and the tests in the test documentation is  
10964 complete.

10965 All TSFIs that are described in the functional specification have to be present in the test coverage  
10966 analysis and mapped to tests in order for completeness to be claimed. Exhaustive specification  
10967 testing of interfaces is required for this mapping. Incomplete coverage would be evident if an  
10968 interface was identified in the functional specification and no test was mapped to it.

10969 The evaluator is reminded that this does not imply that all tests in the test documentation must  
10970 map to interfaces in the functional specification.

### 10971 14.3.3.3.5 Work unit ATE\_COV.3-5

10972 The evaluator **shall examine** the test coverage analysis to determine that the correspondence  
10973 between the interfaces in the functional specification and the tests in the test documentation shows  
10974 that all TSFIs were tested completely.

10975 This means that the evaluator examines whether all aspects of purpose, method of use, parameters,  
10976 parameter descriptions, actions and error messages for all TSFIs present in the functional  
10977 specification are covered by the tests. Note that the level of detail present in the functional  
10978 specification depends on the component of ADV\_FSP chosen in the ST of the TOE.

10979 The evaluator may conclude that the higher level descriptions in the functional specification, like  
 10980 purpose or method of use, are implicitly covered, if coverage of lower level descriptions like  
 10981 parameters, parameter descriptions, actions and error messages are covered. Therefore in general  
 10982 it will only be necessary to confirm coverage on these lower levels.

10983 The evaluator is reminded that (for example) coverage of all parameters does not necessarily mean  
 10984 coverage of every possible value a parameter may allow. However every value for which a distinct  
 10985 qualitative behaviour of the TOE is expected, needs to be covered.

10986 As an example: If one of the parameters of a function call is a two byte value, which specifies the  
 10987 length of further parameters, only some typical values need to be tested. However the evaluator  
 10988 will make sure that some specific cases (like the value zero or the maximal value) will be covered.

10989 If the evaluator sees that a potential attacker might be able to invoke a TSFI with inconsistent  
 10990 parameter values (e. g. if one parameter specifies the length of a second parameter and it is  
 10991 possible to make the second parameter actually longer than the chosen value for the first  
 10992 parameter suggests) and this case is not covered by the developer's testing, the evaluator may  
 10993 decide either to test this during their activities in AVA\_VAN or to require the developer to provide  
 10994 coverage also for this case.

10995 Similar considerations as for parameters hold for error messages specified in the functional  
 10996 specification: Each error message, which belongs to a qualitatively distinct error case, needs to be  
 10997 covered by testing. Note, that there may be exceptions, for example error messages for errors,  
 10998 which cannot be provoked during testing. For such error messages other ways of coverage need to  
 10999 be found as discussed in 15.2.2, "Testing vs. alternate approaches to verify the expected behaviour  
 11000 of functionality".

11001 Note that also the developer is allowed to use such alternative approaches to testing (e. g. checking  
 11002 something in the source code) in the coverage table. Of course the evaluator has to examine in this  
 11003 case, if this use of an alternative approach is acceptable (usually only in cases where testing is  
 11004 practically impossible).

#### 11005 **14.4 Depth (ATE\_DPT)**

##### 11006 **14.4.1 Evaluation of sub-activity (ATE\_DPT.1)**

###### 11007 **14.4.1.1 Objectives**

11008 The objective of this sub-activity is to determine whether the developer has tested the TSF  
 11009 subsystems against the TOE design and the security architecture description.

###### 11010 **14.4.1.2 Input**

- 11011 a) the ST;
- 11012 b) the functional specification;
- 11013 c) the TOE design;
- 11014 d) the security architecture description;
- 11015 e) the test documentation;
- 11016 f) the depth of testing analysis.

## ISO/IEC 18045:2008(E)

### 11017 14.4.1.3 Action ATE\_DPT.1.1E

11018 ISO/IEC 15408-3 ATE\_DPT.1.1C: *The analysis of the depth of testing shall demonstrate the*  
11019 *correspondence between the tests in the test documentation and the TSF subsystems in the TOE*  
11020 *design.*

### 11021 14.4.1.3.1 Work unit ATE\_DPT.1-1

11022 The evaluator **shall examine** the depth of testing analysis to determine that the descriptions of the  
11023 behaviour of TSF subsystems and of their interactions is included within the test documentation.

11024 This work unit verifies the content of the correspondence between the tests and the descriptions in  
11025 the TOE design. In cases where the description of the TSF's architectural soundness (in Security  
11026 Architecture (ADV\_ARC)) cites specific mechanisms, this work unit also verifies the  
11027 correspondence between the tests and the descriptions of the behaviour of such mechanisms.

11028 A simple cross-table may be sufficient to show test correspondence. The identification of the tests  
11029 and the behaviour/interaction presented in the depth-of coverage analysis has to be unambiguous.

11030 When Evaluation of sub-activity (ATE\_DPT.1) is combined with a component of TOE design  
11031 (ADV\_TDS), which includes descriptions at the module level (e.g. Evaluation of sub-activity  
11032 (ADV\_TDS.3)), the level of detail needed to map the test cases to the behaviour of the subsystems  
11033 may require information from the module description to be used. This is because Evaluation of  
11034 sub-activity (ADV\_TDS.3) allows the description of details to be shifted from the subsystem level to  
11035 the module level, or even to omit the subsystems altogether.

11036 In any case, the required level of detail in the provided reference to the tested behaviour can be  
11037 defined as "the level of detail required for the description of subsystem behaviour as defined by  
11038 Evaluation of sub-activity (ADV\_TDS.2) (in particular work unit ADV\_TDS.2-4)". It states that a  
11039 detailed description of the behaviour typically discusses how the functionality is provided, in terms  
11040 of what key data and data structures represent; what control relationships exist within a subsystem  
11041 and how these elements work together to provide the SFR-enforcing behaviour.

11042 The evaluator is reminded that not all tests in the test documentation must map to a subsystem  
11043 behaviour or interaction description.

### 11044 14.4.1.3.2 Work unit ATE\_DPT.1-2

11045 The evaluator **shall examine** the test plan, test prerequisites, test steps and expected result(s) to  
11046 determine that the testing approach for the behaviour description demonstrates the behaviour of  
11047 that subsystem as described in the TOE design.

11048 Guidance on this work unit can be found in:

11049 a) 14.2.1, Understanding the expected behaviour of the TOE

11050 b) 14.2.2, Testing vs. alternate approaches to verify the expected behaviour of  
11051 functionality

11052 When Evaluation of sub-activity (ATE\_DPT.1) is combined with a component of TOE design  
11053 (ADV\_TDS), which includes descriptions at the module level (e.g. Evaluation of sub-activity  
11054 (ADV\_TDS.3)), the level of detail needed to map the test cases to the behaviour of the subsystems  
11055 may require information from the module description to be used. This is because Evaluation of  
11056 sub-activity (ADV\_TDS.3) allows the description of details to be shifted from the subsystem level to  
11057 the module level, or even to omit the subsystems altogether.

11058 In any case, the required level of detail in the provided reference to the tested behaviour can be  
 11059 defined as “the level of detail required for the description of subsystem behaviour as defined by  
 11060 Evaluation of sub-activity (ADV\_TDS.2) (in particular work unit ADV\_TDS.2-4)”. It states that a  
 11061 detailed description of the behaviour typically discusses how the functionality is provided, in terms  
 11062 of what key data and data structures represent; what control relationships exist within a subsystem  
 11063 and how these elements work together to provide the SFR-enforcing behaviour.

11064 If TSF subsystem interfaces are described, the behaviour of those subsystems may be tested  
 11065 directly from those interfaces. Otherwise, the behaviour of those subsystems is tested from the  
 11066 TSFI interfaces. Or a combination of the two may be employed. Whatever strategy is used the  
 11067 evaluator will consider its appropriateness for adequately testing the behaviour that is described  
 11068 in the TOE design.

#### 11069 **14.4.1.3.3 Work unit ATE\_DPT.1-3**

11070 The evaluator **shall examine** the test plan, test prerequisites, test steps and expected result(s) to  
 11071 determine that the testing approach for the behaviour description demonstrates the interactions  
 11072 among subsystems as described in the TOE design.

11073 While the previous work unit addresses behaviour of subsystems, this work unit addresses the  
 11074 interactions among subsystems.

11075 Guidance on this work unit can be found in:

11076 a) 14.2.1, Understanding the expected behaviour of the TOE

11077 b) 14.2.2, Testing vs. alternate approaches to verify the expected behaviour of  
 11078 functionality

11079 If TSF subsystem interfaces are described, the interactions with other subsystems may be tested  
 11080 directly from those interfaces. Otherwise, the interactions among subsystems must be inferred  
 11081 from the TSFI interfaces. Whatever strategy is used the evaluator will consider its appropriateness  
 11082 for adequately testing the interactions among subsystems that are described in the TOE design.

11083 ISO/IEC 15408-3 ATE\_DPT.1.2C: *The analysis of the depth of testing shall demonstrate that all TSF*  
 11084 *subsystems in the TOE design have been tested.*

#### 11085 **14.4.1.3.4 Work unit ATE\_DPT.1-4**

11086 The evaluator **shall examine** the test procedures to determine that all descriptions of TSF  
 11087 subsystem behaviour and interaction are tested.

11088 This work unit verifies the completeness of work unit ATE\_DPT.1-1. All descriptions of TSF  
 11089 subsystem behaviour and of interactions among TSF subsystems that are provided in the TOE  
 11090 design have to be tested. Incomplete depth of testing would be evident if a description of TSF  
 11091 subsystem behaviour or of interactions among TSF subsystems was identified in the TOE design  
 11092 and no tests could be attributed to it.

11093 When Evaluation of sub-activity (ATE\_DPT.1) is combined with a component of TOE design  
 11094 (ADV\_TDS), which includes descriptions at the module level (e.g. Evaluation of sub-activity  
 11095 (ADV\_TDS.3)), the level of detail needed to map the test cases to the behaviour of the subsystems  
 11096 may require information from the module description to be used. This is because Evaluation of  
 11097 sub-activity (ADV\_TDS.3) allows the description of details to be shifted from the subsystem level to  
 11098 the module level, or even to omit the subsystems altogether.

11099 In any case, the required level of detail in the provided reference to the tested behaviour can be  
 11100 defined as “the level of detail required for the description of subsystem behaviour as defined by

## ISO/IEC 18045:2008(E)

11101 Evaluation of sub-activity (ADV\_TDS.2) (in particular work unit ADV\_TDS.2-4)". It states that a  
11102 detailed description of the behaviour typically discusses how the functionality is provided, in terms  
11103 of what key data and data structures represent; what control relationships exist within a subsystem  
11104 and how these elements work together to provide the SFR-enforcing behaviour.

11105 The evaluator is reminded that this does not imply that all tests in the test documentation must  
11106 map to the subsystem behaviour or interaction description in the TOE design.

### 11107 **14.4.2 Evaluation of sub-activity (ATE\_DPT.2)**

#### 11108 **14.4.2.1 Objectives**

11109 The objective of this sub-activity is to determine whether the developer has tested all the TSF  
11110 subsystems and SFR-enforcing modules against the TOE design and the security architecture  
11111 description.

#### 11112 **14.4.2.2 Input**

- 11113 a) the ST;
- 11114 b) the functional specification;
- 11115 c) the TOE design;
- 11116 d) the security architecture description;
- 11117 e) the test documentation;
- 11118 f) the depth of testing analysis.

#### 11119 **14.4.2.3 Action ATE\_DPT.2.1E**

11120 ISO/IEC 15408-3 ATE\_DPT.2.1C: *The analysis of the depth of testing shall demonstrate the*  
11121 *correspondence between the tests in the test documentation and the TSF subsystems and SFR-*  
11122 *enforcing modules in the TOE design.*

#### 11123 **14.4.2.3.1 Work unit ATE\_DPT.2-1**

11124 The evaluator **shall examine** the depth of testing analysis to determine that descriptions of the  
11125 behaviour of TSF subsystems and of their interactions are included within the test documentation.

11126 This work unit verifies the content of the correspondence between the tests and the descriptions in  
11127 the TOE design. In cases where the description of the TSF's architectural soundness (in Security  
11128 Architecture (ADV\_ARC)) cites specific mechanisms, this work unit also verifies the  
11129 correspondence between the tests and the descriptions of the behaviour of such mechanisms.

11130 A simple cross-table may be sufficient to show test correspondence. The identification of the tests  
11131 and the behaviour/interaction presented in the depth-of coverage analysis has to be unambiguous.

11132 The evaluator is reminded that not all tests in the test documentation must map to a subsystem  
11133 behaviour or interaction description.



11134 **14.4.2.3.2 Work unit ATE\_DPT.2-2**

11135 The evaluator *shall examine* the test plan, test prerequisites, test steps and expected result(s) to  
 11136 determine that the testing approach for the behaviour description demonstrates the behaviour of  
 11137 that subsystem as described in the TOE design.

11138 Guidance on this work unit can be found in:

11139 a) 14.2.1, Understanding the expected behaviour of the TOE

11140 b) 14.2.2, Testing vs. alternate approaches to verify the expected behaviour of  
 11141 functionality

11142 If TSF subsystem interfaces are described, the behaviour of those subsystems may be tested  
 11143 directly from those interfaces. Otherwise, the behaviour of those subsystems is tested from the  
 11144 TSFI interfaces. Or a combination of the two may be employed. Whatever strategy is used the  
 11145 evaluator will consider its appropriateness for adequately testing the behaviour that is described  
 11146 in the TOE design.

11147 **14.4.2.3.3 Work unit ATE\_DPT.2-3**

11148 The evaluator *shall examine* the test plan, test prerequisites, test steps and expected result(s) to  
 11149 determine that the testing approach for the behaviour description demonstrates the interactions  
 11150 among subsystems as described in the TOE design.

11151 While the previous work unit addresses behaviour of subsystems, this work unit addresses the  
 11152 interactions among subsystems.

11153 Guidance on this work unit can be found in:

11154 a) 14.2.1, Understanding the expected behaviour of the TOE

11155 b) 14.2.2, Testing vs. alternate approaches to verify the expected behaviour of  
 11156 functionality

11157 If TSF subsystem interfaces are described, the interactions with other subsystems may be tested  
 11158 directly from those interfaces. Otherwise, the interactions among subsystems must be inferred  
 11159 from the TSFI interfaces. Whatever strategy is used the evaluator will consider its appropriateness  
 11160 for adequately testing the interactions among subsystems that are described in the TOE design.

11161 **14.4.2.3.4 Work unit ATE\_DPT.2-4**

11162 The evaluator *shall examine* the depth of testing analysis to determine that the interfaces of SFR-  
 11163 enforcing modules are included within the test documentation.

11164 This work unit verifies the content of the correspondence between the tests and the descriptions in  
 11165 the TOE design. In cases where the description of the TSF's architectural soundness (in Security  
 11166 Architecture (ADV\_ARC)) cites specific mechanisms at the modular level, this work unit also  
 11167 verifies the correspondence between the tests and the descriptions of the behaviour of such  
 11168 mechanisms.

11169 A simple cross-table may be sufficient to show test correspondence. The identification of the tests  
 11170 and the SFR-enforcing modules presented in the depth-of coverage analysis has to be unambiguous.

11171 The evaluator is reminded that not all tests in the test documentation must map to the interfaces of  
 11172 SFR-enforcing modules.

11173 **14.4.2.3.5 Work unit ATE\_DPT.2-5**

11174 The evaluator **shall examine** the test plan, test prerequisites, test steps and expected result(s) to  
11175 determine that the testing approach for each SFR-enforcing module interface demonstrates the  
11176 expected behaviour of that interface.

11177 While work unit ATE\_DPT.2-2 addresses expected behaviour of subsystems, this work unit  
11178 addresses expected behaviour of the SFR-enforcing module interfaces that are covered by  
11179 ATE\_DPT.2-4.

11180 Guidance on this work unit can be found in:

11181 a) 14.2.1, Understanding the expected behaviour of the TOE

11182 b) 14.2.2, Testing vs. alternate approaches to verify the expected behaviour of  
11183 functionality

11184 Testing of an interface may be performed directly at that interface, or at the external interfaces, or  
11185 a combination of both. Whatever strategy is used the evaluator will consider its appropriateness  
11186 for adequately testing the interfaces. Specifically, the evaluator determines whether testing at the  
11187 internal interfaces is necessary or whether these internal interfaces can be adequately tested  
11188 (albeit implicitly) by exercising the external interfaces. This determination is left to the evaluator,  
11189 as is its justification.

11190 ISO/IEC 15408-3 ATE\_DPT.2.2C: *The analysis of the depth of testing shall demonstrate that all TSF*  
11191 *subsystems in the TOE design have been tested.*

11192 **14.4.2.3.6 Work unit ATE\_DPT.2-6**

11193 The evaluator **shall examine** the test procedures to determine that all descriptions of TSF  
11194 subsystem behaviour and interaction are tested.

11195 This work unit verifies the completeness of work unit ATE\_DPT.2-1. All descriptions of TSF  
11196 subsystem behaviour and of interactions among TSF subsystems that are provided in the TOE  
11197 design have to be tested. Incomplete depth of testing would be evident if a description of TSF  
11198 subsystem behaviour or of interactions among TSF subsystems was identified in the TOE design  
11199 and no tests could be attributed to it.

11200 The evaluator is reminded that this does not imply that all tests in the test documentation must  
11201 map to the subsystem behaviour or interaction description in the TOE design.

11202 ISO/IEC 15408-3 ATE\_DPT.2.3C: *The analysis of the depth of testing shall demonstrate that the SFR-*  
11203 *enforcing modules in the TOE design have been tested.*

11204 **14.4.2.3.7 Work unit ATE\_DPT.2-7**

11205 The evaluator **shall examine** the test procedures to determine that all interfaces of SFR-enforcing  
11206 modules are tested.

11207 This work unit verifies the completeness of work unit ATE\_DPT.2-4. All interfaces of SFR-enforcing  
11208 modules that are provided in the TOE design have to be tested. Incomplete depth of testing would  
11209 be evident if any interface of any SFR-enforcing modules was identified in the TOE design and no  
11210 tests could be attributed to it.

11211 The evaluator is reminded that this does not imply that all tests in the test documentation must  
11212 map to an interface of an SFR-enforcing module in the TOE design.

|       |                                                                                                            |
|-------|------------------------------------------------------------------------------------------------------------|
| 11213 | <b>14.4.3 Evaluation of sub-activity (ATE_DPT.3)</b>                                                       |
| 11214 | <b>14.4.3.1 Objectives</b>                                                                                 |
| 11215 | The objective of this sub-activity is to determine whether the developer has tested the all the TSF        |
| 11216 | subsystems and modules against the TOE design and the security architecture description.                   |
| 11217 | <b>14.4.3.2 Input</b>                                                                                      |
| 11218 | a) the ST;                                                                                                 |
| 11219 | b) the functional specification;                                                                           |
| 11220 | c) the TOE design;                                                                                         |
| 11221 | d) the security architecture description;                                                                  |
| 11222 | e) the test documentation;                                                                                 |
| 11223 | f) the depth of testing analysis.                                                                          |
| 11224 | <b>14.4.3.3 Action ATE_DPT.3.1E</b>                                                                        |
| 11225 | ISO/IEC 15408-3 ATE_DPT.3.1C: <i>The analysis of the depth of testing shall demonstrate the</i>            |
| 11226 | <i>correspondence between the tests in the test documentation and the TSF subsystems and modules in</i>    |
| 11227 | <i>the TOE design.</i>                                                                                     |
| 11228 | <b>14.4.3.3.1 Work unit ATE_DPT.3-1</b>                                                                    |
| 11229 | The evaluator <b>shall examine</b> the depth of testing analysis to determine that descriptions of the     |
| 11230 | behaviour of TSF subsystems and of their interactions are included within the test documentation.          |
| 11231 | This work unit verifies the content of the correspondence between the tests and the descriptions in        |
| 11232 | the TOE design. A simple cross-table may be sufficient to show test correspondence. The                    |
| 11233 | identification of the tests and the behaviour/interaction presented in the depth-of coverage               |
| 11234 | analysis has to be unambiguous.                                                                            |
| 11235 | The evaluator is reminded that not all tests in the test documentation must map to a subsystem             |
| 11236 | behaviour or interaction description.                                                                      |
| 11237 | <b>14.4.3.3.2 Work unit ATE_DPT.3-2</b>                                                                    |
| 11238 | The evaluator <b>shall examine</b> the test plan, test prerequisites, test steps and expected result(s) to |
| 11239 | determine that the testing approach for the behaviour description demonstrates the behaviour of            |
| 11240 | that subsystem as described in the TOE design.                                                             |
| 11241 | Guidance on this work unit can be found in:                                                                |
| 11242 | a) 14.2.1, Understanding the expected behaviour of the TOE                                                 |
| 11243 | b) 14.2.2, Testing vs. alternate approaches to verify the expected behaviour of                            |
| 11244 | functionality                                                                                              |

## ISO/IEC 18045:2008(E)

11245 If TSF subsystem interfaces are provided, the behaviour of those subsystems may be performed  
11246 directly from those interfaces. Otherwise, the behaviour of those subsystems is tested from the  
11247 TSFI interfaces. Or a combination of the two may be employed. Whatever strategy is used the  
11248 evaluator will consider its appropriateness for adequately testing the behaviour that is described  
11249 in the TOE design.

### 11250 14.4.3.3.3 Work unit ATE\_DPT.3-3

11251 The evaluator **shall examine** the test plan, test prerequisites, test steps and expected result(s) to  
11252 determine that the testing approach for the behaviour description demonstrates the interactions  
11253 among subsystems as described in the TOE design.

11254 Guidance on this work unit can be found in:

11255 a) 14.2.1, Understanding the expected behaviour of the TOE

11256 b) 14.2.2, Testing vs. alternate approaches to verify the expected behaviour of  
11257 functionality

11258 While the previous work unit addresses behaviour of subsystems, this work unit addresses the  
11259 interactions among subsystems.

11260 If TSF subsystem interfaces are provided, the interactions with other subsystems may be  
11261 performed directly from those interfaces. Otherwise, the interactions among subsystems must be  
11262 inferred from the TSFI interfaces. Whatever strategy is used the evaluator will consider its  
11263 appropriateness for adequately testing the interactions among subsystems that are described in  
11264 the TOE design.

### 11265 14.4.3.3.4 Work unit ATE\_DPT.3-4

11266 The evaluator **shall examine** the depth of testing analysis to determine that the interfaces of TSF  
11267 modules are included within the test documentation.

11268 This work unit verifies the content of the correspondence between the tests and the descriptions in  
11269 the TOE design. A simple cross-table may be sufficient to show test correspondence. The  
11270 identification of the tests and the behaviour/interaction presented in the depth-of coverage  
11271 analysis has to be unambiguous.

11272 The evaluator is reminded that not all tests in the test documentation must map to a subsystem  
11273 behaviour or interaction description.

### 11274 14.4.3.3.5 Work unit ATE\_DPT.3-5

11275 The evaluator **shall examine** the test plan, test prerequisites, test steps and expected result(s) to  
11276 determine that the testing approach for each TSF module interface demonstrates the expected  
11277 behaviour of that interface.

11278 Guidance on this work unit can be found in:

11279 a) 14.2.1, Understanding the expected behaviour of the TOE

11280 b) 14.2.2, Testing vs. alternate approaches to verify the expected behaviour of  
11281 functionality

11282 Testing of an interface may be performed directly at that interface, or at the external interfaces, or  
11283 a combination of both. Whatever strategy is used the evaluator will consider its appropriateness

11284 for adequately testing the interfaces. Specifically the evaluator determines whether testing at the  
11285 internal interfaces is necessary or whether these internal interfaces can be adequately tested  
11286 (albeit implicitly) by exercising the external interfaces. This determination is left to the evaluator,  
11287 as is its justification.

11288 ISO/IEC 15408-3 ATE\_DPT.3.2C: *The analysis of the depth of testing shall demonstrate that all TSF*  
11289 *subsystems in the TOE design have been tested.*

#### 11290 **14.4.3.3.6 Work unit ATE\_DPT.3-6**

11291 The evaluator **shall examine** the test procedures to determine that all descriptions of TSF  
11292 subsystem behaviour and interaction are tested.

11293 This work unit verifies the completeness of work unit ATE\_DPT.3-1. All descriptions of TSF  
11294 subsystem behaviour and of interactions among TSF subsystems that are provided in the TOE  
11295 design have to be tested. Incomplete depth of testing would be evident if a description of TSF  
11296 subsystem behaviour or of interactions among TSF subsystems was identified in the TOE design  
11297 and no tests could be attributed to it.

11298 The evaluator is reminded that this does not imply that all tests in the test documentation must  
11299 map to the subsystem behaviour or interaction description in the TOE design.

11300 ISO/IEC 15408-3 ATE\_DPT.3.3C: *The analysis of the depth of testing shall demonstrate that all TSF*  
11301 *modules in the TOE design have been tested.*

#### 11302 **14.4.3.3.7 Work unit ATE\_DPT.3-7**

11303 The evaluator **shall examine** the test procedures to determine that all interfaces of all TSF modules  
11304 are tested.

11305 This work unit verifies the completeness of work unit ATE\_DPT.3-4. All interfaces of TSF modules  
11306 that are provided in the TOE design have to be tested. Incomplete depth of testing would be  
11307 evident if any interface of any TSF module was identified in the TOE design and no tests could be  
11308 attributed to it.

11309 The evaluator is reminded that this does not imply that all tests in the test documentation must  
11310 map to an interface of a TSF module in the TOE design.

#### 11311 **14.4.4 Evaluation of sub-activity (ATE\_DPT.4)**

11312 There is no general guidance; the scheme should be consulted for guidance on this sub-activity.

### 11313 **14.5 Functional tests (ATE\_FUN)**

#### 11314 **14.5.1 Evaluation of sub-activity (ATE\_FUN.1)**

##### 11315 **14.5.1.1 Objectives**

11316 The objective of this sub-activity is to determine whether the developer correctly performed and  
11317 documented the tests in the test documentation.

##### 11318 **14.5.1.2 Input**

11319 The evaluation evidence for this sub-activity is:

11320 a) the ST;

## ISO/IEC 18045:2008(E)

11321 b) the functional specification;

11322 c) the test documentation.

### 11323 14.5.1.3 Application notes

11324 The extent to which the test documentation is required to cover the TSF is dependent upon the  
11325 coverage assurance component.

11326 For the developer tests provided, the evaluator determines whether the tests are repeatable, and  
11327 the extent to which the developer's tests can be used for the evaluator's independent testing effort.  
11328 Any TSFI for which the developer's test results indicate that it might not perform as specified  
11329 should be tested independently by the evaluator to determine whether or not it does.

### 11330 14.5.1.4 Action ATE\_FUN.1.1E

11331 ISO/IEC 15408-3 ATE\_FUN.1.1C: *The test documentation shall consist of test plans, expected test*  
11332 *results and actual test results.*

#### 11333 14.5.1.4.1 Work unit ATE\_FUN.1-1

11334 The evaluator **shall check** that the test documentation includes test plans, expected test results and  
11335 actual test results.

11336 The evaluator checks that test plans, expected tests results and actual test results are included in  
11337 the test documentation.

11338 ISO/IEC 15408-3 ATE\_FUN.1.2C: *The test plans shall identify the tests to be performed and describe*  
11339 *the scenarios for performing each test. These scenarios shall include any ordering dependencies on the*  
11340 *results of other tests.*

#### 11341 14.5.1.4.2 Work unit ATE\_FUN.1-2

11342 The evaluator **shall examine** the test plan to determine that it describes the scenarios for  
11343 performing each test.

11344 The evaluator determines that the test plan provides information about the test configuration  
11345 being used: both on the configuration of the TOE and on any test equipment being used. This  
11346 information should be detailed enough to ensure that the test configuration is reproducible.

11347 The evaluator also determines that the test plan provides information about how to execute the  
11348 test: any necessary automated set-up procedures (and whether they require privilege to run),  
11349 inputs to be applied, how these inputs are applied, how output is obtained, any automated clean-up  
11350 procedures (and whether they require privilege to run), etc. This information should be detailed  
11351 enough to ensure that the test is reproducible.

11352 The evaluator may wish to employ a sampling strategy when performing this work unit.

#### 11353 14.5.1.4.3 Work unit ATE\_FUN.1-3

11354 The evaluator **shall examine** the test plan to determine that the TOE test configuration is  
11355 consistent with the ST.

11356 The TOE referred to in the developer's test plan should have the same unique reference as  
11357 established by the CM capabilities (ALC\_CMC) sub-activities and identified in the ST introduction.

11358 It is possible for the ST to specify more than one configuration for evaluation. The evaluator  
 11359 verifies that all test configurations identified in the developer test documentation are consistent  
 11360 with the ST. For example, the ST might define configuration options that must be set, which could  
 11361 have an impact upon what constitutes the TOE by including or excluding additional portions. The  
 11362 evaluator verifies that all such variations of the TOE are considered.

11363 The evaluator should consider the security objectives for the operational environment described in  
 11364 the ST that may apply to the test environment. There may be some objectives for the operational  
 11365 environment that do not apply to the test environment. For example, an objective about user  
 11366 clearances may not apply; however, an objective about a single point of connection to a network  
 11367 would apply.

11368 The evaluator may wish to employ a sampling strategy when performing this work unit.

11369 If this work unit is applied to a component TOE that might be used/integrated in a composed TOE  
 11370 (see Class ACO: Composition), the following will apply. In the instances that the component TOE  
 11371 under evaluation depends on other components in the operational environment to support their  
 11372 operation, the developer may wish to consider using the other component(s) that will be used in  
 11373 the composed TOE to fulfil the requirements of the operational environment as one of the test  
 11374 configurations. This will reduce the amount an additional testing that will be required for the  
 11375 composed TOE evaluation.

#### 11376 14.5.1.4.4 Work unit ATE\_FUN.1-4

11377 The evaluator **shall examine** the test plans to determine that sufficient instructions are provided  
 11378 for any ordering dependencies.

11379 Some steps may have to be performed to establish initial conditions. For example, user accounts  
 11380 need to be added before they can be deleted. An example of ordering dependencies on the results  
 11381 of other tests is the need to perform actions in a test that will result in the generation of audit  
 11382 records, before performing a test to consider the searching and sorting of those audit records.  
 11383 Another example of an ordering dependency would be where one test case generates a file of data  
 11384 to be used as input for another test case.

11385 The evaluator may wish to employ a sampling strategy when performing this work unit.

11386 ISO/IEC 15408-3 ATE\_FUN.1.3C: *The expected test results shall show the anticipated outputs from a*  
 11387 *successful execution of the tests.*

#### 11388 14.5.1.4.5 Work unit ATE\_FUN.1-5

11389 The evaluator **shall examine** the test documentation to determine that all expected tests results  
 11390 are included.

11391 The expected test results are needed to determine whether or not a test has been successfully  
 11392 performed. Expected test results are sufficient if they are unambiguous and consistent with  
 11393 expected behaviour given the testing approach.

11394 The evaluator may wish to employ a sampling strategy when performing this work unit.

11395 ISO/IEC 15408-3 ATE\_FUN.1.4C: *The actual test results shall be consistent with the expected test*  
 11396 *results.*

#### 11397 14.5.1.4.6 Work unit ATE\_FUN.1-6

11398 The evaluator **shall check** that the actual test results in the test documentation are consistent with  
 11399 the expected test results in the test documentation.

## ISO/IEC 18045:2008(E)

11400 A comparison of the actual and expected test results provided by the developer will reveal any  
11401 inconsistencies between the results. It may be that a direct comparison of actual results cannot be  
11402 made until some data reduction or synthesis has been first performed. In such cases, the  
11403 developer's test documentation should describe the process to reduce or synthesise the actual data.

11404 For example, the developer may need to test the contents of a message buffer after a network  
11405 connection has occurred to determine the contents of the buffer. The message buffer will contain a  
11406 binary number. This binary number would have to be converted to another form of data  
11407 representation in order to make the test more meaningful. The conversion of this binary  
11408 representation of data into a higher-level representation will have to be described by the developer  
11409 in enough detail to allow an evaluator to perform the conversion process (i.e. synchronous or  
11410 asynchronous transmission, number of stop bits, parity, etc.).

11411 It should be noted that the description of the process used to reduce or synthesise the actual data is  
11412 used by the evaluator not to actually perform the necessary modification but to assess whether this  
11413 process is correct. It is up to the developer to transform the expected test results into a format that  
11414 allows an easy comparison with the actual test results.

11415 The evaluator may wish to employ a sampling strategy when performing this work unit.

### 11416 14.5.1.4.7 Work unit ATE\_FUN.1-7

11417 The evaluator **shall report** the developer testing effort, outlining the testing approach,  
11418 configuration, depth and results.

11419 The developer testing information recorded in the ETR allows the evaluator to convey the overall  
11420 testing approach and effort expended on the testing of the TOE by the developer. The intent of  
11421 providing this information is to give a meaningful overview of the developer testing effort. It is not  
11422 intended that the information regarding developer testing in the ETR be an exact reproduction of  
11423 specific test steps or results of individual tests. The intention is to provide enough detail to allow  
11424 other evaluators and evaluation authorities to gain some insight about the developer's testing  
11425 approach, amount of testing performed, TOE test configurations, and the overall results of the  
11426 developer testing.

11427 Information that would typically be found in the ETR subclause regarding the developer testing  
11428 effort is:

11429 a) TOE test configurations. The particular configurations of the TOE that were tested,  
11430 including whether any privileged code was required to set up the test or clean up  
11431 afterwards;

11432 b) testing approach. An account of the overall developer testing strategy employed;

11433 c) testing results. A description of the overall developer testing results.

11434 This list is by no means exhaustive and is only intended to provide some context as to the type of  
11435 information that should be present in the ETR concerning the developer testing effort.

### 11436 14.5.2 Evaluation of sub-activity (ATE\_FUN.2)

#### 11437 14.5.2.1 Objectives

11438 The objective of this sub-activity is to determine whether the developer correctly performed and  
11439 documented the tests in the test documentation and to ensure that testing is structured such as to  
11440 avoid circular arguments about the correctness of the interfaces being tested.



11441 **14.5.2.2 Input**

11442 The evaluation evidence for this sub-activity is:

- 11443 a) the ST;
- 11444 b) the functional specification;
- 11445 c) the test documentation.

11446 **14.5.2.3 Application notes**

11447 Although the test procedures may state pre-requisite initial test conditions in terms of ordering of  
 11448 tests, they may not provide a rationale for the ordering. An analysis of test ordering, which  
 11449 provides this rationale, is an important factor in determining the adequacy of testing, as there is a  
 11450 possibility of faults being concealed by the ordering of tests.

11451 **14.5.2.4 Action ATE\_FUN.2.1E**

11452 ISO/IEC 15408-3 ATE\_FUN.2.1C *The test documentation shall consist of test plans, expected test*  
 11453 *results and actual test results.*

11454 **14.5.2.4.1 Work unit ATE\_FUN.2-1**

11455 The evaluator **shall check** that the test documentation includes test plans, expected test results and  
 11456 actual test results.

11457 The evaluator checks that test plans, expected tests results and actual test results are included in  
 11458 the test documentation.

11459 ISO/IEC 15408-3 ATE\_FUN.2.2C *The test plans shall identify the tests to be performed and describe*  
 11460 *the scenarios for performing each test. These scenarios shall include any ordering dependencies on the*  
 11461 *results of other tests.*

11462 **14.5.2.4.2 Work unit ATE\_FUN.2-2**

11463 The evaluator **shall examine** the test plan to determine that it describes the scenarios for  
 11464 performing each test.

11465 The evaluator determines that the test plan provides information about the test configuration  
 11466 being used: both on the configuration of the TOE and on any test equipment being used. This  
 11467 information should be detailed enough to ensure that the test configuration is reproducible.

11468 The evaluator also determines that the test plan provides information about how to execute the  
 11469 test: any necessary automated set-up procedures (and whether they require privilege to run),  
 11470 inputs to be applied, how these inputs are applied, how output is obtained, any automated clean-up  
 11471 procedures (and whether they require privilege to run), etc. This information should be detailed  
 11472 enough to ensure that the test is reproducible.

11473 The evaluator may wish to employ a sampling strategy when performing this work unit.

11474 **14.5.2.4.3 Work unit ATE\_FUN.2-3**

11475 The evaluator **shall examine** the test plan to determine that the TOE test configuration is  
 11476 consistent with the ST.

## ISO/IEC 18045:2008(E)

11477 The TOE referred to in the developer's test plan should have the same unique reference as  
11478 established by the CM capabilities (ALC\_CMC) sub-activities and identified in the ST introduction.

11479 It is possible for the ST to specify more than one configuration for evaluation. The evaluator  
11480 verifies that all test configurations identified in the developer test documentation are consistent  
11481 with the ST. For example, the ST might define configuration options that must be set, which could  
11482 have an impact upon what constitutes the TOE by including or excluding additional portions. The  
11483 evaluator verifies that all such variations of the TOE are considered.

11484 The evaluator should consider the security objectives for the operational environment described in  
11485 the ST that may apply to the test environment. There may be some objectives for the operational  
11486 environment that do not apply to the test environment. For example, an objective about user  
11487 clearances may not apply; however, an objective about a single point of connection to a network  
11488 would apply.

11489 The evaluator may wish to employ a sampling strategy when performing this work unit.

11490 If this work unit is applied to a component TOE that might be used/integrated in a composed TOE  
11491 (see Class ACO: Composition), the following will apply. In the instances that the component TOE  
11492 under evaluation depends on other components in the operational environment to support their  
11493 operation, the developer may wish to consider using the other component(s) that will be used in  
11494 the composed TOE to fulfil the requirements of the operational environment as one of the test  
11495 configurations. This will reduce the amount of additional testing that will be required for the  
11496 composed TOE evaluation.

### 11497 14.5.2.4.4 Work unit ATE\_FUN.2-4

11498 The evaluator *shall examine* the test plans to determine that sufficient instructions are provided  
11499 for any ordering dependencies.

11500 Some steps may have to be performed to establish initial conditions. For example, user accounts  
11501 need to be added before they can be deleted. An example of ordering dependencies on the results  
11502 of other tests is the need to perform actions in a test that will result in the generation of audit  
11503 records, before performing a test to consider the searching and sorting of those audit records.  
11504 Another example of an ordering dependency would be where one test case generates a file of data  
11505 to be used as input for another test case.

11506 The evaluator may wish to employ a sampling strategy when performing this work unit.

11507 ATE\_FUN.2.3C *The expected test results shall show the anticipated outputs from a successful*  
11508 *execution of the tests.*

### 11509 14.5.2.4.5 Work unit ATE\_FUN.2-5

11510 The evaluator *shall examine* the test documentation to determine that all expected tests results  
11511 are included.

11512 The expected test results are needed to determine whether or not a test has been successfully  
11513 performed. Expected test results are sufficient if they are unambiguous and consistent with  
11514 expected behaviour given the testing approach.

11515 The evaluator may wish to employ a sampling strategy when performing this work unit.

11516 ATE\_FUN.2.4C *The actual test results shall be consistent with the expected test results.*

### 11517 14.5.2.4.6 Work unit ATE\_FUN.2-6

11518 The evaluator *shall check* that the actual test results in the test documentation are consistent with  
11519 the expected test results in the test documentation.

11520 A comparison of the actual and expected test results provided by the developer will reveal any  
 11521 inconsistencies between the results. It may be that a direct comparison of actual results cannot be  
 11522 made until some data reduction or synthesis has been first performed. In such cases, the  
 11523 developer's test documentation should describe the process to reduce or synthesise the actual data.

11524 For example, the developer may need to test the contents of a message buffer after a network  
 11525 connection has occurred to determine the contents of the buffer. The message buffer will contain a  
 11526 binary number. This binary number would have to be converted to another form of data  
 11527 representation in order to make the test more meaningful. The conversion of this binary  
 11528 representation of data into a higher-level representation will have to be described by the developer  
 11529 in enough detail to allow an evaluator to perform the conversion process (i.e. synchronous or  
 11530 asynchronous transmission, number of stop bits, parity, etc.).

11531 It should be noted that the description of the process used to reduce or synthesise the actual data is  
 11532 used by the evaluator not to actually perform the necessary modification but to assess whether this  
 11533 process is correct. It is up to the developer to transform the expected test results into a format that  
 11534 allows an easy comparison with the actual test results.

11535 The evaluator may wish to employ a sampling strategy when performing this work unit.

#### 11536 14.5.2.4.7 Work unit ATE\_FUN.2-7

11537 The evaluator **shall report** the developer testing effort, outlining the testing approach,  
 11538 configuration, depth and results.

11539 The developer testing information recorded in the ETR allows the evaluator to convey the overall  
 11540 testing approach and effort expended on the testing of the TOE by the developer. The intent of  
 11541 providing this information is to give a meaningful overview of the developer testing effort. It is not  
 11542 intended that the information regarding developer testing in the ETR be an exact reproduction of  
 11543 specific test steps or results of individual tests. The intention is to provide enough detail to allow  
 11544 other evaluators and evaluation authorities to gain some insight about the developer's testing  
 11545 approach, amount of testing performed, TOE test configurations, and the overall results of the  
 11546 developer testing.

11547 Information that would typically be found in the ETR section regarding the developer testing effort  
 11548 is:

11549 a) TOE test configurations. The particular configurations of the TOE that were tested,  
 11550 including whether any privileged code was required to set up the test or clean up  
 11551 afterwards;

11552 b) testing approach. An account of the overall developer testing strategy employed;

11553 c) testing results. A description of the overall developer testing results.

11554 This list is by no means exhaustive and is only intended to provide some context as to the type of  
 11555 information that should be present in the ETR concerning the developer testing effort.

11556 ATE\_FUN.2.5C *The test documentation shall include an analysis of the test procedure ordering*  
 11557 *dependencies.*

#### 11558 14.5.2.4.8 Work unit ATE\_FUN.2-8

11559 The evaluator **shall examine** the analysis of the test procedure ordering dependencies to  
 11560 determine that a sufficient justification for the chosen ordering of test cases is given.

## ISO/IEC 18045:2008(E)

11561 Usually the evaluator will generate a table of all cases, where the test documentation requires a  
11562 certain ordering of the tests and will then examine if sufficient justification is given in any case,  
11563 why testing in this ordering is adequate and sufficient.

11564 As an example we assume that the TSF provide a random number generator, which needs to be  
11565 initialised (for example with an adequate seed) before random numbers of a specified quality can  
11566 be generated. In this case the evaluator will consider the following question:

11567 Does the test documentation only describe an ordering of tests, where the initialisation is done  
11568 before calling the function to generate a random number?

11569 In this case the justification needs to show, why the developer expects, that in the intended  
11570 environment of the TOE the random number function will not be called without initialisation of the  
11571 random number generator.

11572 If for example the user guidance documentation includes a clear instruction that the random  
11573 number generator needs to be initialised adequately before being called, this may be considered  
11574 adequate as a justification. Note that the question of whether it can be plausibly assumed that users  
11575 will follow such instruction is covered by the evaluation activities for the classes ASE and AGD and  
11576 needs not to be re-examined here.

11577 If, on the other hand, the TOE provides an authentication protocol, which implicitly uses random  
11578 numbers provided by the random number generator, and an attacker can therefore "call" the  
11579 random number generator implicitly by simply trying to authenticate himself, and if neither the  
11580 TOE nor the environment prevent an attacker from doing this even before the random number  
11581 generator is initialised, a test case needs to show, what happens in such situation.

11582 If, for example, instead of returning a "bad" random number, the random number function would  
11583 return an error, when called without proper initialisation, it would be much better to include a test  
11584 showing this secure behaviour instead of trying to justify why the functions are only tested in the  
11585 usual order.

11586 Note: Of course even without ATE\_FUN.2 an evaluator would be expected to look for potential  
11587 vulnerabilities like the one described above. However, ATE\_FUN.2.5C adds assurance by requiring  
11588 the developer to give a systematic justification, why their chosen order of test cases doesn't hide  
11589 such potential failures of security functions.

### 11590 **14.6 Independent testing (ATE\_IND)**

#### 11591 **14.6.1 Evaluation of sub-activity (ATE\_IND.1)**

##### 11592 **14.6.1.1 Objectives**

11593 The goal of this activity is to determine, by independently testing a subset of the TSFI, whether the  
11594 TOE behaves as specified in the functional specification and guidance documentation.

##### 11595 **14.6.1.2 Input**

11596 The evaluation evidence for this sub-activity is:

- 11597 a) the ST;
- 11598 b) the functional specification;
- 11599 c) the operational user guidance;

- 11600 d) the preparative user guidance;
- 11601 e) the TOE suitable for testing.
- 11602 **14.6.1.3 Action ATE\_IND.1.1E**
- 11603 ISO/IEC 15408-3 ATE\_IND.1.1C: *The TOE shall be suitable for testing.*
- 11604 **14.6.1.3.1 Work unit ATE\_IND.1-1**
- 11605 The evaluator ***shall examine*** the TOE to determine that the test configuration is consistent with  
11606 the configuration under evaluation as specified in the ST.
- 11607 The TOE provided by the developer should have the same unique reference as established by the  
11608 CM capabilities (ALC\_CMC) sub-activities and identified in the ST introduction.
- 11609 It is possible for the ST to specify more than one configuration for evaluation. The TOE may  
11610 comprise a number of distinct hardware and software entities that need to be tested in accordance  
11611 with the ST. The evaluator verifies that all test configurations are consistent with the ST.
- 11612 The evaluator should consider the security objectives for the operational environment described in  
11613 the ST that may apply to the test environment and ensure they are met in the testing environment.  
11614 There may be some objectives for the operational environment that do not apply to the test  
11615 environment. For example, an objective about user clearances may not apply; however, an  
11616 objective about a single point of connection to a network would apply.
- 11617 If any test resources are used (e.g. meters, analysers) it will be the evaluator's responsibility to  
11618 ensure that these resources are calibrated correctly.
- 11619 **14.6.1.3.2 Work unit ATE\_IND.1-2**
- 11620 The evaluator ***shall examine*** the TOE to determine that it has been installed properly and is in a  
11621 known state.
- 11622 It is possible for the evaluator to determine the state of the TOE in a number of ways. For example,  
11623 previous successful completion of the Evaluation of sub-activity (AGD\_PRE.1) will satisfy this work  
11624 unit if the evaluator still has confidence that the TOE being used for testing was installed properly  
11625 and is in a known state. If this is not the case, then the evaluator should follow the developer's  
11626 procedures to install and start up the TOE, using the supplied guidance only.
- 11627 If the evaluator has to perform the installation procedures because the TOE is in an unknown state,  
11628 this work unit when successfully completed could satisfy work unit AGD\_PRE.1-3.
- 11629 **14.6.1.4 Action ATE\_IND.1.2E**
- 11630 **14.6.1.4.1 Work unit ATE\_IND.1-3**
- 11631 The evaluator ***shall devise*** a test subset.
- 11632 The evaluator selects a test subset and testing strategy that is appropriate for the TOE. One  
11633 extreme testing strategy would be to have the test subset contain as many interfaces as possible  
11634 tested with little rigour. Another testing strategy would be to have the test subset contain a few  
11635 interfaces based on their perceived relevance and rigorously test these interfaces.
- 11636 Typically the testing approach taken by the evaluator should fall somewhere between these two  
11637 extremes. The evaluator should exercise most of the interfaces using at least one test, but testing  
11638 need not demonstrate exhaustive specification testing.

