

Information technology — Security techniques — Methodology for IT security evaluation

ICS 35.040

National foreword

This British Standard reproduces verbatim ISO/IEC 18045:2005 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information technology — Security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the ISO/IEC title page, pages ii to viii, pages 1 to 276, an inside back cover and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 18 November 2005

© BSI 18 November 2005

INTERNATIONAL STANDARD

ISO/IEC 18045

First edition
2005-10-01

Information technology — Security techniques — Methodology for IT security evaluation

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



Reference number
ISO/IEC 18045:2005(E)

AVA Documents
Document Sharing Hub

Contents

Page

Foreword	vii
Introduction	viii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	3
5 Overview	3
5.1 Organisation of this International Standard	3
6 Document Conventions	3
6.1 Terminology	3
6.2 Verb usage	4
6.3 General evaluation guidance	4
6.4 Relationship between ISO/IEC 15408 and ISO/IEC 18045 structures	4
6.5 Evaluator verdicts	4
7 General evaluation tasks	5
7.1 Introduction	5
7.2 Evaluation input task	6
7.2.1 Objectives	6
7.2.2 Application notes	6
7.2.3 Management of evaluation evidence sub-task	7
7.3 Evaluation output task	7
7.3.1 Objectives	7
7.3.2 Application notes	8
7.3.3 Write OR sub-task	8
7.3.4 Write ETR sub-task	8
7.3.5 Evaluation sub-activities	13
8 Protection Profile evaluation	14
8.1 Introduction	14
8.2 PP evaluation relationships	14
8.3 Protection Profile evaluation activity	15
8.3.1 Evaluation of TOE description (APE_DES.1)	15
8.3.2 Evaluation of Security environment (APE_ENV.1)	16
8.3.3 Evaluation of PP introduction (APE_INT.1)	19
8.3.4 Evaluation of Security objectives (APE_OBJ.1)	20
8.3.5 Evaluation of IT security requirements (APE_REQ.1)	23
8.3.6 Evaluation of Explicitly stated IT security requirements (APE_SRE.1)	32
9 Security Target evaluation	35
9.1 Introduction	35
9.2 ST evaluation relationships	35
9.3 Security Target evaluation activity	36
9.3.1 Evaluation of TOE description (ASE_DES.1)	36
9.3.2 Evaluation of Security environment (ASE_ENV.1)	37
9.3.3 Evaluation of ST introduction (ASE_INT.1)	40
9.3.4 Evaluation of Security objectives (ASE_OBJ.1)	42
9.3.5 Evaluation of PP claims (ASE_PPC.1)	45
9.3.6 Evaluation of IT security requirements (ASE_REQ.1)	46
9.3.7 Evaluation of Explicitly stated IT security requirements (ASE_SRE.1)	56