## ISO/IEC 18045:2008(E)

11639 The evaluator, when selecting the subset of the interfaces to be tested, should consider the  
11640 following factors:

- 11641 • The number of interfaces from which to draw upon for the test subset. Where the TSF  
11642 includes only a small number of relatively simple interfaces, it may be practical to  
11643 rigorously test all of the interfaces. In other cases this may not be cost-effective, and  
11644 sampling is required.
- 11645 • Maintaining a balance of evaluation activities. The evaluator effort expended on the test  
11646 activity should be commensurate with that expended on any other evaluation activity.

11647 The evaluator selects the interfaces to compose the subset. This selection will depend on a number  
11648 of factors, and consideration of these factors may also influence the choice of test subset size:

- 11649 1) Significance of interfaces. Those interfaces more significant than others should be  
11650 included in the test subset. One major factor of “significance” is the security-  
11651 relevance (SFR-enforcing interfaces would be more significant than SFR-  
11652 supporting interfaces, which are more significant than SFR-non-interfering  
11653 interfaces; see ISO/IEC 15408-3 Subclause Functional specification (ADV\_FSP)).  
11654 The other major factor of “significance” is the number of SFRs mapping to this  
11655 interface (as determined when identifying the correspondence between levels of  
11656 abstraction in ADV).
- 11657 2) Complexity of the interface. Complex interfaces may require complex tests that  
11658 impose onerous requirements on the developer or evaluator, which may not be  
11659 conducive to cost-effective evaluations. Conversely, they are a likely area to find  
11660 errors and are good candidates for the subset. The evaluator will need to strike a  
11661 balance between these considerations.
- 11662 3) Implicit testing. Testing some interfaces may often implicitly test other interfaces,  
11663 and their inclusion in the subset may maximise the number of interfaces tested  
11664 (albeit implicitly). Certain interfaces will typically be used to provide a variety of  
11665 security functionality, and will tend to be the target of an effective testing  
11666 approach.
- 11667 4) Types of interfaces (e.g. programmatic, command-line, protocol). The evaluator  
11668 should consider including tests for all different types of interfaces that the TOE  
11669 supports.
- 11670 5) Interfaces that give rise to features that are innovative or unusual. Where the  
11671 TOE contains innovative or unusual features, which may feature strongly in  
11672 marketing literature and guidance documents, the corresponding interfaces  
11673 should be strong candidates for testing.

11674 This guidance articulates factors to consider during the selection process of an appropriate test  
11675 subset, but these are by no means exhaustive.

### 11676 14.6.1.4.2 Work unit ATE\_IND.1-4

11677 The evaluator **shall produce** test documentation for the test subset that is sufficiently detailed to  
11678 enable the tests to be reproducible.

11679 With an understanding of the expected behaviour of the TSF, from the ST and the functional  
11680 specification, the evaluator has to determine the most feasible way to test the interface. Specifically  
11681 the evaluator considers:

- 11682 a) the approach that will be used, for instance, whether an external interface will be  
 11683 tested, or an internal interface using a test harness, or will an alternate test approach  
 11684 be employed (e.g. in exceptional circumstances, a code inspection, if the  
 11685 implementation representation is available);
- 11686 b) the interface(s) that will be used to test and observe responses;
- 11687 c) the initial conditions that will need to exist for the test (i.e. any particular objects or  
 11688 subjects that will need to exist and security attributes they will need to have);
- 11689 d) special test equipment that will be required to either stimulate an interface (e.g.  
 11690 packet generators) or make observations of an interface (e.g. network analysers).
- 11691 The evaluator may find it practical to test each interface using a series of test cases, where each test  
 11692 case will test a very specific aspect of expected behaviour.
- 11693 The evaluator's test documentation should specify the derivation of each test, tracing it back to the  
 11694 relevant interface(s).
- 11695 **14.6.1.4.3 Work unit ATE\_IND.1-5**
- 11696 The evaluator **shall conduct** testing.
- 11697 The evaluator uses the test documentation developed as a basis for executing tests on the TOE. The  
 11698 test documentation is used as a basis for testing but this does not preclude the evaluator from  
 11699 performing additional ad hoc tests. The evaluator may devise new tests based on behaviour of the  
 11700 TOE discovered during testing. These new tests are recorded in the test documentation.
- 11701 **14.6.1.4.4 Work unit ATE\_IND.1-6**
- 11702 The evaluator **shall record** the following information about the tests that compose the test subset:
- 11703 a) identification of the interface behaviour to be tested;
- 11704 b) instructions to connect and setup all required test equipment as required to conduct  
 11705 the test;
- 11706 c) instructions to establish all prerequisite test conditions;
- 11707 d) instructions to stimulate the interface;
- 11708 e) instructions for observing the behaviour of the interface;
- 11709 f) descriptions of all expected results and the necessary analysis to be performed on the  
 11710 observed behaviour for comparison against expected results;
- 11711 g) instructions to conclude the test and establish the necessary post-test state for the  
 11712 TOE;
- 11713 h) actual test results.

## ISO/IEC 18045:2008(E)

11714 The level of detail should be such that another evaluator could repeat the tests and obtain an  
11715 equivalent result. While some specific details of the test results may be different (e.g. time and date  
11716 fields in an audit record) the overall result should be identical.

11717 There may be instances when it is unnecessary to provide all the information presented in this  
11718 work unit (e.g. the actual test results of a test may not require any analysis before a comparison  
11719 between the expected results can be made). The determination to omit this information is left to  
11720 the evaluator, as is the justification.

### 11721 14.6.1.4.5 Work unit ATE\_IND.1-7

11722 The evaluator **shall check** that all actual test results are consistent with the expected test results.

11723 Any differences in the actual and expected test results may indicate that the TOE does not perform  
11724 as specified or that the evaluator test documentation may be incorrect. Unexpected actual results  
11725 may require corrective maintenance to the TOE or test documentation and perhaps require re-  
11726 running of impacted tests and modifying the test sample size and composition. This determination  
11727 is left to the evaluator, as is its justification.

### 11728 14.6.1.4.6 Work unit ATE\_IND.1-8

11729 The evaluator **shall report** in the ETR the evaluator testing effort, outlining the testing approach,  
11730 configuration, depth and results.

11731 The evaluator testing information reported in the ETR allows the evaluator to convey the overall  
11732 testing approach and effort expended on the testing activity during the evaluation. The intent of  
11733 providing this information is to give a meaningful overview of the testing effort. It is not intended  
11734 that the information regarding testing in the ETR be an exact reproduction of specific test  
11735 instructions or results of individual tests. The intention is to provide enough detail to allow other  
11736 evaluators and evaluation authorities to gain some insight about the testing approach chosen,  
11737 amount of testing performed, TOE test configurations, and the overall results of the testing activity.

11738 Information that would typically be found in the ETR subclause regarding the evaluator testing  
11739 effort is:

11740 a) TOE test configurations. The particular configurations of the TOE that were tested;

11741 b) subset size chosen. The amount of interfaces that were tested during the evaluation  
11742 and a justification for the size;

11743 c) selection criteria for the interfaces that compose the subset. Brief statements about  
11744 the factors considered when selecting interfaces for inclusion in the subset;

11745 d) interfaces tested. A brief listing of the interfaces that merited inclusion in the subset;

11746 e) verdict for the activity. The overall judgement on the results of testing during the  
11747 evaluation.

11748 This list is by no means exhaustive and is only intended to provide some context as to the type of  
11749 information that should be present in the ETR concerning the testing the evaluator performed  
11750 during the evaluation.



11751 **14.6.2 Evaluation of sub-activity (ATE\_IND.2)**11752 **14.6.2.1 Objectives**

11753 The goal of this activity is to determine, by independently testing a subset of the TSF, whether the  
 11754 TOE behaves as specified in the design documentation, and to gain confidence in the developer's  
 11755 test results by performing a sample of the developer's tests.

11756 **14.6.2.2 Input**

11757 The evaluation evidence for this sub-activity is:

- 11758 a) the ST;
- 11759 b) the functional specification;
- 11760 c) the TOE design description;
- 11761 d) the operational user guidance;
- 11762 e) the preparative user guidance;
- 11763 f) the configuration management documentation;
- 11764 g) the test documentation;
- 11765 h) the TOE suitable for testing.

11766 **14.6.2.3 Action ATE\_IND.2.1E**

11767 ISO/IEC 15408-3 ATE\_IND.2.1C: *The TOE shall be suitable for testing.*

11768 **14.6.2.3.1 Work unit ATE\_IND.2-1**

11769 The evaluator **shall examine** the TOE to determine that the test configuration is consistent with  
 11770 the configuration under evaluation as specified in the ST.

11771 The TOE provided by the developer and identified in the test plan should have the same unique  
 11772 reference as established by the CM capabilities (ALC\_CMC) sub-activities and identified in the ST  
 11773 introduction.

11774 It is possible for the ST to specify more than one configuration for evaluation. The TOE may  
 11775 comprise a number of distinct hardware and software entities that need to be tested in accordance  
 11776 with the ST. The evaluator verifies that all test configurations are consistent with the ST.

11777 The evaluator should consider the security objectives for the operational environment described in  
 11778 the ST that may apply to the test environment and ensure they are met in the testing environment.  
 11779 There may be some objectives for the operational environment that do not apply to the test  
 11780 environment. For example, an objective about user clearances may not apply; however, an  
 11781 objective about a single point of connection to a network would apply.

11782 If any test resources are used (e.g. meters, analysers) it will be the evaluator's responsibility to  
 11783 ensure that these resources are calibrated correctly.

## ISO/IEC 18045:2008(E)

### 11784 14.6.2.3.2 Work unit ATE\_IND.2-2

11785 The evaluator **shall examine** the TOE to determine that it has been installed properly and is in a  
11786 known state.

11787 It is possible for the evaluator to determine the state of the TOE in a number of ways. For example,  
11788 previous successful completion of the Evaluation of sub-activity (AGD\_PRE.1) sub-activity will  
11789 satisfy this work unit if the evaluator still has confidence that the TOE being used for testing was  
11790 installed properly and is in a known state. If this is not the case, then the evaluator should follow  
11791 the developer's procedures to install and start up the TOE, using the supplied guidance only.

11792 If the evaluator has to perform the installation procedures because the TOE is in an unknown state,  
11793 this work unit when successfully completed could satisfy work unit AGD\_PRE.1-3.

11794 ISO/IEC 15408-3 ATE\_IND.2.2C: *The developer shall provide an equivalent set of resources to those*  
11795 *that were used in the developer's functional testing of the TSF.*

### 11796 14.6.2.3.3 Work unit ATE\_IND.2-3

11797 The evaluator **shall examine** the set of resources provided by the developer to determine that they  
11798 are equivalent to the set of resources used by the developer to functionally test the TSF.

11799 The set of resource used by the developer is documented in the developer test plan, as considered  
11800 in the Functional tests (ATE\_FUN) family. The resource set may include laboratory access and  
11801 special test equipment, among others. Resources that are not identical to those used by the  
11802 developer need to be equivalent in terms of any impact they may have on test results.

### 11803 14.6.2.4 Action ATE\_IND.2.2E

#### 11804 14.6.2.4.1 Work unit ATE\_IND.2-4

11805 The evaluator **shall conduct** testing using a sample of tests found in the developer test plan and  
11806 procedures.

11807 The overall aim of this work unit is to perform a sufficient number of the developer tests to confirm  
11808 the validity of the developer's test results. The evaluator has to decide on the size of the sample,  
11809 and the developer tests that will compose the sample (see A.2).

11810 All the developer tests can be traced back to specific interfaces. Therefore, the factors to consider  
11811 in the selection of the tests to compose the sample are similar to those listed for subset selection in  
11812 work-unit ATE\_IND.2-6. Additionally, the evaluator may wish to employ a random sampling  
11813 method to select developer tests to include in the sample.

#### 11814 14.6.2.4.2 Work unit ATE\_IND.2-5

11815 The evaluator **shall check** that all the actual test results are consistent with the expected test  
11816 results.

11817 Inconsistencies between the developer's expected test results and actual test results will compel  
11818 the evaluator to resolve the discrepancies. Inconsistencies encountered by the evaluator could be  
11819 resolved by a valid explanation and resolution of the inconsistencies by the developer.

11820 If a satisfactory explanation or resolution can not be reached, the evaluator's confidence in the  
11821 developer's test results may be lessened and it may be necessary for the evaluator to increase the  
11822 sample size to the extent that the subset identified in work unit ATE\_IND.2-4 is adequately tested:  
11823 deficiencies with the developer's tests need to result in either corrective action to the TOE by the  
11824 developer (e.g., if the inconsistency is caused by incorrect behaviour) or to the developer's tests

11825 (e.g., if the inconsistency is caused by an incorrect test), or in the production of new tests by the  
11826 evaluator.

11827 **14.6.2.5 Action ATE\_IND.2.3E**

11828 **14.6.2.5.1 Work unit ATE\_IND.2-6**

11829 The evaluator *shall devise* a test subset.

11830 The evaluator selects a test subset and testing strategy that is appropriate for the TOE. One  
11831 extreme testing strategy would be to have the test subset contain as many interfaces as possible  
11832 tested with little rigour. Another testing strategy would be to have the test subset contain a few  
11833 interfaces based on their perceived relevance and rigorously test these interfaces.

11834 Typically the testing approach taken by the evaluator should fall somewhere between these two  
11835 extremes. The evaluator should exercise most of the interfaces using at least one test, but testing  
11836 need not demonstrate exhaustive specification testing.

11837 The evaluator, when selecting the subset of the interfaces to be tested, should consider the  
11838 following factors:

11839 a) The developer test evidence. The developer test evidence consists of: the test  
11840 documentation, the available test coverage analysis, and the available depth of  
11841 testing analysis. The developer test evidence will provide insight as to how the TSF  
11842 has been exercised by the developer during testing. The evaluator applies this  
11843 information when developing new tests to independently test the TOE. Specifically  
11844 the evaluator should consider:

11845 1) augmentation of developer testing for interfaces. The evaluator may wish to  
11846 perform more of the same type of tests by varying parameters to more rigorously  
11847 test the interface.

11848 2) supplementation of developer testing strategy for interfaces. The evaluator may  
11849 wish to vary the testing approach of a specific interface by testing it using  
11850 another test strategy.

11851 b) The number of interfaces from which to draw upon for the test subset. Where the TSF  
11852 includes only a small number of relatively simple interfaces, it may be practical to  
11853 rigorously test all of them. In other cases this may not be cost-effective, and sampling  
11854 is required.

11855 c) Maintaining a balance of evaluation activities. The evaluator effort expended on the  
11856 test activity should be commensurate with that expended on any other evaluation  
11857 activity.

11858 The evaluator selects the interfaces to compose the subset. This selection will depend on a number  
11859 of factors, and consideration of these factors may also influence the choice of test subset size:

11860 a) Rigour of developer testing of the interfaces. Those interfaces that the evaluator  
11861 determines require additional testing should be included in the test subset.

11862 b) Developer test results. If the results of developer tests cause the evaluator to doubt  
11863 that an interface is not properly implemented, then the evaluator should include  
11864 such interfaces in the test subset.

## ISO/IEC 18045:2008(E)

- 11865 c) Significance of interfaces. Those interfaces more significant than others should be  
11866 included in the test subset. One major factor of “significance” is the security-  
11867 relevance (SFR-enforcing interfaces would be more significant than SFR-supporting  
11868 interfaces, which are more significant than SFR-non-interfering interfaces; see  
11869 ISO/IEC 15408-3 Subclause ADV\_FSP). The other major factor of “significance” is the  
11870 number of SFRs mapping to this interface (as determined when identifying the  
11871 correspondence between levels of abstraction in ADV).
- 11872 d) Complexity of interfaces. Interfaces that require complex implementation may  
11873 require complex tests that impose onerous requirements on the developer or  
11874 evaluator, which may not be conducive to cost-effective evaluations. Conversely,  
11875 they are a likely area to find errors and are good candidates for the subset. The  
11876 evaluator will need to strike a balance between these considerations.
- 11877 e) Implicit testing. Testing some interfaces may often implicitly test other interfaces, and  
11878 their inclusion in the subset may maximise the number of interfaces tested (albeit  
11879 implicitly). Certain interfaces will typically be used to provide a variety of security  
11880 functionality, and will tend to be the target of an effective testing approach.
- 11881 f) Types of interfaces (e.g. programmatic, command-line, protocol). The evaluator  
11882 should consider including tests for all different types of interfaces that the TOE  
11883 supports.
- 11884 g) Interfaces that give rise to features that are innovative or unusual. Where the TOE  
11885 contains innovative or unusual features, which may feature strongly in marketing  
11886 literature and guidance documents, the corresponding interfaces should be strong  
11887 candidates for testing.
- 11888 This guidance articulates factors to consider during the selection process of an appropriate test  
11889 subset, but these are by no means exhaustive.
- 11890 **14.6.2.5.2 Work unit ATE\_IND.2-7**
- 11891 The evaluator **shall produce** test documentation for the test subset that is sufficiently detailed to  
11892 enable the tests to be reproducible.
- 11893 With an understanding of the expected behaviour of the TSF, from the ST, the functional  
11894 specification, and the TOE design description, the evaluator has to determine the most feasible way  
11895 to test the interface. Specifically the evaluator considers:
- 11896 a) the approach that will be used, for instance, whether an external interface will be  
11897 tested, or an internal interface using a test harness, or will an alternate test approach  
11898 be employed (e.g. in exceptional circumstances, a code inspection);
- 11899 b) the interface(s) that will be used to test and observe responses;
- 11900 c) the initial conditions that will need to exist for the test (i.e. any particular objects or  
11901 subjects that will need to exist and security attributes they will need to have);
- 11902 d) special test equipment that will be required to either stimulate an interface (e.g.  
11903 packet generators) or make observations of an interface (e.g. network analysers).

11904 The evaluator may find it practical to test each interface using a series of test cases, where each test  
11905 case will test a very specific aspect of expected behaviour of that interface.

11906 The evaluator's test documentation should specify the derivation of each test, tracing it back to the  
11907 relevant interface(s).

#### 11908 **14.6.2.5.3 Work unit ATE\_IND.2-8**

11909 The evaluator **shall conduct** testing.

11910 The evaluator uses the test documentation developed as a basis for executing tests on the TOE. The  
11911 test documentation is used as a basis for testing but this does not preclude the evaluator from  
11912 performing additional ad hoc tests. The evaluator may devise new tests based on behaviour of the  
11913 TOE discovered during testing. These new tests are recorded in the test documentation.

#### 11914 **14.6.2.5.4 Work unit ATE\_IND.2-9**

11915 The evaluator **shall record** the following information about the tests that compose the test subset:

- 11916 a) identification of the interface behaviour to be tested;
- 11917 b) instructions to connect and setup all required test equipment as required to conduct  
11918 the test;
- 11919 c) instructions to establish all prerequisite test conditions;
- 11920 d) instructions to stimulate the interface;
- 11921 e) instructions for observing the interface;
- 11922 f) descriptions of all expected results and the necessary analysis to be performed on the  
11923 observed behaviour for comparison against expected results;
- 11924 g) instructions to conclude the test and establish the necessary post-test state for the  
11925 TOE;
- 11926 h) actual test results.

11927 The level of detail should be such that another evaluator could repeat the tests and obtain an  
11928 equivalent result. While some specific details of the test results may be different (e.g. time and date  
11929 fields in an audit record) the overall result should be identical.

11930 There may be instances when it is unnecessary to provide all the information presented in this  
11931 work unit (e.g. the actual test results of a test may not require any analysis before a comparison  
11932 between the expected results can be made). The determination to omit this information is left to  
11933 the evaluator, as is the justification.

#### 11934 **14.6.2.5.5 Work unit ATE\_IND.2-10**

11935 The evaluator **shall check** that all actual test results are consistent with the expected test results.

11936 Any differences in the actual and expected test results may indicate that the TOE does not perform  
11937 as specified or that the evaluator test documentation may be incorrect. Unexpected actual results  
11938 may require corrective maintenance to the TOE or test documentation and perhaps require re-

## ISO/IEC 18045:2008(E)

11939 running of impacted tests and modifying the test sample size and composition. This determination  
11940 is left to the evaluator, as is its justification.

### 11941 14.6.2.5.6 Work unit ATE\_IND.2-11

11942 The evaluator **shall report** in the ETR the evaluator testing effort, outlining the testing approach,  
11943 configuration, depth and results.

11944 The evaluator testing information reported in the ETR allows the evaluator to convey the overall  
11945 testing approach and effort expended on the testing activity during the evaluation. The intent of  
11946 providing this information is to give a meaningful overview of the testing effort. It is not intended  
11947 that the information regarding testing in the ETR be an exact reproduction of specific test  
11948 instructions or results of individual tests. The intention is to provide enough detail to allow other  
11949 evaluators and evaluation authorities to gain some insight about the testing approach chosen,  
11950 amount of evaluator testing performed, amount of developer tests performed, TOE test  
11951 configurations, and the overall results of the testing activity.

11952 Information that would typically be found in the ETR subclause regarding the evaluator testing  
11953 effort is:

- 11954 a) TOE test configurations. The particular configurations of the TOE that were tested.
- 11955 b) subset size chosen. The amount of interfaces that were tested during the evaluation  
11956 and a justification for the size.
- 11957 c) selection criteria for the interfaces that compose the subset. Brief statements about  
11958 the factors considered when selecting interfaces for inclusion in the subset.
- 11959 d) Interfaces tested. A brief listing of the interfaces that merited inclusion in the subset.
- 11960 e) developer tests performed. The amount of developer tests performed and a brief  
11961 description of the criteria used to select the tests.
- 11962 f) verdict for the activity. The overall judgement on the results of testing during the  
11963 evaluation.

11964 This list is by no means exhaustive and is only intended to provide some context as to the type of  
11965 information that should be present in the ETR concerning the testing the evaluator performed  
11966 during the evaluation.

### 11967 14.6.3 Evaluation of sub-activity (ATE\_IND.3)

11968 There is no general guidance; the scheme should be consulted for guidance on this sub-activity.

### 11969 14.7 Composite functional testing (ATE\_COMP)

11970 The composite-specific work units defined here are intended to be integrated as refinements to the  
11971 evaluation activities of the ATE class listed in the following table. The other activities of ATE class  
11972 do not require composite-specific work units.

| CC assurance family | Evaluation activity | Evaluation work unit | Composite-specific work unit |
|---------------------|---------------------|----------------------|------------------------------|
|---------------------|---------------------|----------------------|------------------------------|

|         |              |             |              |
|---------|--------------|-------------|--------------|
| ATE_COV | ATE_COV.1.1C | ATE_COV.1-1 | ATE_COMP.1-1 |
| ATE_FUN | ATE_FUN.1.2C | ATE_FUN.1-3 | ATE_COMP.1-1 |

11973 NB: If the level of the assurance requirement chosen is higher than those identified in this table, the  
11974 composite-specific work unit is also applicable.

11975 **14.7.1 Evaluation of sub-activity (ATE\_COMP.1)**

11976 **14.7.1.1 Objectives**

11977 The aim of this activity is to determine whether composite product as a whole exhibits the  
11978 properties necessary to satisfy the functional requirements of its Security Target.

11979 **14.7.1.2 Application notes**

11980 A composite product can be tested separately and integrated. Separate testing means that the  
11981 platform and the application are being tested independent of each other. A lot of tests of the  
11982 platform may have been performed within the scope of its accomplished evaluation. The  
11983 application may be tested on a simulator or an emulator, which represent a virtual machine.  
11984 Integration testing means that the composite product is being tested as it is: the application is  
11985 running on the platform.

11986 Behaviour of implementation of some SFRs can depend on properties of the underlying platform as  
11987 well as of the application (e.g. correctness of the measures of the composite product to withstand a  
11988 side channel attack or correctness of the implementation of tamper resistance against physical  
11989 attacks). In such a case the SFR implementation shall be tested on the final composite product, but  
11990 not on a simulator or an emulator.

11991 This activity focuses exclusively on testing of the composite product as a whole and represents  
11992 merely partial efforts within the general test approach being covered by the assurance ATE. These  
11993 integration tests shall be specified and performed, whereby the approach of the standard  
11994 assurance families of the class ATE shall be applied.

11995 A correct behaviour of the Platform-TSF being relevant for the Composite-ST (corresponding to the  
11996 group RP\_SFR-SERV and RP\_SFR-MECH in the work unit ADV\_COMP.1-1 above), and-absence of  
11997 exploitable vulnerabilities (sufficient effectiveness) in the context of the Platform-ST, are  
11998 confirmed by the valid Platform Certificate, cf. chapter 6 above.

11999 **14.7.1.3 Action ATE\_COMP.1.1E**

12000 The evaluator shall confirm that the information provided meets all requirements for content and  
12001 presentation of evidence.

12002 **14.7.1.3.1 Work unit ATE\_COMP.1-1**

12003 The evaluator shall examine that the developer performed the integration tests for all SFRs having  
12004 to be tested on the composite product as a whole.

12005 In order to perform this work unit the evaluator shall analyse, for each SFR, whether it directly  
12006 depends on security properties of the platform and of the application. Then the evaluator shall  
12007 verify that the integration tests performed by the developer cover at least all such SFRs.

12008 If the assurance package chosen does not contain the families ATE\_FUN and ATE\_COV (e.g. EAL1),  
12009 this work unit is not applicable.

## ISO/IEC 18045:2008(E)

12010 The result of this work unit shall be integrated to the result of ATE\_COV.1.1C/ ATE\_COV.11 and  
12011 ATE\_FUN.1.2C/ ATE\_FUN.1-3 (or the equivalent higher components if a higher assurance level is  
12012 selected).

### 12013 **15 Class AVA: Vulnerability assessment**

#### 12014 **15.1 Introduction**

12015 The purpose of the vulnerability assessment activity is to determine the exploitability of flaws or  
12016 weaknesses in the TOE in the operational environment. This determination is based upon analysis  
12017 of the evaluation evidence and a search of publicly available material by the evaluator and is  
12018 supported by evaluator penetration testing.

##### 12019 **15.1.1 Vulnerability analysis (AVA\_VAN)**

##### 12020 **15.1.2 Evaluation of sub-activity (AVA\_VAN.1)**

###### 12021 **15.1.2.1 Objectives**

12022 The objective of this sub-activity is to determine whether the TOE, in its operational environment,  
12023 has easily identifiable exploitable vulnerabilities.

###### 12024 **15.1.2.2 Input**

12025 The evaluation evidence for this sub-activity is:

- 12026 a) the ST;
- 12027 b) the guidance documentation;
- 12028 c) the TOE suitable for testing;
- 12029 d) information publicly available to support the identification of potential vulnerabilities.

12030 Other input for this sub-activity is:

- 12031 a) current information regarding potential vulnerabilities (e.g. from an evaluation  
12032 authority).

###### 12033 **15.1.2.3 Application notes**

12034 The evaluator should consider performing additional tests as a result of potential vulnerabilities  
12035 encountered during the conduct of other parts of the evaluation.

12036 The use of the term guidance in this sub-activity refers to the operational guidance and the  
12037 preparative guidance.

12038 Potential vulnerabilities may be in information that is publicly available, or not, and may require  
12039 skill to exploit, or not. These two aspects are related, but are distinct. It should not be assumed that,  
12040 simply because a potential vulnerability is identifiable from information that is publicly available, it  
12041 can be easily exploited.

###### 12042 **15.1.2.4 Action AVA\_VAN.1.1E**

12043 ISO/IEC 15408-3 AVA\_VAN.1.1C: *The TOE shall be suitable for testing.*



12044 **15.1.2.4.1 Work unit AVA\_VAN.1-1**

12045 The evaluator *shall examine* the TOE to determine that the test configuration is consistent with  
12046 the configuration under evaluation as specified in the ST.

12047 The TOE provided by the developer and identified in the test plan should have the same unique  
12048 reference as established by the CM capabilities (ALC\_CMC) sub-activities and identified in the ST  
12049 introduction.

12050 It is possible for the ST to specify more than one configuration for evaluation. The TOE may  
12051 comprise a number of distinct hardware and software entities that need to be tested in accordance  
12052 with the ST. The evaluator verifies that all test configurations are consistent with the ST.

12053 The evaluator should consider the security objectives for the operational environment described in  
12054 the ST that may apply to the test environment and ensure they are met in the testing environment.  
12055 There may be some objectives for the operational environment that do not apply to the test  
12056 environment. For example, an objective about user clearances may not apply; however, an  
12057 objective about a single point of connection to a network would apply.

12058 If any test resources are used (e.g. meters, analysers) it will be the evaluator's responsibility to  
12059 ensure that these resources are calibrated correctly.

12060 **15.1.2.4.2 Work unit AVA\_VAN.1-2**

12061 The evaluator *shall examine* the TOE to determine that it has been installed properly and is in a  
12062 known state

12063 It is possible for the evaluator to determine the state of the TOE in a number of ways. For example,  
12064 previous successful completion of the Evaluation of sub-activity (AGD\_PRE.1) sub-activity will  
12065 satisfy this work unit if the evaluator still has confidence that the TOE being used for testing was  
12066 installed properly and is in a known state. If this is not the case, then the evaluator should follow  
12067 the developer's procedures to install and start up the TOE, using the supplied guidance only.

12068 If the evaluator has to perform the installation procedures because the TOE is in an unknown state,  
12069 this work unit when successfully completed could satisfy work unit AGD\_PRE.1-3.

12070 **15.1.2.5 Action AVA\_VAN.1.2E**12071 **15.1.2.5.1 Work unit AVA\_VAN.1-3**

12072 The evaluator *shall examine* sources of information publicly available to identify potential  
12073 vulnerabilities in the TOE.

12074 The evaluator examines the sources of information publicly available to support the identification  
12075 of possible potential vulnerabilities in the TOE. There are many sources of publicly available  
12076 information, which should be considered, e.g. mailing lists and security forums on the world wide  
12077 web that report known vulnerabilities in specified technologies.

12078 The evaluator should not constrain their consideration of publicly available information to the  
12079 above but should consider any other relevant information available.

12080 While examining the evidence provided the evaluator will use the information in the public domain  
12081 to further search for potential vulnerabilities. Where the evaluators have identified areas of  
12082 concern, the evaluator should consider information publicly available that relate to those areas of  
12083 concern.

12084 The availability of information that may be readily available to an attacker that helps to identify  
12085 and facilitate attacks effectively operates to substantially enhance the attack potential of a given

## ISO/IEC 18045:2008(E)

12086 attacker. The accessibility of vulnerability information and sophisticated attack tools on the  
12087 Internet makes it more likely that this information will be used in attempts to identify potential  
12088 vulnerabilities in the TOE and exploit them. Modern search tools make such information easily  
12089 available to the evaluator, and the determination of resistance to published potential  
12090 vulnerabilities and well-known generic attacks can be achieved in a cost-effective manner.

12091 The search of the information publicly available should be focused on those sources that refer  
12092 specifically to the product from which the TOE is derived. The extensiveness of this search should  
12093 consider the following factors: TOE type, evaluator experience in this TOE type, expected attack  
12094 potential and the level of ADV evidence available.

12095 The identification process is iterative, where the identification of one potential vulnerability may  
12096 lead to identifying another area of concern that requires further investigation.

12097 The evaluator will report what actions were taken to identify potential vulnerabilities in the  
12098 information publicly available. However, in this type of search, the evaluator may not be able to  
12099 describe the steps in identifying potential vulnerabilities before the outset of the examination, as  
12100 the approach may evolve as a result of findings during the search.

12101 The evaluator will report the evidence examined in completing the search for potential  
12102 vulnerabilities.

### 12103 15.1.2.5.2 Work unit AVA\_VAN.1-4

12104 The evaluator ***shall record*** in the ETR the identified potential vulnerabilities that are candidates  
12105 for testing and applicable to the TOE in its operational environment.

12106 It may be identified that no further consideration of the potential vulnerability is required if for  
12107 example the evaluator identifies that measures in the operational environment, either IT or non-IT,  
12108 prevent exploitation of the potential vulnerability in that operational environment. For instance,  
12109 restricting physical access to the TOE to authorised users only may effectively render a potential  
12110 vulnerability to tampering unexploitable.

12111 The evaluator records any reasons for exclusion of potential vulnerabilities from further  
12112 consideration if the evaluator determines that the potential vulnerability is not applicable in the  
12113 operational environment. Otherwise the evaluator records the potential vulnerability for further  
12114 consideration.

12115 A list of potential vulnerabilities applicable to the TOE in its operational environment, which can be  
12116 used as an input into penetration testing activities, shall be reported in the ETR by the evaluators.

### 12117 15.1.2.6 Action AVA\_VAN.1.3E

#### 12118 15.1.2.6.1 Work unit AVA\_VAN.1-5

12119 The evaluator ***shall devise*** penetration tests, based on the independent search for potential  
12120 vulnerabilities.

12121 The evaluator prepares for penetration testing as necessary to determine the susceptibility of the  
12122 TOE, in its operational environment, to the potential vulnerabilities identified during the search of  
12123 the sources of information publicly available. Any current information provided to the evaluator by  
12124 a third party (e.g. evaluation authority) regarding known potential vulnerabilities will be  
12125 considered by the evaluator, together with any encountered potential vulnerabilities resulting  
12126 from the performance of other evaluation activities.

12127 The evaluator will probably find it practical to carry out penetration test using a series of test cases,  
12128 where each test case will test for a specific potential vulnerability.

12129 The evaluator is not expected to test for potential vulnerabilities (including those in the public  
 12130 domain) beyond those which required a Basic attack potential. In some cases, however, it will be  
 12131 necessary to carry out a test before the exploitability can be determined. Where, as a result of  
 12132 evaluation expertise, the evaluator discovers a potential vulnerability that is beyond Basic attack  
 12133 potential, this is reported in the ETR as a residual vulnerability.

#### 12134 15.1.2.6.2 Work unit AVA\_VAN.1-6

12135 The evaluator *shall produce* penetration test documentation for the tests based on the list of  
 12136 potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test  
 12137 documentation shall include:

- 12138 a) identification of the potential vulnerability the TOE is being tested for;
- 12139 b) instructions to connect and setup all required test equipment as required to conduct  
 12140 the penetration test;
- 12141 c) instructions to establish all penetration test prerequisite initial conditions;
- 12142 d) instructions to stimulate the TSF;
- 12143 e) instructions for observing the behaviour of the TSF;
- 12144 f) descriptions of all expected results and the necessary analysis to be performed on the  
 12145 observed behaviour for comparison against expected results;
- 12146 g) instructions to conclude the test and establish the necessary post-test state for the  
 12147 TOE.

12148 The evaluator prepares for penetration testing based on the list of potential vulnerabilities  
 12149 identified during the search of the public domain.

12150 The evaluator is not expected to determine the exploitability for potential vulnerabilities beyond  
 12151 those for which a Basic attack potential is required to effect an attack. However, as a result of  
 12152 evaluation expertise, the evaluator may discover a potential vulnerability that is exploitable only  
 12153 by an attacker with greater than Basic attack potential. Such vulnerabilities are to be reported in  
 12154 the ETR as residual vulnerabilities.

12155 With an understanding of the potential vulnerability, the evaluator determines the most feasible  
 12156 way to test for the TOE's susceptibility. Specifically the evaluator considers:

- 12157 a) the TSFI or other TOE interface that will be used to stimulate the TSF and observe  
 12158 responses;
- 12159 b) initial conditions that will need to exist for the test (i.e. any particular objects or  
 12160 subjects that will need to exist and security attributes they will need to have);
- 12161 c) special test equipment that will be required to either stimulate a TSFI or make  
 12162 observations of a TSFI (although it is unlikely that specialist equipment would be  
 12163 required to exploit a potential vulnerability assuming a Basic attack potential);

## ISO/IEC 18045:2008(E)

- 12164 d) whether theoretical analysis should replace physical testing, particularly relevant  
12165 where the results of an initial test can be extrapolated to demonstrate that repeated  
12166 attempts of an attack are likely to succeed after a given number of attempts.
- 12167 The evaluator will probably find it practical to carry out penetration testing using a series of test  
12168 cases, where each test case will test for a specific potential vulnerability.
- 12169 The intent of specifying this level of detail in the test documentation is to allow another evaluator  
12170 to repeat the tests and obtain an equivalent result.
- 12171 **15.1.2.6.3 Work unit AVA\_VAN.1-7**
- 12172 The evaluator **shall conduct** penetration testing.
- 12173 The evaluator uses the penetration test documentation resulting from work unit AVA\_VAN.1-5 as a  
12174 basis for executing penetration tests on the TOE, but this does not preclude the evaluator from  
12175 performing additional ad hoc penetration tests. If required, the evaluator may devise ad hoc tests  
12176 as a result of information learnt during penetration testing that, if performed by the evaluator, are  
12177 to be recorded in the penetration test documentation. Such tests may be required to follow up  
12178 unexpected results or observations, or to investigate potential vulnerabilities suggested to the  
12179 evaluator during the pre-planned testing.
- 12180 The evaluator is not expected to test for potential vulnerabilities (including those in the public  
12181 domain) beyond those which required a Basic attack potential. In some cases, however, it will be  
12182 necessary to carry out a test before the exploitability can be determined. Where, as a result of  
12183 evaluation expertise, the evaluator discovers a potential vulnerability that is beyond Basic attack  
12184 potential, this is reported in the ETR as a residual vulnerability.
- 12185 **15.1.2.6.4 Work unit AVA\_VAN.1-8**
- 12186 The evaluator **shall record** the actual results of the penetration tests.
- 12187 While some specific details of the actual test results may be different from those expected (e.g. time  
12188 and date fields in an audit record) the overall result should be identical. Any unexpected test  
12189 results should be investigated. The impact on the evaluation should be stated and justified.
- 12190 **15.1.2.6.5 Work unit AVA\_VAN.1-9**
- 12191 The evaluator **shall report** in the ETR the evaluator penetration testing effort, outlining the testing  
12192 approach, configuration, depth and results.
- 12193 The penetration testing information reported in the ETR allows the evaluator to convey the overall  
12194 penetration testing approach and effort expended on this sub-activity. The intent of providing this  
12195 information is to give a meaningful overview of the evaluator's penetration testing effort. It is not  
12196 intended that the information regarding penetration testing in the ETR be an exact reproduction of  
12197 specific test steps or results of individual penetration tests. The intention is to provide enough  
12198 detail to allow other evaluators and evaluation authorities to gain some insight about the  
12199 penetration testing approach chosen, amount of penetration testing performed, TOE test  
12200 configurations, and the overall results of the penetration testing activity.
- 12201 Information that would typically be found in the ETR subclause regarding evaluator penetration  
12202 testing efforts is:
- 12203 a) TOE test configurations. The particular configurations of the TOE that were  
12204 penetration tested;

- 12205 b) TSFI penetration tested. A brief listing of the TSFI and other TOE interfaces that were  
12206 the focus of the penetration testing;
- 12207 c) verdict for the sub-activity. The overall judgement on the results of penetration  
12208 testing.
- 12209 This list is by no means exhaustive and is only intended to provide some context as to the type of  
12210 information that should be present in the ETR concerning the penetration testing the evaluator  
12211 performed during the evaluation.
- 12212 **15.1.2.6.6 Work unit AVA\_VAN.1-10**
- 12213 The evaluator *shall examine* the results of all penetration testing to determine that the TOE, in its  
12214 operational environment, is resistant to an attacker possessing a Basic attack potential.
- 12215 If the results reveal that the TOE, in its operational environment, has vulnerabilities exploitable by  
12216 an attacker possessing less than Enhanced-Basic attack potential, then this evaluator action fails.
- 12217 The guidance in B.2 should be used to determine the attack potential required to exploit a  
12218 particular vulnerability and whether it can therefore be exploited in the intended environment. It  
12219 may not be necessary for the attack potential to be calculated in every instance, only if there is  
12220 some doubt as to whether or not the vulnerability can be exploited by an attacker possessing an  
12221 attack potential less than Enhanced-Basic.
- 12222 **15.1.2.6.7 Work unit AVA\_VAN.1-11**
- 12223 The evaluator *shall report* in the ETR all exploitable vulnerabilities and residual vulnerabilities,  
12224 detailing for each:
- 12225 a) its source (e.g. evaluation methodology activity being undertaken when it was  
12226 conceived, known to the evaluator, read in a publication);
- 12227 b) the SFR(s) not met;
- 12228 c) a description;
- 12229 d) whether it is exploitable in its operational environment or not (i.e. exploitable or  
12230 residual).
- 12231 e) the amount of time, level of expertise, level of knowledge of the TOE, level of  
12232 opportunity and the equipment required to perform the identified vulnerabilities,  
12233 and the corresponding values using the tables B.2 and B.3 of Annex B.2.
- 12234 **15.1.3 Evaluation of sub-activity (AVA\_VAN.2)**
- 12235 **15.1.3.1 Objectives**
- 12236 The objective of this sub-activity is to determine whether the TOE, in its operational environment,  
12237 has vulnerabilities exploitable by attackers possessing Basic attack potential.
- 12238 **15.1.3.2 Input**
- 12239 The evaluation evidence for this sub-activity is:

## ISO/IEC 18045:2008(E)

- 12240 a) the ST;
- 12241 b) the functional specification;
- 12242 c) the TOE design;
- 12243 d) the security architecture description;
- 12244 e) the guidance documentation;
- 12245 f) the TOE suitable for testing;
- 12246 g) information publicly available to support the identification of possible potential  
12247 vulnerabilities.
- 12248 The remaining implicit evaluation evidence for this sub-activity depends on the components that  
12249 have been included in the assurance package. The evidence provided for each component is to be  
12250 used as input in this sub-activity.
- 12251 Other input for this sub-activity is:
- 12252 a) current information regarding public domain potential vulnerabilities and attacks (e.g.  
12253 from an evaluation authority).
- 12254 **15.1.3.3 Application notes**
- 12255 The evaluator should consider performing additional tests as a result of potential vulnerabilities  
12256 encountered during other parts of the evaluation.
- 12257 **15.1.3.4 Action AVA\_VAN.2.1E**
- 12258 ISO/IEC 15408-3 AVA\_VAN.2.1C: *The TOE shall be suitable for testing.*
- 12259 **15.1.3.4.1 Work unit AVA\_VAN.2-1**
- 12260 The evaluator **shall examine** the TOE to determine that the test configuration is consistent with  
12261 the configuration under evaluation as specified in the ST.
- 12262 The TOE provided by the developer and identified in the test plan should have the same unique  
12263 reference as established by the CM capabilities (ALC\_CMC) sub-activities and identified in the ST  
12264 introduction.
- 12265 It is possible for the ST to specify more than one configuration for evaluation. The TOE may  
12266 comprise a number of distinct hardware and software entities that need to be tested in accordance  
12267 with the ST. The evaluator verifies that all test configurations are consistent with the ST.
- 12268 The evaluator should consider the security objectives for the operational environment described in  
12269 the ST that may apply to the test environment and ensure they are met in the testing environment.  
12270 There may be some objectives for the operational environment that do not apply to the test  
12271 environment. For example, an objective about user clearances may not apply; however, an  
12272 objective about a single point of connection to a network would apply.
- 12273 If any test resources are used (e.g. meters, analysers) it will be the evaluator's responsibility to  
12274 ensure that these resources are calibrated correctly.

12275 **15.1.3.4.2 Work unit AVA\_VAN.2-2**

12276 The evaluator *shall examine* the TOE to determine that it has been installed properly and is in a  
12277 known state

12278 It is possible for the evaluator to determine the state of the TOE in a number of ways. For example,  
12279 previous successful completion of the Evaluation of sub-activity (AGD\_PRE.1) sub-activity will  
12280 satisfy this work unit if the evaluator still has confidence that the TOE being used for testing was  
12281 installed properly and is in a known state. If this is not the case, then the evaluator should follow  
12282 the developer's procedures to install and start up the TOE, using the supplied guidance only.

12283 If the evaluator has to perform the installation procedures because the TOE is in an unknown state,  
12284 this work unit when successfully completed could satisfy work unit AGD\_PRE.1-3.

12285 **15.1.3.5 Action AVA\_VAN.2.2E**12286 **15.1.3.5.1 Work unit AVA\_VAN.2-3**

12287 The evaluator *shall examine* sources of information publicly available to identify potential  
12288 vulnerabilities in the TOE.

12289 The evaluator examines the sources of information publicly available to support the identification  
12290 of possible potential vulnerabilities in the TOE. There are many sources of publicly available  
12291 information which the evaluator should consider using items such as those available on the world  
12292 wide web, including:

12293 a) specialist publications (magazines, books);

12294 b) research papers.

12295 The evaluator should not constrain their consideration of publicly available information to the  
12296 above, but should consider any other relevant information available.

12297 While examining the evidence provided the evaluator will use the information in the public domain  
12298 to further search for potential vulnerabilities. Where the evaluators have identified areas of  
12299 concern, the evaluator should consider information publicly available that relate to those areas of  
12300 concern.

12301 The availability of information that may be readily available to an attacker that helps to identify  
12302 and facilitate attacks may substantially enhance the attack potential of a given attacker. The  
12303 accessibility of vulnerability information and sophisticated attack tools on the Internet makes it  
12304 more likely that this information will be used in attempts to identify potential vulnerabilities in the  
12305 TOE and exploit them. Modern search tools make such information easily available to the evaluator,  
12306 and the determination of resistance to published potential vulnerabilities and well known generic  
12307 attacks can be achieved in a cost-effective manner.

12308 The search of the information publicly available should be focused on those sources that refer  
12309 specifically to the product from which the TOE is derived. The extensiveness of this search should  
12310 consider the following factors: TOE type, evaluator experience in this TOE type, expected attack  
12311 potential and the level of ADV evidence available.

12312 The identification process is iterative, where the identification of one potential vulnerability may  
12313 lead to identifying another area of concern that requires further investigation.