9.3.8	Evaluation of TOE summary specification (ASE_TSS.1).....	58
10	EAL1 evaluation	62
10.1	Introduction	62
10.2	Objectives	62
10.3	EAL1 evaluation relationships	62
10.4	Configuration management activity.....	63
10.4.1	Evaluation of CM capabilities (ACM_CAP.1).....	63
10.5	Delivery and operation activity.....	64
10.5.1	Evaluation of Installation, generation and start-up (ADO_IGS.1).....	64
10.6	Development activity	65
10.6.1	Application notes.....	65
10.6.2	Evaluation of Functional specification (ADV_FSP.1).....	66
10.6.3	Evaluation of Representation correspondence (ADV_RCR.1)	69
10.7	Guidance documents activity.....	72
10.7.1	Application notes.....	72
10.7.2	Evaluation of Administrator guidance (AGD_ADM.1).....	72
10.7.3	Evaluation of User guidance (AGD_USR.1)	75
10.8	Tests activity	77
10.8.1	Application notes.....	77
10.8.2	Evaluation of Independent testing (ATE_IND.1)	78
11	EAL2 evaluation	81
11.1	Introduction	81
11.2	Objectives	82
11.3	EAL2 evaluation relationships	82
11.4	Configuration management activity.....	82
11.4.1	Evaluation of CM capabilities (ACM_CAP.2).....	82
11.5	Delivery and operation activity.....	85
11.5.1	Evaluation of Delivery (ADO_DEL.1).....	85
11.5.2	Evaluation of Installation, generation and start-up (ADO_IGS.1).....	86
11.6	Development activity	87
11.6.1	Application notes.....	87
11.6.2	Evaluation of Functional specification (ADV_FSP.1).....	88
11.6.3	Evaluation of High-level design (ADV_HLD.1).....	91
11.6.4	Evaluation of Representation correspondence (ADV_RCR.1)	94
11.7	Guidance documents activity.....	97
11.7.1	Application notes.....	97
11.7.2	Evaluation of Administrator guidance (AGD_ADM.1).....	97
11.7.3	Evaluation of User guidance (AGD_USR.1)	100
11.8	Tests activity	102
11.8.1	Application notes.....	102
11.8.2	Evaluation of Coverage (ATE_COV.1)	103
11.8.3	Evaluation of Functional tests (ATE_FUN.1)	104
11.8.4	Evaluation of Independent testing (ATE_IND.2)	108
11.9	Vulnerability assessment activity	114
11.9.1	Evaluation of Strength of TOE security functions (AVA_SOF.1).....	114
11.9.2	Evaluation of Vulnerability analysis (AVA_VLA.1)	116
12	EAL3 evaluation	121
12.1	Introduction	121
12.2	Objectives	122
12.3	EAL3 evaluation relationships	122
12.4	Configuration management activity.....	122
12.4.1	Evaluation of CM capabilities (ACM_CAP.3).....	122
12.4.2	Evaluation of CM scope (ACM_SCP.1)	126
12.5	Delivery and operation activity.....	127
12.5.1	Evaluation of Delivery (ADO_DEL.1).....	127
12.5.2	Evaluation of Installation, generation and start-up (ADO_IGS.1).....	128
12.6	Development activity	129
12.6.1	Application notes.....	130

12.6.2	Evaluation of Functional specification (ADV_FSP.1)	130
12.6.3	Evaluation of High-level design (ADV_HLD.2)	134
12.6.4	Evaluation of Representation correspondence (ADV_RCR.1)	138
12.7	Guidance documents activity	140
12.7.1	Application notes	140
12.7.2	Evaluation of Administrator guidance (AGD_ADM.1)	140
12.7.3	Evaluation of User guidance (AGD_USR.1)	143
12.8	Life cycle support activity	146
12.8.1	Evaluation of Development security (ALC_DVS.1)	146
12.9	Tests activity	148
12.9.1	Application notes	148
12.9.2	Evaluation of Coverage (ATE_COV.2)	150
12.9.3	Evaluation of Depth (ATE_DPT.1)	152
12.9.4	Evaluation of Functional tests (ATE_FUN.1)	154
12.9.5	Evaluation of Independent testing (ATE_IND.2)	159
12.10	Vulnerability assessment activity	164
12.10.1	Evaluation of Misuse (AVA_MSU.1)	164
12.10.2	Evaluation of Strength of TOE security functions (AVA_SOF.1)	167
12.10.3	Evaluation of Vulnerability analysis (AVA_VLA.1)	169
13	EAL4 evaluation	174
13.1	Introduction	174
13.2	Objectives	175
13.3	EAL4 evaluation relationships	175
13.4	Configuration management activity	175
13.4.1	Evaluation of CM automation (ACM_AUT.1)	175
13.4.2	Evaluation of CM capabilities (ACM_CAP.4)	177
13.4.3	Evaluation of CM scope (ACM_SCP.2)	182
13.5	Delivery and operation activity	183
13.5.1	Evaluation of Delivery (ADO_DEL.2)	183
13.5.2	Evaluation of Installation, generation and start-up (ADO_IGS.1)	185
13.6	Development activity	186
13.6.1	Application notes	186
13.6.2	Evaluation of Functional specification (ADV_FSP.2)	187
13.6.3	Evaluation of High-level design (ADV_HLD.2)	191
13.6.4	Evaluation of Implementation representation (ADV_IMP.1)	195
13.6.5	Evaluation of Low-level design (ADV_LLD.1)	197
13.6.6	Evaluation of Representation correspondence (ADV_RCR.1)	200
13.6.7	Evaluation of Security policy modeling (ADV_SPM.1)	203
13.7	Guidance documents activity	206
13.7.1	Application notes	206
13.7.2	Evaluation of Administrator guidance (AGD_ADM.1)	206
13.7.3	Evaluation of User guidance (AGD_USR.1)	209
13.8	Life cycle support activity	211
13.8.1	Evaluation of Development security (ALC_DVS.1)	212
13.8.2	Evaluation of Life cycle definition (ALC_LCD.1)	214
13.8.3	Evaluation of Tools and techniques (ALC_TAT.1)	215
13.9	Tests activity	217
13.9.1	Application notes	217
13.9.2	Evaluation of Coverage (ATE_COV.2)	218
13.9.3	Evaluation of Depth (ATE_DPT.1)	220
13.9.4	Evaluation of Functional tests (ATE_FUN.1)	222
13.9.5	Evaluation of Independent testing (ATE_IND.2)	227
13.10	Vulnerability assessment activity	232
13.10.1	Evaluation of Misuse (AVA_MSU.2)	232
13.10.2	Evaluation of Strength of TOE security functions (AVA_SOF.1)	236
13.10.3	Evaluation of Vulnerability analysis (AVA_VLA.2)	238
14	Flaw remediation sub-activities	250
14.1	Evaluation of flaw remediation (ALC_FLR.1)	250
14.1.1	Objectives	250