12314 The evaluator will report what actions were taken to identify potential vulnerabilities in the  
12315 evidence. However, in this type of search, the evaluator may not be able to describe the steps in

## ISO/IEC 18045:2008(E)

12316 identifying potential vulnerabilities before the outset of the examination, as the approach may  
12317 evolve as a result of findings during the search.

12318 The evaluator will report the evidence examined in completing the search for potential  
12319 vulnerabilities. This selection of evidence may be derived from those areas of concern identified by  
12320 the evaluator, linked to the evidence the attacker is assumed to be able to obtain, or according to  
12321 another rationale provided by the evaluator.

### 12322 15.1.3.6 Action AVA\_VAN.2.3E

#### 12323 15.1.3.6.1 Work unit AVA\_VAN.2-4

12324 The evaluator **shall conduct** a search of ST, guidance documentation, functional specification, TOE  
12325 design and security architecture description evidence to identify possible potential vulnerabilities  
12326 in the TOE.

12327 A search of the evidence should be completed whereby specifications and documentation for the  
12328 TOE are analysed and then potential vulnerabilities in the TOE are hypothesised, or speculated.  
12329 The list of hypothesised potential vulnerabilities is then prioritised on the basis of the estimated  
12330 probability that a potential vulnerability exists and, assuming an exploitable vulnerability does  
12331 exist the attack potential required to exploit it, and on the extent of control or compromise it would  
12332 provide. The prioritised list of potential vulnerabilities is used to direct penetration testing against  
12333 the TOE.

12334 The security architecture description provides the developer vulnerability analysis, as it  
12335 documents how the TSF protects itself from interference from untrusted subjects and prevents the  
12336 bypass of security enforcement functionality. Therefore, the evaluator should use this description  
12337 of the protection of the TSF as a basis for the search for possible ways to undermine the TSF.

12338 Subject to the SFRs the TOE is to meet in the operational environment, the evaluator's independent  
12339 vulnerability analysis should consider generic potential vulnerabilities under each of the following  
12340 headings:

12341 a) generic potential vulnerabilities relevant for the type of TOE being evaluated, as may  
12342 be supplied by the evaluation authority;

12343 b) bypassing;

12344 c) tampering;

12345 d) direct attacks;

12346 e) monitoring;

12347 f) misuse.

12348 Items b) - f) are explained in greater detail in Annex B.

12349 The security architecture description should be considered in light of each of the above generic  
12350 potential vulnerabilities. Each potential vulnerability should be considered to search for possible  
12351 ways in which to defeat the TSF protection and undermine the TSF.



12352 **15.1.3.6.2 Work unit AVA\_VAN.2-5**

12353 The evaluator **shall record** in the ETR the identified potential vulnerabilities that are candidates  
12354 for testing and applicable to the TOE in its operational environment.

12355 It may be identified that no further consideration of the potential vulnerability is required if for  
12356 example the evaluator identifies that measures in the operational environment, either IT or non-IT,  
12357 prevent exploitation of the potential vulnerability in that operational environment. For instance,  
12358 restricting physical access to the TOE to authorised users only may effectively render a potential  
12359 vulnerability to tampering unexploitable.

12360 The evaluator records any reasons for exclusion of potential vulnerabilities from further  
12361 consideration if the evaluator determines that the potential vulnerability is not applicable in the  
12362 operational environment. Otherwise the evaluator records the potential vulnerability for further  
12363 consideration.

12364 A list of potential vulnerabilities applicable to the TOE in its operational environment, which can be  
12365 used as an input into penetration testing activities, shall be reported in the ETR by the evaluators.

12366 **15.1.3.7 Action AVA\_VAN.2.4E**12367 **15.1.3.7.1 Work unit AVA\_VAN.2-6**

12368 The evaluator **shall devise** penetration tests, based on the independent search for potential  
12369 vulnerabilities.

12370 The evaluator prepares for penetration testing as necessary to determine the susceptibility of the  
12371 TOE, in its operational environment, to the potential vulnerabilities identified during the search of  
12372 the sources of information publicly available. Any current information provided to the evaluator by  
12373 a third party (e.g. evaluation authority) regarding known potential vulnerabilities will be  
12374 considered by the evaluator, together with any encountered potential vulnerabilities resulting  
12375 from the performance of other evaluation activities.

12376 The evaluator is reminded that, as for considering the security architecture description in the  
12377 search for vulnerabilities (as detailed in AVA\_VAN.2-4), testing should be performed to confirm the  
12378 architectural properties. This is likely to require negative tests attempting to disprove the  
12379 properties of the security architecture. In developing the strategy for penetration testing, the  
12380 evaluator will ensure that each of the major characteristics of the security architecture description  
12381 are tested, either in functional testing (as considered in 14) or evaluator penetration testing.

12382 The evaluator will probably find it practical to carry out penetration test using a series of test cases,  
12383 where each test case will test for a specific potential vulnerability.

12384 The evaluator is not expected to test for potential vulnerabilities (including those in the public  
12385 domain) beyond those which required a Basic attack potential. In some cases, however, it will be  
12386 necessary to carry out a test before the exploitability can be determined. Where, as a result of  
12387 evaluation expertise, the evaluator discovers an exploitable vulnerability that is beyond Basic  
12388 attack potential, this is reported in the ETR as a residual vulnerability.

12389 Guidance on determining the necessary attack potential to exploit a potential vulnerability can be  
12390 found in Annex B.2.

12391 Potential vulnerabilities hypothesised as exploitable only by attackers possessing Enhanced-Basic,  
12392 Moderate or High attack potential do not result in a failure of this evaluator action. Where analysis  
12393 supports the hypothesis, these need not be considered further as an input to penetration testing.  
12394 However, such vulnerabilities are reported in the ETR as residual vulnerabilities.

## ISO/IEC 18045:2008(E)

12395 Potential vulnerabilities hypothesised as exploitable by an attacker possessing a Basic attack  
12396 potential and resulting in a violation of the security objectives should be the highest priority  
12397 potential vulnerabilities comprising the list used to direct penetration testing against the TOE.

### 12398 15.1.3.7.2 Work unit AVA\_VAN.2-7

12399 The evaluator **shall produce** penetration test documentation for the tests based on the list of  
12400 potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test  
12401 documentation shall include:

- 12402 a) identification of the potential vulnerability the TOE is being tested for;
- 12403 b) instructions to connect and setup all required test equipment as required to conduct  
12404 the penetration test;
- 12405 c) instructions to establish all penetration test prerequisite initial conditions;
- 12406 d) instructions to stimulate the TSF;
- 12407 e) instructions for observing the behaviour of the TSF;
- 12408 f) descriptions of all expected results and the necessary analysis to be performed on the  
12409 observed behaviour for comparison against expected results;
- 12410 g) instructions to conclude the test and establish the necessary post-test state for the  
12411 TOE.

12412 The evaluator prepares for penetration testing based on the list of potential vulnerabilities  
12413 identified during the search of the public domain and the analysis of the evaluation evidence.

12414 The evaluator is not expected to determine the exploitability for potential vulnerabilities beyond  
12415 those for which a Basic attack potential is required to effect an attack. However, as a result of  
12416 evaluation expertise, the evaluator may discover a potential vulnerability that is exploitable only  
12417 by an attacker with greater than Basic attack potential. Such vulnerabilities are to be reported in  
12418 the ETR as residual vulnerabilities.

12419 With an understanding of the potential vulnerability, the evaluator determines the most feasible  
12420 way to test for the TOE's susceptibility. Specifically the evaluator considers:

- 12421 a) the TSFI or other TOE interface that will be used to stimulate the TSF and observe  
12422 responses (It is possible that the evaluator will need to use an interface to the TOE  
12423 other than the TSFI to demonstrate properties of the TSF such as those described in  
12424 the security architecture description (as required by ADV\_ARC). It should be noted,  
12425 that although these TOE interfaces provide a means of testing the TSF properties,  
12426 they are not the subject of the test.);
- 12427 b) initial conditions that will need to exist for the test (i.e. any particular objects or  
12428 subjects that will need to exist and security attributes they will need to have);
- 12429 c) special test equipment that will be required to either stimulate a TSFI or make  
12430 observations of a TSFI (although it is unlikely that specialist equipment would be  
12431 required to exploit a potential vulnerability assuming a Basic attack potential);

- 12432 d) whether theoretical analysis should replace physical testing, particularly relevant  
 12433 where the results of an initial test can be extrapolated to demonstrate that repeated  
 12434 attempts of an attack are likely to succeed after a given number of attempts.
- 12435 The evaluator will probably find it practical to carry out penetration testing using a series of test  
 12436 cases, where each test case will test for a specific potential vulnerability.
- 12437 The intent of specifying this level of detail in the test documentation is to allow another evaluator  
 12438 to repeat the tests and obtain an equivalent result.
- 12439 **15.1.3.7.3 Work unit AVA\_VAN.2-8**
- 12440 The evaluator *shall conduct* penetration testing.
- 12441 The evaluator uses the penetration test documentation resulting from work unit AVA\_VAN.2-6 as a  
 12442 basis for executing penetration tests on the TOE, but this does not preclude the evaluator from  
 12443 performing additional ad hoc penetration tests. If required, the evaluator may devise ad hoc tests  
 12444 as a result of information learnt during penetration testing that, if performed by the evaluator, are  
 12445 to be recorded in the penetration test documentation. Such tests may be required to follow up  
 12446 unexpected results or observations, or to investigate potential vulnerabilities suggested to the  
 12447 evaluator during the pre-planned testing.
- 12448 Should penetration testing show that a hypothesised potential vulnerability does not exist, then the  
 12449 evaluator should determine whether or not the evaluator's own analysis was incorrect, or if  
 12450 evaluation deliverables are incorrect or incomplete.
- 12451 The evaluator is not expected to test for potential vulnerabilities (including those in the public  
 12452 domain) beyond those which required a Basic attack potential. In some cases, however, it will be  
 12453 necessary to carry out a test before the exploitability can be determined. Where, as a result of  
 12454 evaluation expertise, the evaluator discovers an exploitable vulnerability that is beyond basic  
 12455 attack potential, this is reported in the ETR as a residual vulnerability.
- 12456 **15.1.3.7.4 Work unit AVA\_VAN.2-9**
- 12457 The evaluator *shall record* the actual results of the penetration tests.
- 12458 While some specific details of the actual test results may be different from those expected (e.g. time  
 12459 and date fields in an audit record) the overall result should be identical. Any unexpected test  
 12460 results should be investigated. The impact on the evaluation should be stated and justified.
- 12461 **15.1.3.7.5 Work unit AVA\_VAN.2-10**
- 12462 The evaluator *shall report* in the ETR the evaluator penetration testing effort, outlining the testing  
 12463 approach, configuration, depth and results.
- 12464 The penetration testing information reported in the ETR allows the evaluator to convey the overall  
 12465 penetration testing approach and effort expended on this sub-activity. The intent of providing this  
 12466 information is to give a meaningful overview of the evaluator's penetration testing effort. It is not  
 12467 intended that the information regarding penetration testing in the ETR be an exact reproduction of  
 12468 specific test steps or results of individual penetration tests. The intention is to provide enough  
 12469 detail to allow other evaluators and evaluation authorities to gain some insight about the  
 12470 penetration testing approach chosen, amount of penetration testing performed, TOE test  
 12471 configurations, and the overall results of the penetration testing activity.
- 12472 Information that would typically be found in the ETR subclause regarding evaluator penetration  
 12473 testing efforts is:

## ISO/IEC 18045:2008(E)

- 12474 a) TOE test configurations. The particular configurations of the TOE that were  
12475 penetration tested;
- 12476 b) TSFI penetration tested. A brief listing of the TSFI and other TOE interfaces that were  
12477 the focus of the penetration testing;
- 12478 c) Verdict for the sub-activity. The overall judgement on the results of penetration  
12479 testing.
- 12480 This list is by no means exhaustive and is only intended to provide some context as to the type of  
12481 information that should be present in the ETR concerning the penetration testing the evaluator  
12482 performed during the evaluation.
- 12483 **15.1.3.7.6 Work unit AVA\_VAN.2-11**
- 12484 The evaluator *shall examine* the results of all penetration testing to determine that the TOE, in its  
12485 operational environment, is resistant to an attacker possessing a Basic attack potential.
- 12486 If the results reveal that the TOE, in its operational environment, has vulnerabilities exploitable by  
12487 an attacker possessing less than an Enhanced-Basic attack potential, then this evaluator action fails.
- 12488 The guidance in B.2 should be used to determine the attack potential required to exploit a  
12489 particular vulnerability and whether it can therefore be exploited in the intended environment. It  
12490 may not be necessary for the attack potential to be calculated in every instance, only if there is  
12491 some doubt as to whether or not the vulnerability can be exploited by an attacker possessing an  
12492 attack potential less than Enhanced-Basic.
- 12493 **15.1.3.7.7 Work unit AVA\_VAN.2-12**
- 12494 The evaluator *shall report* in the ETR all exploitable vulnerabilities and residual vulnerabilities,  
12495 detailing for each:
- 12496 a) its source (e.g. evaluation methodology activity being undertaken when it was  
12497 conceived, known to the evaluator, read in a publication);
- 12498 b) the SFR(s) not met;
- 12499 c) a description;
- 12500 d) whether it is exploitable in its operational environment or not (i.e. exploitable or  
12501 residual).
- 12502 e) the amount of time, level of expertise, level of knowledge of the TOE, level of  
12503 opportunity and the equipment required to perform the identified vulnerabilities,  
12504 and the corresponding values using the tables B.2 and B.3 of Annex B.2.
- 12505 **15.1.4 Evaluation of sub-activity (AVA\_VAN.3)**
- 12506 **15.1.4.1 Objectives**
- 12507 The objective of this sub-activity is to determine whether the TOE, in its operational environment,  
12508 has vulnerabilities exploitable by attackers possessing Enhanced-Basic attack potential.

12509 **15.1.4.2 Input**

12510 The evaluation evidence for this sub-activity is:

- 12511 a) the ST;
- 12512 b) the functional specification;
- 12513 c) the TOE design;
- 12514 d) the security architecture description;
- 12515 e) the implementation subset selected;
- 12516 f) the guidance documentation;
- 12517 g) the TOE suitable for testing;
- 12518 h) information publicly available to support the identification of possible potential
- 12519 vulnerabilities;
- 12520 a) the results of the testing of the basic design.

12521 The remaining implicit evaluation evidence for this sub-activity depends on the components that  
 12522 have been included in the assurance package. The evidence provided for each component is to be  
 12523 used as input in this sub-activity.

12524 Other input for this sub-activity is:

- 12525 a) current information regarding public domain potential vulnerabilities and attacks (e.g.  
 12526 from an evaluation authority).

12527 **15.1.4.3 Application notes**

12528 During the conduct of evaluation activities the evaluator may also identify areas of concern. These  
 12529 are specific portions of the TOE evidence that the evaluator has some reservation about, although  
 12530 the evidence meets the requirements for the activity with which the evidence is associated. For  
 12531 example, a particular interface specification looks particularly complex, and therefore may be  
 12532 prone to error either in the development of the TOE or in the operation of the TOE. There is no  
 12533 potential vulnerability apparent at this stage, further investigation is required. This is beyond the  
 12534 bounds of encountered, as further investigation is required.

12535 The focused approach to the identification of potential vulnerabilities is an analysis of the evidence  
 12536 with the aim of identifying any potential vulnerabilities evident through the contained information.  
 12537 It is an unstructured analysis, as the approach is not predetermined. Further guidance on focused  
 12538 vulnerability analysis can be found in Annex B.1.4.2.2.

12539 **15.1.4.4 Action AVA\_VAN.3.1E**

12540 ISO/IEC 15408-3 AVA\_VAN.3.1C: *The TOE shall be suitable for testing.*

## ISO/IEC 18045:2008(E)

### 12541 15.1.4.4.1 Work unit AVA\_VAN.3-1

12542 The evaluator **shall examine** the TOE to determine that the test configuration is consistent with  
12543 the configuration under evaluation as specified in the ST.

12544 The TOE provided by the developer and identified in the test plan should have the same unique  
12545 reference as established by the CM capabilities (ALC\_CMC) sub-activities and identified in the ST  
12546 introduction.

12547 It is possible for the ST to specify more than one configuration for evaluation. The TOE may  
12548 comprise a number of distinct hardware and software entities that need to be tested in accordance  
12549 with the ST. The evaluator verifies that all test configurations are consistent with the ST.

12550 The evaluator should consider the security objectives for the operational environment described in  
12551 the ST that may apply to the test environment and ensure they are met in the testing environment.  
12552 There may be some objectives for the operational environment that do not apply to the test  
12553 environment. For example, an objective about user clearances may not apply; however, an  
12554 objective about a single point of connection to a network would apply.

12555 If any test resources are used (e.g. meters, analysers) it will be the evaluator's responsibility to  
12556 ensure that these resources are calibrated correctly.

### 12557 15.1.4.4.2 Work unit AVA\_VAN.3-2

12558 The evaluator **shall examine** the TOE to determine that it has been installed properly and is in a  
12559 known state

12560 It is possible for the evaluator to determine the state of the TOE in a number of ways. For example,  
12561 previous successful completion of the Evaluation of sub-activity (AGD\_PRE.1) sub-activity will  
12562 satisfy this work unit if the evaluator still has confidence that the TOE being used for testing was  
12563 installed properly and is in a known state. If this is not the case, then the evaluator should follow  
12564 the developer's procedures to install and start up the TOE, using the supplied guidance only.

12565 If the evaluator has to perform the installation procedures because the TOE is in an unknown state,  
12566 this work unit when successfully completed could satisfy work unit AGD\_PRE.1-3.

### 12567 15.1.4.5 Action AVA\_VAN.3.2E

#### 12568 15.1.4.5.1 Work unit AVA\_VAN.3-3

12569 The evaluator **shall examine** sources of information publicly available to identify potential  
12570 vulnerabilities in the TOE.

12571 The evaluator examines the sources of information publicly available to support the identification  
12572 of possible potential vulnerabilities in the TOE. There are many sources of publicly available  
12573 information which the evaluator should consider using items such as those available on the world  
12574 wide web, including:

12575 a) specialist publications (magazines, books);

12576 b) research papers;

12577 c) conference proceedings.

12578 The evaluator should not constrain their consideration of publicly available information to the  
12579 above but should consider any other relevant information available.

12580 While examining the evidence provided the evaluator will use the information in the public domain  
12581 to further search for potential vulnerabilities. Where the evaluators have identified areas of  
12582 concern, the evaluator should consider information publicly available that relate to those areas of  
12583 concern.

12584 The availability of information that may be readily available to an attacker that helps to identify  
12585 and facilitate attacks may substantially enhance the attack potential of a given attacker. The  
12586 accessibility of vulnerability information and sophisticated attack tools on the Internet makes it  
12587 more likely that this information will be used in attempts to identify potential vulnerabilities in the  
12588 TOE and exploit them. Modern search tools make such information easily available to the evaluator,  
12589 and the determination of resistance to published potential vulnerabilities and well-known generic  
12590 attacks can be achieved in a cost-effective manner.

12591 The search of the information publicly available should be focused on those sources that refer to  
12592 the technologies used in the development of the product from which the TOE is derived. The  
12593 extensiveness of this search should consider the following factors: TOE type, evaluator experience  
12594 in this TOE type, expected attack potential and the level of ADV evidence available.

12595 The identification process is iterative, where the identification of one potential vulnerability may  
12596 lead to identifying another area of concern that requires further investigation.

12597 The evaluator will report what actions were taken to identify potential vulnerabilities in the  
12598 evidence. However, in this type of search, the evaluator may not be able to describe the steps in  
12599 identifying potential vulnerabilities before the outset of the examination, as the approach may  
12600 evolve as a result of findings during the search.

12601 The evaluator will report the evidence examined in completing the search for potential  
12602 vulnerabilities. This selection of evidence may be derived from those areas of concern identified by  
12603 the evaluator, linked to the evidence the attacker is assumed to be able to obtain, or according to  
12604 another rationale provided by the evaluator.

#### 12605 **15.1.4.6 Action AVA\_VAN.3.3E**

##### 12606 **15.1.4.6.1 Work unit AVA\_VAN.3-4**

12607 The evaluator **shall conduct** a focused search of ST, guidance documentation, functional  
12608 specification, TOE design, security architecture description and implementation representation to  
12609 identify possible potential vulnerabilities in the TOE.

12610 A flaw hypothesis methodology needs to be used whereby specifications and development and  
12611 guidance evidence are analysed and then potential vulnerabilities in the TOE are hypothesised, or  
12612 speculated.

12613 The evaluator uses the knowledge of the TOE design and operation gained from the TOE  
12614 deliverables to conduct a flaw hypothesis to identify potential flaws in the development of the TOE  
12615 and potential errors in the specified method of operation of the TOE.

12616 The security architecture description provides the developer vulnerability analysis, as it  
12617 documents how the TSF protects itself from interference from untrusted subjects and prevents the  
12618 bypass of security enforcement functionality. Therefore, the evaluator should build upon the  
12619 understanding of the TSF protection gained from the analysis of this evidence and then develop  
12620 this in the knowledge gained from other development ADV evidence.

12621 The approach taken is directed by areas of concern identified during examination of the evidence  
12622 during the conduct of evaluation activities and ensuring a representative sample of the  
12623 development and guidance evidence provided for the evaluation is searched.

## ISO/IEC 18045:2008(E)

12624 For guidance on sampling see Annex A.2. This guidance should be considered when selecting the  
12625 subset, giving reasons for:

- 12626 a) the approach used in selection;
- 12627 b) qualification that the evidence to be examined supports that approach.

12628 The areas of concern may relate to the sufficiency of specific protection features detailed in the  
12629 security architecture description.

12630 The evidence to be considered during the vulnerability analysis may be linked to the evidence the  
12631 attacker is assumed to be able to obtain. For example, the developer may protect the TOE design  
12632 and implementation representations, so the only information assumed to be available to an  
12633 attacker is the functional specification and guidance (publicly available). So, although the  
12634 objectives for assurance in the TOE ensure the TOE design and implementation representation  
12635 requirements are met, these design representations may only be searched to further investigate  
12636 areas of concerns.

12637 On the other hand, if the source is publicly available it would be reasonable to assume that the  
12638 attacker has access to the source and can use this in attempts to attack the TOE. Therefore, the  
12639 source should be considered in the focused examination approach.

12640 The following indicates examples for the selection of the subset of evidence to be considered:

- 12641 a) For an evaluation where all levels of design abstraction from functional specification  
12642 to implementation representation are provided, examination of information in the  
12643 functional specification and the implementation representation may be selected, as  
12644 the functional specification provides detail of interfaces available to an attacker, and  
12645 the implementation representation incorporates the design decisions made at all  
12646 other design abstractions. Therefore, the TOE design information will be considered  
12647 as part of the implementation representation.
- 12648 b) Examination of a particular subset of information in each of the design  
12649 representations provided for the evaluation.
- 12650 c) Coverage of particular SFRs through each of the design representations provided for  
12651 the evaluation.
- 12652 d) Examination of each of the design representations provided for the evaluation,  
12653 considering different SFRs within each design representations.
- 12654 e) Examination of aspects of the evidence provided for the evaluation relating to current  
12655 potential vulnerability information the evaluator has received (e.g. from a scheme).

12656 This approach to identification of potential vulnerabilities is to take an ordered and planned  
12657 approach; applying a system to the examination. The evaluator is to describe the method to be  
12658 used in terms of what evidence will be considered, the information within the evidence that is to be  
12659 examined, the manner in which this information is to be considered and the hypothesis that is to be  
12660 created.

12661 The following provide some examples that a hypothesis may take:

- 12662 a) consideration of malformed input for interfaces available to an attacker at the  
12663 external interfaces;



- 12664 b) examination of a key security mechanism cited in the security architecture  
12665 description, such as process separation, hypothesising internal buffer overflows that  
12666 may lead to degradation of separation;
- 12667 c) search to identify any objects created in the TOE implementation representation that  
12668 are then not fully controlled by the TSF, and could be used by an attacker to  
12669 undermine SFRs.
- 12670 For example, the evaluator may identify that interfaces are a potential area of weakness in the TOE  
12671 and specify an approach to the search that "all interface specifications provided in the functional  
12672 specification and TOE design will be searched to hypothesise potential vulnerabilities" and go on to  
12673 explain the methods used in the hypothesis.
- 12674 The identification process is iterative, where the identification of one potential vulnerability may  
12675 lead to identifying another area of concern that requires further investigation.
- 12676 The evaluator will report what actions were taken to identify potential vulnerabilities in the  
12677 evidence. However, in this type of search, the evaluator may not be able to describe the steps in  
12678 identifying potential vulnerabilities before the outset of the examination, as the approach may  
12679 evolve as a result of findings during the search.
- 12680 The evaluator will report the evidence examine in completing the search for potential  
12681 vulnerabilities. This selection of evidence may be derived from those areas of concern identified by  
12682 the evaluator, linked to the evidence the attacker is assumed to be able to obtain, or according to  
12683 another rationale provided by the evaluator.
- 12684 Subject to the SFRs the TOE is to meet in the operational environment, the evaluator's independent  
12685 vulnerability analysis should consider generic potential vulnerabilities under each of the following  
12686 headings:
- 12687 a) generic potential vulnerabilities relevant for the type of TOE being evaluated, as may  
12688 be supplied by the evaluation authority;
- 12689 b) bypassing;
- 12690 c) tampering;
- 12691 d) direct attacks;
- 12692 e) monitoring;
- 12693 f) misuse.
- 12694 Items b) - f) are explained in greater detail in Annex B.
- 12695 The security architecture description should be considered in light of each of the above generic  
12696 potential vulnerabilities. Each potential vulnerability should be considered to search for possible  
12697 ways in which to defeat the TSF protection and undermine the TSF.
- 12698 **15.1.4.6.2 Work unit AVA\_VAN.3-5**
- 12699 The evaluator **shall record** in the ETR the identified potential vulnerabilities that are candidates  
12700 for testing and applicable to the TOE in its operational environment.

## ISO/IEC 18045:2008(E)

12701 It may be identified that no further consideration of the potential vulnerability is required if for  
12702 example the evaluator identifies that measures in the operational environment, either IT or non-IT,  
12703 prevent exploitation of the potential vulnerability in that operational environment. For instance,  
12704 restricting physical access to the TOE to authorised users only may effectively render a potential  
12705 vulnerability to tampering unexploitable.

12706 The evaluator records any reasons for exclusion of potential vulnerabilities from further  
12707 consideration if the evaluator determines that the potential vulnerability is not applicable in the  
12708 operational environment. Otherwise the evaluator records the potential vulnerability for further  
12709 consideration.

12710 A list of potential vulnerabilities applicable to the TOE in its operational environment, which can be  
12711 used as an input into penetration testing activities, shall be reported in the ETR by the evaluators.

### 12712 15.1.4.7 Action AVA\_VAN.3.4E

#### 12713 15.1.4.7.1 Work unit AVA\_VAN.3-6

12714 The evaluator *shall devise* penetration tests, based on the independent search for potential  
12715 vulnerabilities.

12716 The evaluator prepares for penetration testing as necessary to determine the susceptibility of the  
12717 TOE, in its operational environment, to the potential vulnerabilities identified during the search of  
12718 the sources of information publicly available. Any current information provided to the evaluator by  
12719 a third party (e.g. evaluation authority) regarding known potential vulnerabilities will be  
12720 considered by the evaluator, together with any encountered potential vulnerabilities resulting  
12721 from the performance of other evaluation activities.

12722 The evaluator is reminded that, as for considering the security architecture description in the  
12723 search for vulnerabilities (as detailed in AVA\_VAN.3-4), testing should be performed to confirm the  
12724 architectural properties. If requirements from ATE\_DPT are included in the SARs, the developer  
12725 testing evidence will include testing performed to confirm the correct implementation of any  
12726 specific mechanisms detailed in the security architecture description. However, the developer  
12727 testing will not necessarily include testing of all aspects of the architectural properties that protect  
12728 the TSF, as much of this testing will be negative testing in nature, attempting to disprove the  
12729 properties. In developing the strategy for penetration testing, the evaluator will ensure that all  
12730 aspects of the security architecture description are tested, either in functional testing (as  
12731 considered in 14) or evaluator penetration testing.

12732 It will probably be practical to carry out penetration test using a series of test cases, where each  
12733 test case will test for a specific potential vulnerability.

12734 The evaluator is not expected to test for potential vulnerabilities (including those in the public  
12735 domain) beyond those which required an Enhanced-Basic attack potential. In some cases, however,  
12736 it will be necessary to carry out a test before the exploitability can be determined. Where, as a  
12737 result of evaluation expertise, the evaluator discovers an exploitable vulnerability that is beyond  
12738 Enhanced-Basic attack potential, this is reported in the ETR as a residual vulnerability.

12739 Guidance on determining the necessary attack potential to exploit a potential vulnerability can be  
12740 found in Annex B.2.

12741 Potential vulnerabilities hypothesised as exploitable only by attackers possessing Moderate or  
12742 High attack potential do not result in a failure of this evaluator action. Where analysis supports the  
12743 hypothesis, these need not be considered further as an input to penetration testing. However, such  
12744 vulnerabilities are reported in the ETR as residual vulnerabilities.

12745 Potential vulnerabilities hypothesised as exploitable by an attacker possessing a Basic or  
12746 Enhanced-Basic attack potential and resulting in a violation of the security objectives should be the

12747 highest priority potential vulnerabilities comprising the list used to direct penetration testing  
12748 against the TOE.

12749 **15.1.4.7.2 Work unit AVA\_VAN.3-7**

12750 The evaluator **shall produce** penetration test documentation for the tests based on the list of  
12751 potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test  
12752 documentation shall include:

- 12753 a) identification of the potential vulnerability the TOE is being tested for;
- 12754 b) instructions to connect and setup all required test equipment as required to conduct  
12755 the penetration test;
- 12756 c) instructions to establish all penetration test prerequisite initial conditions;
- 12757 d) instructions to stimulate the TSF;
- 12758 e) instructions for observing the behaviour of the TSF;
- 12759 f) descriptions of all expected results and the necessary analysis to be performed on the  
12760 observed behaviour for comparison against expected results;
- 12761 g) instructions to conclude the test and establish the necessary post-test state for the  
12762 TOE.

12763 The evaluator prepares for penetration testing based on the list of potential vulnerabilities  
12764 identified during the search of the public domain and the analysis of the evaluation evidence.

12765 The evaluator is not expected to determine the exploitability for potential vulnerabilities beyond  
12766 those for which an Enhanced-Basic attack potential is required to effect an attack. However, as a  
12767 result of evaluation expertise, the evaluator may discover a potential vulnerability that is  
12768 exploitable only by an attacker with greater than Enhanced-Basic attack potential. Such  
12769 vulnerabilities are to be reported in the ETR as residual vulnerabilities.

12770 With an understanding of the potential vulnerability, the evaluator determines the most feasible  
12771 way to test for the TOE's susceptibility. Specifically the evaluator considers:

- 12772 a) the TSFI or other TOE interface that will be used to stimulate the TSF and observe  
12773 responses (It is possible that the evaluator will need to use an interface to the TOE  
12774 other than the TSFI to demonstrate properties of the TSF such as those described in  
12775 the security architecture description (as required by ADV\_ARC). It should be noted,  
12776 that although these TOE interfaces provide a means of testing the TSF properties,  
12777 they are not the subject of the test);
- 12778 b) initial conditions that will need to exist for the test (i.e. any particular objects or  
12779 subjects that will need to exist and security attributes they will need to have);
- 12780 c) special test equipment that will be required to either stimulate a TSFI or make  
12781 observations of a TSFI (although it is unlikely that specialist equipment would be  
12782 required to exploit a potential vulnerability assuming an Enhanced-Basic attack  
12783 potential);

## ISO/IEC 18045:2008(E)

- 12784 d) whether theoretical analysis should replace physical testing, particularly relevant  
12785 where the results of an initial test can be extrapolated to demonstrate that repeated  
12786 attempts of an attack are likely to succeed after a given number of attempts.
- 12787 The evaluator will probably find it practical to carry out penetration testing using a series of test  
12788 cases, where each test case will test for a specific potential vulnerability.
- 12789 The intent of specifying this level of detail in the test documentation is to allow another evaluator  
12790 to repeat the tests and obtain an equivalent result.
- 12791 **15.1.4.7.3 Work unit AVA\_VAN.3-8**
- 12792 The evaluator **shall conduct** penetration testing.
- 12793 The evaluator uses the penetration test documentation resulting from work unit AVA\_VAN.3-6 as a  
12794 basis for executing penetration tests on the TOE, but this does not preclude the evaluator from  
12795 performing additional ad hoc penetration tests. If required, the evaluator may devise ad hoc tests  
12796 as a result of information learnt during penetration testing that, if performed by the evaluator, are  
12797 to be recorded in the penetration test documentation. Such tests may be required to follow up  
12798 unexpected results or observations, or to investigate potential vulnerabilities suggested to the  
12799 evaluator during the pre-planned testing.
- 12800 Should penetration testing show that a hypothesised potential vulnerability does not exist, then the  
12801 evaluator should determine whether or not the evaluator's own analysis was incorrect, or if  
12802 evaluation deliverables are incorrect or incomplete.
- 12803 The evaluator is not expected to test for potential vulnerabilities (including those in the public  
12804 domain) beyond those which required an Enhanced-Basic attack potential. In some cases, however,  
12805 it will be necessary to carry out a test before the exploitability can be determined. Where, as a  
12806 result of evaluation expertise, the evaluator discovers an exploitable vulnerability that is beyond  
12807 Enhanced-Basic attack potential, this is reported in the ETR as a residual vulnerability.
- 12808 **15.1.4.7.4 Work unit AVA\_VAN.3-9**
- 12809 The evaluator **shall record** the actual results of the penetration tests.
- 12810 While some specific details of the actual test results may be different from those expected (e.g. time  
12811 and date fields in an audit record) the overall result should be identical. Any unexpected test  
12812 results should be investigated. The impact on the evaluation should be stated and justified.
- 12813 **15.1.4.7.5 Work unit AVA\_VAN.3-10**
- 12814 The evaluator **shall report** in the ETR the evaluator penetration testing effort, outlining the testing  
12815 approach, configuration, depth and results.
- 12816 The penetration testing information reported in the ETR allows the evaluator to convey the overall  
12817 penetration testing approach and effort expended on this sub-activity. The intent of providing this  
12818 information is to give a meaningful overview of the evaluator's penetration testing effort. It is not  
12819 intended that the information regarding penetration testing in the ETR be an exact reproduction of  
12820 specific test steps or results of individual penetration tests. The intention is to provide enough  
12821 detail to allow other evaluators and evaluation authorities to gain some insight about the  
12822 penetration testing approach chosen, amount of penetration testing performed, TOE test  
12823 configurations, and the overall results of the penetration testing activity.
- 12824 Information that would typically be found in the ETR subclause regarding evaluator penetration  
12825 testing efforts is:

12826 a) TOE test configurations. The particular configurations of the TOE that were  
12827 penetration tested;

12828 b) TSFI penetration tested. A brief listing of the TSFI and other TOE interfaces that were  
12829 the focus of the penetration testing;

12830 c) Verdict for the sub-activity. The overall judgement on the results of penetration  
12831 testing.

12832 This list is by no means exhaustive and is only intended to provide some context as to the type of  
12833 information that should be present in the ETR concerning the penetration testing the evaluator  
12834 performed during the evaluation.

#### 12835 15.1.4.7.6 Work unit AVA\_VAN.3-11

12836 The evaluator *shall examine* the results of all penetration testing to determine that the TOE, in its  
12837 operational environment, is resistant to an attacker possessing an Enhanced-Basic attack potential.

12838 If the results reveal that the TOE, in its operational environment, has vulnerabilities exploitable by  
12839 an attacker possessing less than Moderate attack potential, then this evaluator action fails.

12840 The guidance in B.2 should be used to determine the attack potential required to exploit a  
12841 particular vulnerability and whether it can therefore be exploited in the intended environment. It  
12842 may not be necessary for the attack potential to be calculated in every instance, only if there is  
12843 some doubt as to whether or not the vulnerability can be exploited by an attacker possessing an  
12844 attack potential less than Moderate.

#### 12845 15.1.4.7.7 Work unit AVA\_VAN.3-12

12846 The evaluator *shall report* in the ETR all exploitable vulnerabilities and residual vulnerabilities,  
12847 detailing for each:

12848 a) its source (e.g. evaluation methodology activity being undertaken when it was  
12849 conceived, known to the evaluator, read in a publication);

12850 b) the SFR(s) not met;

12851 c) a description;

12852 d) whether it is exploitable in its operational environment or not (i.e. exploitable or  
12853 residual).

12854 e) the amount of time, level of expertise, level of knowledge of the TOE, level of  
12855 opportunity and the equipment required to perform the identified vulnerabilities,  
12856 and the corresponding values using the tables B.2 and B.3 of Annex B.2.

### 12857 15.1.5 Evaluation of sub-activity (AVA\_VAN.4)

#### 12858 15.1.5.1 Objectives

12859 The objective of this sub-activity is to determine whether the TOE, in its operational environment,  
12860 has vulnerabilities exploitable by attackers possessing Moderate attack potential.

## ISO/IEC 18045:2008(E)

### 12861 15.1.5.2 Input

12862 The evaluation evidence for this sub-activity is:

- 12863 a) the ST;
- 12864 b) the functional specification;
- 12865 c) the TOE design;
- 12866 d) the security architecture description;
- 12867 e) the implementation representation;
- 12868 f) the guidance documentation;
- 12869 g) the TOE suitable for testing;
- 12870 h) information publicly available to support the identification of possible potential  
12871 vulnerabilities;
- 12872 i) the results of the testing of the basic design.

12873 The remaining implicit evaluation evidence for this sub-activity depends on the components that  
12874 have been included in the assurance package. The evidence provided for each component is to be  
12875 used as input in this sub-activity.

12876 Other input for this sub-activity is:

- 12877 a) current information regarding public domain potential vulnerabilities and attacks (e.g.  
12878 from an evaluation authority).

### 12879 15.1.5.3 Application notes

12880 The methodical analysis approach takes the form of a structured examination of the evidence. This  
12881 method requires the evaluator to specify the structure and form the analysis will take (i.e. the  
12882 manner in which the analysis is performed is predetermined, unlike the focused analysis). The  
12883 method is specified in terms of the information that will be considered and how/why it will be  
12884 considered. Further guidance on methodical vulnerability analysis can be found in Annex B.1.4.2.3.

### 12885 15.1.5.4 Action AVA\_VAN.4.1E

12886 ISO/IEC 15408-3 AVA\_VAN.4.1C: *The TOE shall be suitable for testing.*

#### 12887 15.1.5.4.1 Work unit AVA\_VAN.4-1

12888 The evaluator **shall examine** the TOE to determine that the test configuration is consistent with  
12889 the configuration under evaluation as specified in the ST.

12890 The TOE provided by the developer and identified in the test plan should have the same unique  
12891 reference as established by the CM capabilities (ALC\_CMC) sub-activities and identified in the ST  
12892 introduction.

12893 It is possible for the ST to specify more than one configuration for evaluation. The TOE may  
12894 comprise a number of distinct hardware and software entities that need to be tested in accordance  
12895 with the ST. The evaluator verifies that all test configurations are consistent with the ST.

12896 The evaluator should consider the security objectives for the operational environment described in  
12897 the ST that may apply to the test environment and ensure they are met in the testing environment.  
12898 There may be some objectives for the operational environment that do not apply to the test  
12899 environment. For example, an objective about user clearances may not apply; however, an  
12900 objective about a single point of connection to a network would apply.

12901 If any test resources are used (e.g. meters, analysers) it will be the evaluator's responsibility to  
12902 ensure that these resources are calibrated correctly.

#### 12903 **15.1.5.4.2 Work unit AVA\_VAN.4-2**

12904 The evaluator **shall examine** the TOE to determine that it has been installed properly and is in a  
12905 known state

12906 It is possible for the evaluator to determine the state of the TOE in a number of ways. For example,  
12907 previous successful completion of the Evaluation of sub-activity (AGD\_PRE.1) sub-activity will  
12908 satisfy this work unit if the evaluator still has confidence that the TOE being used for testing was  
12909 installed properly and is in a known state. If this is not the case, then the evaluator should follow  
12910 the developer's procedures to install and start up the TOE, using the supplied guidance only.

12911 If the evaluator has to perform the installation procedures because the TOE is in an unknown state,  
12912 this work unit when successfully completed could satisfy work unit AGD\_PRE.1-3.

#### 12913 **15.1.5.5 Action AVA\_VAN.4.2E**

##### 12914 **15.1.5.5.1 Work unit AVA\_VAN.4-3**

12915 The evaluator **shall examine** sources of information publicly available to identify potential  
12916 vulnerabilities in the TOE.

12917 The evaluator examines the sources of information publicly available to support the identification  
12918 of possible potential vulnerabilities in the TOE. There are many sources of publicly available  
12919 information which the evaluator should consider using items such as those available on the world  
12920 wide web, including:

- 12921 a) specialist publications (magazines, books);
- 12922 b) research papers;
- 12923 c) conference proceedings.

12924 The evaluator should not constrain their consideration of publicly available information to the  
12925 above, but should consider any other relevant information available.

12926 While examining the evidence provided the evaluator will use the information in the public domain  
12927 to further search for potential vulnerabilities. Where the evaluators have identified areas of  
12928 concern, the evaluator should consider information publicly available that relate to those areas of  
12929 concern.

12930 The availability of information that may be readily available to an attacker that helps to identify  
12931 and facilitate attacks may substantially enhance the attack potential of a given attacker. The  
12932 accessibility of vulnerability information and sophisticated attack tools on the Internet makes it  
12933 more likely that this information will be used in attempts to identify potential vulnerabilities in the  
12934 TOE and exploit them. Modern search tools make such information easily available to the evaluator,

## ISO/IEC 18045:2008(E)

12935 and the determination of resistance to published potential vulnerabilities and well known generic  
12936 attacks can be achieved in a cost-effective manner.

12937 The search of the information publicly available should be focused on those sources that refer to  
12938 the technologies used in the development of the product from which the TOE is derived. The  
12939 extensiveness of this search should consider the following factors: TOE type, evaluator experience  
12940 in this TOE type, expected attack potential and the level of ADV evidence available.

12941 The identification process is iterative, where the identification of one potential vulnerability may  
12942 lead to identifying another area of concern that requires further investigation.

12943 The evaluator will describe the approach to be taken to identify potential vulnerabilities in the  
12944 publicly available material, detailing the search to be performed. This may be driven by factors  
12945 such as areas of concern identified by the evaluator, linked to the evidence the attacker is assumed  
12946 to be able to obtain. However, it is recognised that in this type of search the approach may further  
12947 evolve as a result of findings during the search. Therefore, the evaluator will also report any  
12948 actions taken in addition to those described in the approach to further investigate issues thought to  
12949 lead to potential vulnerabilities, and will report the evidence examined in completing the search  
12950 for potential vulnerabilities.

12951 **15.1.5.6 Action AVA\_VAN.4.3E**

12952 **15.1.5.6.1 Work unit AVA\_VAN.4-4**

12953 The evaluator **shall conduct** a methodical analysis of ST, guidance documentation, functional  
12954 specification, TOE design, security architecture description and implementation representation to  
12955 identify possible potential vulnerabilities in the TOE.

12956 Guidance on methodical vulnerability analysis is provided in Annex B.1.4.2.3.

12957 This approach to identification of potential vulnerabilities is to take an ordered and planned  
12958 approach. A system is to be applied in the examination. The evaluator is to describe the method to  
12959 be used in terms of the manner in which this information is to be considered and the hypothesis  
12960 that is to be created.

12961 A flaw hypothesis methodology needs to be used whereby the ST, development (functional  
12962 specification, TOE design and implementation representation) and guidance evidence are analysed  
12963 and then vulnerabilities in the TOE are hypothesised, or speculated.

12964 The evaluator uses the knowledge of the TOE design and operation gained from the TOE  
12965 deliverables to conduct a flaw hypothesis to identify potential flaws in the development of the TOE  
12966 and potential errors in the specified method of operation of the TOE.

12967 The security architecture description provides the developer vulnerability analysis, as it  
12968 documents how the TSF protects itself from interference from untrusted subjects and prevents the  
12969 bypass of security enforcement functionality. Therefore, the evaluator should build upon the  
12970 understanding of the TSF protection gained from the analysis of this evidence and then develop  
12971 this in the knowledge gained from other development ADV evidence.

12972 The approach taken to the methodical search for vulnerabilities is to consider any areas of concern  
12973 identified in the results of the evaluator's assessment of the development and guidance evidence.  
12974 However, the evaluator should also consider each aspect of the security architecture analysis to  
12975 search for any ways in which the protection of the TSF can be undermined. It may be helpful to  
12976 structure the methodical analysis on the basis of the material presented in the security architecture  
12977 description, introducing concerns from other ADV evidence as appropriate. The analysis can then  
12978 be further developed to ensure all other material from the ADV evidence is considered.



12979 The following provide some examples of hypotheses that may be created when examining the  
12980 evidence:

12981 a) consideration of malformed input for interfaces available to an attacker at the  
12982 external interfaces;

12983 b) examination of a key security mechanism cited in the security architecture  
12984 description, such as process separation, hypothesising internal buffer overflows that  
12985 may lead to degradation of separation;

12986 c) search to identify any objects created in the TOE implementation representation that  
12987 are then not fully controlled by the TSF, and could be used by an attacker to  
12988 undermine SFRs.

12989 For example, the evaluator may identify that interfaces are a potential area of weakness in the TOE  
12990 and specify an approach to the search that 'all interface specifications in the evidence provided will  
12991 be searched to hypothesise potential vulnerabilities' and go on to explain the methods used in the  
12992 hypothesis.

12993 In addition, areas of concern the evaluator has identified during examination of the evidence  
12994 during the conduct of evaluation activities. Areas of concern may also be identified during the  
12995 conduct of other work units associated with this component, in particular AVA\_VAN.4-7,  
12996 AVA\_VAN.4-5 and AVA\_VAN.4-6 where the development and conduct of penetration tests may  
12997 identify further areas of concerns for investigation, or potential vulnerabilities.

12998 However, examination of only a subset of the development and guidance evidence or their contents  
12999 is not permitted in this level of rigour. The approach description should provide a demonstration  
13000 that the methodical approach used is complete, providing confidence that the approach used to  
13001 search the deliverables has considered all of the information provided in those deliverables.

13002 This approach to identification of potential vulnerabilities is to take an ordered and planned  
13003 approach; applying a system to the examination. The evaluator is to describe the method to be  
13004 used in terms of how the evidence will be considered; the manner in which this information is to be  
13005 considered and the hypothesis that is to be created. This approach should be agreed with the  
13006 evaluation authority, and the evaluation authority may provide detail of any additional approaches  
13007 the evaluator should take to the vulnerability analysis and identify any additional information that  
13008 should be considered by the evaluator.

13009 Although a system to identifying potential vulnerabilities is predefined, the identification process  
13010 may still be iterative, where the identification of one potential vulnerability may lead to identifying  
13011 another area of concern that requires further investigation.

13012 Subject to the SFRs the TOE is to meet in the operational environment, the evaluator's independent  
13013 vulnerability analysis should consider generic potential vulnerabilities under each of the following  
13014 headings:

13015 a) generic potential vulnerabilities relevant for the type of TOE being evaluated, as may  
13016 be supplied by the evaluation authority;

13017 b) bypassing;

13018 c) tampering;

13019 d) direct attacks;

## ISO/IEC 18045:2008(E)

- 13020 e) monitoring;
- 13021 f) misuse.
- 13022 Items b) - f) are explained in greater detail in Annex B.
- 13023 The security architecture description should be considered in light of each of the above generic  
13024 potential vulnerabilities. Each potential vulnerability should be considered to search for possible  
13025 ways in which to defeat the TSF protection and undermine the TSF.
- 13026 **15.1.5.6.2 Work unit AVA\_VAN.4-5**
- 13027 The evaluator ***shall record*** in the ETR the identified potential vulnerabilities that are candidates  
13028 for testing and applicable to the TOE in its operational environment.
- 13029 It may be identified that no further consideration of the potential vulnerability is required if for  
13030 example the evaluator identifies that measures in the operational environment, either IT or non-IT,  
13031 prevent exploitation of the potential vulnerability in that operational environment. For instance,  
13032 restricting physical access to the TOE to authorised users only may effectively render a potential  
13033 vulnerability to tampering unexploitable.
- 13034 The evaluator records any reasons for exclusion of potential vulnerabilities from further  
13035 consideration if the evaluator determines that the potential vulnerability is not applicable in the  
13036 operational environment. Otherwise the evaluator records the potential vulnerability for further  
13037 consideration.
- 13038 A list of potential vulnerabilities applicable to the TOE in its operational environment, which can be  
13039 used as an input into penetration testing activities, shall be reported in the ETR by the evaluators.
- 13040 **15.1.5.7 Action AVA\_VAN.4.4E**
- 13041 **15.1.5.7.1 Work unit AVA\_VAN.4-6**
- 13042 The evaluator ***shall devise*** penetration tests, based on the independent search for potential  
13043 vulnerabilities.
- 13044 The evaluator prepares for penetration testing as necessary to determine the susceptibility of the  
13045 TOE, in its operational environment, to the potential vulnerabilities identified during the search of  
13046 the sources of information publicly available. Any current information provided to the evaluator by  
13047 a third party (e.g. evaluation authority) regarding known potential vulnerabilities will be  
13048 considered by the evaluator, together with any encountered potential vulnerabilities resulting  
13049 from the performance of other evaluation activities.
- 13050 The evaluator is reminded that, as for considering the security architecture description in the  
13051 search for vulnerabilities (as detailed in AVA\_VAN.4-3), testing should be performed to confirm the  
13052 architectural properties. If requirements from ATE\_DPT are included in the SARs, the developer  
13053 testing evidence will include testing performed to confirm the correct implementation of any  
13054 specific mechanisms detailed in the security architecture description. However, the developer  
13055 testing will not necessarily include testing of all aspects of the architectural properties that protect  
13056 the TSF, as much of this testing will be negative testing in nature, attempting to disprove the  
13057 properties. In developing the strategy for penetration testing, the evaluator will ensure that all  
13058 aspects of the security architecture description are tested, either in functional testing (as  
13059 considered in 14) or evaluator penetration testing.
- 13060 The evaluator will probably find it practical to carry out penetration test using a series of test cases,  
13061 where each test case will test for a specific potential vulnerability.

- 13062 The evaluator is not expected to test for potential vulnerabilities (including those in the public  
13063 domain) beyond those which required a Moderate attack potential. In some cases, however, it will  
13064 be necessary to carry out a test before the exploitability can be determined. Where, as a result of  
13065 evaluation expertise, the evaluator discovers an exploitable vulnerability that is beyond Moderate  
13066 attack potential, this is reported in the ETR as a residual vulnerability.
- 13067 Guidance on determining the necessary attack potential to exploit a potential vulnerability can be  
13068 found in Annex B.2.
- 13069 Potential vulnerabilities hypothesised as exploitable by an attacker possessing a Moderate (or less)  
13070 attack potential and resulting in a violation of the security objectives should be the highest priority  
13071 potential vulnerabilities comprising the list used to direct penetration testing against the TOE.
- 13072 **15.1.5.7.2 Work unit AVA\_VAN.4-7**
- 13073 The evaluator *shall produce* penetration test documentation for the tests based on the list of  
13074 potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test  
13075 documentation shall include:
- 13076 a) identification of the potential vulnerability the TOE is being tested for;
  - 13077 b) instructions to connect and setup all required test equipment as required to conduct  
13078 the penetration test;
  - 13079 c) instructions to establish all penetration test prerequisite initial conditions;
  - 13080 d) instructions to stimulate the TSF;
  - 13081 e) instructions for observing the behaviour of the TSF;
  - 13082 f) descriptions of all expected results and the necessary analysis to be performed on the  
13083 observed behaviour for comparison against expected results;
  - 13084 g) instructions to conclude the test and establish the necessary post-test state for the  
13085 TOE.
- 13086 The evaluator prepares for penetration testing based on the list of potential vulnerabilities  
13087 identified during the search of the public domain and the analysis of the evaluation evidence.
- 13088 The evaluator is not expected to determine the exploitability for potential vulnerabilities beyond  
13089 those for which a Moderate attack potential is required to effect an attack. However, as a result of  
13090 evaluation expertise, the evaluator may discover a potential vulnerability that is exploitable only  
13091 by an attacker with greater than Moderate attack potential. Such vulnerabilities are to be reported  
13092 in the ETR as residual vulnerabilities.
- 13093 With an understanding of the potential vulnerability, the evaluator determines the most feasible  
13094 way to test for the TOE's susceptibility. Specifically the evaluator considers:
- 13095 a) the TSFI or other TOE interface that will be used to stimulate the TSF and observe  
13096 responses (It is possible that the evaluator will need to use an interface to the TOE  
13097 other than the TSFI to demonstrate properties of the TSF such as those described in  
13098 the security architecture description (as required by ADV\_ARC). It should be noted,  
13099 that although these TOE interfaces provide a means of testing the TSF properties,  
13100 they are not the subject of the test.);

## ISO/IEC 18045:2008(E)

- 13101 b) initial conditions that will need to exist for the test (i.e. any particular objects or  
13102 subjects that will need to exist and security attributes they will need to have);
- 13103 c) special test equipment that will be required to either stimulate a TSFI or make  
13104 observations of a TSFI;
- 13105 d) whether theoretical analysis should replace physical testing, particularly relevant  
13106 where the results of an initial test can be extrapolated to demonstrate that repeated  
13107 attempts of an attack are likely to succeed after a given number of attempts.
- 13108 The evaluator will probably find it practical to carry out penetration testing using a series of test  
13109 cases, where each test case will test for a specific potential vulnerability.
- 13110 The intent of specifying this level of detail in the test documentation is to allow another evaluator  
13111 to repeat the tests and obtain an equivalent result.
- 13112 **15.1.5.7.3 Work unit AVA\_VAN.4-8**
- 13113 The evaluator **shall conduct** penetration testing.
- 13114 The evaluator uses the penetration test documentation resulting from work unit AVA\_VAN.4-6 as a  
13115 basis for executing penetration tests on the TOE, but this does not preclude the evaluator from  
13116 performing additional ad hoc penetration tests. If required, the evaluator may devise ad hoc tests  
13117 as a result of information learnt during penetration testing that, if performed by the evaluator, are  
13118 to be recorded in the penetration test documentation. Such tests may be required to follow up  
13119 unexpected results or observations, or to investigate potential vulnerabilities suggested to the  
13120 evaluator during the pre-planned testing.
- 13121 Should penetration testing show that a hypothesised potential vulnerability does not exist, then the  
13122 evaluator should determine whether or not the evaluator's own analysis was incorrect, or if  
13123 evaluation deliverables are incorrect or incomplete.
- 13124 The evaluator is not expected to test for potential vulnerabilities (including those in the public  
13125 domain) beyond those which required a Moderate attack potential. In some cases, however, it will  
13126 be necessary to carry out a test before the exploitability can be determined. Where, as a result of  
13127 evaluation expertise, the evaluator discovers an exploitable vulnerability that is beyond Moderate  
13128 attack potential, this is reported in the ETR as a residual vulnerability.
- 13129 **15.1.5.7.4 Work unit AVA\_VAN.4-9**
- 13130 The evaluator **shall record** the actual results of the penetration tests.
- 13131 While some specific details of the actual test results may be different from those expected (e.g. time  
13132 and date fields in an audit record) the overall result should be identical. Any unexpected test  
13133 results should be investigated. The impact on the evaluation should be stated and justified.
- 13134 **15.1.5.7.5 Work unit AVA\_VAN.4-10**
- 13135 The evaluator **shall report** in the ETR the evaluator penetration testing effort, outlining the testing  
13136 approach, configuration, depth and results.
- 13137 The penetration testing information reported in the ETR allows the evaluator to convey the overall  
13138 penetration testing approach and effort expended on this sub-activity. The intent of providing this  
13139 information is to give a meaningful overview of the evaluator's penetration testing effort. It is not  
13140 intended that the information regarding penetration testing in the ETR be an exact reproduction of  
13141 specific test steps or results of individual penetration tests. The intention is to provide enough

13142 detail to allow other evaluators and evaluation authorities to gain some insight about the  
13143 penetration testing approach chosen, amount of penetration testing performed, TOE test  
13144 configurations, and the overall results of the penetration testing activity.

13145 Information that would typically be found in the ETR subclause regarding evaluator penetration  
13146 testing efforts is:

13147 a) TOE test configurations. The particular configurations of the TOE that were  
13148 penetration tested;

13149 b) TSFI penetration tested. A brief listing of the TSFI and other TOE interfaces that were  
13150 the focus of the penetration testing;

13151 c) Verdict for the sub-activity. The overall judgement on the results of penetration  
13152 testing.

13153 This list is by no means exhaustive and is only intended to provide some context as to the type of  
13154 information that should be present in the ETR concerning the penetration testing the evaluator  
13155 performed during the evaluation.

#### 13156 15.1.5.7.6 Work unit AVA\_VAN.4-11

13157 The evaluator **shall examine** the results of all penetration testing to determine that the TOE, in its  
13158 operational environment, is resistant to an attacker possessing a Moderate attack potential.

13159 If the results reveal that the TOE, in its operational environment, has vulnerabilities exploitable by  
13160 an attacker possessing less than a High attack potential, then this evaluator action fails.

13161 The guidance in B.2 should be used to determine the attack potential required to exploit a  
13162 particular vulnerability and whether it can therefore be exploited in the intended environment. It  
13163 may not be necessary for the attack potential to be calculated in every instance, only if there is  
13164 some doubt as to whether or not the vulnerability can be exploited by an attacker possessing an  
13165 attack potential less than High.

#### 13166 15.1.5.7.7 Work unit AVA\_VAN.4-12

13167 The evaluator **shall report** in the ETR all exploitable vulnerabilities and residual vulnerabilities,  
13168 detailing for each:

13169 a) its source (e.g. evaluation methodology activity being undertaken when it was  
13170 conceived, known to the evaluator, read in a publication);

13171 b) the SFR(s) not met;

13172 c) a description;

13173 d) whether it is exploitable in its operational environment or not (i.e. exploitable or  
13174 residual).

13175 e) the amount of time, level of expertise, level of knowledge of the TOE, level of  
13176 opportunity and the equipment required to perform the identified vulnerabilities,  
13177 and the corresponding values using the tables B.2 and B.3 of Annex B.2.

13178 **15.1.6 Evaluation of sub-activity (AVA\_VAN.5)**

13179 The work units for the evaluation of the sub-activity AVA\_VAN.5 are copied from the work units of  
13180 AVA\_VAN.4 as far as possible except that the TOE is attacked by attackers possessing High attack  
13181 potential.

13182 **15.1.6.1 Objectives**

13183 The objective of this sub-activity is to determine whether the TOE, in its operational environment,  
13184 has vulnerabilities exploitable by attackers possessing **High** attack potential.

13185 **15.1.6.2 Input**

13186 The evaluation evidence for this sub-activity is:

- 13187 a) the ST;
- 13188 b) the functional specification;
- 13189 c) the TOE design;
- 13190 d) the security architecture description;
- 13191 e) the implementation representation;
- 13192 f) the guidance documentation;
- 13193 g) the TOE suitable for testing;
- 13194 h) information publicly available to support the identification of possible potential  
13195 vulnerabilities;
- 13196 i) the results of the testing of the basic design.

13197 The remaining implicit evaluation evidence for this sub-activity depends on the components that  
13198 have been included in the assurance package. The evidence provided for each component is to be  
13199 used as input in this sub-activity.

13200 Other input for this sub-activity is:

- 13201 a) current information regarding public domain potential vulnerabilities and attacks (e.g.  
13202 from an evaluation authority).

13203 **15.1.6.3 Application notes**

13204 The methodical analysis approach takes the form of a structured examination of the evidence. This  
13205 method requires the evaluator to specify the structure and form the analysis will take (i.e. the  
13206 manner in which the analysis is performed is predetermined, unlike the focused analysis). The  
13207 method is specified in terms of the information that will be considered and how/why it will be  
13208 considered. Further guidance on methodical vulnerability analysis can be found in Annex B.2.2.2.3.

13209      **15.1.6.4 Action AVA\_VAN.5.1E**13210      **AVA\_VAN.5.1C**    *The TOE shall be suitable for testing.*13211      **15.1.6.4.1 Work unit AVA\_VAN.5-1**

13212      The evaluator **shall examine** the TOE to determine that the test configuration is consistent with  
 13213      the configuration under evaluation as specified in the ST.

13214      The TOE provided by the developer and identified in the test plan should have the same unique  
 13215      reference as established by the CM capabilities (ALC\_CMC) sub-activities and identified in the ST  
 13216      introduction.

13217      It is possible for the ST to specify more than one configuration for evaluation. The TOE may  
 13218      comprise a number of distinct hardware and software entities that need to be tested in accordance  
 13219      with the ST. The evaluator verifies that all test configurations are consistent with the ST.

13220      The evaluator should consider the security objectives for the operational environment described in  
 13221      the ST that may apply to the test environment and ensure they are met in the testing environment.  
 13222      There may be some objectives for the operational environment that do not apply to the test  
 13223      environment. For example, an objective about user clearances may not apply; however, an  
 13224      objective about a single point of connection to a network would apply.

13225      If any test resources are used (e.g. meters, analysers) it will be the evaluator's responsibility to  
 13226      ensure that these resources are calibrated correctly.

13227      **15.1.6.4.2 Work unit AVA\_VAN.5-2**

13228      The evaluator **shall examine** the TOE to determine that it has been installed properly and is in a  
 13229      known state

13230      It is possible for the evaluator to determine the state of the TOE in a number of ways. For example,  
 13231      previous successful completion of the Evaluation of sub-activity (AGD\_PRE.1) sub-activity will  
 13232      satisfy this work unit if the evaluator still has confidence that the TOE being used for testing was  
 13233      installed properly and is in a known state. If this is not the case, then the evaluator should follow  
 13234      the developer's procedures to install and start up the TOE, using the supplied guidance only.

13235      If the evaluator has to perform the installation procedures because the TOE is in an unknown state,  
 13236      this work unit when successfully completed could satisfy work unit AGD\_PRE.1-3.

13237      **15.1.6.5 Action AVA\_VAN.5.2E**13238      **15.1.6.5.1 Work unit AVA\_VAN.5-3**

13239      The evaluator **shall examine** sources of information publicly available to identify potential  
 13240      vulnerabilities in the TOE.

13241      The evaluator examines the sources of information publicly available to support the identification  
 13242      of possible potential vulnerabilities in the TOE. There are many sources of publicly available  
 13243      information which the evaluator should consider using items such as those available on the world  
 13244      wide web, including:

13245              a) specialist publications (magazines, books);

13246              b) research papers;

13247              c) conference proceedings.

## ISO/IEC 18045:2008(E)

13248 The evaluator should not constrain their consideration of publicly available information to the  
13249 above but should consider any other relevant information available.

13250 While examining the evidence provided the evaluator will use the information in the public domain  
13251 to further search for potential vulnerabilities. Where the evaluators have identified areas of  
13252 concern, the evaluator should consider information publicly available that relate to those areas of  
13253 concern.

13254 The availability of information that may be readily available to an attacker that helps to identify  
13255 and facilitate attacks may substantially enhance the attack potential of a given attacker. The  
13256 accessibility of vulnerability information and sophisticated attack tools on the Internet makes it  
13257 more likely that this information will be used in attempts to identify potential vulnerabilities in the  
13258 TOE and exploit them. Modern search tools make such information easily available to the evaluator,  
13259 and the determination of resistance to published potential vulnerabilities and well-known generic  
13260 attacks can be achieved in a cost-effective manner.

13261 The search of the information publicly available should be focused on those sources that refer to  
13262 the technologies used in the development of the product from which the TOE is derived. The  
13263 extensiveness of this search should consider the following factors: TOE type, evaluator experience  
13264 in this TOE type, expected attack potential and the level of ADV evidence available.

13265 The identification process is iterative, where the identification of one potential vulnerability may  
13266 lead to identifying another area of concern that requires further investigation.

13267 The evaluator will describe the approach to be taken to identify potential vulnerabilities in the  
13268 publicly available material, detailing the search to be performed. This may be driven by factors  
13269 such as areas of concern identified by the evaluator, linked to the evidence the attacker is assumed  
13270 to be able to obtain. However, it is recognised that in this type of search the approach may further  
13271 evolve as a result of findings during the search. Therefore, the evaluator will also report any  
13272 actions taken in addition to those described in the approach to further investigate issues thought to  
13273 lead to potential vulnerabilities, and will report the evidence examined in completing the search  
13274 for potential vulnerabilities.

### 13275 15.1.6.6 Action AVA\_VAN.5.3E

#### 13276 15.1.6.6.1 Work unit AVA\_VAN.5-4

13277 The evaluator **shall conduct** a methodical analysis of ST, guidance documentation, functional  
13278 specification, TOE design, security architecture description and implementation representation to  
13279 identify possible potential vulnerabilities in the TOE.

13280 Guidance on methodical vulnerability analysis is provided in Annex B.2.2.2.3.

13281 This approach to identification of potential vulnerabilities is to take an ordered and planned  
13282 approach. A system is to be applied in the examination. The evaluator is to describe the method to  
13283 be used in terms of the manner in which this information is to be considered and the hypothesis  
13284 that is to be created.

13285 A flaw hypothesis methodology should be used whereby the ST, development (functional  
13286 specification, TOE design and implementation representation) and guidance evidence are analysed  
13287 and then vulnerabilities in the TOE are hypothesised, or speculated.

13288 The evaluator should use the knowledge of the TOE design and operation gained from the TOE  
13289 deliverables to conduct a flaw hypothesis to identify potential flaws in the development of the TOE  
13290 and potential errors in the specified method of operation of the TOE.

13291 The security architecture description provides the developer vulnerability analysis, as it  
13292 documents how the TSF protects itself from interference from untrusted subjects and prevents the



- 13293 bypass of security enforcement functionality. Therefore, the evaluator should build upon the  
13294 understanding of the TSF protection gained from the analysis of this evidence and then develop  
13295 this in the knowledge gained from other development (e.g. ADV) evidence.
- 13296 The approach taken to the methodical search for vulnerabilities is to consider any areas of concern  
13297 identified in the results of the evaluator's assessment of the development and guidance evidence.  
13298 However, the evaluator should also consider each aspect of the security architecture analysis to  
13299 search for any ways in which the protection of the TSF can be undermined. It may be helpful to  
13300 structure the methodical analysis on the basis of the material presented in the security architecture  
13301 description, introducing concerns from other ADV evidence as appropriate. The analysis can then  
13302 be further developed to ensure all other material from the ADV evidence is considered.
- 13303 The following provide some examples of hypotheses that may be created when examining the  
13304 evidence:
- 13305 consideration of malformed input for interfaces available to an attacker at the external interfaces;
- 13306 examination of a key security mechanism cited in the security architecture description, such as  
13307 process separation, hypothesising internal buffer overflows that may lead to degradation of  
13308 separation;
- 13309 search to identify any objects created in the TOE implementation representation that are then not  
13310 fully controlled by the TSF, and could be used by an attacker to undermine SFRs.
- 13311 For example, the evaluator may identify that interfaces are a potential area of weakness in the TOE  
13312 and specify an approach to the search that 'all interface specifications in the evidence provided will  
13313 be searched to hypothesise potential vulnerabilities' and go on to explain the methods used in the  
13314 hypothesis.
- 13315 In addition, areas of concern the evaluator has identified during examination of the evidence  
13316 during the conduct of evaluation activities. Areas of concern may also be identified during the  
13317 conduct of other work units associated with this component, in particular AVA\_VAN.5-7,  
13318 AVA\_VAN.5-5 and AVA\_VAN.5-6) where the development and conduct of penetration tests may  
13319 identify further areas of concerns for investigation, or potential vulnerabilities.
- 13320 However, examination of only a subset of the development and guidance evidence or their contents  
13321 is not permitted in this level of rigour. The approach description should provide a demonstration  
13322 that the methodical approach used is complete, providing confidence that the approach used to  
13323 search the deliverables has considered all of the information provided in those deliverables.
- 13324 This approach to identification of potential vulnerabilities is to take an ordered and planned  
13325 approach; applying a system to the examination. The evaluator is to describe the method to be  
13326 used in terms of how the evidence will be considered; the manner in which this information is to be  
13327 considered and the hypothesis that is to be created. This approach should be agreed with the  
13328 evaluation authority, and the evaluation authority should provide detail of any additional  
13329 approaches the evaluator should take to the vulnerability analysis and identify any additional  
13330 information that should be considered by the evaluator.
- 13331 Although a system to identifying potential vulnerabilities is predefined, the identification process  
13332 may still be iterative, where the identification of one potential vulnerability may lead to identifying  
13333 another area of concern that requires further investigation.
- 13334 Subject to the SFRs the TOE is to meet in the operational environment, the evaluator's independent  
13335 vulnerability analysis should consider generic potential vulnerabilities under each of the following  
13336 headings:
- 13337 a) generic potential vulnerabilities relevant for the type of TOE being evaluated, as may  
13338 be supplied by the evaluation authority;

## ISO/IEC 18045:2008(E)

- 13339 b) bypassing;
- 13340 c) tampering;
- 13341 d) direct attacks;
- 13342 e) monitoring;
- 13343 f) misuse.
- 13344 Items b) - f) are explained in greater detail in Annex B.2.1.
- 13345 The security architecture description should be considered in light of each of the above generic  
13346 potential vulnerabilities. Each potential vulnerability should be considered to search for possible  
13347 ways in which to defeat the TSF protection and undermine the TSF.
- 13348 **15.1.6.6.2 Work unit AVA\_VAN.5-5**
- 13349 The evaluator *shall record* in the ETR the identified potential vulnerabilities that are candidates  
13350 for testing and applicable to the TOE in its operational environment.
- 13351 It may be identified that no further consideration of the potential vulnerability is required if for  
13352 example the evaluator identifies that measures in the operational environment, either IT or non-IT,  
13353 prevent exploitation of the potential vulnerability in that operational environment. For instance,  
13354 restricting physical access to the TOE to authorised users only may effectively render a potential  
13355 vulnerability to tampering unexploitable.
- 13356 The evaluator records any reasons for exclusion of potential vulnerabilities from further  
13357 consideration if the evaluator determines that the potential vulnerability is not applicable in the  
13358 operational environment. Otherwise the evaluator records the potential vulnerability for further  
13359 consideration.
- 13360 A list of potential vulnerabilities applicable to the TOE in its operational environment, which can be  
13361 used as an input into penetration testing activities, shall be reported in the ETR by the evaluators.
- 13362 **15.1.6.7 Action AVA\_VAN.5.4E**
- 13363 **15.1.6.7.1 Work unit AVA\_VAN.5-6**
- 13364 The evaluator *shall devise* penetration tests, based on the independent search for potential  
13365 vulnerabilities.
- 13366 The evaluator prepares for penetration testing as necessary to determine the susceptibility of the  
13367 TOE, in its operational environment, to the potential vulnerabilities identified during the search of  
13368 the sources of publicly available information and the analysis of the TOE guidance and design  
13369 evidence. The evaluator should have access to current information (e.g. from the evaluation  
13370 authority) regarding known potential vulnerabilities that may not have been considered by the  
13371 evaluator.
- 13372 The evaluator is reminded that, as for considering the security architecture description in the  
13373 search for vulnerabilities (as detailed in AVA\_VAN.5-3), testing should be performed to confirm the  
13374 architectural properties. If requirements from ATE\_DPT are included in the SARs, the developer  
13375 testing evidence will include testing performed to confirm the correct implementation of any  
13376 specific mechanisms detailed in the security architecture description. However, the developer  
13377 testing will not necessarily include testing of all aspects of the architectural properties that protect

- 13378 the TSF, as much of this testing will be negative testing in nature, attempting to disprove the  
 13379 properties. In developing the strategy for penetration testing, the evaluator will ensure that all  
 13380 aspects of the security architecture description are tested, either in functional testing (as  
 13381 considered in 15, ) or evaluator penetration testing.
- 13382 The evaluator will probably find it practical to carry out penetration test using a series of test cases,  
 13383 where each test case will test for a specific potential vulnerability.
- 13384 The evaluator is not expected to test for potential vulnerabilities (including those in the public  
 13385 domain) beyond those which required a **High** attack potential. In some cases, however, it will be  
 13386 necessary to carry out a test before the exploitability can be determined. Where, as a result of  
 13387 evaluation expertise, the evaluator discovers an exploitable vulnerability that is beyond **High**  
 13388 attack potential, this is reported in the ETR as a residual vulnerability.
- 13389 Guidance on determining the necessary attack potential to exploit a potential vulnerability can be  
 13390 found in Annex B.4.
- 13391 Potential vulnerabilities hypothesised as exploitable by an attacker possessing a **High** (or less)  
 13392 attack potential and resulting in a violation of the security objectives should be the highest priority  
 13393 potential vulnerabilities comprising the list used to direct penetration testing against the TOE.
- 13394 **15.1.6.7.2 Work unit AVA\_VAN.5-7**
- 13395 The evaluator **shall produce** penetration test documentation for the tests based on the list of  
 13396 potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test  
 13397 documentation shall include:
- 13398 a) identification of the potential vulnerability the TOE is being tested for;
  - 13399 b) instructions to connect and setup all required test equipment as required to conduct  
 13400 the penetration test;
  - 13401 c) instructions to establish all penetration test prerequisite initial conditions;
  - 13402 d) instructions to stimulate the TSF;
  - 13403 e) instructions for observing the behaviour of the TSF;
  - 13404 f) descriptions of all expected results and the necessary analysis to be performed on the  
 13405 observed behaviour for comparison against expected results;
  - 13406 g) instructions to conclude the test and establish the necessary post-test state for the  
 13407 TOE.
- 13408 The evaluator prepares for penetration testing based on the list of potential vulnerabilities  
 13409 identified during the search of the public domain and the analysis of the evaluation evidence.
- 13410 The evaluator is not expected to determine the exploitability for potential vulnerabilities beyond  
 13411 those for which a **High** attack potential is required to effect an attack. However, as a result of  
 13412 evaluation expertise, the evaluator may discover a potential vulnerability that is exploitable only  
 13413 by an attacker with greater than **High** attack potential. Such vulnerabilities are to be reported in  
 13414 the ETR as residual vulnerabilities.

## ISO/IEC 18045:2008(E)

13415 With an understanding of the potential vulnerability, the evaluator determines the most feasible  
13416 way to test for the TOE's susceptibility. Specifically the evaluator considers:

13417 the TSFI or other TOE interface that will be used to stimulate the TSF and observe responses (It is  
13418 possible that the evaluator will need to use an interface to the TOE other than the TSFI to  
13419 demonstrate properties of the TSF such as those described in the security architecture description  
13420 (as required by ADV\_ARC). It should be noted, that although these TOE interfaces provide a means  
13421 of testing the TSF properties, they are not the subject of the test.);

13422 initial conditions that will need to exist for the test (i.e. any particular objects or subjects that will  
13423 need to exist and security attributes they will need to have);

13424 special test equipment that will be required to either stimulate a TSFI or make observations of a  
13425 TSFI;

13426 whether theoretical analysis should replace physical testing, particularly relevant where the  
13427 results of an initial test can be extrapolated to demonstrate that repeated attempts of an attack are  
13428 likely to succeed after a given number of attempts.

13429 The evaluator will probably find it practical to carry out penetration testing using a series of test  
13430 cases, where each test case will test for a specific potential vulnerability.

13431 The intent of specifying this level of detail in the test documentation is to allow another evaluator  
13432 to repeat the tests and obtain an equivalent result.

### 13433 15.1.6.7.3 Work unit AVA\_VAN.5-8

13434 The evaluator **shall conduct** penetration testing.

13435 The evaluator uses the penetration test documentation resulting from work unit AVA\_VAN.5-6 as a  
13436 basis for executing penetration tests on the TOE, but this does not preclude the evaluator from  
13437 performing additional ad hoc penetration tests. If required, the evaluator may devise ad hoc tests  
13438 as a result of information learnt during penetration testing that, if performed by the evaluator, are  
13439 to be recorded in the penetration test documentation. Such tests may be required to follow up  
13440 unexpected results or observations, or to investigate potential vulnerabilities suggested to the  
13441 evaluator during the pre-planned testing.

13442 Should penetration testing show that a hypothesised potential vulnerability does not exist, then the  
13443 evaluator should determine whether or not the evaluator's own analysis was incorrect, or if  
13444 evaluation deliverables are incorrect or incomplete.

13445 The evaluator is not expected to test for potential vulnerabilities (including those in the public  
13446 domain) beyond those which required a **High** attack potential. In some cases, however, it will be  
13447 necessary to carry out a test before the exploitability can be determined. Where, as a result of  
13448 evaluation expertise, the evaluator discovers an exploitable vulnerability that is beyond **High**  
13449 attack potential, this is reported in the ETR as a residual vulnerability.

### 13450 15.1.6.7.4 Work unit AVA\_VAN.5-9

13451 The evaluator **shall record** the actual results of the penetration tests.

13452 While some specific details of the actual test results may be different from those expected (e.g. time  
13453 and date fields in an audit record) the overall result should be identical. Any unexpected test  
13454 results should be investigated. The impact on the evaluation should be stated and justified.

13455 **15.1.6.7.5 Work unit AVA\_VAN.5-10**

13456 The evaluator **shall report** in the ETR the evaluator penetration testing effort, outlining the testing  
13457 approach, configuration, depth and results.

13458 The penetration testing information reported in the ETR allows the evaluator to convey the overall  
13459 penetration testing approach and effort expended on this sub-activity. The intent of providing this  
13460 information is to give a meaningful overview of the evaluator's penetration testing effort. It is not  
13461 intended that the information regarding penetration testing in the ETR be an exact reproduction of  
13462 specific test steps or results of individual penetration tests. The intention is to provide enough  
13463 detail to allow other evaluators and evaluation authorities to gain some insight about the  
13464 penetration testing approach chosen, amount of penetration testing performed, TOE test  
13465 configurations, and the overall results of the penetration testing activity.

13466 Information that would typically be found in the ETR section regarding evaluator penetration  
13467 testing efforts is:

- 13468 • TOE test configurations. The particular configurations of the TOE that were penetration  
13469 tested;
- 13470 • TSFI penetration tested. A brief listing of the TSFI and other TOE interfaces that were  
13471 the focus of the penetration testing;
- 13472 • Verdict for the sub-activity. The overall judgement on the results of penetration testing.

13473 This list is by no means exhaustive and is only intended to provide some context as to the type of  
13474 information that should be present in the ETR concerning the penetration testing the evaluator  
13475 performed during the evaluation.

13476

13477 **15.1.6.7.6 Work unit AVA\_VAN.5-11**

13478 The evaluator **shall examine** the results of all penetration testing to determine that the TOE, in its  
13479 operational environment, is resistant to an attacker possessing a **High** attack potential.

13480 If the results reveal that the TOE, in its operational environment, has vulnerabilities exploitable by  
13481 an attacker possessing an attack potential less than **or equal to** High, then this evaluator action  
13482 fails.

13483 The guidance in B.4 and the guidance for special technical areas that is relevant for the national  
13484 scheme should be used to determine the attack potential required to exploit a particular  
13485 vulnerability and whether it can therefore be exploited in the intended environment. It may not be  
13486 necessary for the attack potential to be calculated in every instance, only if there is some doubt as  
13487 to whether or not the vulnerability can be exploited by an attacker possessing an attack potential  
13488 less than **or equal to** High.

13489 **15.1.6.7.7 Work unit AVA\_VAN.5-12**

13490 The evaluator **shall report** in the corresponding ETR-part all exploitable vulnerabilities and  
13491 residual vulnerabilities, detailing for each:

- 13492 a) its source (e.g. ISO/IEC 18045 activity being undertaken when it was conceived,  
13493 known to the evaluator, read in a publication);
- 13494 b) the SFR(s) not met;

- 13495 c) a description;
- 13496 d) whether it is exploitable in its operational environment or not (i.e. exploitable or  
13497 residual);
- 13498 e) the amount of time, level of expertise, level of knowledge of the TOE, level of  
13499 opportunity and the equipment required to perform the identified vulnerabilities,  
13500 and the corresponding values using the tables 3 and 4 of Annex B.4.

## 13501 15.2 Composite vulnerability assessment (AVA\_COMP)

13502 The composite-specific work units defined in this chapter are intended to be integrated as  
13503 refinements to the evaluation activities of the AVA class listed in the following table. The other  
13504 activities of AVA class do not require composite-specific work units.

| CC assurance family | Evaluation activity | Evaluation work unit | Composite-specific work unit |
|---------------------|---------------------|----------------------|------------------------------|
| AVA_VAN             | AVA_VAN.1.3E        | AVA_VAN.1-5          | AVA_COMP.1-1                 |
|                     | AVA_VAN.1.3E        | AVA_VAN.1-6          | AVA_COMP.1-2                 |
|                     | AVA_VAN.1.3E        | AVA_VAN.1-7          | AVA_COMP.1-2                 |
|                     | AVA_VAN.1.3E        | AVA_VAN.1-8          | AVA_COMP.1-2                 |

13505 NB: If the level of the assurance requirement chosen is higher than those identified in this table, the  
13506 composite-specific work unit is also applicable.

### 13507 15.2.1 Evaluation of sub-activity (AVA\_COMP.1)

#### 13508 15.2.1.1 Objectives

13509 The aim of this activity is to determine the exploitability of flaws or weaknesses in the composite  
13510 TOE as a whole in the intended environment.

#### 13511 15.2.1.2 Application notes

13512 This activity focuses exclusively on vulnerability assessment of the composite product as a whole  
13513 and represents merely partial efforts within the general approach being covered by the standard  
13514 assurance family of the class AVA: AVA\_VAN. The results of the vulnerability assessment for the  
13515 underlying platform represented in the ETR\_COMP can be reused under the following conditions:  
13516 they are up to date and all composite activities for correctness – ASE\_COMP.1, ALC\_COMP.1,  
13517 ADV\_COMP.1 and ATE\_COMP.1 – are finalised with the verdict PASS.

#### 13518 15.2.1.3 AVA\_COMP.1.1E

13519 The evaluator **shall conduct** penetration testing of the composite product as a whole building on  
13520 evaluator's own vulnerability analysis, to ensure that the vulnerabilities being relevant for the  
13521 Composite-ST are not exploitable.

##### 13522 15.2.1.3.1 Work unit AVA\_COMP.1-1

13523 The evaluator shall examine the results of the vulnerability assessment for the underlying platform  
13524 to determine that they can be reused for the composite evaluation.

13525 The results of the vulnerability assessment for the underlying platform are usually represented in  
 13526 the ETR\_COMP. They can be reused if the following conditions are met: they are up to date and all  
 13527 composite activities for correctness – ASE\_COMP.1, ALC\_COMP.1, ADV\_COMP.1 and ATE\_COMP.1 –  
 13528 are finalised with the verdict PASS. The evaluator shall also consider the relevant determinations in  
 13529 any Platform Certification Report. It is noted that the platform itself could be a composite TOE.  
 13530 This means also that the validity of each ETR for composition of the TOEs that compose the  
 13531 platform TOE must be checked.

13532 When the validity of the ETRs for composition is checked, the necessity of checking the contents  
 13533 depends on the application and user available TSFI. If the TSFI are available to the user or used by  
 13534 the application, the content of the ETR must be checked. If not and formal platform TSFI are no  
 13535 longer available as TSFI, the validity date of the ETR\_COMP is sufficient.

13536 The result of this work unit shall be integrated to the result of AVA\_VAN.1.3E/ AVA\_VAN.1-5 (or the  
 13537 equivalent higher components if a higher assurance level is selected).

#### 13538 15.2.1.3.2 Work unit AVA\_COMP.1-2

13539 The evaluator shall *specify, conduct and document* penetration testing of the composite product  
 13540 as a whole, using the standard approach of the assurance family AVA\_VAN.

13541 If the correctness-related activities – ASE\_COMP.1, ALC\_COMP.1, ADV\_COMP.1 and ATE\_COMP.1 –  
 13542 are finalised with the verdict PASS and the certificate for the platform covers all security properties  
 13543 needed for the composite product, composing of the platform and the application must not create  
 13544 additional vulnerabilities of the platform.

13545 If the evaluator determined that composing of the platform and the application creates additional  
 13546 vulnerabilities of the platform, a contradiction to the verdict PASS for the correctness activities has  
 13547 to be supposed or the certificate for the platform does not cover all security properties needed for  
 13548 the current composite product.

13549 The result of this work unit shall be integrated to the result of AVA\_VAN.1.3E/ AVA\_VAN.1-6,  
 13550 AVA\_VAN.1-7, AVA\_VAN.1-8 (or the equivalent higher components if a higher assurance level  
 13551 is selected).

### 13552 16 Class ACO: Composition

#### 13553 16.1 Introduction

13554 The goal of this activity is to determine whether the components can be integrated in a secure  
 13555 manner, as defined in the ST for the composed TOE. This is achieved through examination and  
 13556 testing of the interfaces between the components, supported by examination of the design of the  
 13557 components and the conduct of vulnerability analysis.

#### 13558 16.2 Application notes

13559 The Reliance of dependent component (ACO\_REL) family identifies where the dependent  
 13560 component is reliant upon IT in its operational environment (satisfied by a base component in the  
 13561 composed TOE evaluation) in order to provide its own security services. This reliance is identified  
 13562 in terms of the interfaces expected by the dependent component to be provided by the base  
 13563 component. Development evidence (ACO\_DEV) then determines which interfaces of the base  
 13564 component were considered (as TSFI) during the component evaluation of the base component.

13565 It should be noted that Reliance of dependent component (ACO\_REL) does not cover other  
 13566 evidence that may be needed to address the technical integration problem of composing  
 13567 components (e.g. descriptions of non-TSF interfaces of the operating system, rules for integration,

13568 etc.). This is outside the security assessment of the composition and is a functional composition  
13569 issue.

13570 As part of Composed TOE testing (ACO\_CTT) the evaluator will perform testing of the composed  
13571 TOE SFRs at the composed TOE interfaces and of the interfaces of the base component relied upon  
13572 by the dependent component to confirm they operate as specified. The subset selected will  
13573 consider the possible effects of changes to the configuration/use of the base component as used in  
13574 the composed TOE. These changes are identified from the configuration of the base component  
13575 determined during the base component evaluation. The developer will provide test evidence for  
13576 each of the base component interfaces (the requirements for coverage are consistent with those  
13577 applied to the evaluation of the base component).

13578 Composition rationale (ACO\_COR) requires the evaluator to determine whether the appropriate  
13579 assurance measures have been applied to the base component, and whether the base component is  
13580 being used in its evaluated configuration. This includes determination of whether all security  
13581 functionality required by the dependent component was within the TSF of the base component.  
13582 The Composition rationale (ACO\_COR) requirement may be met through the production of  
13583 evidence that each of these is demonstrated to be upheld. This evidence may be in the form of the  
13584 security target and a public report of the component evaluation (e.g. certification report).

13585 If, on the other hand, one of the above have not been upheld, then it may be possible that an  
13586 argument can be made as to why the assurance gained during an original evaluation is unaffected.  
13587 If this is not possible then additional evaluation evidence for those aspects of the base component  
13588 not covered may have to be provided. This material is then assessed in Development evidence  
13589 (ACO\_DEV).

13590 For example, it may be the case as described in the Interactions between entities (see Annex B.3,  
13591 Interactions between composed IT entities in ISO/IEC 15408-3) that the dependent component  
13592 requires the base component to provide more security functionality in the composed TOE than  
13593 included in the base component evaluation. This would be determined during the application of the  
13594 Reliance of dependent component (ACO\_REL) and Development evidence (ACO\_DEV) families. In  
13595 this case the composition rationale evidence provided for Composition rationale (ACO\_COR) would  
13596 demonstrate that the assurance gained from the base component evaluation is unaffected. This  
13597 may be achieved by means including:

13598 a) Performing a re-evaluation of the base component focusing on the evidence relating  
13599 to the extended part of the TSF;

13600 b) Demonstrating that the extended part of the TSF cannot affect other portions of the  
13601 TSF, and providing evidence that the extended part of the TSF provides the  
13602 necessary security functionality.

## 13603 **16.3 Composition rationale (ACO\_COR)**

### 13604 **16.3.1 Evaluation of sub-activity (ACO\_COR.1)**

#### 13605 **16.3.1.1 Input**

13606 The evaluation evidence for this sub-activity is:

13607 a) the composed ST;

13608 b) the composition rationale;

13609 c) the reliance information;



13610 d) the development information;

13611 e) unique identifier.

#### 13612 **16.3.1.2 Action ACO\_COR.1.1E**

13613 ISO/IEC 15408-3 ACO\_COR.1.1C: *The composition rationale shall demonstrate that a level of*  
 13614 *assurance at least as high as that of the dependent component has been obtained for the support*  
 13615 *functionality of the base component, when the base component is configured as required to support*  
 13616 *the TSF of the dependent component.*

##### 13617 **16.3.1.2.1 Work unit ACO\_COR.1-1**

13618 The evaluator ***shall examine*** the correspondence analysis with the development information and  
 13619 the reliance information to identify the interfaces that are relied upon by the dependent  
 13620 component which are not detailed in the development information.

13621 The evaluator's goal in this work unit is two fold:

13622 a) to determine which interfaces relied upon by the dependent component have had the  
 13623 appropriate assurance measures applied.

13624 b) to determine that the assurance package applied to the base component during the  
 13625 base component evaluation contained either the same assurance requirements as  
 13626 those in the package applied to the dependent component during its' evaluation, or  
 13627 hierarchically higher assurance requirements.

13628 The evaluator may use the correspondence tracing in the development information developed  
 13629 during the Development evidence (ACO\_DEV) activities (e.g. ACO\_DEV.1-2, ACO\_DEV.2-4,  
 13630 ACO\_DEV.3-6) to help identify the interfaces identified in the reliance information that are not  
 13631 considered in the development information.

13632 The evaluator will record the SFR-enforcing interfaces described in the reliance information that  
 13633 are not included in the development information. These will provide input to ACO\_COR.1-3 work  
 13634 unit, helping to identify the portions of the base component in which further assurance is required.

13635 If the both the base and dependent components were evaluated against the same assurance  
 13636 package, then the determination of whether the level of assurance in the portions within the base  
 13637 component evaluation is at least as high as that of the dependent component is trivial. If however,  
 13638 the assurance packages applied to the components during the component evaluations differ, the  
 13639 evaluator needs to determine that the assurance requirements applied to the base component are  
 13640 all hierarchically higher to the assurance requirements applied to the dependent component.

##### 13641 **16.3.1.2.2 Work unit ACO\_COR.1-2**

13642 The evaluator ***shall examine*** the composition rationale to determine, for those included base  
 13643 component interfaces on which the dependent TSF relies, whether the interface was considered  
 13644 during the evaluation of the base component.

13645 The ST, component public evaluation report (e.g. certification report) and guidance documents for  
 13646 the base component all provide information on the scope and boundary of the base component.  
 13647 The ST provides details of the logical scope and boundary of the composed TOE, allowing the  
 13648 evaluator to determine whether an interface relates to a portion of the product that was within the  
 13649 scope of the evaluation. The guidance documentation provides details of use of all interfaces for the  
 13650 composed TOE. Although the guidance documentation may include details of interfaces in the  
 13651 product that are not within the scope of the evaluation, any such interfaces should be identifiable,

## ISO/IEC 18045:2008(E)

13652 either from the scoping information in the ST or through a portion of the guidance that deals with  
13653 the evaluated configuration. The public evaluation report may provide any additional constraints  
13654 on the use of the composed TOE that are necessary.

13655 Therefore, the combination of these inputs allows the evaluator to determine whether an interface  
13656 described in the composition rationale has the necessary assurance associated with it, or whether  
13657 further assurance is required. The evaluator will record those interfaces of the base component for  
13658 which additional assurance is required, for consideration during ACO\_COR.1-3.

### 13659 16.3.1.2.3 Work unit ACO\_COR.1-3

13660 The evaluator *shall examine* the composition rationale to determine that the necessary assurance  
13661 measures have been applied to the base component.

13662 The evaluation verdicts, and resultant assurance, for the base component can be reused provided  
13663 the same portions of the base component are used in the composed TOE and they are used in a  
13664 consistent manner.

13665 In order to determine whether the necessary assurance measures have already been applied to the  
13666 component, and the portions of the component for which assurance measures still need to be  
13667 applied, the evaluator should use the output of the ACO\_DEV.\*.2E action and the work units  
13668 ACO\_COR.1-1 and ACO\_COR.1-2:

13669 a) For those interfaces identified in the reliance information (Reliance of dependent  
13670 component (ACO\_REL)), but not discussed in development information  
13671 (Development evidence (ACO\_DEV)), additional information is required. (Identified  
13672 in ACO\_COR.1-1.)

13673 b) For those interfaces used inconsistently in the composed TOE from the base  
13674 component (difference between the information provided in Development evidence  
13675 (ACO\_DEV) and Reliance of dependent component (ACO\_REL) the impact of the  
13676 differences in use need to be considered. (Identified in ACO\_DEV.\*.2E.)