14.1.2	Input	250
14.1.3	Action ALC_FLR.1.1E	250
14.2	Evaluation of flaw remediation (ALC_FLR.2)	252
14.2.1	Objectives	252
14.2.2	Input	252
14.2.3	Action ALC_FLR.2.1E	252
14.3	Evaluation of flaw remediation (ALC_FLR.3)	255
14.3.1	Objectives	255
14.3.2	Input	255
14.3.3	Action ALC_FLR.3.1E	255
Annex A	(normative) General evaluation guidance	260
A.1	Objectives	260
A.2	Sampling	260
A.3	Consistency analysis	262
A.4	Dependencies	264
A.4.1	Dependencies between activities	264
A.4.2	Dependencies between sub-activities	264
A.4.3	Dependencies between actions	264
A.5	Site Visits	264
A.6	TOE Boundary	265
A.6.1	Product and system	265
A.6.2	TOE	266
A.6.3	TSF	266
A.6.4	Evaluation	266
A.6.5	Certification	267
A.7	Threats and FPT Requirements	267
A.7.1	TOEs not necessarily requiring the FPT class	268
A.7.2	Impact upon Assurance Families	268
A.8	Strength of function and vulnerability analysis	269
A.8.1	Attack potential	270
A.8.2	Calculating attack potential	271
A.8.3	Example strength of function analysis	274
A.9	Scheme Responsibilities	275

Foreword

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

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

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

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

ISO/IEC 18045 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*. The identical text of ISO/IEC 18045 is published by the Common Criteria Project Sponsoring Organisations as *Common Methodology for Information Technology Security Evaluation*.

Legal notice

The governmental organizations listed below contributed to the development of this version of the Common Methodology for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Methodology for Information Technology Security Evaluations, version 2.3 (called CEM 2.3), they hereby grant non-exclusive license to ISO/IEC to use CEM 2.3 in the continued development/maintenance of the ISO/IEC 18045 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CEM 2.3 as they see fit.

Australia/New Zealand:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Canada:	Communications Security Establishment;
France:	Direction Centrale de la Sécurité des Systèmes d'Information;
Germany:	Bundesamt für Sicherheit in der Informationstechnik;
Japan:	Information Technology Promotion Agency;
Netherlands:	Netherlands National Communications Security Agency;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

Introduction

The methodology for IT security evaluation presented in this International Standard is limited to evaluations for EAL1 through EAL4, as defined in ISO/IEC 15408. It does not provide guidance for EALs 5 through 7, nor for evaluations using other assurance packages.

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

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

Information technology — Security techniques — Methodology for IT security evaluation

1 Scope

This International Standard is a companion document to ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security*. This International Standard describes the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408.