13677 c) For those interfaces identified in composition rationale for which no assurance has  
13678 previously been gained, additional information is required. (Identified in  
13679 ACO\_COR.1-2.)

13680 d) For those interfaces consistently described in the reliance information, composition  
13681 rationale and the development information, no further action is required as the  
13682 results from the base component evaluation can be re-used.

13683 The interfaces of the base component reported to be required by the reliance information but not  
13684 included in the development information indicate the portions of the base component where  
13685 further assurance is required. The interfaces identify the entry points into the base component.

13686 For those interfaces included in both the development information and reliance information, the  
13687 evaluator is to determine whether the interfaces are being used in the composed TOE in a manner  
13688 that is consistent with the base component evaluation. The method of use of the interface will be  
13689 considered during the Development evidence (ACO\_DEV) activities to determine that the use of the  
13690 interface is consistent in both the base component and the composed TOE. The remaining  
13691 consideration is the determination of whether the configurations of the base component and the  
13692 composed TOE are consistent. To determine this, the evaluator will consider the guidance  
13693 documentation of each to ensure they are consistent (see further guidance below regarding  
13694 consistent guidance documentation). Any deviation in the documentation will be further analysed  
13695 by the evaluation to determine the possible effects.

13696 For those interfaces that are consistently described in the reliance information and development  
 13697 information, and for which the guidance is consistent for the base component and the composed  
 13698 TOE, the required level of assurance has been provided.

13699 Table 1 provides guidance on how to determine consistency between assurance gained in the base  
 13700 component, the evidence provided for the composed TOE, and the analysis performed by the  
 13701 evaluator in the instances where inconsistencies are identified.

13702 **Table 1 guidance on how to determine consistency**

|    |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a) | Development | <p>The reliance information identifies the interfaces in the dependent component that are to be matched by the base component. If an interface identified in the reliance information is not identified in the development information, then the composition rationale is to provide a justification of how the base component provides the required interfaces.</p> <p>If an interface identified in the reliance information is identified in the development information, but there are inconsistencies between the descriptions, further analysis is required. The evaluator identifies the differences in use of the base component as considered in the base component evaluation and the composed TOE evaluation. The evaluator will devise testing to be performed (during the conduct of Composed TOE testing (ACO_CTT)) to test the interface.</p> <p>The patch status of the base and dependent components as used in the composed TOE should be compared to the patch status of the components during the component evaluations. If any patches have been applied to the components, the composition rationale is to include details of the patches, including any potential impact to the SFRs of the evaluated component. The evaluator should consider the details of the changes provided and verify the accuracy of the potential impact of the change on the component SFRs. The evaluator should then consider whether the changes made by the patch should be verified through testing, and will identify the necessary testing approach. The testing may take the form of repeating the applicable evaluator/developer testing performed for the component evaluation of the component or it may be necessary for the evaluator to devise new tests to confirm the modified component.</p> <p>If any of the individual components have been the subject of assurance continuity activities since the completion of the component evaluation, the evaluator will consider the changes assessed in the assurance continuity activities during the independent vulnerability analysis activity for the composed TOE (in Composition vulnerability analysis (ACO_VUL)).</p> |
| b) | Guidance    | <p>The guidance for the composed TOE is likely to make substantial reference out to the guidance for the individual components. The minimal guidance expected to be necessary is the identification of any ordering dependencies in the application of guidance for the dependent and base components, particularly during the preparation (installation) of the composed TOE.</p> <p>In addition to the application of the Preparative procedures (AGD_PRE) and Operational user guidance (AGD_OPE) families to the guidance for the composed TOE, it is necessary to analyse the consistency between the guidance for the components and the composed TOE, to identify any deviations.</p> <p>If the composed TOE guidance refers out to the base component and dependent component guidance, then the consideration for consistency is</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>limited to consistency between the guidance documentation provided for each of the components (i.e. consistency between the base component guidance and the dependent component guidance). However, if additional guidance is provided for the composed TOE, to that provided for the components, greater analysis is required, as consistency is also required between the guidance documentation for the components and guidance documentation for the composed TOE.</p> <p><i>Consistent</i> in this instance is understood to mean that either the guidance is the same or it places additional constraints on the operation of the individual components when combined, in a similar manner to <i>refinement</i> of functional/assurance components.</p> <p>With the information available (that used as input for Development evidence (ACO_DEV) or the development aspects discussed above) the evaluator may be able to determine all possible impacts of the deviation from the configuration of the base component specified in the component evaluation. However, for high EALs (where evaluation of the base component included requirements) it is possible that, unless detailed design abstractions for the base component are delivered as part of the development information for the composed TOE, the possible impacts of the modification to the guidance cannot be fully determined as the internals are unknown. In this case the evaluator will report the residual risk of the analysis.</p> <p>These residual risks are to be included in any public evaluation report for the composed TOE.</p> <p>The evaluator will note these variances in the guidance for input into evaluator independent testing activities (Composed TOE testing (ACO_CTT)).</p> <p>The guidance for the composed TOE may add to the guidance for the components, particularly in terms of installation and the ordering of installation steps for the base component in relation to the installation steps for the dependent component. The ordering of the steps for the installation of the individual components should not change, however they may need to be interleaved. The evaluator will examine this guidance to ensure that it still meets the requirement of the AGD_PRE activity performed during the evaluations of the components.</p> <p>It may be the case that the reliance information identifies that interfaces of the base component, in addition to those identified as TSFIs of the base component, are relied upon by the dependent component are identified in the reliance information. It may be necessary for guidance to be provided for the use of any such additional interfaces in the base component. Provided the consumer of the composed TOE is to receive the guidance documentation for the base component, then the results of the AGD_PRE and AGD_OPE verdicts for the base component can be reused for those interfaces considered in the evaluation of the base component. However, for the additional interfaces relied upon by the dependent component, the evaluator will need to determine that the guidance documentation for the base component meets the requirements of AGD_PRE and AGD_OPE, as applied in the base component evaluations.</p> <p>For those interfaces considered during the base component evaluation, and therefore, for which assurance has already been gained, the evaluator will ensure that the guidance for the use of each interface for the composed TOE is consistent with that provided for the base component. To determine the guidance for the composed TOE is consistent with that for the base</p> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>component, the evaluator should perform a mapping for each interface to the guidance provided for both the composed TOE and the base component. The evaluator then compares the guidance to determine consistency.</p> <p>Examples of additional constraints provided in composed TOE guidance that would be considered to be consistent with component guidance are (guidance for a component is given followed by an example of guidance for a composed TOE that would be considered to provide additional constraints):</p> <ul style="list-style-type: none"> <li>— Component: The password length must be set to a minimum of 8 characters length, including alphabetic and numeric characters.</li> <li>— Composed TOE: The password length must be set to a minimum of 10 characters in length, including alphabetic and numeric characters and <i>at least one of the following special characters: ( ) { } ^ &lt; &gt; - _</i></li> <li>— NOTE: It would only be acceptable to increase the password length to <i>[integer &gt; 8]</i> characters while removing the mandate for the inclusion of both alphabetic and numeric characters for the composed TOE, if the same or a higher metric was achieved for the strength rating (taking into account the likelihood of the password being guessed).</li> <li>— Component: The following services are to be disabled in the registry settings: WWW Publishing Service and ICDBReporter service.</li> <li>— Composed TOE: The following services are to be disabled in the registry settings: Publishing Service, ICDBReporter service, Remote Procedure Call (RPC) Locator and Procedure Call (RPC) Service.</li> <li>— Component: Select the following attributes to be included in the accounting log files: date, time, type of event, subject identity and success/failure.</li> <li>— Composed TOE: Select the following attributes to be included in the accounting log files: date, time, type of event, subject identity, success/failure, <i>event message and process thread</i>.</li> </ul> <p>If the guidance for the composed TOE deviates (is not a refinement) from that provided for the base component, the evaluator will assess the potential risks of the modification to the guidance. The evaluator will use the information available (including that provided in the public domain, the architectural description of the base component in the public evaluation report (e.g. certification report), the context of the guidance from the remainder of the guidance documentation) to identify likely impact of the modification to the guidance on the SFRs of the composed TOE.</p> <p>If during the dependent component evaluation the trial installation used the base component to satisfy the environment requirements of the dependent component this work unit for the composed TOE is considered to be satisfied. If the base component was not used in satisfaction of the work unit AGD_PRE.1-3 during the dependent component evaluation, the evaluator will apply the user procedures provided for the composed TOE to prepare the composed TOE, in accordance with the guidance specified in AGD_PRE.1-3. This will allow the evaluator to determine that the preparative guidance provided for the composed TOE is sufficient to prepare the composed TOE and its operational environment securely.</p> |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|    |                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| c) | <b>Delivery</b>        | <p>If there is a different delivery mechanism used for the delivery of the composed TOE (i.e. the components are not delivered to the consumer in accordance with the secure delivery procedures defined and assessed during the evaluation of the components), the delivery procedures for the composed TOE will require evaluation against the Delivery (ALC_DEL) requirements applied during the components evaluations.</p> <p>The composed TOE may be delivered as an integrated product or may require the components to be delivered separately.</p> <p>If the components are delivered separately, the results of the delivery of the base component and dependent component are reused. The delivery of the base component is checked during the evaluator trial installation of the dependent component, using the specified guidance and checking the aspects of delivery that are the responsibility of the user, as described in the guidance documentation for the base component.</p> <p>If the composed TOE is delivered as a new entity, then the method of delivery of that entity must be considered in the composed TOE evaluation activities.</p> <p>The assessment of the delivery procedures for composed TOE items is to be performed in accordance with the methodology for Delivery (ALC_DEL) as for any other [component] TOE, ensuring any additional items (e.g. additional guidance documents for the composed TOE) are considered in the delivery procedures.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| d) | <b>CM Capabilities</b> | <p>The unique identification of the composed TOE is considered during the application of Evaluation of sub-activity (ALC_CMC.1) and the items from which that composed TOE is comprised are considered during the application of Evaluation of sub-activity (ALC_CMS.2).</p> <p>Although additional guidance may be produced for the composed TOE, the unique identification of this guidance (considered as part of the unique identification of the composed TOE during Evaluation of sub-activity (ALC_CMC.1)) is considered sufficient control of the guidance.</p> <p>The verdicts of the remaining (not considered above) Class ALC: Life-cycle support activities can be reused from the base component evaluation, as no further development is performed during integration of the composed TOE.</p> <p>There are no additional considerations for development security as the integration is assumed to take place at either the consumer's site or, in the instance that the composed TOE is delivered as an integrated product, at the site of the dependent component developer. Control at the consumer's site is outside the consideration of ISO/IEC 15408. No additional requirements or guidance are necessary if integration is at the same site as that for the dependent component, as all components are considered to be configuration items for the composed TOE, and should therefore be considered under the dependent component developer's security procedures anyway.</p> <p>Tools and techniques adopted during integration will be considered in the evidence provided by the dependent component developer. Any tools/techniques relevant to the base component will have been considered during the evaluation of the base component. For example, if the base component is delivered as source code and requires compilation by the consumer (e.g. dependent component developer who is performing integration) the compiler would have been specified and assessed, along with</p> |

|    |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |              | <p>the appropriate arguments, during evaluation of the base component.</p> <p>There is no life-cycle definition applicable to the composed TOE, as no further development of items is taking place.</p> <p>The results of flaw remediation for a component are not applicable to the composed TOE. If flaw remediation is included in the assurance package for the composed TOE, then the Flaw remediation (ALC_FLR) requirements are to be applied during the composed TOE evaluation (as for any augmentation).</p>                                                                                                                                                                                   |
| e) | <b>Tests</b> | <p>The composed TOE will have been tested during the conduct of the Class ATE: Tests activities for evaluation of the dependent component, as the configurations used for testing of the dependent component should have included the base component to satisfy the requirements for IT in the operational environment. If the base component was not used in the testing of the dependent component for the dependent component evaluation, or the configuration of either component varied from their evaluated configurations, then the developer testing performed for evaluation of the dependent component to satisfy the Class ATE: Tests requirements is to be repeated on the composed TOE.</p> |

#### 13703 16.4 Development evidence (ACO\_DEV)

#### 13704 16.4.1 Evaluation of sub-activity (ACO\_DEV.1)

##### 13705 16.4.1.1 Objectives

13706 The objective of this sub-activity is to determine that the appropriate security functionality is  
 13707 provided by the base component to support the dependent component. This is achieved through  
 13708 examination of the interfaces of the base component to determine that they are consistent with the  
 13709 interfaces specified in the reliance information; those required by the dependent component.

13710 The description of the interfaces into the base component is to be provided at a level of detail  
 13711 consistent with Evaluation of sub-activity (ADV\_FSP.2) although not all of the aspects necessary for  
 13712 satisfaction of Evaluation of sub-activity (ADV\_FSP.2) are required for Evaluation of sub-activity  
 13713 (ACO\_DEV.1), as once the interface has been identified and the purpose described the remaining  
 13714 detail of the interface specification can be reused from evaluation of the base component.

##### 13715 16.4.1.2 Input

13716 The evaluation evidence for this sub-activity is:

- 13717 a) the composed ST;
- 13718 b) the development information;
- 13719 c) the reliance information.

##### 13720 16.4.1.3 Action ACO\_DEV.1.1E

13721 ISO/IEC 15408-3 ACO\_DEV.1.1C: *The development information shall describe the purpose of each*  
 13722 *interface of the base component used in the composed TOE.*

## ISO/IEC 18045:2008(E)

### 13723 16.4.1.3.1 Work unit ACO\_DEV.1-1

13724 The evaluator **shall examine** the development information to determine that it describes the  
13725 purpose of each interface.

13726 The base component provides interfaces to support interaction with the dependent component in  
13727 the provision of the dependent TSF. The purpose of each interface is to be described at the same  
13728 level as the description of the interfaces to the dependent component TSF functionality, as would  
13729 be provided between subsystems in the TOE design (Evaluation of sub-activity (ADV\_TDS.1)). This  
13730 description is to provide the reader with an understanding of how the base component provides  
13731 the services required by the dependent component TSF.

13732 This work unit may be satisfied by the provision of the functional specification for the base  
13733 component for those interfaces that are TSFIs of the base component.

13734 ISO/IEC 15408-3 ACO\_DEV.1.2C: *The development information shall show correspondence between*  
13735 *the interfaces, used in the composed TOE, of the base component and the dependent component to*  
13736 *support the TSF of the dependent component.*

### 13737 16.4.1.3.2 Work unit ACO\_DEV.1-2

13738 The evaluator **shall examine** the development information to determine the correspondence,  
13739 between the interfaces of the base component and the interfaces on which the dependent  
13740 component relies, is accurate.

13741 The correspondence between the interfaces of the base component and the interfaces on which the  
13742 dependent component relies may take the form of a matrix or table. The interfaces that are relied  
13743 upon by the dependent component are identified in the reliance information (as examined during  
13744 Reliance of dependent component (ACO\_REL) activity).

13745 There is, during this activity, no requirement to determine completeness of the coverage of  
13746 interfaces that are relied upon by the dependent component, only that the correspondence is  
13747 correct and ensuring that interfaces of the base component are mapped to interfaces required by  
13748 the dependent component wherever possible. The completeness of the coverage is considered in  
13749 Composition rationale (ACO\_COR) activities.

### 13750 16.4.1.4 Action ACO\_DEV.1.2E

#### 13751 16.4.1.4.1 Work unit ACO\_DEV.1-3

13752 The evaluator **shall examine** the development information and the reliance information to  
13753 determine that the interfaces are described consistently.

13754 The evaluator's goal in this work unit is to determine that the interfaces described in the  
13755 development information for the base component and the reliance information for the dependent  
13756 component are represented consistently.

### 13757 16.4.2 Evaluation of sub-activity (ACO\_DEV.2)

#### 13758 16.4.2.1 Objectives

13759 The objective of this sub-activity is to determine that the appropriate security functionality is  
13760 provided by the base component to support the dependent component. This is achieved through  
13761 examination of the interfaces and associated security behaviour of the base component to  
13762 determine that they are consistent with the interfaces specified in the reliance information; those  
13763 required by the dependent component.



13764 **16.4.2.2 Input**

13765 The evaluation evidence for this sub-activity is:

- 13766 a) the composed ST;
- 13767 b) the development information;
- 13768 c) reliance information.

13769 **16.4.2.3 Action ACO\_DEV.2.1E**

13770 ISO/IEC 15408-3 ACO\_DEV.2.1C: *The development information shall describe the purpose and*  
 13771 *method of use of each interface of the base component used in the composed TOE.*

13772 **16.4.2.3.1 Work unit ACO\_DEV.2-1**

13773 The evaluator **shall examine** the development information to determine that it describes the  
 13774 purpose of each interface.

13775 The base component provides interfaces to support interaction with the dependent component in  
 13776 the provision of the dependent TSF. The purpose of each interface is to be described at the same  
 13777 level as the description of the interfaces to the dependent component TSF functionality, as would  
 13778 be provided between subsystems in the TOE design (Evaluation of sub-activity (ADV\_TDS.1)). This  
 13779 description is to provide the reader with an understanding of how the base component provides  
 13780 the services required by the dependent component TSF.

13781 This work unit may be satisfied by the provision of the functional specification for the base  
 13782 component for those interfaces that are TSFIs of the base component.

13783 **16.4.2.3.2 Work unit ACO\_DEV.2-2**

13784 The evaluator **shall examine** the development information to determine that it describes the  
 13785 method of use for each interface.

13786 The method of use for an interface summarises how the interface is manipulated in order to invoke  
 13787 the operations and obtain results associated with the interface. The evaluator should be able to  
 13788 determine from reading this material in the development information how to use each interface.  
 13789 This does not necessarily mean that there needs to be a separate method of use for each interface,  
 13790 as it may be possible to describe in general how APIs are invoked, for instance, and then identify  
 13791 each interface using that general style.

13792 This work unit may be satisfied by the provision of the functional specification for the base  
 13793 component for those interfaces that are TSFIs of the base component.

13794 ISO/IEC 15408-3 ACO\_DEV.2.2C: *The development information shall provide a high-level description*  
 13795 *of the behaviour of the base component, which supports the enforcement of the dependent component*  
 13796 *SFRs.*

13797 **16.4.2.3.3 Work unit ACO\_DEV.2-3**

13798 The evaluator **shall examine** the development information to determine that it describes the  
 13799 behaviour of the base component that supports the enforcement of the dependent component SFRs.

13800 The dependent component invokes interfaces of the base component for the provision of services  
 13801 by the base component. For the interfaces of the base component that are invoked, the

13802 development information shall provide a high-level description of the associated security  
13803 behaviour of the base component. The description of the base component security behaviour will  
13804 outline how the base component provides the necessary service when the call to the interface is  
13805 made. This description is to be at a level similar to that provided for ADV\_TDS.1.4C. Therefore, the  
13806 provision of the TOE design evidence from the base component evaluation would satisfy this work  
13807 unit, where the interfaces invoked by the dependent component are TSFI of the base component. If  
13808 the interfaces invoked by the dependent component are not TSFIs of the base component it is the  
13809 associated security behaviour will not necessarily be described in the base component TOE design  
13810 evidence.

13811 ISO/IEC 15408-3 ACO\_DEV.2.3C: *The development information shall show correspondence between*  
13812 *the interfaces, used in the composed TOE, of the base component and the dependent component to*  
13813 *support the TSF of the dependent component.*

#### 13814 **16.4.2.3.4 Work unit ACO\_DEV.2-4**

13815 The evaluator ***shall examine*** the development information to determine the correspondence,  
13816 between the interfaces of the base component and the interfaces on which the dependent  
13817 component relies, is accurate.

13818 The correspondence between the interfaces of the base component and the interfaces on which the  
13819 dependent component relies may take the form of a matrix or table. The interfaces that are relied  
13820 upon by the dependent component are identified in the reliance information (as examined during  
13821 Reliance of dependent component (ACO\_REL)).

13822 There is, during this activity, no requirement to determine completeness of the coverage of  
13823 interfaces that are relied upon by the dependent component, only that the correspondence is  
13824 correct and ensuring that interfaces of the base component are mapped to interfaces required by  
13825 the dependent component wherever possible. The completeness of the coverage is considered in  
13826 Composition rationale (ACO\_COR) activities.

#### 13827 **16.4.2.4 Action ACO\_DEV.2.2E**

##### 13828 **16.4.2.4.1 Work unit ACO\_DEV.2-5**

13829 The evaluator ***shall examine*** the development information and the reliance information to  
13830 determine that the interfaces are described consistently.

13831 The evaluator's goal in this work unit is to determine that the interfaces described in the  
13832 development information for the base component and the reliance information for the dependent  
13833 component are represented consistently.

#### 13834 **16.4.3 Evaluation of sub-activity (ACO\_DEV.3)**

##### 13835 **16.4.3.1 Objectives**

13836 The objective of this sub-activity is to determine that the appropriate security functionality is  
13837 provided by the base component to support the dependent component. This is achieved through  
13838 examination of the interfaces and associated security behaviour of the base component to  
13839 determine that they are consistent with the interfaces specified in the reliance information; those  
13840 required by the dependent component.

13841 In addition to the interface description, the subsystems of the base component that provide the  
13842 security functionality required by the dependent component will be described to enable the  
13843 evaluator to determine whether or not that interface formed part of the TSF of the base component.

13844 **16.4.3.2 Input**

13845 The evaluation evidence for this sub-activity is:

13846 a) the composed ST;

13847 b) the development information;

13848 c) reliance information.

13849 **16.4.3.3 Action ACO\_DEV.3.1E**13850 ISO/IEC 15408-3 ACO\_DEV.3.1C: *The development information shall describe the purpose and*  
13851 *method of use of each interface of the base component used in the composed TOE.*13852 **16.4.3.3.1 Work unit ACO\_DEV.3-1**13853 The evaluator **shall examine** the development information to determine that it describes the  
13854 purpose of each interface.13855 The base component provides interfaces to support interaction with the dependent component in  
13856 the provision of the dependent TSF. The purpose of each interface is to be described at the same  
13857 level as the description of the interfaces to the dependent component TSF functionality, as would  
13858 be provided between subsystems in the TOE design (Evaluation of sub-activity (ADV\_TDS.1)). This  
13859 description is to provide the reader with an understanding of how the base component provides  
13860 the services required by the dependent component TSF.13861 This work unit may be satisfied by the provision of the functional specification for the base  
13862 component for those interfaces that are TSFIs of the base component.13863 **16.4.3.3.2 Work unit ACO\_DEV.3-2**13864 The evaluator **shall examine** the development information to determine that it describes the  
13865 method of use for each interface.13866 The method of use for an interface summarises how the interface is manipulated in order to invoke  
13867 the operations and obtain results associated with the interface. The evaluator should be able to  
13868 determine from reading this material in the development information how to use each interface.  
13869 This does not necessarily mean that there needs to be a separate method of use for each interface,  
13870 as it may be possible to describe in general how APIs are invoked, for instance, and then identify  
13871 each interface using that general style.13872 This work unit may be satisfied by the provision of the functional specification for the base  
13873 component for those interfaces that are TSFIs of the base component.13874 ISO/IEC 15408-3 ACO\_DEV.3.2C: *The development information shall identify the subsystems of the*  
13875 *base component that provide interfaces of the base component used in the composed TOE.*13876 **16.4.3.3.3 Work unit ACO\_DEV.3-3**13877 The evaluator **shall examine** the development information to determine that all subsystems of the  
13878 base component that provide interfaces to the dependent component are identified.13879 For those interfaces that are considered to form part of the TSFI of the base component, the  
13880 subsystems associated with the interface will be subsystems considered in the TOE design  
13881 (ADV\_TDS) activity during the base component evaluation. The interfaces on which the dependent

## ISO/IEC 18045:2008(E)

13882 component relies that did not form part of the TSFI of the base component will map to subsystems  
13883 outside of the base component TSF.

13884 ISO/IEC 15408-3 ACO\_DEV.3.3C: *The development information shall provide a high-level description*  
13885 *of the behaviour of the base component subsystems, which support the enforcement of the dependent*  
13886 *component SFRs.*

### 13887 16.4.3.3.4 Work unit ACO\_DEV.3-4

13888 The evaluator **shall examine** the development information to determine that it describes the  
13889 behaviour of the base component subsystems that support the enforcement of the dependent  
13890 component SFRs.

13891 The dependent component invokes interfaces of the base component for the provision of services  
13892 by the base component. For the interfaces of the base component that are invoked, the  
13893 development information shall provide a high-level description of the associated security  
13894 behaviour of the base component. The description of the base component security behaviour will  
13895 outline how the base component provides the necessary service when the call to the interface is  
13896 made. This description is to be at a level similar to that provided for ADV\_TDS.1.4C. Therefore, the  
13897 provision of the TOE design evidence from the base component evaluation would satisfy this work  
13898 unit, where the interfaces invoked by the dependent component are TSFI of the base component. If  
13899 the interfaces invoked by the dependent component are not TSFIs of the base component it is the  
13900 associated security behaviour will not necessarily be described in the base component TOE design  
13901 evidence.

13902 ISO/IEC 15408-3 ACO\_DEV.3.4C: *The development information shall provide a mapping from the*  
13903 *interfaces to the subsystems of the base component.*

### 13904 16.4.3.3.5 Work unit ACO\_DEV.3-5

13905 The evaluator **shall examine** the development information to determine that the correspondence  
13906 between the interfaces and subsystems of the base component is accurate.

13907 If the TOE design and functional specification evidence from the base component evaluation is  
13908 available, this can be used to verify the accuracy of the correspondence between the interfaces and  
13909 subsystems of the base component as used in the composed TOE. Those interfaces of the base  
13910 component, which formed part of the base component TSFI will be described in the base  
13911 component functional specification, and the associated subsystems will be described in the base  
13912 component TOE design evidence. The tracing between the two will be provided in the base  
13913 component TOE design evidence.

13914 If, however, the base component interface did not form part of the TSFI of the base component, the  
13915 description of the subsystem behaviour provided in the development information will be used to  
13916 verify the accuracy of the correspondence.

13917 ISO/IEC 15408-3 ACO\_DEV.3.5C: *The development information shall show correspondence between*  
13918 *the interfaces, used in the composed TOE, of the base component and the dependent component to*  
13919 *support the TSF of the dependent component.*

### 13920 16.4.3.3.6 Work unit ACO\_DEV.3-6

13921 The evaluator **shall examine** the development information to determine the correspondence,  
13922 between the interfaces of the base component and the interfaces on which the dependent  
13923 component relies, is accurate.

13924 The correspondence between the interfaces of the base component and the interfaces on which the  
13925 dependent component relies may take the form of a matrix or table. The interfaces that are relied

13926 upon by the dependent component are identified in the reliance information (as examined during  
13927 Reliance of dependent component (ACO\_REL)).

13928 There is, during this activity, no requirement to determine completeness of the coverage of  
13929 interfaces that are relied upon by the dependent component, only that the correspondence is  
13930 correct and ensuring that interfaces of the base component are mapped to interfaces required by  
13931 the dependent component wherever possible. The completeness of the coverage is considered in  
13932 Composition rationale (ACO\_COR) activities.

#### 13933 **16.4.3.4 Action ACO\_DEV.3.2E**

##### 13934 **16.4.3.4.1 Work unit ACO\_DEV.3-7**

13935 The evaluator *shall examine* the development information and the reliance information to  
13936 determine that the interfaces are described consistently.

13937 The evaluator's goal in this work unit is to determine that the interfaces described in the  
13938 development information for the base component and the reliance information for the dependent  
13939 component are represented consistently.

### 13940 **16.5 Reliance of dependent component (ACO\_REL)**

#### 13941 **16.5.1 Evaluation of sub-activity (ACO\_REL.1)**

##### 13942 **16.5.1.1 Objectives**

13943 The objectives of this sub-activity are to determine whether the developer's reliance evidence  
13944 provides sufficient information to determine that the necessary functionality is available in the  
13945 base component, and the means by which that functionality is invoked. These are provided in  
13946 terms of a high-level description.

##### 13947 **16.5.1.2 Input**

13948 The evaluation evidence for this sub-activity is:

- 13949 a) the composed ST;
- 13950 b) the dependent component functional specification;
- 13951 c) the dependent component design;
- 13952 d) the dependent component architectural design;
- 13953 e) the reliance information.

##### 13954 **16.5.1.3 Application notes**

13955 A dependent component whose TSF interacts with the base component requires functionality  
13956 provided by that base component (e.g., remote authentication, remote audit data storage). In these  
13957 cases, those invoked services need to be described for those charged with configuring the  
13958 composed TOE for end users. The rationale for requiring this documentation is to aid integrators of  
13959 the composed TOE to determine what services in the base component might have adverse effects  
13960 on the dependent component, and to provide information against which to determine the  
13961 compatibility of the components when applying the Development evidence (ACO\_DEV) family.

## ISO/IEC 18045:2008(E)

### 13962 16.5.1.4 Action ACO\_REL.1.1E

13963 ISO/IEC 15408-3 ACO\_REL.1.1C: *The reliance information shall describe the functionality of the base*  
13964 *component hardware, firmware and/or software that is relied upon by the dependent component TSF.*

### 13965 16.5.1.4.1 Work unit ACO\_REL.1-1

13966 The evaluator **shall check** the reliance information to determine that it describes the functionality  
13967 of the base dependent hardware, firmware and/or software that is relied upon by the dependent  
13968 component TSF.

13969 The evaluator assesses the description of the security functionality that the dependent component  
13970 TSF requires to be provided by the base component's hardware, firmware and software. The  
13971 emphasis of this work unit is on the level of detail of this description, rather than on an assessment  
13972 of the information's accuracy. (The assessment of the accuracy of the information is the focus of the  
13973 next work unit.)

13974 This description of the base component's functionality need not be any more detailed than the level  
13975 of the description of a component of the TSF, as would be provided in the TOE Design (TOE design  
13976 (ADV\_TDS))

### 13977 16.5.1.4.2 Work unit ACO\_REL.1-2

13978 The evaluator **shall examine** the reliance information to determine that it accurately reflects the  
13979 objectives specified for the operational environment of the dependent component.

13980 The reliance information contains the description of the base component's security functionality  
13981 relied upon by the dependent component. To ensure that the reliance information is consistent  
13982 with the expectations of the operational environment of the dependent component, the evaluator  
13983 compares the reliance information with the statement of objectives for the environment in the ST  
13984 for the dependent component.

13985 For example, if the reliance information claims that the dependent component TSF relies upon the  
13986 base component to store and protect audit data, yet other evaluation evidence (e.g. the dependent  
13987 component design) makes it clear that the dependent component TSF itself is storing and  
13988 protecting the audit data, this would indicate an inaccuracy.

13989 It should be noted that the objectives for the operational environment may include objectives that  
13990 can be met by non-IT measures. While the services that the base component environment is  
13991 expected to provide may be described in the description of IT objectives for the operational  
13992 environment in the dependent component ST, it is not required that all such expectations on the  
13993 environment be described in the reliance information.

13994 ISO/IEC 15408-3 ACO\_REL.1.2C: *The reliance information shall describe all interactions through*  
13995 *which the dependent component TSF requests services from the base component.*

### 13996 16.5.1.4.3 Work unit ACO\_REL.1-3

13997 The evaluator **shall examine** the reliance information to determine that it describes all  
13998 interactions between the dependent component and the base component, through which the  
13999 dependent component TSF requests services from the base component.

14000 The dependent component TSF may request services of the base component that were not within  
14001 the TSF of the base component (see B.3, Interactions between composed IT entities in ISO/IEC  
14002 15408-3).

14003 The interfaces to the base component's functionality are described at the same level as the  
 14004 description of the interfaces to the dependent component TSF functionality, as would be provided  
 14005 between subsystems in the TOE design (Evaluation of sub-activity (ADV\_TDS.1)).

14006 The purpose of describing the interactions between the dependent component and the base  
 14007 component is to provide an understanding of how the dependent component TSF relies upon the  
 14008 base component for the provision of services to support the operation of security functionality of  
 14009 the dependent component. These interactions do not need to be characterised at the  
 14010 implementation level (e.g. parameters passed from one routine in a component to a routine in  
 14011 another component), but the data elements identified for a particular component that are going to  
 14012 be used by another component should be covered in this description. The statement should help  
 14013 the reader understand in general why the interaction is necessary.

14014 Accuracy and completeness of the interfaces is based on the security functionality that the TSF  
 14015 requires to be provided by the base component, as assessed in work units ACO\_REL.1-1 and  
 14016 ACO\_REL.1-2. It should be possible to map all of the functionality described in the earlier work  
 14017 units to the interfaces identified in this work unit, and vice versa. An interface that does not  
 14018 correspond to described functionality would also indicate an inadequacy.

14019 ISO/IEC 15408-3 ACO\_REL.1.3C: *The reliance information shall describe how the dependent TSF*  
 14020 *protects itself from interference and tampering by the base component.*

#### 14021 **16.5.1.4.4 Work unit ACO\_REL.1-4**

14022 The evaluator **shall examine** the reliance information to determine that it describes how the  
 14023 dependent TSF protects itself from interference and tampering by the base component.

14024 The description of how the dependent component protects itself from interference and tampering  
 14025 by the base component is to be provided at the same level of detail as necessary for ADV\_ARC.1-4.

#### 14026 **16.5.2 Evaluation of sub-activity (ACO\_REL.2)**

##### 14027 **16.5.2.1 Objectives**

14028 The objectives of this sub-activity are to determine whether the developer's reliance evidence  
 14029 provides sufficient information to determine that the necessary functionality is available in the  
 14030 base component, and the means by which that functionality is invoked. This is provided in terms of  
 14031 the interfaces between the dependent and base component and the return values from those  
 14032 interfaces called by the dependent component.

##### 14033 **16.5.2.2 Input**

14034 The evaluation evidence for this sub-activity is:

- 14035 a) the composed ST;
- 14036 b) the dependent component functional specification;
- 14037 c) the dependent component design;
- 14038 d) the dependent component implementation representation;
- 14039 e) the dependent component architectural design;
- 14040 f) the reliance information.

14041      **16.5.2.3 Application notes**

14042      A dependent component whose TSF interacts with the base component requires functionality  
14043      provided by that base component (e.g., remote authentication, remote audit data storage). In these  
14044      cases, those invoked services need to be described for those charged with configuring the  
14045      composed TOE for end users. The rationale for requiring this documentation is to aid integrators of  
14046      the composed TOE to determine what services in the base component might have adverse effects  
14047      on the dependent component, and to provide information against which to determine the  
14048      compatibility of the components when applying the Development evidence (ACO\_DEV) family.

14049      **16.5.2.4 Action ACO\_REL.2.1E**

14050      ISO/IEC 15408-3 ACO\_REL.2.1C: *The reliance information shall describe the functionality of the base*  
14051      *component hardware, firmware and/or software that is relied upon by the dependent component TSF.*

14052      **16.5.2.4.1 Work unit ACO\_REL.2-1**

14053      The evaluator **shall check** the reliance information to determine that it describes the functionality  
14054      of the base dependent hardware, firmware and/or software that is relied upon by the dependent  
14055      component TSF.

14056      The evaluator assesses the description of the security functionality that the dependent component  
14057      TSF requires to be provided by the base component's hardware, firmware and software. The  
14058      emphasis of this work unit is on the level of detail of this description, rather than on an assessment  
14059      of the information's accuracy. (The assessment of the accuracy of the information is the focus of the  
14060      next work unit.)

14061      This description of the base component's functionality need not be any more detailed than the level  
14062      of the description of a component of the TSF, as would be provided in the TOE Design (TOE design  
14063      (ADV\_TDS))

14064      **16.5.2.4.2 Work unit ACO\_REL.2-2**

14065      The evaluator **shall examine** the reliance information to determine that it accurately reflects the  
14066      objectives specified for the operational environment of the dependent component.

14067      The reliance information contains the description of the base component's security functionality  
14068      relied upon by the dependent component. To ensure that the reliance information is consistent  
14069      with the expectations of the operational environment of the dependent component, the evaluator  
14070      compares the reliance information with the statement of objectives for the environment in the ST  
14071      for the dependent component.

14072      For example, if the reliance information claims that the dependent component TSF relies upon the  
14073      base component to store and protect audit data, yet other evaluation evidence (e.g. the dependent  
14074      component design) makes it clear that the dependent component TSF itself is storing and  
14075      protecting the audit data, this would indicate an inaccuracy.

14076      It should be noted that the objectives for the operational environment may include objectives that  
14077      can be met by non-IT measures. While the services that the base component environment is  
14078      expected to provide may be described in the description of IT objectives for the operational  
14079      environment in the dependent component ST, it is not required that all such expectations on the  
14080      environment be described in the reliance information.

14081      ISO/IEC 15408-3 ACO\_REL.2.2C: *The reliance information shall describe all interactions through*  
14082      *which the dependent component TSF requests services from the base component.*



14083 **16.5.2.4.3 Work unit ACO\_REL.2-3**

14084 The evaluator *shall examine* the reliance information to determine that it describes all  
 14085 interactions between the dependent component and the base component, through which the  
 14086 dependent component TSF requests services from the base component.

14087 The dependent component TSF may request services of the base component that were not within  
 14088 the TSF of the base component (see Annex B.3, Interactions between composed IT entities in  
 14089 ISO/IEC 15408-3).

14090 The interfaces to the base component's functionality are described at the same level as the  
 14091 description of the interfaces to the dependent component TSF functionality, as would be provided  
 14092 between subsystems in the TOE design (Evaluation of sub-activity (ADV\_TDS.1)).

14093 The purpose of describing the interactions between the dependent component and the base  
 14094 component is to provide an understanding of how the dependent component TSF relies upon the  
 14095 base component for the provision of services to support the operation of security functionality of  
 14096 the dependent component. These interactions do not need to be characterised at the  
 14097 implementation level (e.g. parameters passed from one routine in a component to a routine in  
 14098 another component), but the data elements identified for a particular component that are going to  
 14099 be used by another component should be covered in this description. The statement should help  
 14100 the reader understand in general why the interaction is necessary.

14101 Accuracy and completeness of the interfaces is based on the security functionality that the TSF  
 14102 requires to be provided by the base component, as assessed in work units ACO\_REL.2-1 and  
 14103 ACO\_REL.2-2. It should be possible to map all of the functionality described in the earlier work  
 14104 units to the interfaces identified in this work unit, and vice versa. An interface that does not  
 14105 correspond to described functionality would also indicate an inadequacy.

14106 ISO/IEC 15408-3 ACO\_REL.2.3C: *The reliance information shall describe each interaction in terms of*  
 14107 *the interface used and the return values from those interfaces.*

14108 **16.5.2.4.4 Work unit ACO\_REL.2-4**

14109 The reliance information shall describe each interaction in terms of the interface used and the  
 14110 return values from those interfaces.

14111 The identification of the interfaces used by the dependent component TSF when making services  
 14112 requests of the base component allows an integrator to determine whether the base component  
 14113 provides all the necessary corresponding interfaces. This understanding is further gained through  
 14114 the specification of the return values expected by the dependent component. The evaluator ensures  
 14115 that interfaces are described for each interaction specified (as analysed in ACO\_REL.2-3).

14116 ISO/IEC 15408-3 ACO\_REL.2.4C: *The reliance information shall describe how the dependent TSF*  
 14117 *protects itself from interference and tampering by the base component.*

14118 **16.5.2.4.5 Work unit ACO\_REL.2-5**

14119 The evaluator *shall examine* the reliance information to determine that it describes how the  
 14120 dependent TSF protects itself from interference and tampering by the base component.

14121 The description of how the dependent component protects itself from interference and tampering  
 14122 by the base component is to be provided at the same level of detail as necessary for ADV\_ARC.1-4.

14123 **16.6 Composed TOE testing (ACO\_CTT)**

14124 **16.6.1 Evaluation of sub-activity (ACO\_CTT.1)**

14125 **16.6.1.1 Objectives**

14126 The objective of this sub-activity is to determine whether the developer correctly performed and  
14127 documented tests for each of the base component interfaces on which the dependent component  
14128 relies. As part of this determination the evaluator repeats a sample of the tests performed by the  
14129 developer and performs any additional tests required to ensure the expected behaviour of all  
14130 composed TOE SFRs and interfaces of the base component relied upon by the dependent  
14131 component is demonstrated.

14132 **16.6.1.2 Input**

14133 The evaluation evidence for this sub-activity is:

- 14134 a) the composed TOE suitable for testing;
- 14135 b) the composed TOE testing evidence;
- 14136 c) the reliance information;
- 14137 d) the development information.

14138 **16.6.1.3 Action ACO\_CTT.1.1E**

14139 ISO/IEC 15408-3 ACO\_CTT.1.1C: *The composed TOE and base component interface test*  
14140 *documentation shall consist of test plans, expected test results and actual test results.*

14141 **16.6.1.3.1 Work unit ACO\_CTT.1-1**

14142 The evaluator **shall examine** the composed TOE test documentation to determine that it consists  
14143 of test plans, expected test results and actual test results.

14144 This work unit may be satisfied by provision of the test evidence from the evaluation of the  
14145 dependent component if the base component was used to satisfy the requirements for IT in the  
14146 operational environment of the dependent component.

14147 All work units necessary for the satisfaction of ATE\_FUN.1.1E will be applied to determine:

- 14148 a) that the test documentation consists of test plans, expected test results, and actual  
14149 test results;
- 14150 b) that the test documentation contains the information necessary to ensure the tests  
14151 are repeatable;
- 14152 c) the level of developer effort that was applied to testing of the base component.

14153 **16.6.1.3.2 Work unit ACO\_CTT.1-2**

14154 The evaluator **shall examine** the base component interface test documentation to determine that it  
14155 consists of test plans, expected test results and actual test results.

14156 This work unit may be satisfied by provision of the test evidence from the evaluation of the base  
14157 component for those interfaces relied upon in the composed TOE by the dependent component are  
14158 TSFIs of the successfully evaluated base component. The determination of whether the interfaces  
14159 of the base component relied upon by the dependent component were in fact TSFIs of the  
14160 evaluated base component is made during the ACO\_COR activity.

14161 All work units necessary for the satisfaction of ATE\_FUN.1.1E will be applied to determine:

14162 a) that the test documentation consist of test plans expected test results and actual test  
14163 results;

14164 b) that the test documentation contains the information necessary to ensure the tests  
14165 are repeatable;

14166 c) the level of developer effort that was applied to testing of the base component.

14167 ISO/IEC 15408-3 ACO\_CTT.1.2C: *The test documentation from the developer execution of the*  
14168 *composed TOE tests shall demonstrate that the TSF behaves as specified.*

#### 14169 **16.6.1.3.3 Work unit ACO\_CTT.1-3**

14170 The evaluator **shall examine** the test documentation to determine that the developer execution of  
14171 the composed TOE tests shall demonstrate that the TSF behaves as specified.

14172 The evaluator should construct a mapping between the tests described in the test plan and the  
14173 SFRs specified for the composed TOE to identify which SFRs have been tested by the developer.

14174 Guidance on this work unit can be found in:

14175 a) Clause 14.2.1.

14176 b) Clause 14.2.2.

14177 The outputs from the successful execution of the tests (as assessed for ATE\_FUN.1.3C can be  
14178 compared with the mapping to determine that the SFRs of the composed TOE, as tested by the  
14179 developer, behave as expected.

14180 ISO/IEC 15408-3 ACO\_CTT.1.3C: *The test documentation from the developer execution of the base*  
14181 *component interface tests shall demonstrate that the base component interface relied upon by the*  
14182 *dependent component behaves as specified.*

#### 14183 **16.6.1.3.4 Work unit ACO\_CTT.1-4**

14184 The evaluator **shall examine** the test documentation to determine that the developer execution of  
14185 the base component interface tests shall demonstrate that the base component interfaces relied  
14186 upon by the dependent component behave as specified.

14187 The evaluator should construct a mapping between the tests described in the test plan and the  
14188 interfaces of the base component relied upon by the dependent component (as specified in the  
14189 reliance information, examined under ACO\_REL) to identify which base component interfaces have  
14190 been tested by the developer.

14191 Guidance on this work unit can be found in:

14192 a) Clause 14.2.1.

## ISO/IEC 18045:2008(E)

14193 b) Clause 14.2.2.

14194 The outputs from the successful execution of the tests (as assessed for ATE\_FUN.1.3C can be  
14195 compared with the mapping to determine that the interfaces of the base component, as tested by  
14196 the developer, behave as expected.

14197 ISO/IEC 15408-3 ACO\_CTT.1.4C: *The base component shall be suitable for testing.*

### 14198 **16.6.1.3.5 Work unit ACO\_CTT.1-5**

14199 The evaluator ***shall examine*** the composed TOE to determine that it has been installed properly  
14200 and is in a known state.

14201 To determine that the composed TOE has been installed properly and is in a known state the  
14202 ATE\_IND.2-1 and ATE\_IND.2-2 work units will be applied to the TOE provided by the developer for  
14203 testing.

### 14204 **16.6.1.3.6 Work unit ACO\_CTT.1-6**

14205 The evaluator ***shall examine*** the set of resources provided by the developer to determine that they  
14206 are equivalent to the set of resources used by the base component developer to functionally test  
14207 the base component.

14208 To determine that the set of resources provided are equivalent to those used to functionally test  
14209 the base component as used in the composed TOE, the ATE\_IND.2-3 work unit will be applied.

### 14210 **16.6.1.4 Action ACO\_CTT.1.2E**

#### 14211 **16.6.1.4.1 Work unit ACO\_CTT.1-7**

14212 The evaluator ***shall perform*** testing in accordance with ATE\_IND.2.2E, for a subset of the SFRs  
14213 specified in the composed security target, to verify the developer test results.

14214 The evaluator will apply all work units necessary for the satisfaction of ATE\_IND.2.2E, reporting in  
14215 the ETR for the composed TOE all analysis, results and verdicts as dictated by the associated work  
14216 units.

### 14217 **16.6.1.5 Action ACO\_CTT.1.3E**

#### 14218 **16.6.1.5.1 Work unit ACO\_CTT.1-8**

14219 The evaluator ***shall perform*** testing in accordance with ATE\_IND.2.3E, for a subset of the SFRs  
14220 specified in the composed security target, to confirm that the TSF operates as specified.

14221 The evaluator will apply all work units necessary for the satisfaction of ATE\_IND.2.3E, reporting in  
14222 the ETR for the composed TOE all analysis, results and verdicts as dictated by the work units.