2 Normative references

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

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

3 Terms and definitions

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

NOTE Bold-faced type is used in the definitions to indicate terms which are themselves defined in this clause.

3.1

action

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

3.2

activity

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

3.3

check

to generate a **verdict** by a simple comparison. Evaluator expertise is not required. The statement that uses this verb describes what is mapped.

3.4

evaluation deliverable

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

3.5

evaluation evidence

a tangible **evaluation deliverable**.

3.6

evaluation technical report

a report that documents the **overall verdict** and its justification, produced by the evaluator and submitted to an overseer.

3.7

examine

to generate a **verdict** by analysis using evaluator expertise. The statement that uses this verb identifies what is analysed and the properties for which it is analysed.

3.8

interpretation

a clarification or amplification of an ISO/IEC 15408, ISO/IEC 18045 or **scheme** requirement.

3.9

methodology

the system of principles, procedures and processes applied to IT security evaluations.

3.10

observation report

a report written by the evaluator requesting a clarification or identifying a problem during the evaluation.

3.11

overall verdict

a *pass or fail* statement issued by an evaluator with respect to the result of an evaluation.

3.12

oversight verdict

a statement issued by an overseer confirming or rejecting an *overall verdict* based on the results of evaluation oversight activities.

3.13

record

to retain a written description of procedures, events, observations, insights and results in sufficient detail to enable the work performed during the evaluation to be reconstructed at a later time.

3.14

report

to include evaluation results and supporting material in the **evaluation technical report** or an **observation report**.

3.15

scheme

set of rules, established by an evaluation authority, defining the evaluation environment, including criteria and **methodology** required to conduct IT security evaluations.

3.16

sub-activity

the application of an assurance component of ISO/IEC 15408-3. Assurance families are not explicitly addressed in this International Standard because evaluations are conducted on a single assurance component from an assurance family.

3.17

tracing

a simple directional relation between two sets of entities, which shows which entities in the first set correspond to which entities in the second.

3.18**verdict**

a *pass*, *fail* or *inconclusive* statement issued by an evaluator with respect to an ISO/IEC 15408 evaluator action element, assurance component, or class. Also see **overall verdict**.

3.19**work unit**

the most granular level of evaluation work. Each evaluation methodology action comprises one or more work units, which are grouped within the evaluation methodology action by ISO/IEC 15408 content and presentation of evidence or developer action element. The work units are presented in this International Standard in the same order as ISO/IEC 15408 elements from which they are derived. Work units are identified in the left margin by a symbol such as 4:ALC_TAT.1-2. In this symbol, the first digit (4) indicates the EAL; the string ALC_TAT.1 indicates ISO/IEC 15408 component (i.e. this International Standard sub-activity), and the final digit (2) indicates that this is the second work unit in the ALC_TAT.1 sub-activity.

4 Symbols and abbreviated terms

ETR Evaluation Technical Report

OR Observation Report

5 Overview**5.1 Organisation of this International Standard**

Clause 6 defines the conventions used in this International Standard.

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

Clause 8 defines the evaluation of a PP.

Clause 9 defines the evaluation of an ST.

Clauses 10 to 13 define the minimal evaluation effort for achieving EAL1 to EAL4 evaluations and to provide guidance on ways and means of accomplishing the evaluation.

Clause 14 defines the flaw remediation evaluation activities.

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

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 International Standard 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. For example, because an additional work unit labeled 4:ADV_FSP.2-7 was added at EAL4, the subsequent sequential numbering of FSP work units is offset by one. Thus work unit 3:ADV_FSP.1-8 is now mirrored by work unit 4:ADV_FSP.2-9; each express the same requirement though their numbering no longer directly correspond.

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 described method is normative, meaning that the verb usage is in accordance with ISO definitions for these verbs; that is: the auxiliary verb *should* is used when the described method is strongly preferred and the auxiliary verb *may* is used where the described method(s) is allowed but no preference is indicated. (The auxiliary verb *shall* is used only for the text of work units.)

The verbs *check*, *examine*, *report* and *record* are used with a precise meaning within this International Standard and the 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 International Standard. 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.