14223 When selecting interfaces of the TSF of the composed TOE to test, the evaluator should take into  
14224 account any modifications to the components from the evaluated version or configuration.  
14225 Modifications to the component from that evaluated may include patches introduced, a different  
14226 configuration as a result of modified guidance documentation, reliance an additional portion of the  
14227 component that was not within the TSF of the component. These modifications will have been  
14228 identified during the Composition rationale (ACO\_COR) activity.

14229 **16.6.2 Evaluation of sub-activity (ACO\_CTT.2)**14230 **16.6.2.1 Objectives**

14231 The objective of this sub-activity is to determine whether the developer correctly performed and  
 14232 documented tests for each of the base component interfaces on which the dependent component  
 14233 relies. As part of this determination the evaluator repeats a sample of the tests performed by the  
 14234 developer and performs any additional tests required to fully demonstrate the expected behaviour  
 14235 of the composed TOE and the interfaces of the base component relied upon by the dependent  
 14236 component.

14237 **16.6.2.2 Input**

14238 The evaluation evidence for this sub-activity is:

- 14239 a) the composed TOE suitable for testing;
- 14240 b) the composed TOE testing evidence;
- 14241 c) the reliance information;
- 14242 d) the development information.

14243 **16.6.2.3 Action ACO\_CTT.2.1E**

14244 ISO/IEC 15408-3 ACO\_CTT.2.1C: *The composed TOE and base component interface test*  
 14245 *documentation shall consist of test plans, expected test results and actual test results.*

14246 **16.6.2.3.1 Work unit ACO\_CTT.2-1**

14247 The evaluator **shall examine** the composed TOE test documentation to determine that it consists  
 14248 of test plans, expected test results and actual test results.

14249 This work unit may be satisfied by provision of the test evidence from the evaluation of the  
 14250 dependent component if the base component was used to satisfy the requirements for IT in the  
 14251 operational environment of the dependent component.

14252 All work units necessary for the satisfaction of ATE\_FUN.1.1E will be applied to determine:

- 14253 a) that the test documentation consist of test plans expected test results and actual test  
 14254 results;
- 14255 b) that the test documentation contains the information necessary to ensure the tests  
 14256 are repeatable;
- 14257 c) the level of developer effort that was applied to testing of the base component.

14258 **16.6.2.3.2 Work unit ACO\_CTT.2-2**

14259 The evaluator **shall examine** the base component interface test documentation to determine that it  
 14260 consists of test plans, expected test results and actual test results.

14261 This work unit may be satisfied by provision of the test evidence from the evaluation of the base  
 14262 component for those interfaces relied upon in the composed TOE by the dependent component are

## ISO/IEC 18045:2008(E)

14263 TSFIs of the successfully evaluated base component. The determination of whether the interfaces  
14264 of the base component relied upon by the dependent component were in fact TSFIs of the  
14265 evaluated base component is made during the ACO\_COR activity.

14266 All work units necessary for the satisfaction of ATE\_FUN.1.1E will be applied to determine:

14267 a) that the test documentation consists of test plans, expected test results, and actual  
14268 test results;

14269 b) that the test documentation contains the information necessary to ensure the tests  
14270 are repeatable;

14271 c) the level of developer effort that was applied to testing of the base component.

14272 ISO/IEC 15408-3 ACO\_CTT.2.2C: *The test documentation from the developer execution of the*  
14273 *composed TOE tests shall demonstrate that the TSF behaves as specified and is complete.*

### 14274 **16.6.2.3.3 Work unit ACO\_CTT.2-3**

14275 The evaluator **shall examine** the test documentation to determine that it provides accurate  
14276 correspondence between the tests in the test documentation relating to the testing of the  
14277 composed TOE and the composed TOE SFRs in the composed TOE security target.

14278 A simple cross-table may be sufficient to show test correspondence. The identification of  
14279 correspondence between the tests and SFRs presented in the test documentation has to be  
14280 unambiguous.

### 14281 **16.6.2.3.4 Work unit ACO\_CTT.2-4**

14282 The evaluator **shall examine** the test documentation to determine that the developer execution of  
14283 the composed TOE tests shall demonstrate that the TSF behaves as specified.

14284 Guidance on this work unit can be found in:

14285 a) Clause 14.2.1.

14286 b) Clause 14.2.2.

14287 The outputs from the successful execution of the tests (as assessed for ATE\_FUN.1.3C can be  
14288 compared with the mapping to determine that the SFRs of the composed TOE, as tested by the  
14289 developer, behave as expected.

14290 ISO/IEC 15408-3 ACO\_CTT.2.3C: *The test documentation from the developer execution of the base*  
14291 *component interface tests shall demonstrate that the base component interface relied upon by the*  
14292 *dependent component behaves as specified and is complete.*

### 14293 **16.6.2.3.5 Work unit ACO\_CTT.2-5**

14294 The evaluator **shall examine** the test documentation to determine that it provides accurate  
14295 correspondence between the tests in the test documentation relating to the testing of the base  
14296 component interfaces relied upon by the dependent component and the interfaces specified in the  
14297 reliance information.

14298 A simple cross-table may be sufficient to show test correspondence. The identification of  
 14299 correspondence between the tests and interfaces presented in the test documentation has to be  
 14300 unambiguous.

14301 **16.6.2.3.6 Work unit ACO\_CTT.2-6**

14302 The evaluator *shall examine* the test documentation to determine that the developer execution of  
 14303 the base component interface tests shall demonstrate that the base component interfaces relied  
 14304 upon by the dependent component behave as specified.

14305 Guidance on this work unit can be found in:

14306 a) Clause 14.2.1.

14307 b) Clause 14.2.2.

14308 The outputs from the successful execution of the tests (as assessed for ATE\_FUN.1.3C can be  
 14309 compared with the mapping to determine that the interfaces of the base component, as tested by  
 14310 the developer, behave as expected.

14311 ISO/IEC 15408-3 ACO\_CTT.2.4C: *The base component shall be suitable for testing.*

14312 **16.6.2.3.7 Work unit ACO\_CTT.2-7**

14313 The evaluator *shall examine* the composed TOE to determine that it has been installed properly  
 14314 and is in a known state.

14315 To determine that the composed TOE has been installed properly and is in a known state the  
 14316 ATE\_IND.2-1 and ATE\_IND.2-2 work units will be applied to the TOE provided by the developer for  
 14317 testing.

14318 **16.6.2.3.8 Work unit ACO\_CTT.2-8**

14319 The evaluator *shall examine* the set of resources provided by the developer to determine that they  
 14320 are equivalent to the set of resources used by the base component developer to functionally test  
 14321 the base component.

14322 To determine that the set of resources provided are equivalent to those used to functionally test  
 14323 the base component as used in the composed TOE, the ATE\_IND.2-3 work unit will be applied.

14324 **16.6.2.4 Action ACO\_CTT.2.2E**

14325 **16.6.2.4.1 Work unit ACO\_CTT.2-9**

14326 The tests are to be selected and executed in accordance with ATE\_IND.2.2E, to demonstrate the  
 14327 correct behaviour of the SFRs specified in the composed TOE security target.

14328 The evaluator will apply all work units necessary for the satisfaction of ATE\_IND.2.2E, reporting in  
 14329 the ETR for the composed TOE all analysis, results and verdicts as dictated by the associated work  
 14330 units.

14331 **16.6.2.5 Action ACO\_CTT.2.3E**

14332 **16.6.2.5.1 Work unit ACO\_CTT.2-10**

14333 The evaluator *shall perform* testing in accordance with ATE\_IND.2.3E, for a subset of the SFRs  
 14334 specified in the composed security target, to confirm that the TSF operates as specified.

14335 The evaluator will apply all work units necessary for the satisfaction of ATE\_IND.2.3E, reporting in  
14336 the ETR for the composed TOE all analysis, results and verdicts as dictated by the work units.

14337 When selecting interfaces of the TSF of the composed TOE to test, the evaluator should take into  
14338 account any modifications to the components from the evaluated version or configuration.  
14339 Modifications to the component from that evaluated may include patches introduced, a different  
14340 configuration as a result of modified guidance documentation, reliance on an additional portion of the  
14341 component that was not within the TSF of the component. These modifications will have been  
14342 identified during the Composition rationale (ACO\_COR) activity.

#### 14343 16.6.2.5.2 Work unit ACO\_CTT.2-11

14344 The evaluator *shall perform* testing, in accordance with Evaluation of sub-activity (ATE\_IND.2), for  
14345 a subset of the interfaces to the base component to confirm they operate as specified.

14346 The evaluator will apply all work units necessary for the satisfaction of ATE\_IND.2.3E, reporting in  
14347 the ETR for the composed TOE all analysis, results and verdicts as dictated by the work units.

14348 When selecting interfaces of the base component to test, the evaluator should take into account any  
14349 modifications to the base component from the evaluated version or configuration. In particular, the  
14350 evaluator should consider the development of tests to demonstrate the correct behaviour of  
14351 interfaces of the base component that were not considered during the evaluation of the base  
14352 component. These additional interfaces and other modifications to the base component will have  
14353 been identified during the Composition rationale (ACO\_COR) activity.

### 14354 16.7 Composition vulnerability analysis (ACO\_VUL)

#### 14355 16.7.1 Evaluation of sub-activity (ACO\_VUL.1)

##### 14356 16.7.1.1 Objectives

14357 The objective of this sub-activity is to determine whether the composed TOE, in its operational  
14358 environment, has easily exploitable vulnerabilities.

14359 The developer provides details of any residual vulnerabilities reported from evaluation of the  
14360 components. The evaluator performs an analysis of the disposition the residual vulnerabilities  
14361 reported and also performs a search of the public domain, to identify any new potential  
14362 vulnerabilities in the components (i.e. those issues that have been reported in the public domain  
14363 since evaluation of the base component). The evaluator then performs penetration testing to  
14364 demonstrate that the potential vulnerabilities cannot be exploited in the TOE, in its operational  
14365 environment, by an attacker with basic attack potential.

##### 14366 16.7.1.2 Input

14367 The evaluation evidence for this sub-activity is:

14368 a) the composed TOE suitable for testing;

14369 b) the composed ST;

14370 c) the composition rationale;

14371 d) the guidance documentation;

14372 e) information publicly available to support the identification of possible security  
14373 vulnerabilities;



14374 f) residual vulnerabilities reported during evaluation of each component.

#### 14375 16.7.1.3 Application notes

14376 See the application notes for Evaluation of sub-activity (AVA\_VAN.1).

#### 14377 16.7.1.4 Action ACO\_VUL.1.1E

14378 ISO/IEC 15408-3 ACO\_VUL.1.1C: *The composed TOE shall be suitable for testing.*

##### 14379 16.7.1.4.1 Work unit ACO\_VUL.1-1

14380 The evaluator **shall examine** the composed TOE to determine that it has been installed properly  
14381 and is in a known state.

14382 To determine that the composed TOE has been installed properly and is in a known state the  
14383 ATE\_IND.2-1 and ATE\_IND.2-2 work units will be applied to the composed TOE.

14384 If the assurance package includes a component from the ACO\_CTT family, then the evaluator may  
14385 refer to the result of the work unit ACO\_CTT\*-1 to demonstrate this has been satisfied.

##### 14386 16.7.1.4.2 Work unit ACO\_VUL.1-2

14387 The evaluator **shall examine** the composed TOE configuration to determine that any assumptions  
14388 and objectives in the STs the components relating to IT entities for are fulfilled by the other  
14389 components.

14390 The STs for the component may include assumptions about other components that may use the  
14391 component to which the ST relates, e.g. the ST for an operating system used as a base component  
14392 may include an assumption that any applications loaded on the operating system do not run in  
14393 privileged mode. These assumptions and objectives are to be fulfilled by other components in the  
14394 composed TOE.

#### 14395 16.7.1.5 Action ACO\_VUL.1.2E

##### 14396 16.7.1.5.1 Work unit ACO\_VUL.1-3

14397 The evaluator **shall examine** the residual vulnerabilities from the base component evaluation to  
14398 determine that they are not exploitable in the composed TOE in its operational environment.

14399 The list of vulnerabilities identified in the product during the evaluation of the base component,  
14400 which were demonstrated to be non-exploitable in the base component, is to be used as an input  
14401 into this activity. The evaluator will determine that the premise(s) on which a vulnerability was  
14402 deemed to be non-exploitable is upheld in the composed TOE, or whether the combination has re-  
14403 introduced the potential vulnerability. For example, if during evaluation of the base component it  
14404 was assumed that a particular operating system service was disabled, which is enabled in the  
14405 composed TOE evaluation, any potential vulnerabilities relating to that service previously scoped  
14406 out should now be considered.

14407 Also, this list of known, non-exploitable vulnerabilities resulting from the evaluation of the base  
14408 component should be considered in the light of any known, non-exploitable vulnerabilities for the  
14409 other components (e.g. dependent component) within the composed TOE. This is to consider the  
14410 case where a potential vulnerability that is non-exploitable in isolation is exploitable when  
14411 integrated with an IT entity containing another potential vulnerability.

14412 **16.7.1.5.2 Work unit ACO\_VUL.1-4**

14413 The evaluator *shall examine* the residual vulnerabilities from the dependent component  
14414 evaluation to determine that they are not exploitable in the composed TOE in its operational  
14415 environment.

14416 The list of vulnerabilities identified in the product during the evaluation of the dependent  
14417 component, which were demonstrated to be non-exploitable in the dependent component, is to be  
14418 used as an input into this activity. The evaluator will determine that the premise(s) on which a  
14419 vulnerability was deemed to be non-exploitable is upheld in the composed TOE, or whether the  
14420 combination has re-introduced the potential vulnerability. For example, if during evaluation of the  
14421 dependent component it was assumed that IT meeting the operational environment requirements  
14422 would not return a certain value in response to a service request, which is provided by the base  
14423 component in the composed TOE evaluation, any potential vulnerabilities relating to that return  
14424 value previously scoped out should now be considered.

14425 Also, this list of known, non-exploitable vulnerabilities resulting from the evaluation of the  
14426 dependent component should be considered in the light of any known, non-exploitable  
14427 vulnerabilities for the other components (e.g. base component) within the composed TOE. This is  
14428 to consider the case where a potential vulnerability that is non-exploitable in isolation is  
14429 exploitable when integrated with an IT entity containing another potential vulnerability.

14430 **16.7.1.6 Action ACO\_VUL.1.3E**

14431 **16.7.1.6.1 Work unit ACO\_VUL.1-5**

14432 The evaluator *shall examine* the sources of information publicly available to support the  
14433 identification of possible security vulnerabilities in the base component that have become known  
14434 since the completion of evaluation of the base component.

14435 The evaluator will use the information in the public domain as described in AVA\_VAN.1-2 to search  
14436 for vulnerabilities in the base component.

14437 Those potential vulnerabilities that were publicly available prior to the evaluation of the base  
14438 component do not have to be further investigated unless it is apparent to the evaluator that the  
14439 attack potential required by an attacker to exploit the potential vulnerability has been significantly  
14440 reduced. This may be through the introduction of some new technology since the base component  
14441 evaluation that means the exploitation of the potential vulnerability has been simplified.

14442 **16.7.1.6.2 Work unit ACO\_VUL.1-6**

14443 The evaluator *shall examine* the sources of information publicly available to support the  
14444 identification of possible security vulnerabilities in the dependent component that have become  
14445 known since the completion of the dependent component evaluation.

14446 The evaluator will use the information in the public domain as described in AVA\_VAN.1-2 to search  
14447 for vulnerabilities in the dependent component.

14448 Those potential vulnerabilities that were publicly available prior to the evaluation of the  
14449 dependent component do not have to be further investigated unless it is apparent to the evaluator  
14450 that the attack potential required by an attacker to exploit the potential vulnerability has been  
14451 significantly reduced. This may be through the introduction of some new technology since  
14452 evaluation of the dependent component that means the exploitation of the potential vulnerability  
14453 has been simplified.

14454 **16.7.1.6.3 Work unit ACO\_VUL.1-7**

14455 The evaluator **shall record** in the ETR the identified potential security vulnerabilities that are  
14456 candidates for testing and applicable to the composed TOE in its operational environment.

14457 The ST, guidance documentation and functional specification are used to determine whether the  
14458 vulnerabilities are relevant to the composed TOE in its operational environment.

14459 The evaluator records any reasons for exclusion of vulnerabilities from further consideration if the  
14460 evaluator determines that the vulnerability is not applicable in the operational environment.  
14461 Otherwise the evaluator records the potential vulnerability for further consideration.

14462 A list of potential vulnerabilities applicable to the composed TOE in its operational environment,  
14463 which can be used as an input into penetration testing activities (i.e. ACO\_VUL.1.4E), shall be  
14464 reported in the ETR by the evaluators.

14465 **16.7.1.7 Action ACO\_VUL.1.4E**14466 **16.7.1.7.1 Work unit ACO\_VUL.1-8**

14467 The evaluator **shall conduct** penetration testing as detailed for AVA\_VAN.1.3E.

14468 The evaluator will apply all work units necessary for the satisfaction of evaluator action  
14469 AVA\_VAN.1.3E, reporting in the ETR for the composed TOE all analysis and verdicts as dictated by  
14470 the work units.

14471 The evaluator will also apply the work units for the evaluator action AVA\_VAN.1.1E to determine  
14472 that the composed TOE provided by the developer is suitable for testing.

14473 **16.7.2 Evaluation of sub-activity (ACO\_VUL.2)**14474 **16.7.2.1 Objectives**

14475 The objective of this sub-activity is to determine whether the composed TOE, in its operational  
14476 environment, has vulnerabilities exploitable by attackers possessing basic attack potential.

14477 The developer provides an analysis of the disposition of any residual vulnerabilities reported for  
14478 the components and of any vulnerabilities introduced through the combination of the base and  
14479 dependent components. The evaluator performs a search of the public domain to identify any new  
14480 potential vulnerabilities in the components (i.e. those issues that have been reported in the public  
14481 domain since the completion of the evaluation of the components). The evaluator will also perform  
14482 an independent vulnerability analysis of the composed TOE and penetration testing.

14483 **16.7.2.2 Input**

14484 The evaluation evidence for this sub-activity is:

14485 a) the composed TOE suitable for testing;

14486 b) the composed ST;

14487 c) the composition rationale;

14488 d) the reliance information;

14489 e) the guidance documentation;

## ISO/IEC 18045:2008(E)

- 14490 f) information publicly available to support the identification of possible security  
14491 vulnerabilities.
- 14492 g) residual vulnerabilities reported during evaluation of each component.
- 14493 **16.7.2.3 Application notes**
- 14494 See the application notes for Evaluation of sub-activity (AVA\_VAN.2).
- 14495 **16.7.2.4 Action ACO\_VUL.2.1E**
- 14496 ISO/IEC 15408-3 ACO\_VUL.2.1C: *The composed TOE shall be suitable for testing.*
- 14497 **16.7.2.4.1 Work unit ACO\_VUL.2-1**
- 14498 The evaluator **shall examine** the composed TOE to determine that it has been installed properly  
14499 and is in a known state.
- 14500 To determine that the composed TOE has been installed properly and is in a known state the  
14501 ATE\_IND.2-1 and ATE\_IND.2-2 work units will be applied to the composed TOE.
- 14502 If the assurance package includes ACO\_CTT family, then the evaluator may refer to the result of the  
14503 work unit Composed TOE testing (ACO\_CTT)\*-1 to demonstrate this has been satisfied.
- 14504 **16.7.2.4.2 Work unit ACO\_VUL.2-2**
- 14505 The evaluator **shall examine** the composed TOE configuration to determine that any assumptions  
14506 and objectives in the STs the components relating to IT entities for are fulfilled by the other  
14507 components.
- 14508 The STs for the component may include assumptions about other components that may use the  
14509 component to which the ST relates, e.g. the ST for an operating system used as a base component  
14510 may include an assumption that any applications loaded on the operating system do not run in  
14511 privileged mode. These assumptions and objectives are to be fulfilled by other components in the  
14512 composed TOE.
- 14513 **16.7.2.5 Action ACO\_VUL.2.2E**
- 14514 **16.7.2.5.1 Work unit ACO\_VUL.2-3**
- 14515 The evaluator **shall examine** the residual vulnerabilities from the base component evaluation to  
14516 determine that they are not exploitable in the composed TOE in its operational environment.
- 14517 The list of vulnerabilities identified in the product during the evaluation of the base component,  
14518 which were demonstrated to be non-exploitable in the base component, is to be used as an input  
14519 into this activity. The evaluator will determine that the premise(s) on which a vulnerability was  
14520 deemed to be non-exploitable is upheld in the composed TOE, or whether the combination has re-  
14521 introduced the potential vulnerability. For example, if during evaluation of the base component it  
14522 was assumed that a particular operating system service was disabled, which is enabled in the  
14523 composed TOE evaluation, any potential vulnerabilities relating to that service previously scoped  
14524 out should now be considered.
- 14525 Also, this list of known, non-exploitable vulnerabilities resulting from the evaluation of the base  
14526 component should be considered in the light of any known, non-exploitable vulnerabilities for the  
14527 other components (e.g. dependent component) within the composed TOE. This is to consider the  
14528 case where a potential vulnerability that is non-exploitable in isolation is exploitable when  
14529 integrated with an IT entity containing another potential vulnerability.

14530 **16.7.2.5.2 Work unit ACO\_VUL.2-4**

14531 The evaluator *shall examine* the residual vulnerabilities from the dependent component  
 14532 evaluation to determine that they are not exploitable in the composed TOE in its operational  
 14533 environment.

14534 The list of vulnerabilities identified in the product during the evaluation of the dependent  
 14535 component, which were demonstrated to be non-exploitable in the dependent component, is to be  
 14536 used as an input into this activity. The evaluator will determine that the premise(s) on which a  
 14537 vulnerability was deemed to be non-exploitable is upheld in the composed TOE, or whether the  
 14538 combination has re-introduced the potential vulnerability. For example, if during evaluation of the  
 14539 dependent component it was assumed that IT meeting the operational environment requirements  
 14540 would not return a certain value in response to a service request, which is provided by the base  
 14541 component in the composed TOE evaluation, any potential vulnerabilities relating to that return  
 14542 value previously scoped out should now be considered.

14543 Also, this list of known, non-exploitable vulnerabilities resulting from the evaluation of the  
 14544 dependent component should be considered in the light of any known, non-exploitable  
 14545 vulnerabilities for the other components (e.g. base component) within the composed TOE. This is  
 14546 to consider the case where a potential vulnerability that is non-exploitable in isolation is  
 14547 exploitable when integrated with an IT entity containing another potential vulnerability.

14548 **16.7.2.6 Action ACO\_VUL.2.3E**14549 **16.7.2.6.1 Work unit ACO\_VUL.2-5**

14550 The evaluator *shall examine* the sources of information publicly available to support the  
 14551 identification of possible security vulnerabilities in the base component that have become known  
 14552 since the completion of the base component evaluation.

14553 The evaluator will use the information in the public domain as described in AVA\_VAN.2-2 to search  
 14554 for vulnerabilities in the base component.

14555 Those potential vulnerabilities that were publicly available prior to the evaluation of the base  
 14556 component do not have to be further investigated unless it is apparent to the evaluator that the  
 14557 attack potential required by an attacker to exploit the potential vulnerability has been significantly  
 14558 reduced. This may be through the introduction of some new technology since the base component  
 14559 evaluation that means the exploitation of the potential vulnerability has been simplified.

14560 **16.7.2.6.2 Work unit ACO\_VUL.2-6**

14561 The evaluator *shall examine* the sources of information publicly available to support the  
 14562 identification of possible security vulnerabilities in the dependent component that have become  
 14563 known since the completion of the dependent component evaluation.

14564 The evaluator will use the information in the public domain as described in AVA\_VAN.2-2 to search  
 14565 for vulnerabilities in the dependent component.

14566 Those potential vulnerabilities that were publicly available prior to the evaluation of the  
 14567 dependent component do not have to be further investigated unless it is apparent to the evaluator  
 14568 that the attack potential required by an attacker to exploit the potential vulnerability has been  
 14569 significantly reduced. This may be through the introduction of some new technology since  
 14570 evaluation of the dependent component that means the exploitation of the potential vulnerability  
 14571 has been simplified.

## ISO/IEC 18045:2008(E)

### 14572 16.7.2.6.3 Work unit ACO\_VUL.2-7

14573 The evaluator **shall record** in the ETR the identified potential security vulnerabilities that are  
14574 candidates for testing and applicable to the composed TOE in its operational environment.

14575 The ST, guidance documentation and functional specification are used to determine whether the  
14576 vulnerabilities are relevant to the composed TOE in its operational environment.

14577 The evaluator records any reasons for exclusion of vulnerabilities from further consideration if the  
14578 evaluator determines that the vulnerability is not applicable in the operational environment.  
14579 Otherwise the evaluator records the potential vulnerability for further consideration.

14580 A list of potential vulnerabilities applicable to the composed TOE in its operational environment,  
14581 which can be used as an input into penetration testing activities (ACO\_VUL.2.5E), shall be reported  
14582 in the ETR by the evaluators.

### 14583 16.7.2.7 Action ACO\_VUL.2.4E

#### 14584 16.7.2.7.1 Work unit ACO\_VUL.2-8

14585 The evaluator **shall conduct** a search of the composed TOE ST, guidance documentation, reliance  
14586 information and composition rationale to identify possible security vulnerabilities in the composed  
14587 TOE.

14588 The consideration of the components of the composed TOE in the independent evaluator  
14589 vulnerability analysis will take a slightly different form to that documented in AVA\_VAN.2.3E for a  
14590 component evaluation, as it will not necessarily consider all layers of design abstraction relevant to  
14591 the assurance package. These will have already been considered during the evaluation of the  
14592 components, but the evidence may not be available for the composed TOE evaluation. However, the  
14593 general approach described in the work units associated with AVA\_VAN.2.3E is applicable and  
14594 should form the basis of the evaluator's search for potential vulnerabilities in the composed TOE.

14595 A vulnerability analysis of the individual components used in the composed TOE will have already  
14596 been performed during evaluation of the individual components. The focus of the vulnerability  
14597 analysis during the composed TOE evaluation is to identify any vulnerabilities introduced as a  
14598 result of the integration of the components or due to any changes in the use of the components  
14599 between the evaluated component configuration to the composed TOE configuration.

14600 The evaluator will use the understanding of the component's construction as detailed in the  
14601 reliance information for the dependent component, and the development information and  
14602 composition rationale for the base component, together with the dependent component design  
14603 information. This information will allow the evaluator to gain an understanding of how the base  
14604 component and dependent component interact and identify potential vulnerabilities that may be  
14605 introduced as a result of this interaction.

14606 The evaluator will consider any new guidance provided for the installation, start-up and operation  
14607 of the composed TOE to identify any potential vulnerabilities introduced through this revised  
14608 guidance.

14609 If any of the individual components have been through assurance continuity activities since the  
14610 completion of the component evaluation, the evaluator will consider the patch(es) in the  
14611 independent vulnerability analysis. Information related to the change provided in a public report of  
14612 the assurance continuity activities (e.g. Maintenance Report) will be the main source of input  
14613 material of the change. This will be supplemented by any updates to the guidance documentation  
14614 resulting from the change and any information regarding the change available in the public domain,  
14615 e.g. vendor website.

14616 Any risks identified due to the lack of evidence to establish the full impact of any patches or  
 14617 deviations in the configuration of a component from the evaluated configuration are to be  
 14618 documented in the evaluator's vulnerability analysis.

14619 **16.7.2.8 Action ACO\_VUL.2.5E**

14620 **16.7.2.8.1 Work unit ACO\_VUL.2-9**

14621 The evaluator **shall conduct** penetration testing as detailed for AVA\_VAN.2.4E.

14622 The evaluator will apply all work units necessary for the satisfaction of evaluator action  
 14623 AVA\_VAN.2.4E, reporting in the ETR for the composed TOE all analysis and verdicts as dictated by  
 14624 the work units.

14625 The evaluator will also apply the work units for the evaluator action AVA\_VAN.2.1E to determine  
 14626 that the composed TOE provided by the developer is suitable for testing.

14627 **16.7.3 Evaluation of sub-activity (ACO\_VUL.3)**

14628 **16.7.3.1 Objectives**

14629 The objective of this sub-activity is to determine whether the composed TOE, in its operational  
 14630 environment, has vulnerabilities exploitable by attackers possessing Enhanced-Basic attack  
 14631 potential.

14632 The developer provides an analysis of the disposition of any residual vulnerabilities reported for  
 14633 the components and of any vulnerabilities introduced through the combination of the base and  
 14634 dependent components. The evaluator performs a search of the public domain to identify any new  
 14635 potential vulnerabilities in the components (i.e. those issues that have been reported in the public  
 14636 domain since the completion of the component evaluations). The evaluator will also perform an  
 14637 independent vulnerability analysis of the composed TOE and penetration testing.

14638 **16.7.3.2 Input**

14639 The evaluation evidence for this sub-activity is:

- 14640 a) the composed TOE suitable for testing;
- 14641 b) the composed ST;
- 14642 c) the composition rationale;
- 14643 d) the reliance information;
- 14644 e) the guidance documentation;
- 14645 f) information publicly available to support the identification of possible security  
 14646 vulnerabilities.
- 14647 g) residual vulnerabilities reported during evaluation of each component.

14648 **16.7.3.3 Application notes**

14649 See the application notes for Evaluation of sub-activity (AVA\_VAN.3).

## ISO/IEC 18045:2008(E)

### 14650 16.7.3.4 Action ACO\_VUL.3.1E

14651 ISO/IEC 15408-3 ACO\_VUL.3.1C: *The composed TOE shall be suitable for testing.*

#### 14652 16.7.3.4.1 Work unit ACO\_VUL.3-1

14653 The evaluator **shall examine** the composed TOE to determine that it has been installed properly  
14654 and is in a known state.

14655 To determine that the composed TOE has been installed properly and is in a known state the  
14656 ATE\_IND.2-1 and ATE\_IND.2-2 work units will be applied to the composed TOE.

14657 If the assurance package includes ACO\_CTT family, then the evaluator may refer to the result of the  
14658 work unit Composed TOE testing (ACO\_CTT)\*-1 to demonstrate this has been satisfied.

#### 14659 16.7.3.4.2 Work unit ACO\_VUL.3-2

14660 The evaluator **shall examine** the composed TOE configuration to determine that any assumptions  
14661 and objectives in the STs the components relating to IT entities for are fulfilled by the other  
14662 components.

14663 The STs for the component may include assumptions about other components that may use the  
14664 component to which the ST relates, e.g. the ST for an operating system used as a base component  
14665 may include an assumption that any applications loaded on the operating system do not run in  
14666 privileged mode. These assumptions and objectives are to be fulfilled by other components in the  
14667 composed TOE.

### 14668 16.7.3.5 Action ACO\_VUL.3.2E

#### 14669 16.7.3.5.1 Work unit ACO\_VUL.3-3

14670 The evaluator **shall examine** the residual vulnerabilities from the base component evaluation to  
14671 determine that they are not exploitable in the composed TOE in its operational environment.

14672 The list of vulnerabilities identified in the product during the evaluation of the base component,  
14673 which were demonstrated to be non-exploitable in the base component, is to be used as an input  
14674 into this activity. The evaluator will determine that the premise(s) on which a vulnerability was  
14675 deemed to be non-exploitable is upheld in the composed TOE, or whether the combination has re-  
14676 introduced the potential vulnerability. For example, if during evaluation of the base component it  
14677 was assumed that a particular operating system service was disabled, which is enabled in the  
14678 composed TOE evaluation, any potential vulnerabilities relating to that service previously scoped  
14679 out should now be considered.

14680 Also, this list of known, non-exploitable vulnerabilities resulting from the evaluation of the base  
14681 component should be considered in the light of any known, non-exploitable vulnerabilities for the  
14682 other components (e.g. dependent component) within the composed TOE. This is to consider the  
14683 case where a potential vulnerability that is non-exploitable in isolation is exploitable when  
14684 integrated with an IT entity containing another potential vulnerability.

#### 14685 16.7.3.5.2 Work unit ACO\_VUL.3-4

14686 The evaluator **shall examine** the residual vulnerabilities from the dependent component  
14687 evaluation to determine that they are not exploitable in the composed TOE in its operational  
14688 environment.

14689 The list of vulnerabilities identified in the product during the evaluation of the dependent  
14690 component, which were demonstrated to be non-exploitable in the dependent component, is to be  
14691 used as an input into this activity. The evaluator will determine that the premise(s) on which a



14692 vulnerability was deemed to be non-exploitable is upheld in the composed TOE, or whether the  
 14693 combination has re-introduced the potential vulnerability. For example, if during evaluation of the  
 14694 dependent component it was assumed that IT meeting the operational environment requirements  
 14695 would not return a certain value in response to a service request, which is provided by the base  
 14696 component in the composed TOE evaluation, any potential vulnerabilities relating to that return  
 14697 value previously scoped out should now be considered.

14698 Also, this list of known, non-exploitable vulnerabilities resulting from the evaluation of the  
 14699 dependent component should be considered in the light of any known, non-exploitable  
 14700 vulnerabilities for the other components (e.g. base component) within the composed TOE. This is  
 14701 to consider the case where a potential vulnerability that is non-exploitable in isolation is  
 14702 exploitable when integrated with an IT entity containing another potential vulnerability.

#### 14703 **16.7.3.6 Action ACO\_VUL.3.3E**

##### 14704 **16.7.3.6.1 Work unit ACO\_VUL.3-5**

14705 The evaluator *shall examine* the sources of information publicly available to support the  
 14706 identification of possible security vulnerabilities in the base component that have become known  
 14707 since the completion of the base component evaluation.

14708 The evaluator will use the information in the public domain as described in AVA\_VAN.3-2 to search  
 14709 for vulnerabilities in the base component.

14710 Those potential vulnerabilities that were publicly available prior to the evaluation of the base  
 14711 component do not have to be further investigated unless it is apparent to the evaluator that the  
 14712 attack potential required by an attacker to exploit the potential vulnerability has been significantly  
 14713 reduced. This may be through the introduction of some new technology since the base component  
 14714 evaluation that means the exploitation of the potential vulnerability has been simplified.

##### 14715 **16.7.3.6.2 Work unit ACO\_VUL.3-6**

14716 The evaluator *shall examine* the sources of information publicly available to support the  
 14717 identification of possible security vulnerabilities in the dependent component that have become  
 14718 known since completion of the dependent component evaluation.

14719 The evaluator will use the information in the public domain as described in AVA\_VAN.3-2 to search  
 14720 for vulnerabilities in the dependent component.

14721 Those potential vulnerabilities that were publicly available prior to the evaluation of the  
 14722 dependent component do not have to be further investigated unless it is apparent to the evaluator  
 14723 that the attack potential required by an attacker to exploit the potential vulnerability has been  
 14724 significantly reduced. This may be through the introduction of some new technology since  
 14725 evaluation of the dependent component that means the exploitation of the potential vulnerability  
 14726 has been simplified.

##### 14727 **16.7.3.6.3 Work unit ACO\_VUL.3-7**

14728 The evaluator *shall record* in the ETR the identified potential security vulnerabilities that are  
 14729 candidates for testing and applicable to the composed TOE in its operational environment.

14730 The ST, guidance documentation and functional specification are used to determine whether the  
 14731 vulnerabilities are relevant to the composed TOE in its operational environment.

14732 The evaluator records any reasons for exclusion of vulnerabilities from further consideration if the  
 14733 evaluator determines that the vulnerability is not applicable in the operational environment.  
 14734 Otherwise the evaluator records the potential vulnerability for further consideration.

## ISO/IEC 18045:2008(E)

14735 A list of potential vulnerabilities applicable to the composed TOE in its operational environment,  
14736 which can be used as an input into penetration testing activities (ACO\_VUL.3.5E), shall be reported  
14737 in the ETR by the evaluators.

### 14738 16.7.3.7 Action ACO\_VUL.3.4E

#### 14739 16.7.3.7.1 Work unit ACO\_VUL.3-8

14740 The evaluator **shall conduct** a search of the composed TOE ST, guidance documentation, reliance  
14741 information and composition rationale to identify possible security vulnerabilities in the composed  
14742 TOE.

14743 The consideration of the components in the independent evaluator vulnerability analysis will take  
14744 a slightly different form to that documented in AVA\_VAN.3.3E for a component evaluation, as it will  
14745 not necessarily consider all layers of design abstraction relevant to the assurance package. These  
14746 will have already been considered during the evaluation of the base component, but the evidence  
14747 may not be available for the composed TOE evaluation. However, the general approach described  
14748 in the work units associated with AVA\_VAN.3.3E is applicable and should form the basis of the  
14749 evaluator's search for potential vulnerabilities in the composed TOE.

14750 A vulnerability analysis of the individual components used in the composed TOE will have already  
14751 been performed during evaluation of the components. The focus of the vulnerability analysis  
14752 during the composed TOE evaluation is to identify any vulnerabilities introduced as a result of the  
14753 integration of the components or due to any changes in the use of the components between the  
14754 configuration of the component determined during the component evaluation and the composed  
14755 TOE configuration.

14756 The evaluator will use the understanding of the component's construction as detailed in the  
14757 reliance information for the dependent component, and the composition rationale and  
14758 development information for the base component, together with the dependent component design  
14759 information. This information will allow the evaluator to gain an understanding of how the base  
14760 component and dependent component interact.

14761 The evaluator will consider any new guidance provided for the installation, start-up and operation  
14762 of the composed TOE to identify any potential vulnerabilities introduced through this revised  
14763 guidance.

14764 If any of the individual components have been through assurance continuity activities since the  
14765 completion of the component evaluation, the evaluator will consider the patch in the independent  
14766 vulnerability analysis. Information related to the change provided in a public report of the  
14767 assurance continuity activities (e.g. Maintenance Report). This will be supplemented by any  
14768 updates to the guidance documentation resulting from the change and any information regarding  
14769 the change available in the public domain, e.g. vendor website.

14770 Any risks identified due to the lack of evidence to establish the full impact of any patches or  
14771 deviations in the configuration of a component from the evaluated configuration are to be  
14772 documented in the evaluator's vulnerability analysis.

### 14773 16.7.3.8 Action ACO\_VUL.3.5E

#### 14774 16.7.3.8.1 Work unit ACO\_VUL.3-9

14775 The evaluator **shall conduct** penetration testing as detailed for AVA\_VAN.3.4E.

14776 The evaluator will apply all work units necessary for the satisfaction of evaluator action  
14777 AVA\_VAN.3.4E, reporting in the ETR for the composed TOE all analysis and verdicts as dictated by  
14778 the work units.

14779 The evaluator will also apply the work units for the evaluator action AVA\_VAN.3.1E to determine  
14780 that the composed TOE provided by the developer is suitable for testing.

**Annex A**  
(informative)

**General evaluation guidance**

**A.1 Objectives**

The objective of this clause is to cover general guidance used to provide technical evidence of evaluation results. The use of such general guidance helps in achieving objectivity, repeatability and reproducibility of the work performed by the evaluator.

**A.2 Sampling**

This Subclause provides general guidance on sampling. Specific and detailed information is given in those work units under the specific evaluator action elements where sampling has to be performed.

Sampling is a defined procedure of an evaluator whereby some subset of a required set of evaluation evidence is examined and assumed to be representative for the entire set. It allows the evaluator to gain enough confidence in the correctness of particular evaluation evidence without analysing the whole evidence. The reason for sampling is to conserve resources while maintaining an adequate level of assurance. Sampling of the evidence can provide two possible outcomes:

- a) The subset reveals no errors, allowing the evaluator to have some confidence that the entire set is correct.
- b) The subset reveals errors and therefore the validity of the entire set is called into question. Even the resolution of all errors that were found may be insufficient to provide the evaluator the necessary confidence and as a result the evaluator may have to increase the size of the subset, or stop using sampling for this particular evidence.

Sampling is a technique which can be used to reach a reliable conclusion if a set of evidence is relatively homogeneous in nature, e.g. if the evidence has been produced during a well defined process.

Sampling in the cases identified in ISO/IEC 15408, and in cases specifically covered in evaluation methodology work items, is recognised as a cost-effective approach to performing evaluator actions. Sampling in other areas is permitted only in exceptional cases, where performance of a particular activity in its entirety would require effort disproportionate to the other evaluation activities, and where this would not add correspondingly to assurance. In such cases a rationale for the use of sampling in that area will need to be made. Neither the fact that the TOE is large and complex, nor that it has many security functional requirements, is sufficient justification, since evaluations of large, complex TOEs can be expected to require more effort. Rather it is intended that this exception be limited to cases such as that where the TOE development approach yields large quantities of material for a particular ISO/IEC 15408 SERIES requirement that would normally all need to be checked or examined, and where such an action would not be expected to raise assurance correspondingly.

Sampling needs to be justified taking into account the possible impact on the security objectives and threats of the TOE. The impact depends on what might be missed as a result of sampling. Consideration also needs to be given to the nature of the evidence to be sampled, and the requirement not to diminish or ignore any security functions.

14823 It should be recognised that sampling of evidence directly related to the implementation of the TOE  
 14824 (e.g. developer test results) requires a different approach to sampling, then sampling related to the  
 14825 determination of whether a process is being followed. In many cases the evaluator is required to  
 14826 determine that a process is being followed, and a sampling strategy is recommended. The approach  
 14827 for sampling a developer's test results will differ. This is because the former case is concerned with  
 14828 ensuring that a process is in place, and the latter deals with determining correct implementation of  
 14829 the TOE. Typically, larger sample sizes should be analysed in cases related to the correct  
 14830 implementation of the TOE than would be necessary to ensure that a process is in place.

14831 In certain cases it may be appropriate for the evaluator to give greater emphasis to the repetition  
 14832 of developer testing. For example if the independent tests left for the evaluator to perform would  
 14833 be only superficially different from those included in an extensive developer test set (possibly  
 14834 because the developer has performed more testing than necessary to satisfy the Coverage  
 14835 (ATE\_COV) and Depth (ATE\_DPT) criteria) then it would be appropriate for the evaluator to give  
 14836 greater focus to the repetition of developer tests. Note that this does not necessarily imply a  
 14837 requirement for a high percentage sample for repetition of developer tests; indeed, given an  
 14838 extensive developer test set, the evaluator may be able to justify a low percentage sample.

14839 Where the developer has used an automated test suite to perform functional testing, it will usually  
 14840 be easier for the evaluator to re-run the entire test suite rather than repeat only a sample of  
 14841 developer tests. However the evaluator does have an obligation to check that the automatic testing  
 14842 does not give misrepresentative results. The implication is thus that this check must be performed  
 14843 for a sample of the automatic test suite, with the principles for selecting some tests in preference to  
 14844 others and ensuring a sufficient sample size applying equally in this case.

14845 The principles in the list below should be followed whenever sampling is performed:

14846 a) Sampling should not be random, rather it should be chosen such that it is  
 14847 representative of all of the evidence. The sample size and composition must always  
 14848 be justified.

14849 b) When sampling relates to the correct implementation of the TOE, the sample should  
 14850 be representative of all aspects relevant to the areas that are sampled. In particular,  
 14851 the selection should cover a variety of components, interfaces, developer and  
 14852 operational sites (if more than one is involved) and hardware platform types (if  
 14853 more than one is involved). The sample size should be commensurate with the cost  
 14854 effectiveness of the evaluation and will depend on a number of TOE dependent  
 14855 factors (e.g. the size and complexity of the TOE, the amount of documentation).

14856 c) Also, when sampling relates to specifically gaining evidence that the developer testing  
 14857 is repeatable and reproducible the sample used must be sufficient to represent all  
 14858 distinct aspects of developer testing, such as different test regimes. The sample used  
 14859 must be sufficient to detect any systematic problem in the developer's functional  
 14860 testing process. The evaluator contribution resulting from the combination of  
 14861 repeating developer tests and performing independent tests must be sufficient to  
 14862 address the major points of concern for the TOE.

14863 d) Where sampling relates to gaining evidence that a process (e.g. visitor control or  
 14864 design review) the evaluator should sample sufficient information to gain reasonable  
 14865 confidence that the procedure is being followed.

14866 e) The sponsor and developer should not be informed in advance of the exact  
 14867 composition of the sample, subject to ensuring timely delivery of the sample and  
 14868 supporting deliverable, e.g. test harnesses and equipment to the evaluator in  
 14869 accordance with the evaluation schedule.

## ISO/IEC 18045:2008(E)

14870 f) The choice of the sample should be free from bias to the degree possible (one should  
14871 not always choose the first or last item). Ideally the sample selection should be done  
14872 by someone other than the evaluator.

14873 Errors found in the sample can be categorised as being either systematic or sporadic. If the error is  
14874 systematic, the problem should be corrected and a complete new sample taken. If properly  
14875 explained, sporadic errors might be solved without the need for a new sample, although the  
14876 explanation should be confirmed. The evaluator should use judgement in determining whether to  
14877 increase the sample size or use a different sample.

### 14878 A.3 Dependencies

#### 14879 A.3.1 General

14880 In general it is possible to perform the required evaluation activities, sub-activities, and actions in  
14881 any order or in parallel. However, there are different kinds of dependencies which have to be  
14882 considered by the evaluator. This Subclause provides general guidance on dependencies between  
14883 different activities, sub-activities, and actions.

#### 14884 A.3.2 Dependencies between activities

14885 For some cases the different assurance classes may recommend or even require a sequence for the  
14886 related activities. A specific instance is the ST activity. The ST evaluation activity is started prior to  
14887 any TOE evaluation activities since the ST provides the basis and context to perform them.  
14888 However, a final verdict on the ST evaluation may not be possible until the TOE evaluation is  
14889 complete, since changes to the ST may result from activity findings during the TOE evaluation.

#### 14890 A.3.3 Dependencies between sub-activities

14891 Dependencies identified between components in ISO/IEC 15408-3 have to be considered by the  
14892 evaluator. Most dependencies are one way, e.g. Evaluation of sub-activity (AVA\_VAN.1) claims a  
14893 dependency on Evaluation of sub-activity (ADV\_FSP.1) and Evaluation of sub-activity (AGD\_OPE.1).  
14894 There are also instances of mutual dependencies, where both components depend on each other.  
14895 An example of this is Evaluation of sub-activity (ATE\_FUN.1) and Evaluation of sub-activity  
14896 (ATE\_COV.1).

14897 A sub-activity can be assigned a pass verdict normally only if all those sub-activities are  
14898 successfully completed on which it has a one-way dependency. For example, a pass verdict on  
14899 Evaluation of sub-activity (AVA\_VAN.1) can normally only be assigned if the sub-activities related  
14900 to Evaluation of sub-activity (ADV\_FSP.1) and Evaluation of sub-activity (AGD\_OPE.1) are assigned  
14901 a pass verdict too. In the case of mutual dependency the ordering of these components is down to  
14902 the evaluator deciding which sub-activity to perform first. Note this indicates that pass verdicts can  
14903 normally only be assigned once both sub-activities have been successful.

14904 So when determining whether a sub-activity will impact another sub-activity, the evaluator should  
14905 consider whether this activity depends on potential evaluation results from any dependent sub-  
14906 activities. Indeed, it may be the case that a dependent sub-activity will impact this sub-activity,  
14907 requiring previously completed evaluator actions to be performed again.

14908 A significant dependency effect occurs in the case of evaluator-detected flaws. If a flaw is identified  
14909 as a result of conducting one sub-activity, the assignment of a pass verdict to a dependent sub-  
14910 activity may not be possible until all flaws related to the sub-activity upon which it depends are  
14911 resolved.

14912 **A.3.4 Dependencies between actions**

14913 It may be the case, that results which are generated by the evaluator during one action are used for  
 14914 performing another action. For example, actions for completeness and consistency cannot be  
 14915 completed until the checks for content and presentation have been completed. This means for  
 14916 example that the evaluator is recommended to evaluate the PP/ST rationale after evaluating the  
 14917 constituent parts of the PP/ST.

14918 **A.4 Site Visits**14919 **A.4.1 Introduction**

14920 The assurance class ALC includes requirements for

- 14921 a) the application of configuration management, ensuring that the integrity of the TOE is  
 14922 preserved;
- 14923 b) measures, procedures, and standards concerned with secure delivery of the TOE,  
 14924 ensuring that the security protection offered by the TOE is not compromised during  
 14925 the transfer to the user,
- 14926 c) security measures, used to protect the development environment.

14927 A development site visit is a useful means whereby the evaluator determines whether procedures  
 14928 are being followed in a manner consistent with that described in the documentation.

14929 Reasons for visiting sites include:

- 14930 a) to observe the use of the CM system as described in the CM plan;
- 14931 b) to observe the practical application of delivery procedures as described in the delivery  
 14932 documentation;
- 14933 c) to observe the application of security measures during development and maintenance of  
 14934 the TOE as described in the development security documentation.

14935 Specific and detailed information is given in work units for those activities where site visits are  
 14936 performed:

- 14937 a) CM capabilities (ALC\_CMC).n with  $n \geq 3$  (especially work unit ALC\_CMC.3-10 =  
 14938 ALC\_CMC.4-13 = ALC\_CMC.5-19);
- 14939 b) Delivery (ALC\_DEL) (especially work unit ALC\_DEL.1-2);
- 14940 c) Development security (ALC\_DVS) (especially work unit ALC\_DVS.1-3 = ALC\_DVS.2-4).

14941 **A.4.2 General Approach**

14942 During an evaluation, it is often necessary that the evaluator will meet the developer more than  
 14943 once and it is a question of good planning to combine the site visit with another meeting to reduce  
 14944 costs. For example, one might combine the site visits for configuration management, for the  
 14945 developer's security and for delivery. It may also be necessary to perform more than one site visit  
 14946 to the same site to allow the checking of all development phases. It should be considered that

## ISO/IEC 18045:2008(E)

14947 development could occur at multiple facilities within a single building, multiple buildings at the  
14948 same site, or at multiple sites.

14949 The first site visit should be scheduled early during the evaluation. In the case of an evaluation  
14950 which starts during the development phase of the TOE, this will allow corrective actions to be  
14951 taken, if necessary. In the case of an evaluation which starts after the development of the TOE, an  
14952 early site visit could allow corrective measures to be put in place if serious deficiencies in the  
14953 applied procedures emerge. This avoids unnecessary evaluation effort.

14954 Interviews are also a useful means of determining whether the written procedures reflect what is  
14955 done. In conducting such interviews, the evaluator aims to gain a deeper understanding of the  
14956 analysed procedures at the development site, how they are used in practise and whether they are  
14957 being applied as described in the provided evaluation evidence. Such interviews complement but  
14958 do not replace the examination of evaluation evidence.

14959 As a first step preparing the site visits the evaluators should perform the evaluator work units  
14960 concerning the assurance class ALC excluding the aspects describing the results of the site visit.  
14961 Based on the information provided by the relevant developer documentation and the remaining  
14962 open questions which were not answered by the documentation the evaluators compile a check list  
14963 of the questions which are to be resolved by the site visits.

14964 The first version of the evaluation report concerning the ALC class and the check list serves as  
14965 input for the consultation with the evaluation authority concerning the site visits.

14966 The check list serves as a guide line for the site visits, which questions are to be answered by  
14967 inspection of the relevant measures, their application and results, and by interviews. Where  
14968 appropriate, sampling is used for gaining the required level of confidence (see Subclause A.2).

14969 The results of the site visits are recorded and serve as input for the final version of the evaluation  
14970 report concerning the assurance class ALC.

14971 Other approaches to gain confidence should be considered that provide an equivalent level of  
14972 assurance (e.g. to analyse evaluation evidence). Any decision not to make a visit should be  
14973 determined in consultation with the evaluation authority. Appropriate security criteria and a  
14974 methodology should be based on other standards of the Information Security Management Systems  
14975 area.

### 14976 **A.4.3 Orientation Guide for the Preparation of the Check List**

14977 In the following some keywords are provided, which topics should be checked during an audit.

#### 14978 **A.4.3.1 Aspects of configuration management**

14979 Basic

- 14980 • Items of the configuration list, including TOE, source code, run time libraries, design  
14981 documentation, development tools (ALC\_CMC.3-8).
- 14982 • Tracking of design documentation, source code, user guidance to different versions of the  
14983 TOE.
- 14984 • Integration of the configuration system in the design and development process, test  
14985 planning, test analysis and quality management procedures.
- 14986 Test analysis
- 14987 • Tracking of test plans and results to specific configurations and versions of the TOE.



- 14988 • Access control to development systems
- 14989 • Policies for access control and logging.
- 14990 • Policies for project specific assignment and changing of access rights.
- 14991 Clearance
- 14992 • Policies for clearance of the TOE and user guidance to the customer.
- 14993 • Policies for testing and approving of components and the TOE before deployment.
- 14994 **A.4.3.2 Aspects of development security**
- 14995 Infrastructure
- 14996 • Security measures for physical access control to the development site and rationale for  
14997 the effectiveness of these measures.
- 14998 Organisational measures
- 14999 • Organisational structure of the company in respect of the security of the development  
15000 environment.
- 15001 • Organisational separation between development, production, testing and quality  
15002 assurance.
- 15003 Personal measures
- 15004 • Measures for education of the personnel in respect of development security.
- 15005 • Measures and legal agreements of non-disclosure of internal information.
- 15006 Access control
- 15007 • Assignment of secured objects (for instance TOE, source code, run time libraries, design  
15008 documentation, development tools, user guidance) and security policies.
- 15009 • Policies and responsibilities concerning the access control and the handling of  
15010 authentication information.
- 15011 • Policies for logging of any kind access to the development site and protection of the  
15012 logging data.
- 15013 Input, processing and output of data
- 15014 • Security measures for protection of output and output devices (printer, plotter and  
15015 displays).
- 15016 • Securing of local networks and communication connections.
- 15017 • Storage, transfer and destruction of documents and data media.
- 15018 • Policies for handling of documents and data media.

## ISO/IEC 18045:2008(E)

- 15019 • Policies and responsibilities for destruction of sorted out documents and logging of these  
15020 events.
- 15021 Data protection
- 15022 • Policies and responsibilities for data and information protection (e.g. for performing  
15023 backups).
- 15024 Contingency plan
- 15025 • Practises in case of emergency and responsibilities.
- 15026 • Documentation of the contingency measures concerning access control.
- 15027 • Information of the personnel about applicable practises in extreme cases. protection (e.g.  
15028 for performing backups).
- 15029 **A.4.4 Example of a checklist**
- 15030 The examples of checklists for site visits consist in tables for the preparation of an audit and for the  
15031 presentation of the results of an audit.
- 15032 The checklist structure given in the following is preliminary. Dependent on the concrete contents  
15033 of the new guideline, changes might become necessary.
- 15034 The checklist is divided into three subclauses according to the subjects indicated in the  
15035 introduction (Subclause A.4.1).
- 15036 a) Configuration management system.
- 15037 b) Delivery procedures.
- 15038 c) Security measures during development.
- 15039 These subclauses correspond to the actual ISO/IEC 15408-3 class ALC, especially the families CM  
15040 capabilities (ALC\_CMC).n with  $n \geq 3$ , Delivery (ALC\_DEL) and Development security (ALC\_DVS).
- 15041 The subclauses are subdivided further into rows corresponding to the relevant work units of this  
15042 document.
- 15043 The columns of the checklist contain in turn
- 15044 • a consecutive number,
- 15045 • the referenced work unit,
- 15046 • the references to the corresponding developer documentation,
- 15047 • the explicit reproduction of the developer measures,
- 15048 • special remarks and questions to be clarified on the visit (beyond the standard evaluator  
15049 task to verify the application of the indicated measures),
- 15050 • the result of the examinations during the visit.

15051 If it is decided to have separate checklists for preparation and reporting of the audit, the result  
 15052 column is omitted in the preparation list and the remarks and questions column is omitted in the  
 15053 reporting list. The remaining columns should be identical in both lists.

15054

**Table A.1 Example of a checklist at EAL 4 (extract)**

| A. Examination of the CM system (ALC_CMC.4 and ALC_CMS.4)                                                     |                               |                                                               |                                                                                                                                                                                         |                                                                                             |                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------|-------------------------------|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| No.                                                                                                           | Work Unit                     | Developer Documentation                                       | Measures                                                                                                                                                                                | Questions and Remarks                                                                       | Result                                                                                                           |
| A.1                                                                                                           | ALC_CMC.4-11,<br>ALC_CMC.4-12 | "Configuration Management System", ch. ...                    | The system automatically managing the source code files is capable of administering user profiles and graded access rights, and of checking identification and authentication of users. | Does reading or updating of a source code file require a user authentication?               | If a user has not the right to access a confidential document, it is not even displayed to him in the file list. |
| B. Examination of the Delivery Procedures (ALC_DEL.1)                                                         |                               |                                                               |                                                                                                                                                                                         |                                                                                             |                                                                                                                  |
| No.                                                                                                           | Work Unit                     | Developer Documentation                                       | Measures                                                                                                                                                                                | Questions and Remarks                                                                       | Result                                                                                                           |
| B.1                                                                                                           | ALC_DEL.1-1,<br>ALC_DEL.1-2   | "Delivery of the TOE", ch. ...                                | The software is transmitted PGP-signed and encrypted to the customer.                                                                                                                   | ---                                                                                         | The evaluators have checked the process and found it as described, additionally a checksum is transmitted.       |
| C. Examination of the organisational and infrastructural developer security (ALC_DVS.1, ALC_LCD.1, ALC_TAT.1) |                               |                                                               |                                                                                                                                                                                         |                                                                                             |                                                                                                                  |
| No.                                                                                                           | Work Unit                     | Developer Documentation                                       | Measures                                                                                                                                                                                | Questions and Remarks                                                                       | Result                                                                                                           |
| C.1                                                                                                           | ALC_DVS.1-1,<br>ALC_DVS.1-2   | "Security of the development environment", ch. ... (Premises) | The premises are protected by security fencing.                                                                                                                                         | Is the fencing sufficiently strong and high to prevent an easy intrusion into the premises? | The evaluators considered the fencing to be sufficiently strong and high.                                        |
| C.2                                                                                                           | ALC_DVS.1-1,<br>ALC_DVS.1-2   | "Security of the development environment", ch. ... (Building) | The building has the following access possibilities:<br>The main                                                                                                                        | Is the listing of the access possibilities complete?                                        | Beyond the indicated access possibilities, there is an emergency                                                 |

| C. Examination of the organisational and infrastructural developer security (ALC_DVS.1, ALC_LCD.1, ALC_TAT.1) |           |                         |                                                                                                                                                                         |                       |                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------|-----------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------|
| No.                                                                                                           | Work Unit | Developer Documentation | Measures                                                                                                                                                                | Questions and Remarks | Result                                                                                                              |
|                                                                                                               |           |                         | entrance which is surveyed by the reception and is closed if the reception is not manned. And an access in the goods reception which is secured by two roller shutters. |                       | exit that cannot be opened from the outside. The roller shutters mentioned before can be operated only from inside. |

#### 15057 A.5 Scheme Responsibilities

15058 This document describes the minimum technical work that evaluations conducted under oversight  
 15059 (scheme) bodies must perform. However, it also recognises (both explicitly and implicitly) that  
 15060 there are activities or methods upon which mutual recognition of evaluation results do not rely.  
 15061 For the purposes of thoroughness and clarity, and to better delineate where this document ends  
 15062 and an individual scheme's methodology begins, the following matters are left up to the discretion  
 15063 of the schemes. Schemes may choose to provide the following, although they may choose to leave  
 15064 some unspecified. (Every effort has been made to ensure this list is complete; evaluators  
 15065 encountering a subject neither listed here nor addressed in this document should consult with  
 15066 their evaluation schemes to determine under whose auspices the subject falls.)

15067 The matters that schemes may choose to specify include:

- 15068 a) what is required in ensuring that an evaluation was done sufficiently - every scheme  
 15069 has a means of verifying the technical competence, understanding of work and the  
 15070 work of its evaluators, whether by requiring the evaluators to present their findings  
 15071 to the oversight body, by requiring the oversight body to redo the evaluator's work,  
 15072 or by some other means that assures the scheme that all evaluation bodies are  
 15073 adequate and comparable;
- 15074 b) process for disposing of evaluation evidence upon completion of an evaluation;
- 15075 c) any requirements for confidentiality (on the part of the evaluator and the non-  
 15076 disclosure of information obtained during evaluation);
- 15077 d) the course of action to be taken if a problem is encountered during the evaluation  
 15078 (whether the evaluation continues once the problem is remedied, or the evaluation  
 15079 ends immediately, and the remedied product must be re-submitted for evaluation);
- 15080 e) any specific (natural) language in which documentation must be provided;

- 15081 f) any recorded evidence that must be submitted in the ETR - this document specifies  
15082 the minimum to be reported in an ETR; however, individual schemes may require  
15083 additional information to be included;
- 15084 g) any additional reports (other than the ETR) required from the evaluators -for  
15085 example, testing reports;
- 15086 h) any specific ORs that may be required by the scheme, including the structure,  
15087 recipients, etc. of any such ORs;
- 15088 i) any specific content structure of any written report as a result from an ST evaluation -  
15089 a scheme may have a specific format for all of its reports detailing results of an  
15090 evaluation, be it the evaluation of a TOE or of an ST;
- 15091 j) any additional PP/ST identification information required;
- 15092 k) any activities to determine the suitability of explicitly-stated requirements in an ST;
- 15093 l) any requirements for provision of evaluator evidence to support re-evaluation and  
15094 re-use of evidence;
- 15095 m) any specific handling of scheme identifiers, logos, trademarks, etc.;
- 15096 n) any specific guidance in dealing with cryptography;
- 15097 o) handling and application of scheme, national and international interpretations;
- 15098 p) a list or characterisations of suitable alternative approaches to testing where testing  
15099 is infeasible;
- 15100 q) the mechanism by which an evaluation authority can determine what steps an  
15101 evaluator took while testing;
- 15102 r) preferred test approach (if any): at internal interface or at external interface;
- 15103 s) a list or characterisation of acceptable means of conducting the evaluator's  
15104 vulnerability analysis (e.g. flaw hypothesis methodology);
- 15105 t) information regarding any vulnerabilities and weaknesses to be considered.

**Annex B**  
(informative)

**Vulnerability Assessment (AVA)**

15106  
15107  
15108  
15109

15110 This annex provides an explanation of the AVA\_VAN criteria and examples of their application. This  
15111 annex does not define the AVA criteria; this definition can be found in ISO/IEC 15408-3 Subclause  
15112 Class AVA: Vulnerability assessment.

15113 This annex consists of 2 major parts:

15114 a) *Guidance for completing an independent vulnerability analysis.* This is summarised in  
15115 subclause B.1.1, and described in more detail in subclause B.1.2 . These subclauses  
15116 describe how an evaluator should approach the construction of an independent  
15117 Vulnerability Analysis.

15118 b) How to characterise and use assumed Attack Potential of an attacker. This is  
15119 described in subclauses B.1.5 to B.3. These subclauses provide an example of how an  
15120 attack potential can be characterised and should be used, and provide examples.

15121 **B.1.1 What is Vulnerability Analysis**

15122 The purpose of the vulnerability assessment activity is to determine the existence and  
15123 exploitability of flaws or weaknesses in the TOE in the operational environment. This  
15124 determination is based upon analysis performed by the evaluator, and is supported by evaluator  
15125 testing.

15126 At the lowest levels of Vulnerability analysis (AVA\_VAN) the evaluator simply performs a search of  
15127 publicly available information to identify any known weaknesses in the TOE, while at the higher  
15128 levels the evaluator performs a structured analysis of the TOE evaluation evidence.

15129 There are three main factors in performing a vulnerability analysis, namely:

15130 a) the identification of potential vulnerabilities;

15131 b) assessment to determine whether the identified potential vulnerabilities could allow  
15132 an attacker with the relevant attack potential to violate the SFRs.

15133 c) penetration testing to determine whether the identified potential vulnerabilities are  
15134 exploitable in the operational environment of the TOE.

15135 The identification of vulnerabilities can be further decomposed into the evidence to be searched  
15136 and how hard to search that evidence to identify potential vulnerabilities. In a similar manner, the  
15137 penetration testing can be further decomposed into analysis of the potential vulnerability to  
15138 identify attack methods and the demonstration of the attack methods.

15139 These main factors are iterative in nature, i.e. penetration testing of potential vulnerabilities may  
15140 lead to the identification of further potential vulnerabilities. Hence, these are performed as a single  
15141 vulnerability analysis activity.

## 15142 **B.1.2 Evaluator construction of a Vulnerability Analysis**

15143 The evaluator vulnerability analysis is to determine that the TOE is resistant to penetration attacks  
 15144 performed by an attacker possessing a Basic (for AVA\_VAN.1 and AVA\_VAN.2), Enhanced-Basic (for  
 15145 AVA\_VAN.3), Moderate (for AVA\_VAN.4) or High (for AVA\_VAN.5) attack potential. The evaluator  
 15146 first assesses the exploitability of all identified potential vulnerabilities. This is accomplished by  
 15147 conducting penetration testing. The evaluator should assume the role of an attacker with a Basic  
 15148 (for AVA\_VAN.1 and AVA\_VAN.2), Enhanced-Basic (for AVA\_VAN.3), Moderate (for AVA\_VAN.4) or  
 15149 High (for AVA\_VAN.5) attack potential when attempting to penetrate the TOE.

15150 The evaluator considers potential vulnerabilities encountered by the evaluator during the conduct  
 15151 of other evaluation activities. The evaluator penetration testing determining TOE resistance to  
 15152 these potential vulnerabilities should be performed assuming the role of an attacker with a Basic  
 15153 (for AVA\_VAN.1 and AVA\_VAN.2), Enhanced-Basic (for AVA\_VAN.3), Moderate (for AVA\_VAN.4) or  
 15154 High (for AVA\_VAN.5) attack potential.

15155 However, vulnerability analysis should not be performed as an isolated activity. It is closely linked  
 15156 with ADV and AGD. The evaluator performs these other evaluation activities with a focus on  
 15157 identifying potential vulnerabilities or "areas of concern". Therefore, evaluator familiarity with the  
 15158 generic vulnerability guidance (provided in Subclause B.1.3) is required.

## 15159 **B.1.3 Generic vulnerability guidance**

15160 The following five categories provide discussion of generic vulnerabilities.

### 15161 **B.1.3.1 Bypassing**

15162 Bypassing includes any means by which an attacker could avoid security enforcement, by:

- 15163 a) exploiting the capabilities of interfaces to the TOE, or of utilities which can interact  
 15164 with the TOE;
- 15165 b) inheriting privileges or other capabilities that should otherwise be denied;
- 15166 c) (where confidentiality is a concern) reading sensitive data stored or copied to  
 15167 inadequately protected areas.

15168 Each of the following should be considered (where relevant) in the evaluator's independent  
 15169 vulnerability analysis.

- 15170 a) Attacks based on exploiting the capabilities of interfaces or utilities generally take  
 15171 advantage of the absence of the required security enforcement on those interfaces.  
 15172 For example, gaining access to functionality that is implemented at a lower level than  
 15173 that at which access control is enforced. Relevant items include:
  - 15174 1) changing the predefined sequence of invocation of TSFI;
  - 15175 2) invoking an additional TSFI;
  - 15176 3) using a component in an unexpected context or for an unexpected purpose;
  - 15177 4) using implementation detail introduced in less abstract representations;

- 15178 5) using the delay between time of access check and time of use.
- 15179 b) Changing the predefined sequence of invocation of components should be considered  
 15180 where there is an expected order in which interfaces to the TOE (e.g. user  
 15181 commands) are called to invoke a TSFI (e.g. opening a file for access and then  
 15182 reading data from it). If a TSFI is invoked through one of the TOE interfaces (e.g. an  
 15183 access control check), the evaluator should consider whether it is possible to bypass  
 15184 the control by performing the call at a later point in the sequence or by missing it out  
 15185 altogether.
- 15186 c) Executing an additional component (in the predefined sequence) is a similar form of  
 15187 attack to the one described above, but involves the calling of some other TOE  
 15188 interface at some point in the sequence. It can also involve attacks based on  
 15189 interception of sensitive data passed over a network by use of network traffic  
 15190 analysers (the additional component here being the network traffic analyser).
- 15191 d) Using a component in an unexpected context or for an unexpected purpose includes  
 15192 using an unrelated TOE interface to bypass the TSF by using it to achieve a purpose  
 15193 that it was not designed or intended to achieve. Covert channels are an example of  
 15194 this type of attack (see B.1.3.4 for further discussion of covert channels). The use of  
 15195 undocumented interfaces, which may be insecure, also falls into this category. Such  
 15196 interfaces may include undocumented support and help facilities.
- 15197 e) Using implementation detail introduced in lower representations may allow an  
 15198 attacker to take advantage of additional functions, resources or attributes that are  
 15199 introduced to the TOE as a consequence of the refinement process. Additional  
 15200 functionality may include test harness code contained in software modules and back-  
 15201 doors introduced during the implementation process.
- 15202 f) Using the delay between time of check and time of use includes scenarios where an  
 15203 access control check is made and access granted, and an attacker is subsequently  
 15204 able to create conditions in which, had they applied at the time the access check was  
 15205 made, would have caused the check to fail. An example would be a user creating a  
 15206 background process to read and send highly sensitive data to the user's terminal,  
 15207 and then logging out and logging back in again at a lower sensitivity level. If the  
 15208 background process is not terminated when the user logs off, the MAC checks would  
 15209 have been effectively bypassed.
- 15210 g) Attacks based on inheriting privileges are generally based on illicitly acquiring the  
 15211 privileges or capabilities of some privileged component, usually by exiting from it in  
 15212 an uncontrolled or unexpected manner. Relevant items include:
- 15213 1) executing data not intended to be executable, or making it executable;
- 15214 2) generating unexpected input for a component;
- 15215 3) invalidating assumptions and properties on which lower-level components rely.
- 15216 h) Executing data not intended to be executable, or making it executable includes attacks  
 15217 involving viruses (e.g. putting executable code or commands in a file which are  
 15218 automatically executed when the file is edited or accessed, thus inheriting any  
 15219 privileges the owner of the file has).



- 15220 i) Generating unexpected input for a component can have unexpected effects which an  
 15221 attacker could take advantage of. For example, if the TSF could be bypassed if a user  
 15222 gains access to the underlying operating system, it may be possible to gain such  
 15223 access following the login sequence by exploring the effect of hitting various control  
 15224 or escape sequences whilst a password is being authenticated.
- 15225 j) Invalidating assumptions and properties on which lower level components rely  
 15226 includes attacks based on breaking out of the constraints of an application to gain  
 15227 access to an underlying operating system in order to bypass the TSF of an  
 15228 application. In this case the assumption being invalidated is that it is not possible for  
 15229 a user of the application to gain such access. A similar attack can be envisaged  
 15230 against an application on an underlying database management system: again the TSF  
 15231 could be bypassed if an attacker can break out of the constraints of the application.
- 15232 k) Attacks based on reading sensitive data stored in inadequately protected areas  
 15233 (applicable where confidentiality is a concern) include the following issues which  
 15234 should be considered as possible means of gaining access to sensitive data:
- 15235 1) disk scavenging;
- 15236 2) access to unprotected memory;
- 15237 3) exploiting access to shared writable files or other shared resources (e.g. swap  
 15238 files);
- 15239 4) Activating error recovery to determine what access users can obtain. For example,  
 15240 after a crash an automatic file recovery system may employ a lost and found  
 15241 directory for headerless files, which are on disk without labels. If the TOE  
 15242 implements mandatory access controls, it is important to investigate at what  
 15243 security level this directory is kept (e.g. at system high), and who has access to  
 15244 this directory.
- 15245 There are a number of different methods through which an evaluator may identify a back-door,  
 15246 including two main techniques. Firstly, by the evaluator inadvertently identifying during testing an  
 15247 interface that can be misused. Secondly, through testing each external interface of the TSF in a  
 15248 debugging mode to identify any modules that are not called as a part of testing the documented  
 15249 interfaces and then inspecting the code that is not called to consider whether it is a back-door.
- 15250 For a software TOE where Evaluation of sub-activity (ADV\_IMP.2) and ALC\_TAT.2 or higher  
 15251 components are included in the assurance package, the evaluator may consider during their  
 15252 analysis of the tools the libraries and packages that are linked by the compiler at compilation stage  
 15253 to determine that back-doors are not introduced at this stage.
- 15254 **B.1.3.2 Tampering**
- 15255 Tampering includes any attack based on an attacker attempting to influence the behaviour of the  
 15256 TSF (i.e. corruption or de-activation), for example by:
- 15257 a) accessing data on whose confidentiality or integrity the TSF relies;
- 15258 b) forcing the TOE to cope with unusual or unexpected circumstances;
- 15259 c) disabling or delaying security enforcement;

## ISO/IEC 18045:2008(E)

- 15260 d) physically modifying the TOE.
- 15261 Each of the following should be considered (where relevant) in the evaluator's independent  
15262 vulnerability analysis.
- 15263 a) Attacks based on accessing data, whose confidentiality or integrity are protected,  
15264 include:
- 15265 1) reading, writing or modifying internal data directly or indirectly;
- 15266 2) using a component in an unexpected context or for an unexpected purpose;
- 15267 3) using interfaces between components that are not visible at a higher level of  
15268 abstraction.
- 15269 b) Reading, writing or modifying internal data directly or indirectly includes the  
15270 following types of attack which should be considered:
- 15271 1) reading "secrets" stored internally, such as user passwords;
- 15272 2) spoofing internal data that security enforcing mechanisms rely upon;
- 15273 3) modifying environment variables (e.g. logical names), or data in configuration  
15274 files or temporary files.
- 15275 c) It may be possible to deceive a trusted process into modifying a protected file that it  
15276 wouldn't normally access.
- 15277 d) The evaluator should also consider the following "dangerous features":
- 15278 1) source code resident on the TOE along with a compiler (for instance, it may be  
15279 possible to modify the login source code);
- 15280 2) an interactive debugger and patch facility (for instance, it may be possible to  
15281 modify the executable image);
- 15282 3) the possibility of making changes at device controller level, where file protection  
15283 does not exist;
- 15284 4) diagnostic code which exists in the source code and that may be optionally  
15285 included;
- 15286 5) developer's tools left in the TOE.
- 15287 e) Using a component in an unexpected context or for an unexpected purpose includes  
15288 (for example), where the TOE is an application built upon an operating system, users  
15289 exploiting knowledge of a word processor package or other editor to modify their  
15290 own command file (e.g. to acquire greater privileges).

- 15291 f) Using interfaces between components which are not visible at a higher level of  
15292 abstraction includes attacks exploiting shared access to resources, where  
15293 modification of a resource by one component can influence the behaviour of another  
15294 (trusted) component, e.g. at source code level, through the use of global data or  
15295 indirect mechanisms such as shared memory or semaphores.
- 15296 g) Attacks based on forcing the TOE to cope with unusual or unexpected circumstances  
15297 should always be considered. Relevant items include:
- 15298 1) generating unexpected input for a component;
- 15299 2) invalidating assumptions and properties on which lower-level components rely.
- 15300 h) Generating unexpected input for a component includes investigating the behaviour of  
15301 the TOE when:
- 15302 1) command input buffers overflow (possibly "crashing the stack" or overwriting  
15303 other storage, which an attacker may be able to take advantage of, or forcing a  
15304 crash dump that may contain sensitive information such as clear-text  
15305 passwords);
- 15306 2) invalid commands or parameters are entered (including supplying a read-only  
15307 parameter to an interface which expects to return data via that parameter and  
15308 supplying improperly formatted input that should fail parsing such as SQL-  
15309 injection, format strings);
- 15310 3) an end-of-file marker (e.g. CTRL-Z or CTRL-D) or null character is inserted in an  
15311 audit trail.
- 15312 i) Invalidating assumptions and properties on which lower-level components rely  
15313 includes attacks taking advantage of errors in the source code where the code  
15314 assumes (explicitly or implicitly) that security relevant data is in a particular format  
15315 or has a particular range of values. In these cases the evaluator should determine  
15316 whether they can invalidate such assumptions by causing the data to be in a different  
15317 format or to have different values, and if so whether this could confer advantage to  
15318 an attacker.
- 15319 j) The correct behaviour of the TSF may be dependent on assumptions that are  
15320 invalidated under extreme circumstances where resource limits are reached or  
15321 parameters reach their maximum value. The evaluator should consider (where  
15322 practical) the behaviour of the TOE when these limits are reached, for example:
- 15323 1) changing dates (e.g. examining how the TOE behaves when a critical date  
15324 threshold is passed);
- 15325 2) filling disks;
- 15326 3) exceeding the maximum number of users;
- 15327 4) filling the audit log;

## ISO/IEC 18045:2008(E)

- 15328 5) saturating security alarm queues at a console;
- 15329 6) overloading various parts of a multi-user TOE which relies heavily upon  
15330 communications components;
- 15331 7) swamping a network, or individual hosts, with traffic;
- 15332 8) filling buffers or fields.
- 15333 k) Attacks based on disabling or delaying security enforcement include the following  
15334 items:
- 15335 1) using interrupts or scheduling functions to disrupt sequencing;
- 15336 2) disrupting concurrence;
- 15337 3) using interfaces between components which are not visible at a higher level of  
15338 abstraction.
- 15339 l) Using interrupts or scheduling functions to disrupt sequencing includes investigating  
15340 the behaviour of the TOE when:
- 15341 1) a command is interrupted (with CTRL-C, CTRL-Y, etc.);
- 15342 2) a second interrupt is issued before the first is acknowledged.
- 15343 m) The effects of terminating security critical processes (e.g. an audit daemon) should be  
15344 explored. Similarly, it may be possible to delay the logging of audit records or the  
15345 issuing or receipt of alarms such that it is of no use to an administrator (since the  
15346 attack may already have succeeded).
- 15347 n) Disrupting concurrence includes investigating the behaviour of the TOE when two or  
15348 more subjects attempt simultaneous access. It may be that the TOE can cope with the  
15349 interlocking required when two subjects attempt simultaneous access, but that the  
15350 behaviour becomes less well defined in the presence of further subjects. For example,  
15351 a critical security process could be put into a resource-wait state if two other  
15352 processes are accessing a resource which it requires.
- 15353 o) Using interfaces between components which are not visible at a higher level of  
15354 abstraction may provide a means of delaying a time-critical trusted process.
- 15355 p) Physical attacks can be categorised into physical probing, physical manipulation,  
15356 physical modification, and substitution.
- 15357 1) Physical probing by penetrating the TOE targeting internals of the TOE, e.g.  
15358 reading at internal communication interfaces, lines or memories.
- 15359 2) Physical manipulation can be with the TOE internals aiming at internal  
15360 modifications of the TOE (e.g. by using optical fault induction as an interaction

15361 process), at the external interfaces of the TOE (e.g. by power or clock glitches)  
15362 and at the TOE environment (e.g. by modifying temperature).

15363 3) Physical modification of TOE internal security enforcing attributes to inherit  
15364 privileges or other capabilities that should be denied in regular operation. Such  
15365 modifications can be caused, e.g., by optical fault induction. Attacks based on  
15366 physical modification may also yield a modification of the TSF itself, e.g. by  
15367 causing faults at TOE internal program data transfers before execution. Note, that  
15368 such kind of bypassing by modifying the TSF itself can jeopardise every TSF  
15369 unless there are other measures (possibly environmental measures) that prevent  
15370 an attacker from gaining physical access to the TOE.

15371 4) Physical substitution to replace the TOE with another IT entity, during delivery or  
15372 operation of the TOE. Substitution during delivery of the TOE from the  
15373 development environment to the user should be prevented through application  
15374 of secure delivery procedures (such as those considered under Development  
15375 security (ALC\_DVS)). Substitution of the TOE during operation may be considered  
15376 through a combination of user guidance and the operational environment, such  
15377 that the user is able to be confident that they are interacting with the TOE.

#### 15378 B.1.3.3 Direct attacks

15379 Direct attack includes the identification of any penetration tests necessary to test the strength of  
15380 permutational or probabilistic mechanism and other mechanisms to ensure they withstand direct  
15381 attack.

15382 For example, it may be a flawed assumption that a particular implementation of a pseudo-random  
15383 number generator will possess the required entropy necessary to seed the security mechanism.

15384 Where a probabilistic or permutational mechanism relies on selection of security attribute value  
15385 (e.g. selection of password length) or entry of data by a human user (e.g. choice of password), the  
15386 assumptions made should reflect the worst case.

15387 Probabilistic or permutational mechanisms should be identified during examination of evaluation  
15388 evidence required as input to this sub-activity (security target, functional specification, TOE design  
15389 and implementation representation subset) and any other TOE (e.g. guidance) documentation may  
15390 identify additional probabilistic or permutational mechanisms.

15391 Where the design evidence or guidance includes assertions or assumptions (e.g. about how many  
15392 authentication attempts are possible per minute), the evaluator should independently confirm that  
15393 these are correct. This may be achieved through testing or through independent analysis.

15394 Direct attacks reliant upon a weakness in a cryptographic algorithm should not be considered  
15395 under Vulnerability analysis (AVA\_VAN), as this is outside the scope of ISO/IEC 15408-3.  
15396 Correctness of the implementation of the cryptographic algorithm is considered during the ADV  
15397 and ATE activities.

#### 15398 B.1.3.4 Monitoring

15399 Information is an abstract view on relation between the properties of entities, i.e. a signal contains  
15400 information for a system, if the TOE is able to react to this signal. The TOE resources processes and  
15401 stores information represented by user data. Therefore:

15402 a) information may flow with the user data between subjects by internal TOE transfer or  
15403 export from the TOE;

## ISO/IEC 18045:2008(E)

- 15404        b) information may be generated and passed to other user data;
- 15405        c) information may be gained through monitoring the operations on data representing  
15406        the information.
- 15407        The information represented by user data may be characterised by security attributes like  
15408        “classification level” having values, for example unclassified, confidential, secret, top secret, to  
15409        control operations to the data. This information and therefore the security attributes may be  
15410        changed by operations e.g. FDP\_ACC.2 may describe decrease of the level by “sanitisation” or  
15411        increase of level by combination of data. This is one aspects of an information flow analysis focused  
15412        on controlled operations of controlled subjects on controlled objects.
- 15413        The other aspect is the analysis of *illicit information flow*. This aspect is more general than the  
15414        direct access to objects containing user data addressed by the FDP\_ACC family. An *unenforced*  
15415        signalling channel carrying information under control of the information flow control policy can  
15416        also be caused by monitoring of the processing of any object containing or related to this  
15417        information (e.g. side channels). An *enforced* signalling channels may be identified in terms of the  
15418        subjects manipulating resources and the subject or user that observe such manipulation.  
15419        Classically, covert channels have been identified as timing or storage channels, according to the  
15420        resource being modified or modulated. As for other monitoring attacks, the use of the TOE is in  
15421        accordance with the SFRs.
- 15422        Covert channels are normally applicable in the case when the TOE has unobservability and multi-  
15423        level separation policy requirements. Covert channels may be routinely spotted during  
15424        vulnerability analysis and design activities, and should therefore be tested. However, generally  
15425        such monitoring attacks are only identified through specialised analysis techniques commonly  
15426        referred to as “covert channel analysis”. These techniques have been the subject of much research  
15427        and there are many papers published on this subject. Guidance for the conduct of covert channel  
15428        analysis should be sought from the evaluation authority.
- 15429        *Unenforced* information flow monitoring attacks include passive analysis techniques aiming at  
15430        disclosure of sensitive internal data of the TOE by operating the TOE in the way that corresponds  
15431        to the guidance documents.
- 15432        Side Channel Analysis includes crypt analytical techniques based on physical leakage of the TOE.  
15433        Physical leakage can occur by timing information, power consumption or power emanation during  
15434        computation of a TSF. Timing information can be collected also by a remote-attacker (having  
15435        network access to the TOE), power based information channels require that the attacker is in the  
15436        near-by environment of the TOE.
- 15437        Eavesdropping techniques include interception of all forms of energy, e.g., electromagnetic or  
15438        optical emanation of computer displays, not necessarily in the near-field of the TOE.
- 15439        Monitoring also includes exploits of protocol flaws, e.g., an attack on SSL implementation.
- 15440        **B.1.3.5 Misuse**
- 15441        Misuse may arise from:
- 15442        a) incomplete guidance documentation;
- 15443        b) unreasonable guidance;
- 15444        c) unintended misconfiguration of the TOE;

15445 d) forced exception behaviour of the TOE.

15446 If the guidance documentation is incomplete the user may not know how to operate the TOE in  
 15447 accordance with the SFRs. The evaluator should apply familiarity with the TOE gained from  
 15448 performing other evaluation activities to determine that the guidance is complete. In particular, the  
 15449 evaluator should consider the functional specification. The TSF described in this document should  
 15450 be described in the guidance as required to permit secure administration and use through the TSFI  
 15451 available to human users. In addition, the different modes of operation should be considered to  
 15452 ensure that guidance is provided for all modes of operation.

15453 The evaluator may, as an aid, prepare an informal mapping between the guidance and these  
 15454 documents. Any omissions in this mapping may indicate incompleteness.

15455 The guidance is considered to be unreasonable if it makes demands on the TOE's usage or  
 15456 operational environment that are inconsistent with the ST or unduly onerous to maintain security.

15457 A TOE may use a variety of ways to assist the consumer in effectively using that TOE in accordance  
 15458 with the SFRs and prevent unintentional misconfiguration. A TOE may employ functionality  
 15459 (features) to alert the consumer when the TOE is in a state that is inconsistent with the SFRs, whilst  
 15460 other TOEs may be delivered with enhanced guidance containing suggestions, hints, procedures,  
 15461 etc. on using the existing security features most effectively; for instance, guidance on using the  
 15462 audit feature as an aid for detecting when the SFRs are being compromised; namely insecure.

15463 The evaluator considers the TOE's functionality, its purpose and security objectives for the  
 15464 operational environment to arrive at a conclusion of whether or not there is reasonable  
 15465 expectation that use of the guidance would permit transition into an insecure state to be detected  
 15466 in a timely manner.

15467 The potential for the TOE to enter into insecure states may be determined using the evaluation  
 15468 deliverables, such as the ST, the functional specification and any other design representations  
 15469 provided as evidence for components included in the assurance package for the TOE (e.g. the  
 15470 TOE/TSF design specification if a component from TOE design (ADV\_TDS) is included).

15471 Instances of forced exception behaviour of the TSF could include, but are not limited to, the  
 15472 following:

15473 a) behaviour of the TOE when start-up, close-down or error recovery is activated;

15474 b) behaviour of the TOE under extreme circumstances (sometimes termed overload or  
 15475 asymptotic behaviour), particularly where this could lead to the de-activation or  
 15476 disabling of parts of the TSF;

15477 c) any potential for unintentional misconfiguration or insecure use arising from attacks  
 15478 noted in the subclause on tampering above.

#### 15479 **B.1.4 Identification of Potential Vulnerabilities**

15480 Potential vulnerabilities may be identified by the evaluator during different activities. They may  
 15481 become apparent during an evaluation activity or they may be identified as a result of analysis of  
 15482 evidence to search for vulnerabilities.

##### 15483 **B.1.4.1 Encountered**

15484 The encountered identification of vulnerabilities is where potential vulnerabilities are identified by  
 15485 the evaluator during the conduct of evaluation activities, i.e. the evidence are not being analysed  
 15486 with the express aim of identifying potential vulnerabilities.

## ISO/IEC 18045:2008(E)

15487 The encountered method of identification is dependent on the evaluator's experience and  
15488 knowledge; which is monitored and controlled by the evaluation authority. It is not reproducible in  
15489 approach but will be documented to ensure repeatability of the conclusions from the reported  
15490 potential vulnerabilities.

15491 There are no formal analysis criteria required for this method. Potential vulnerabilities are  
15492 identified from the evidence provided as a result of knowledge and experience. However, this  
15493 method of identification is not constrained to any particular subset of evidence.

15494 Evaluator is assumed to have knowledge of the TOE-type technology and known security flaws as  
15495 documented in the public domain. The level of knowledge assumed is that which can be gained  
15496 from a security e-mail list relevant to the TOE type, the regular bulletins (bug, vulnerability and  
15497 security flaw lists) published by those organisations researching security issues in products and  
15498 technologies in widespread use. This knowledge is not expected to extend to specific conference  
15499 proceedings or detailed theses produced by university research for AVA\_VAN.1 or AVA\_VAN.2.  
15500 However, to ensure the knowledge applied is up to date, the evaluator may need to perform a  
15501 search of public domain material.

15502 For AVA\_VAN.3 to AVA\_VAN.5 the search of publicly available information is expected to include  
15503 conference proceeding and theses produced during research activities by universities and other  
15504 relevant organisations.

15505 Examples of how these may arise (how the evaluator may encounter potential vulnerabilities):

15506 a) while the evaluator is examining some evidence, it sparks a memory of a potential  
15507 vulnerability identified in a similar product type, that the evaluator believes to also  
15508 be present in the TOE under evaluation;

15509 b) while examining some evidence, the evaluator spots a flaw in the specification of an  
15510 interface, that reflects a potential vulnerability.

15511 This may include becoming aware of a potential vulnerability in a TOE through reading about  
15512 generic vulnerabilities in a particular product type in an IT security publication or on a security e-  
15513 mail list to which the evaluator is subscribed.

15514 Attack methods can be developed directly from these potential vulnerabilities. Therefore, the  
15515 encountered potential vulnerabilities are collated at the time of producing penetration tests based  
15516 on the evaluator's vulnerability analysis. There is no explicit action for the evaluator to encounter  
15517 potential vulnerabilities. Therefore, the evaluator is directed through an implicit action specified in  
15518 AVA\_VAN.1.2E and AVA\_VAN.\*.4E.

15519 Current information regarding public domain vulnerabilities and attacks may be provided to the  
15520 evaluator by, for example, an evaluation authority. This information is to be taken into account by  
15521 the evaluator when collating encountered vulnerabilities and attack methods when developing  
15522 penetration tests.

### 15523 B.1.4.2 Analysis

15524 The following types of analysis are presented in terms of the evaluator actions.

#### 15525 B.1.4.2.1 Unstructured Analysis

15526 The unstructured analysis to be performed by the evaluator (for Evaluation of sub-activity  
15527 (AVA\_VAN.2)) permits the evaluator to consider the generic vulnerabilities (as discussed in B.1.3).  
15528 The evaluator will also apply their experience and knowledge of flaws in similar technology types.



15529 **B.1.4.2.2 Focused**

15530 During the conduct of evaluation activities, the evaluator may also identify areas of concern. These  
 15531 are specific portions of the TOE evidence that the evaluator has some reservation about, although  
 15532 the evidence meets the requirements for the activity with which the evidence is associated. For  
 15533 example, a particular interface specification looks particularly complex, and therefore may be  
 15534 prone to error either in the development of the TOE or in the operation of the TOE. There is no  
 15535 potential vulnerability apparent at this stage, further investigation is required. This is beyond the  
 15536 bounds of encountered, as further investigation is required.

15537 Difference between potential vulnerability and area of concern:

15538 a) Potential vulnerability - The evaluator knows a method of attack that can be used to  
 15539 exploit the weakness or the evaluator knows of vulnerability information that is  
 15540 relevant to the TOE.

15541 b) Area of concern - The evaluator may be able to discount concern as a potential  
 15542 vulnerability based on information provided elsewhere. While reading interface  
 15543 specification, the evaluator identifies that due to the extreme (unnecessary)  
 15544 complexity of an interface a potential vulnerability may lay within that area,  
 15545 although it is not apparent through this initial examination.

15546 The focused approach to the identification of vulnerabilities is an analysis of the evidence with the  
 15547 aim of identifying any potential vulnerabilities evident through the contained information. It is an  
 15548 unstructured analysis, as the approach is not predetermined. This approach to the identification of  
 15549 potential vulnerabilities can be used during the independent vulnerability analysis required by  
 15550 Evaluation of sub-activity (AVA\_VAN.3).

15551 This analysis can be achieved through different approaches, that will lead to commensurate levels  
 15552 of confidence. None of the approaches have a rigid format for the examination of evidence to be  
 15553 performed.

15554 The approach taken is directed by the results of the evaluator's assessment of the evidence to  
 15555 determine it meets the requirements of the AVA/AGD sub-activities. Therefore, the investigation of  
 15556 the evidence for the existence of potential vulnerabilities may be directed by any of the following:

15557 a) areas of concern identified during examination of the evidence during the conduct of  
 15558 evaluation activities;

15559 b) reliance on particular functionality to provide separation, identified during the  
 15560 analysis of the architectural design (as in Evaluation of sub-activity (ADV\_ARC.1)),  
 15561 requiring further analysis to determine it cannot be bypassed;

15562 c) representative examination of the evidence to hypothesise potential vulnerabilities in  
 15563 the TOE.

15564 The evaluator will report what actions were taken to identify potential vulnerabilities in the  
 15565 evidence. However, the evaluator may not be able to describe the steps in identifying potential  
 15566 vulnerabilities before the outset of the examination. The approach will evolve as a result of the  
 15567 outcome of evaluation activities.

15568 The areas of concern may arise from examination of any of the evidence provided to satisfy the  
 15569 SARs specified for the TOE evaluation. The information publicly accessible is also considered.

## ISO/IEC 18045:2008(E)

15570 The activities performed by the evaluator can be repeated and the same conclusions, in terms of  
15571 the level of assurance in the TOE, can be reached although the steps taken to achieve those  
15572 conclusions may vary. As the evaluator is documenting the form the analysis took, the actual steps  
15573 taken to achieve those conclusions are also reproducible.

### 15574 **B.1.4.2.3 Methodical**

15575 The methodical analysis approach takes the form of a structured examination of the evidence. This  
15576 method requires the evaluator to specify the structure and form the analysis will take (i.e. the  
15577 manner in which the analysis is performed is predetermined, unlike the focused identification  
15578 method). The method is specified in terms of the information that will be considered and how/why  
15579 it will be considered. This approach to the identification of potential vulnerabilities can be used  
15580 during the independent vulnerability analysis required by Evaluation of sub-activity (AVA\_VAN.4)  
15581 and Evaluation of sub-activity (AVA\_VAN.5).

15582 This analysis of the evidence is deliberate and pre-planned in approach, considering all evidence  
15583 identified as an input into the analysis.

15584 All evidence provided to satisfy the (ADV) assurance requirements specified in the assurance  
15585 package are used as input to the potential vulnerability identification activity.

15586 The “methodical” descriptor for this analysis has been used in an attempt to capture the  
15587 characterisation that this identification of potential vulnerabilities is to take an ordered and  
15588 planned approach. A “method” or “system” is to be applied in the examination. The evaluator is to  
15589 describe the method to be used in terms of what evidence will be considered, the information  
15590 within the evidence that is to be examined, the manner in which this information is to be  
15591 considered; and the hypothesis that is to be generated.

15592 The following provide some examples that a hypothesis may take:

15593 a) consideration of malformed input for interfaces available to an attacker at the  
15594 external interfaces;

15595 b) examination of a security mechanism, such as domain separation, hypothesising  
15596 internal buffer overflows leading to degradation of separation;

15597 c) analysis to identify any objects created in the TOE implementation representation  
15598 that are then not fully controlled by the TSF, and could be used by an attacker to  
15599 undermine the SFRs.

15600 For example, the evaluator may identify that interfaces are a potential area of weakness in the TOE  
15601 and specify an approach to the analysis that “all interface specifications provided in the functional  
15602 specification and TOE design will be analysed to hypothesise potential vulnerabilities” and go on to  
15603 explain the methods used in the hypothesis.

15604 This identification method will provide a plan of attack of the TOE, that would be performed by an  
15605 evaluator completing penetration testing of potential vulnerabilities in the TOE. The rationale for  
15606 the method of identification would provide the evidence for the coverage and depth of exploitation  
15607 determination that would be performed on the TOE.

### 15608 **B.1.5 When attack potential is used**

### 15609 **B.1.6 Developer**

15610 Attack potential is used by a PP/ST author during the development of the PP/ST, in consideration  
15611 of the threat environment and the selection of assurance components. This may simply be a

determination that the attack potential possessed by the assumed attackers of the TOE is generically characterised as Basic, Enhanced-Basic, Moderate or High. Alternatively, the PP/ST may wish to specify particular levels of individual factors assumed to be possessed by attackers. (e.g. the attackers are assumed to be experts in the TOE technology type, with access to specialised equipment.)

The PP/ST author considers the threat profile developed during a risk assessment (outside the scope of the ISO/IEC 15408 series, but used as an input into the development of the PP/ST in terms of the Security Problem Definition or in the case of Direct Rationale STs, the requirements statement). Consideration of this threat profile in terms of one of the approaches discussed in the following subclauses will permit the specification of the attack potential the TOE is to resist.

#### B.1.7 Evaluator

Attack potential is especially considered by the evaluator in two distinct ways during the ST evaluation and the vulnerability assessment activities.

Attack potential is used by an evaluator during the conduct of the vulnerability analysis sub-activity to determine whether or not the TOE is resistant to attacks assuming a specific attack potential of an attacker. If the evaluator determines that a potential vulnerability is exploitable in the TOE, they have to confirm that it is exploitable considering all aspects of the intended environment, including the attack potential assumed by an attacker.

Therefore, using the information provided in the threat statement of the Security Target, the evaluator determines the minimum attack potential required by an attacker to effect an attack, and arrives at some conclusion about the TOE's resistance to attacks. Table B.1 demonstrates the relationship between this analysis and attack potential.

| Vulnerability Component | TOE resistant to attacker with attack potential of: | Residual vulnerabilities only exploitable by attacker with attack potential of: |
|-------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------|
| VAN.5                   | High                                                | Beyond High                                                                     |
| VAN.4                   | Moderate                                            | High                                                                            |
| VAN.3                   | Enhanced-Basic                                      | Moderate                                                                        |
| VAN.2                   | Basic                                               | Enhanced-Basic                                                                  |
| VAN.1                   | Basic                                               | Enhanced-Basic                                                                  |

**Table B.1 Vulnerability testing and attack potential**

15634

The "beyond high" entry in the residual vulnerabilities column of the above table represents those potential vulnerabilities that would require an attacker to have an attack potential greater than that of "high" in order to exploit the potential vulnerability. A vulnerability classified as residual in this instance reflects the fact that a known weakness exists in the TOE, but in the current operational environment, with the assumed attack potential, the weakness cannot be exploited.

At any level of attack potential a potential vulnerability may be deemed "infeasible" due to a countermeasure in the operational environment that prevents the vulnerability from being exploited.

A vulnerability analysis applies to all TSFI, including ones that access probabilistic or permutational mechanisms. No assumptions are made regarding the correctness of the design and implementation of the TSFI; nor are constraints placed on the attack method or the attacker's interaction with the TOE - if an attack is possible, then it is to be considered during the vulnerability analysis. As shown in Table B.1, successful evaluation against a vulnerability assurance component reflects that the TSF is designed and implemented to protect against the required level of threat.

## ISO/IEC 18045:2008(E)

15650 It is not necessary for an evaluator to perform an attack potential calculation for each potential  
15651 vulnerability. In some cases, it is apparent when developing the attack method whether or not the  
15652 attack potential required to develop and run the attack method is commensurate with that  
15653 assumed of the attacker in the operational environment. For any vulnerabilities for which an  
15654 exploitation is determined, the evaluator performs an attack potential calculation to determine that  
15655 the exploitation is appropriate to the level of attack potential assumed for the attacker.

15656 The approach described below is to be applied whenever it is necessary to calculate attack  
15657 potential, unless the evaluation authority provides mandatory guidance that an alternative  
15658 approach is to be applied. The values given in Tables B.2 and B.3 below are not mathematically  
15659 proven. Therefore, the values given in these example tables may need to be adjusted according to  
15660 the technology type and specific environments. The evaluator should seek guidance from the  
15661 evaluation authority.

### 15662 **B.2 Calculating attack potential**

#### 15663 **B.2.1 Application of attack potential**

15664 Attack potential is a function of expertise, resources and motivation. There are multiple methods of  
15665 representing and quantifying these factors. Also, there may be other factors that are applicable for  
15666 particular TOE types.

##### 15667 **B.2.1.1 Treatment of motivation**

15668 Motivation is an attack potential factor that can be used to describe several aspects related to the  
15669 attacker and the assets the attacker desires. Firstly, motivation can imply the likelihood of an  
15670 attack - one can infer from a threat described as highly motivated that an attack is imminent, or  
15671 that no attack is anticipated from an un-motivated threat. However, except for the two extreme  
15672 levels of motivation, it is difficult to derive a probability of an attack occurring from motivation.

15673 Secondly, motivation can imply the value of the asset, monetarily or otherwise, to either the  
15674 attacker or the asset holder. An asset of very high value is more likely to motivate an attack  
15675 compared to an asset of little value. However, other than in a very general way, it is difficult to  
15676 relate asset value to motivation because the value of an asset is subjective - it depends largely upon  
15677 the value an asset holder places on it.

15678 Thirdly, motivation can imply the expertise and resources with which an attacker is willing to  
15679 effect an attack. One can infer that a highly-motivated attacker is likely to acquire sufficient  
15680 expertise and resources to defeat the measures protecting an asset. Conversely, one can infer that  
15681 an attacker with significant expertise and resources is not willing to effect an attack using them if  
15682 the attacker's motivation is low.

15683 During the course of preparing for and conducting an evaluation, all three aspects of motivation are  
15684 at some point considered. The first aspect, likelihood of attack, is what may inspire a developer to  
15685 pursue an evaluation. If the developer believes that the attackers are sufficiently motivated to  
15686 mount an attack, then an evaluation can provide assurance of the ability of the TOE to thwart the  
15687 attacker's efforts. Where the operational environment is well defined, for example in a system  
15688 evaluation, the level of motivation for an attack may be known, and will influence the selection of  
15689 countermeasures.

15690 Considering the second aspect, an asset holder may believe that the value of the assets (however  
15691 measured) is sufficient to motivate attack against them. Once an evaluation is deemed necessary,  
15692 the attacker's motivation is considered to determine the methods of attack that may be attempted,  
15693 as well as the expertise and resources used in those attacks. Once examined, the developer is able  
15694 to choose the appropriate assurance level, in particular the AVA requirement components,  
15695 commensurate with the attack potential for the threats. During the course of the evaluation, and in  
15696 particular as a result of completing the vulnerability assessment activity, the evaluator determines

15697 whether or not the TOE, operating in its operational environment, is sufficient to thwart attackers  
15698 with the identified expertise and resources.

15699 It may be possible for a PP author to quantify the motivation of an attacker, as the PP author has  
15700 greater knowledge of the operational environment in which the TOE (conforming to the  
15701 requirements of the PP) is to be placed. Therefore, the motivation could form an explicit part of the  
15702 expression of the attack potential in the PP, along with the necessary methods and measures to  
15703 quantify the motivation.

## 15704 **B.2.2 Characterising attack potential**

15705 This subclause examines the factors that determine attack potential, and provides some guidelines  
15706 to help remove some of the subjectivity from this aspect of the evaluation process.

### 15707 **B.2.2.1 Determining the attack potential**

15708 The determination of the attack potential for an attack corresponds to the identification of the  
15709 effort required to create the attack, and to demonstrate that it can be successfully applied to the  
15710 TOE (including setting up or building any necessary test equipment), thereby exploiting the  
15711 vulnerability in the TOE. The demonstration that the attack can be successfully applied needs to  
15712 consider any difficulties in expanding a result shown in the laboratory to create a useful attack. For  
15713 example, where an experiment reveals some bits or bytes of a confidential data item (such as a key),  
15714 it is necessary to consider how the remainder of the data item would be obtained (in this example  
15715 some bits might be measured directly by further experiments, while others might be found by a  
15716 different technique such as exhaustive search). It may not be necessary to carry out all of the  
15717 experiments to identify the full attack, provided it is clear that the attack actually proves that  
15718 access has been gained to a TOE asset, and that the complete attack could realistically be carried  
15719 out in exploitation according to the AVA\_VAN component targeted. In some cases, the only way to  
15720 prove that an attack can realistically be carried out in exploitation according to the AVA\_VAN  
15721 component targeted is to perform completely the attack and then rate it based upon the resources  
15722 actually required. One of the outputs from the identification of a potential vulnerability is assumed  
15723 to be a script that gives a step-by-step description of how to carry out the attack that can be used in  
15724 the exploitation of the vulnerability on another instance of the TOE.

15725 In many cases, the evaluators will estimate the parameters for exploitation, rather than carry out  
15726 the full exploitation. The estimates and their rationale will be documented in the ETR.

### 15727 **B.2.2.2 Factors to be considered**

15728 The following factors should be considered during analysis of the attack potential required to  
15729 exploit a vulnerability:

- 15730 a) Time taken to identify and exploit (*Elapsed Time*);
- 15731 b) Specialist technical expertise required (*Specialist Expertise*);
- 15732 c) Knowledge of the TOE design and operation (*Knowledge of the TOE*);
- 15733 d) Window of opportunity;
- 15734 e) IT hardware/software or other equipment required for exploitation.

15735 In many cases these factors are not independent, but may be substituted for each other in varying  
15736 degrees. For example, expertise or hardware/software may be a substitute for time. A discussion of

## ISO/IEC 18045:2008(E)

15737 these factors follows. (The levels of each factor are discussed in increasing order of magnitude.)  
15738 When it is the case, the less “expensive” combination is considered in the exploitation phase.

15739 **Elapsed time** is the total amount of time taken by an attacker to identify that a particular potential  
15740 vulnerability may exist in the TOE, to develop an attack method and to sustain effort required to  
15741 mount the attack against the TOE. When considering this factor, the worst-case scenario is used to  
15742 estimate the amount of time required. The identified amount of time is as follows:

- 15743 a) less than one day;
- 15744 b) between one day and one week;
- 15745 c) between one week and two weeks;
- 15746 d) between two weeks and one month;
- 15747 e) each additional month up to 6 months leads to an increased value;
- 15748 f) more than 6 months.

15749 **Specialist expertise** refers to the level of generic knowledge of the underlying principles, product  
15750 type or attack methods (e.g. Internet protocols, Unix operating systems, buffer overflows). The  
15751 identified levels are as follows:

- 15752 a) Laymen are unknowledgeable compared to experts or proficient persons, with no  
15753 particular expertise;
- 15754 b) Proficient persons are knowledgeable in that they are familiar with the security  
15755 behaviour of the product or system type;
- 15756 c) Experts are familiar with the underlying algorithms, protocols, hardware, structures,  
15757 security behaviour, principles and concepts of security employed, techniques and  
15758 tools for the definition of new attacks, cryptography, classical attacks for the product  
15759 type, attack methods, etc. implemented in the product or system type.
- 15760 d) The level “Multiple Expert” is introduced to allow for a situation, where different  
15761 fields of expertise are required at an Expert level for distinct steps of an attack.

15762 It may occur that several types of expertise are required. By default, the higher of the different  
15763 expertise factors is chosen. In very specific cases, the “multiple expert” level could be used but it  
15764 should be noted that the expertise must concern fields that are strictly different like for example  
15765 HW manipulation and cryptography.

15766 **Knowledge of the TOE** refers to specific expertise in relation to the TOE. This is distinct from  
15767 generic expertise, but not unrelated to it. Identified levels are as follows:

- 15768 a) Public information concerning the TOE (e.g. as gained from the Internet);
- 15769 b) Restricted information concerning the TOE (e.g. knowledge that is controlled within  
15770 the developer organisation and shared with other organisations under a non-  
15771 disclosure agreement)

- 15772 c) Sensitive information about the TOE (e.g. knowledge that is shared between discreet  
15773 teams within the developer organisation, access to which is constrained only to  
15774 members of the specified teams);
- 15775 d) Critical information about the TOE (e.g. knowledge that is known by only a few  
15776 individuals, access to which is very tightly controlled on a strict need to know basis  
15777 and individual undertaking).
- 15778 The knowledge of the TOE may graduate according to design abstraction, although this can only be  
15779 done on a TOE by TOE basis. Some TOE designs may be public source (or heavily based on public  
15780 source) and therefore even the design representation would be classified as public or at most  
15781 restricted, while the implementation representation for other TOEs is very closely controlled as it  
15782 would give an attacker information that would aid an attack and is therefore considered to be  
15783 sensitive or even critical.
- 15784 It may occur that several types of knowledge are required. In such cases, the higher of the different  
15785 knowledge factors is chosen.
- 15786 **Window of opportunity** (Opportunity) is also an important consideration, and has a relationship  
15787 to the **Elapsed Time** factor. Identification or exploitation of a vulnerability may require  
15788 considerable amounts of access to a TOE that may increase the likelihood of detection. Some attack  
15789 methods may require considerable effort off-line, and only brief access to the TOE to exploit. Access  
15790 may also need to be continuous, or over a number of sessions.
- 15791 For some TOEs the **Window of opportunity** may equate to the number of samples of the TOE that  
15792 the attacker can obtain. This is particularly relevant where attempts to penetrate the TOE and  
15793 undermine the SFRs may result in the destruction of the TOE preventing use of that TOE sample for  
15794 further testing, e.g. hardware devices. Often in these cases distribution of the TOE is controlled and  
15795 so the attacker must apply effort to obtain further samples of the TOE.
- 15796 For the purposes of this discussion:
- 15797 a) unnecessary/unlimited access means that the attack doesn't need any kind of  
15798 opportunity to be realised because there is no risk of being detected during access to  
15799 the TOE and it is no problem to access the number of TOE samples for the attack;
- 15800 b) easy means that access is required for less than a day and that the number of TOE  
15801 samples required to perform the attack is less than ten;
- 15802 c) moderate means that access is required for less than a month and that the number of  
15803 TOE samples required to perform the attack is less than one hundred;
- 15804 d) difficult means that access is required for at least a month or that the number of TOE  
15805 samples required to perform the attack is at least one hundred;
- 15806 e) none means that the opportunity window is not sufficient to perform the attack (the  
15807 length for which the asset to be exploited is available or is sensitive is less than the  
15808 opportunity length needed to perform the attack - for example, if the asset key is  
15809 changed each week and the attack needs two weeks); another case is, that a  
15810 sufficient number of TOE samples needed to perform the attack is not accessible to  
15811 the attacker - for example if the TOE is a hardware and the probability to destroy the  
15812 TOE during the attack instead of being successful is very high and the attacker has  
15813 only access to one sample of the TOE.

## ISO/IEC 18045:2008(E)

15814 Consideration of this factor may result in determining that it is not possible to complete the exploit,  
15815 due to requirements for time availability that are greater than the opportunity time.

15816 **IT hardware/software or other equipment** refers to the equipment required to identify or exploit  
15817 a vulnerability.

15818 a) Standard equipment is readily available to the attacker, either for the identification of  
15819 a vulnerability or for an attack. This equipment may be a part of the TOE itself (e.g. a  
15820 debugger in an operating system), or can be readily obtained (e.g. Internet  
15821 downloads, protocol analyser or simple attack scripts).

15822 b) Specialised equipment is not readily available to the attacker, but could be acquired  
15823 without undue effort. This could include purchase of moderate amounts of  
15824 equipment (e.g. power analysis tools, use of hundreds of PCs linked across the  
15825 Internet would fall into this category), or development of more extensive attack  
15826 scripts or programs. If clearly different test benches consisting of specialised  
15827 equipment are required for distinct steps of an attack this would be rated as bespoke.

15828 c) Bespoke equipment is not readily available to the public as it may need to be specially  
15829 produced (e.g. very sophisticated software), or because the equipment is so  
15830 specialised that its distribution is controlled, possibly even restricted. Alternatively,  
15831 the equipment may be very expensive.

15832 d) The level "Multiple Bespoke" is introduced to allow for a situation, where different  
15833 types of bespoke equipment are required for distinct steps of an attack.

15834 Specialist expertise and **Knowledge of the TOE** are concerned with the information required for  
15835 persons to be able to attack a TOE. There is an implicit relationship between an attacker's expertise  
15836 (where the attacker may be one or more persons with complementary areas of knowledge) and the  
15837 ability to effectively make use of equipment in an attack. The weaker the attacker's expertise, the  
15838 lower the potential to use equipment (IT hardware/software or other equipment). Likewise, the  
15839 greater the expertise, the greater the potential for equipment to be used in the attack. Although  
15840 implicit, this relationship between expertise and the use of equipment does not always apply, for  
15841 instance, when environmental measures prevent an expert attacker's use of equipment, or when,  
15842 through the efforts of others, attack tools requiring little expertise to be effectively used are  
15843 created and freely distributed (e.g. via the Internet).

### 15844 B.2.2.3 Calculation of attack potential

15845 Table B.2 identifies the factors discussed in the previous subclause and associates numeric values  
15846 with the total value of each factor.

15847 Where a factor falls close to the boundary of a range the evaluator should consider use of an  
15848 intermediate value to those in the table. For example, if twenty samples are required to perform  
15849 the attack then a value between one and four may be selected for that factor, or if the design is  
15850 based on a publicly available design but the developer has made some alterations then a value  
15851 between zero and three should be selected according to the evaluator's view of the impact of those  
15852 design changes. The table is intended as a guide.

15853 The "\*\*\*" specification in the table in considering **Window of Opportunity** is not to be seen as a  
15854 natural progression from the timescales specified in the preceding ranges associated with this  
15855 factor. This specification identifies that for a particular reason the potential vulnerability cannot be  
15856 exploited in the TOE in its intended operational environment. For example, access to the TOE may  
15857 be detected after a certain amount of time in a TOE with a known environment (i.e. in the case of a  
15858 system) where regular patrols are completed, and the attacker could not gain access to the TOE for  
15859 the required two weeks undetected. However, this would not be applicable to a TOE connected to



15860 the network where remote access is possible, or where the physical environment of the TOE is  
 15861 unknown.

| Factor                         | Value             |
|--------------------------------|-------------------|
| <b>Elapsed Time</b>            |                   |
| <= one day                     | 0                 |
| <= one week                    | 1                 |
| <= two weeks                   | 2                 |
| <= one month                   | 4                 |
| <= two months                  | 7                 |
| <= three months                | 10                |
| <= four months                 | 13                |
| <= five months                 | 15                |
| <= six months                  | 17                |
| > six months                   | 19                |
| <b>Expertise</b>               |                   |
| Layman                         | 0                 |
| Proficient                     | 3 <sup>*(1)</sup> |
| Expert                         | 6                 |
| Multiple experts               | 8                 |
| <b>Knowledge of TOE</b>        |                   |
| Public                         | 0                 |
| Restricted                     | 3                 |
| Sensitive                      | 7                 |
| Critical                       | 11                |
| <b>Window of Opportunity</b>   |                   |
| Unnecessary / unlimited access | 0                 |
| Easy                           | 1                 |
| Moderate                       | 4                 |
| Difficult                      | 10                |
| None                           | ** <sup>(2)</sup> |
| <b>Equipment</b>               |                   |
| Standard                       | 0                 |
| Specialised                    | 4 <sup>(3)</sup>  |
| Bespoke                        | 7                 |
| Multiple bespoke               | 9                 |

15862 <sup>(1)</sup> When several proficient persons are required to complete the attack path, the resulting level of  
 15863 expertise still remains “proficient” (which leads to a 3 rating).

15864 <sup>(2)</sup> Indicates that the attack path is not exploitable due to other measures in the intended operational  
 15865 environment of the TOE.

15866 <sup>(3)</sup> If clearly different test benches consisting of specialised equipment are required for distinct steps of an  
 15867 attack, this should be rated as bespoke.

15868 **Table B.2 Calculation of attack potential**

## ISO/IEC 18045:2008(E)

15869 To determine the resistance of the TOE to the potential vulnerabilities identified the following  
15870 steps should be applied:

15871 a) Define the possible attack scenarios {AS1, AS2, ..., ASn} for the TOE in the operational  
15872 environment.

15873 b) For each attack scenario, perform a theoretical analysis and calculate the relevant  
15874 attack potential using Table B.2.

15875 c) For each attack scenario, if necessary, perform penetration tests in order to confirm  
15876 or to disprove the theoretical analysis.

15877 d) Divide all attack scenarios {AS1, AS2, ..., ASn} into two groups:

15878 1) the attack scenarios having been successful (i.e. those that have been used to  
15879 successfully undermine the SFRs), and

15880 2) the attack scenarios that have been demonstrated to be unsuccessful.

15881 e) For each successful attack scenario, apply Table B.3 and determine, whether there is a  
15882 contradiction between the resistance of the TOE and the chosen AVA\_VAN assurance  
15883 component, see the last column of Table B.3.

15884 f) Should one contradiction be found, the vulnerability assessment will fail, e.g. the  
15885 author of the ST chose the component AVA\_VAN.5 and an attack scenario with an  
15886 attack potential of 21 points (high) has broken the security of the TOE. In this case,  
15887 the TOE is resistant to attacker with attack potential 'Moderate', this contradicts to  
15888 AVA\_VAN.5, hence, the vulnerability assessment fails.

15889 The "Values" column of Table B.3 indicates the range of attack potential values (calculated using  
15890 Table B.2) of an attack scenario that results in the SFRs being undermined.

| Values | Attack potential required to exploit scenario: | Meets assurance components:                         | Failure of components:                                            |
|--------|------------------------------------------------|-----------------------------------------------------|-------------------------------------------------------------------|
| 0-9    | Basic                                          | -                                                   | AVA_VAN.1,<br>AVA_VAN.2,<br>AVA_VAN.3,<br>AVA_VAN.4,<br>AVA_VAN.5 |
| 10-13  | Enhanced-Basic                                 | AVA_VAN.1,<br>AVA_VAN.2                             | AVA_VAN.3,<br>AVA_VAN.4,<br>AVA_VAN.5                             |
| 14-19  | Moderate                                       | AVA_VAN.1,<br>AVA_VAN.2,<br>AVA_VAN.3               | AVA_VAN.4,<br>AVA_VAN.5                                           |
| 20-24  | High                                           | AVA_VAN.1,<br>AVA_VAN.2,<br>AVA_VAN.3,<br>AVA_VAN.4 | AVA_VAN.5                                                         |
| =>25   | Beyond High                                    | AVA_VAN.1,                                          | -                                                                 |

| Values | Attack potential required to exploit scenario: | Meets assurance components:                         | Failure of components: |
|--------|------------------------------------------------|-----------------------------------------------------|------------------------|
|        |                                                | AVA_VAN.2,<br>AVA_VAN.3,<br>AVA_VAN.4,<br>AVA_VAN.5 |                        |

**Table B.3 Rating of vulnerabilities and TOE resistance**

15891

15892 An approach such as this cannot take account of every circumstance or factor, but should give a  
 15893 better indication of the level of resistance to attack required to achieve the standard ratings. Other  
 15894 factors, such as the reliance on unlikely chance occurrences are not included in the basic model, but  
 15895 can be used by an evaluator as justification for a rating other than those that the basic model might  
 15896 indicate.

15897 It should be noted that whereas a number of vulnerabilities rated individually may indicate high  
 15898 resistance to attack, collectively the combination of vulnerabilities may indicate that overall a  
 15899 lower rating is applicable. The presence of one vulnerability may make another easier to exploit.

15900 If a PP/ST author wants to use the attack potential table for the determination of the level of attack  
 15901 the TOE should withstand (selection of Vulnerability analysis (AVA\_VAN) component), they should  
 15902 proceed as follows: For all different attack scenarios (i.e. for all different types of attacker and/or  
 15903 different types of attack the author has in mind) which must not violate the SFRs, several passes  
 15904 through Table B.2 should be made to determine the different values of attack potential assumed for  
 15905 each such unsuccessful attack scenario. The PP/ST author then chooses the highest value of them  
 15906 in order to determine the level of the TOE resistance to be claimed from Table B.3: the TOE  
 15907 resistance must be at least equal to this highest value determined. For example, the highest value of  
 15908 attack potentials of all attack scenarios, which must not undermine the TOE security policy,  
 15909 determined in such a way is Moderate; hence, the TOE resistance shall be at least Moderate (i.e.  
 15910 Moderate or High); therefore, the PP/ST author can choose either AVA\_VAN.4 (for Moderate) or  
 15911 AVA\_VAN.5 (for High) as the appropriate assurance component.

### 15912 B.3 Example calculation for direct attack

15913 Mechanisms subject to direct attack are often vital for system security and developers often  
 15914 strengthen these mechanisms. As an example, a TOE might use a simple pass number  
 15915 authentication mechanism that can be overcome by an attacker who has the opportunity to  
 15916 repeatedly guess another user's pass number. The system can strengthen this mechanism by  
 15917 restricting pass numbers and their use in various ways. During the course of the evaluation an  
 15918 analysis of this direct attack could proceed as follows:

15919 Information gleaned from the ST and design evidence reveals that identification and authentication  
 15920 provides the basis upon which to control access to network resources from widely distributed  
 15921 terminals. Physical access to the terminals is not controlled by any effective means. The duration of  
 15922 access to a terminal is not controlled by any effective means. Authorised users of the system choose  
 15923 their own pass numbers when initially authorised to use the system, and thereafter upon user  
 15924 request. The system places the following restrictions on the pass numbers selected by the user:

15925 a) the pass number must be at least four and no greater than six digits long;

15926 b) consecutive numerical sequences are disallowed (such as 7,6,5,4,3);

15927 c) repeating digits is disallowed (each digit must be unique).

## ISO/IEC 18045:2008(E)

15928 Guidance provided to the users at the time of pass number selection is that pass numbers should be  
15929 as random as possible and should not be affiliated with the user in some way - a date of birth, for  
15930 instance.

15931 The pass number space is calculated as follows:

15932 Patterns of human usage are important considerations that can influence the approach to  
15933 searching a password space. Assuming the worst-case scenario and the user chooses a number  
15934 comprising only four digits, the number of pass number permutations assuming that each digit  
15935 must be unique is:

15936 
$$7(8)(9)(10) = 5040$$

15937 The number of possible increasing sequences is seven, as is the number of decreasing sequences.  
15938 The pass number space after disallowing sequences is:

15939 
$$5040 - 14 = 5026$$

15940 Based on further information gleaned from the design evidence, the pass number mechanism is  
15941 designed with a terminal locking feature. Upon the sixth failed authentication attempt the terminal  
15942 is locked for one hour. The failed authentication count is reset after five minutes so that an attacker  
15943 can at best attempt five pass number entries every five minutes, or 60 pass number entries every  
15944 hour.

15945 On average, an attacker would have to enter 2513 pass numbers, over 2513 minutes, before  
15946 entering the correct pass number. The average successful attack would, as a result, occur in slightly  
15947 less than:

15948 
$$\frac{2513min}{60\frac{min}{hour}} \approx 42hours$$

15949 Using the approach to calculate the attack potential, described in the previous subclause, identifies  
15950 that it is possible that a layman can defeat the mechanism within days (given easy access to the  
15951 TOE), with the use of standard equipment, and with no knowledge of the TOE, giving a value of 1.  
15952 Given the resulting sum, 1, the attack potential required to effect a successful attack is not rated, as  
15953 it falls below that considered to be Basic.

## Annex C (informative)

### Evaluation Techniques and Tools

#### C.1 Semiformal and formal methods

In ISO/IEC 15408-3:20xx, Annex A.5, supplementary material on formal methods is provided.

##### C.1.1 Description of styles

This section provides general guidance on specification styles. Specific and detailed information is in those work units under the specific evaluator action elements where examination of the style of specifications, TSP model and correspondence demonstrations has to be performed.

The ADV class mandates three types of specification styles: informal, semiformal and formal. These styles are briefly described in the application notes to the ADV class in ISO/IEC 15408-2. The functional specification and design specification will be written using one or more of these specification styles. The TSF representations (in the following referred to as specifications) may use one or more notations in semiformal and formal style. The level of formality of the correspondence representation depends on the style of the adjacent pair of provided TSF representation (see the ADV\_TDS family for details).

The hierarchy of components within these families increase the formality of the style:

- to reduce the ambiguity of the TSF representation through the hierarchy of components within the families,
  - to reduce the likelihood of refinement errors in the available TSF representations,
  - to strengthen the evidence for correctness of the TSF representations and the methods for their examination.
- The styles are characterised by:
- informal style- defined semantics
  - semiformal style - defined semantics and syntax
  - formal style - defined semantics, syntax and rules of inference.

Regarding the notions of semantics and syntax the degree of precision varies with the style of description.

Informal descriptions require the semantics to provide meaning to all terms with the help of natural language explanations.

Semiformal descriptions restrict the syntax formation of terms to well defined expressions having a precise meaning in the technical community.

Formal style descriptions restrict the semantics and syntax even further: The formation of syntactical terms follows a formal language description required to be decidable. Examples include well established implicit formation rules being as precise as the formation of terms and formulas in

## ISO/IEC 18045:2008(E)

15990 first order predicate calculus or formal meta language descriptions using Extended Backus Naur  
15991 Form. Apart from informal descriptions the semantics of formal terms is restricted to well  
15992 established mathematical models. Formal derivation of theorems is restricted to predefined  
15993 inference rules, which are based on well known logical reasoning (classical logic, intuitionistic logic,  
15994 modal logic, temporal logic, etc.). Algorithmic model checking can serve as a substitute for theorem  
15995 proving whenever the reference to well established model checkers is clear and appropriate meta  
15996 theorems are given to guarantee the equivalence to an inference by proof rules.

15997 In the context of the level of formality informal, semiformal and formal styles are considered to be  
15998 hierarchical in nature. Thus, requirements for a informal or semiformal style of specification may  
15999 also be met with either a semiformal or formal specification style provided, that is supported by  
16000 informal, explanatory text where appropriate. The set of presentation elements, syntactic and  
16001 semantic rules is referred in the following as notation. A formal style of presentation uses a formal  
16002 notation and rules of inference which is referred to in the following as formal system.

16003 The content and presentation elements of ADV\_FSP and ADV\_TDS components describe the style  
16004 in which the presentation of evidence shall be provided by the developer. The evaluator action  
16005 element ADV\_x.y.1E requires the evaluator to confirm that the information provided meets all  
16006 requirements for presentation of evidence. If the content and presentation elements require an  
16007 informal style the evaluator may perform the work units for the evaluator action elements in  
16008 parallel with the other work units examining the content of evidence. If the content and  
16009 presentation elements require a semiformal or a formal style this implies the application of  
16010 semiformal or formal methods to examine the content. Therefore it is recommended to perform  
16011 the work units for the evaluator action elements concerning the correct use of the method and its  
16012 rigour before the analysis of the content of evidence. If a notation or their usage in the  
16013 documentation does not provide the level of formality the necessary rigorous methods of analysis  
16014 may be not applicable. The work unit for the evaluator action elements examining the necessary  
16015 informal explanatory text may be performed in parallel with the other work units. Of course the  
16016 evaluator might detect errors in the presentation of evidence during the evaluator action as well  
16017 which result in a fail verdict for the evaluator action elements.

16018 The following text provides a guidance for the examination of specification styles and their use for  
16019 correspondence demonstration in the sub-activities for the assurance families ADV\_FSP, ADV\_TDS  
16020 and ADV\_SPM.

### 16021 C.1.1.1 Informal style

16022 An informal specification is one that is expressed in a natural language. If content and presentation  
16023 elements require an informal specification the work unit for the evaluator action elements will  
16024 require the evaluator to determine that it contains all necessary informal explanatory text. The  
16025 evaluator should examine the specification to make sure that it

16026 • provides defined meanings of terms, abbreviations and acronyms that are used in a  
16027 context other than that accepted by normal usage,

16028 • if semiformal or formal notations are used appropriate informal, explanatory text shall  
16029 support the understanding.

16030 This enforces the informal specification to provide defined **semantics** of its statements. An  
16031 informal specification uses the ordinary conventions for the natural language i.e. any common  
16032 spoken tongue. It may use figures and semiformal elements of presentation like data flow diagrams  
16033 to illustrate the informal specification. If the specification uses a semiformal notation it will be  
16034 accompanied by supporting explanatory informal text appropriate for unambiguous common  
16035 understanding.

16036 Examples for the use of informal style are:

16037 ISO/IEC 15408-1 identifies a glossary of terms specific to ISO/IEC 15408 (all parts) and reserved  
 16038 terms in accordance with the ISO definitions contained in ISO/IEC Directives Part 2, Rules for the  
 16039 structure and drafting of International Standards. This clarifies the use of the verbs "shall",  
 16040 "should", "may" and "can" in the context of ISO/IEC 15408 (all parts)

16041 • International standards and the Request for Interpretation (RFC) are specified in an  
 16042 informal style. They use semiformal notations as well e.g. the abstract syntax notation  
 16043 ASN.1 for specification of message formats.

16044 Informal style does not excuse the absence of precision or informal definitions. The evaluator's  
 16045 verdict fails if some technical term remains undefined, the evaluators lack of information prevents  
 16046 decision, or ambiguous interpretations cause confusion.

#### 16047 C.1.1.2 Semiformal style

16048 A semiformal specification is expressed in a restricted syntax language with defined semantics. It  
 16049 reduces the ambiguity of specification and strengthens the method of analysis.

16050 The evaluator should examine the identified notations to make sure that

16051 • The syntax rules are defined or a definition is referenced.

16052 • The notations with the explanatory text provide a defined **semantics** which is  
 16053 characterised by:

16054 a) defined meanings of terms, abbreviations and acronyms that are used in a context  
 16055 other than that accepted by normal usage,

16056 b) the use of a semiformal notation is accompanied by supporting explanatory text in  
 16057 informal style appropriate for unambiguous meaning,

16058 c) expression of rules and characteristics of applicable policies, security functionality  
 16059 and interfaces (providing details of effects, exceptions and error messages) of TSF,  
 16060 their subsystems or modules to be specified for the assurance family for which the  
 16061 notations are used.

16062 • The notations contain a restricted **syntax** language which means that a set of conventions  
 16063 must be supplied to define the restrictions imposed on the syntax.

16064 Examples for the use of semiformal style are:

16065 • The restricted syntax language may be a natural language with restricted sentence  
 16066 structure and keywords with special meanings. -> ISO/IEC 15408-1 and ISO/IEC 15408-  
 16067 2 provide a semiformal notation for the security functional requirements consisting of  
 16068 classes, families and components together with rules for permitted operations. As  
 16069 required by the ECD families of classes ASE and APE, an explicitly stated IT security  
 16070 requirement shall use the CC requirements components, families and classes as a model  
 16071 for presentation.

16072 • Formally specified languages may be used to define the data structures for the use of  
 16073 TSFI or an interface of subsystems or modules in semiformal style. Thus e.g. ISO/IEC  
 16074 8824 and 8825 define the abstract syntax notation ASN.1 and ISO/IEC 8834 the semantic  
 16075 of the object identifier (OID). ASN.1 makes possible extracting the encoded information  
 16076 by automated tools (parser). The interface specification may describe the complete

## ISO/IEC 18045:2008(E)

- 16077 details of all effects caused by interface usage by means of other semiformal notations  
16078 e.g. state-transition diagrams.
- 16079 • Diagrams are commonly used for the specification of data-flow, state-transition, entity-  
16080 relation-ship, data or process or program structures in a semiformal style, e.g. the Unified  
16081 Modelling Language (UML) for object-oriented analysis and design includes model  
16082 diagrams, their semantics and an interchange format between case tools. The graphical  
16083 presentation assists the understanding of interaction and behaviour of entities depending  
16084 on events. The abstraction accompanied by the graphical presentation normally needs to  
16085 be compensated by informal description. Data-flow and state-transition diagrams may be  
16086 very helpful, e.g. for the precise description and the analysis of protocols.
- 16087 • Programming languages like ANSI C defines a strong syntax and well-defined semantics.  
16088 The source code together with supporting explanatory text and documentation of well-  
16089 defined development tools provides an unambiguous semiformal description of the TSF  
16090 implementation, their security features and interfaces. Although having a very high level  
16091 of formality programming languages may be of semiformal styles only because of  
16092 missing inference rules. But some software development tools support also formal  
16093 methods in software design including theorem prover.
- 16094 These examples show that semiformal style covers a wide range of capabilities and level of  
16095 formality. The developer should use appropriate notation for presentation of evidence depending  
16096 on the type of TOE (e.g. hardware, software), the development methodology and the purpose of the  
16097 specification.
- 16098 The semiformal style supports a structured analysis of the content, the consistency, the  
16099 completeness and the correspondence of the representation. A semiformal analysis is one that  
16100 results from a structured approach with a substantial degree of rigor in terms of completeness and  
16101 correctness.
- 16102 A semiformal interface specification supports the evaluator in analysing and assessing the external  
16103 behaviour of a TSF, their subsystems or modules for any input (e.g. to decide about acceptance or  
16104 rejection of a message and its content analysis). Semiformal evidence for conservation of  
16105 properties can be obtained by means of flow charts and state transition diagrams visualizing the  
16106 uniquely defined states and their interrelationship during the course of security preserving  
16107 transitions. The developer may use semiformal notations like software specification languages to  
16108 ensure correct refinement of the specifications from functional specification via high and low level  
16109 design down to the implementation level.
- 16110 This way the semiformal presentation clearly establishes its accuracy and superiority over  
16111 informal descriptions.
- 16112 **C.1.1.3 Formal style**
- 16113 A formal specification is expressed within a formal system based upon well-established  
16114 mathematical concepts. These mathematical concepts are used to define well-defined semantics,  
16115 syntax and rules of inference. A formal system is an abstract system of identities and relations that  
16116 can be described by specifying a formal alphabet, a formal language over that alphabet which is  
16117 based on a formal syntax, and a set of formal rules of inference for constructing derivations of  
16118 sentences in the formal language.
- 16119 The evaluator should examine the identified formal systems to make sure that
- 16120 • The semantics, syntax and inference rules of the formal system are defined or a definition  
16121 is referenced.



- 16122 • Each formal system with the explanatory text provides a defined **semantics** which:
  - 16123 a) provides defined meanings of terms, abbreviations and acronyms that are used in a
  - 16124 context other than that accepted by normal usage,
  - 16125 b) the use of a formal system and semiformal notation if any use is accompanied by
  - 16126 supporting explanatory text in informal style appropriate for unambiguous meaning,
  - 16127 c) the formal system is able to express rules and characteristics of applicable policies,
  - 16128 security functionality and interfaces (providing details of effects, exceptions and
  - 16129 error messages) of the TSF, their subsystems or modules to be specified for the
  - 16130 assurance family for which the notations are used.
  - 16131 d) the notation provides rules to determine the meaning of syntactical valid constructs.
  - 16132 e) Each formal system uses a formal **syntax** that
  - 16133 f) provides rules to unambiguously recognise constructs.
  - 16134 g) Each formal system provides **proof rules** which
  - 16135 h) support logical reasoning of well-established mathematical concepts,
  - 16136 i) help to prevent derivation of contradictions.
- 16137 If the developer uses a formal system which is already accepted by the certification body the
- 16138 evaluator can rely on the level of formality and strength of the system and focus on the
- 16139 instantiation of the formal system to the TOE specifications and correspondence proofs.
- 16140 The formal style supports mathematical proofs of the security properties based on the security
- 16141 features, the consistency of refinements and the correspondence of the representations. Formal
- 16142 tool support seems adequate whenever manual derivations would otherwise become long winded
- 16143 and incomprehensible. Formal tools are also apt to reduce the error probability inherent in manual
- 16144 derivations.
- 16145 **C.1.2 Security policy models and styles**
- 16146 The assurance family Security policy modelling ADV\_SPM requires in their components an
- 16147 increasing level of formality of the TSP model and correspondence demonstration between the TSP
- 16148 model and the functional specification. The following section provides some guidance how the
- 16149 general requirements on styles applies to the TSP models.
- 16150 The TOE Security Policy (TSP) is a set of rules and characteristics that regulate how assets are
- 16151 managed, protected and distributed within a TOE. The TSP can be explicitly stated in the ST by the
- 16152 SFR (e.g. of families FDP\_ACC or FDP\_AFC) or be drawn from other SFR (e.g. of classes FAU, FIA or
- 16153 FPR) claimed in the ST. Although these TSF are provided in semiformal style the policies are
- 16154 normally described by rules and characteristics in informal style. A TOE security policy model is a
- 16155 structured representation of security policies to be enforced by the TOE.
- 16156 According to ADV\_SPM.\*.2C the TSP model shall model all security policies of the TSP that can be
- 16157 modelled by the respective level defined by ADV\_SPM.\*.1C or a rationale shall be given why a lower
- 16158 level of formality is applied. Thus the TSP model may contain for policy sets of the TSP different
- 16159 models of different levels of formality as state of the art.

16160

16161

16162

16163

16164

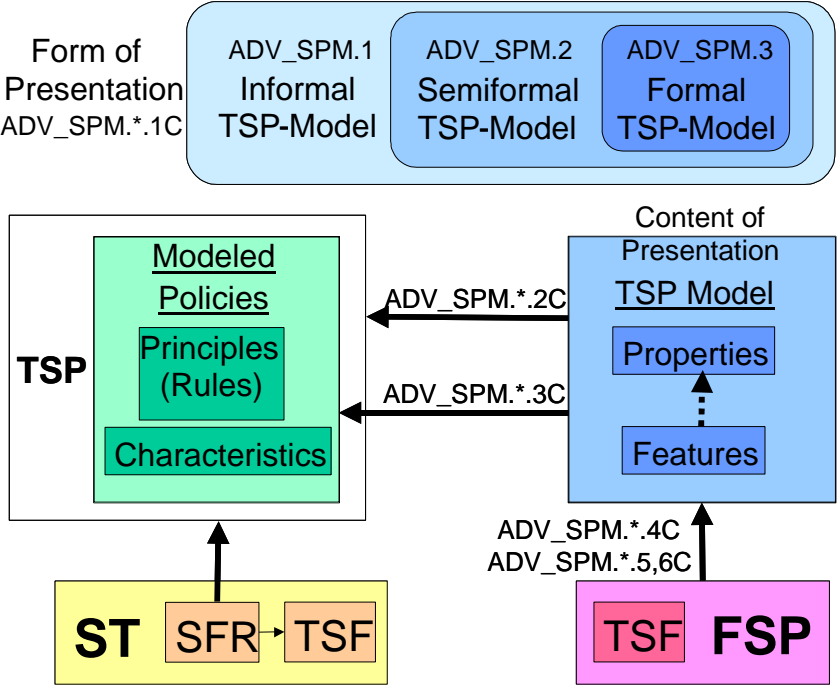
16165

16166

ISO/IEC 18045:2008(E)

An informal TSP model is a description of the TSP enforced by the security functional requirements claimed in the ST. All TSP in the ST can be informally modelled.

Modelling means to describe the rules and characteristics of the policies by the properties and features in the TSP model and to provide evidence that the features imply these properties. The strength of this evidence depends on the level of formality: an informal model may provide a rationale but a formal model shall provide a formal proof that the security features imply the security properties.



16167

16168

16169

16170

16171

16172

16173

16174

16175

16176

16177

**Figure C.1 TOE security policy models and correspondence demonstration**

The possibility of formally modelling TSPs is dependent on the state of the art. A wide range of examples have already been given in the past for successfully modelling Access Control including Identification and Authentication. Hence inclusion of access control policies almost always requires the developer to provide the model in a formal style.

Whenever in doubt the evaluator should negotiate the type of style (formal, semiformal or informal) with the certification body in advance in order to agree upon the state of the art for the specific policy under question.



16179

## Bibliography

- 16180 This bibliography contains references to further material and standards useful to the readers of  
16181 ISO/IEC 15408 (all parts). For undated references the reader is recommended to refer to the latest  
16182 edition of the referenced document.
- 16183 ISO/IEC 15408-4:20XX, *IT Security techniques — Evaluation criteria for IT security — Part 4:*  
16184 *Framework for the specification of evaluation methods and activities*
- 16185 ISO/IEC 15408-5:20XX, *IT Security techniques — Evaluation criteria for IT security — Part 5: Pre-*  
16186 *defined packages of security requirements*
- 16187