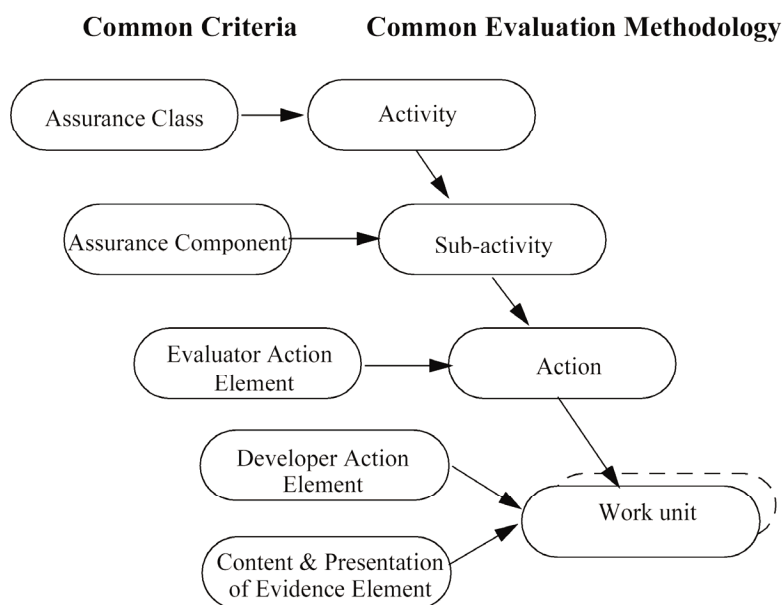


Figure 1 - Mapping of ISO/IEC 15408 and ISO/IEC 18045 structures

6.5 Evaluator verdicts

The evaluator assigns verdicts to the requirements of ISO/IEC 15408 and not to those of this International Standard. 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, Subclause 6.3.

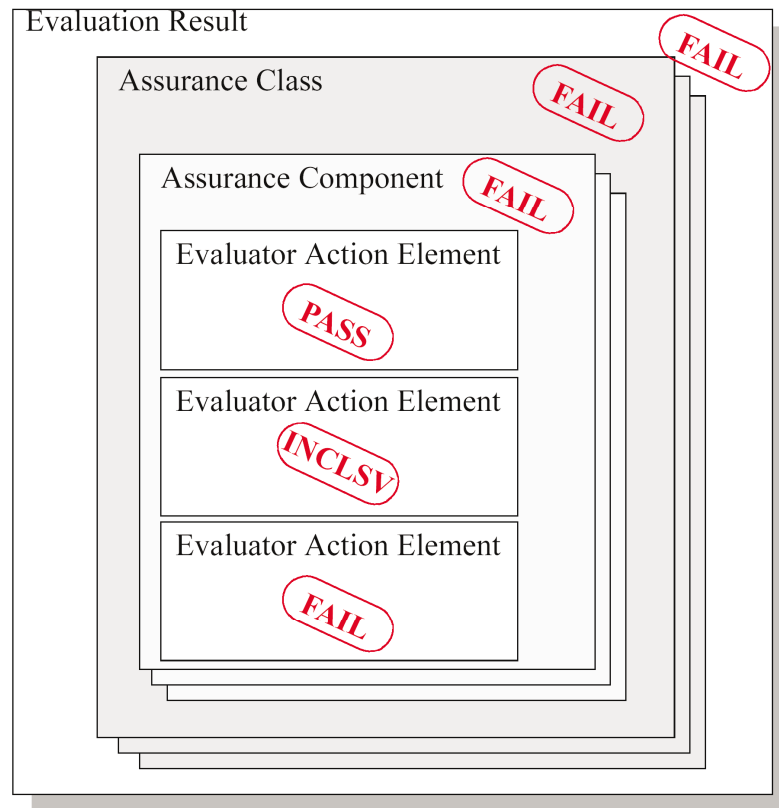


Figure 2 - Example of the verdict assignment rule

This International Standard recognises three mutually exclusive verdict states:

- 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 the constituent work units of the related evaluation methodology action;
- Conditions for an *inconclusive* verdict are defined as an evaluator incompleteness of one or more work units of the evaluation methodology action related to ISO/IEC 15408 evaluator action element;
- 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.

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 2, 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 General evaluation tasks

7.1 Introduction

All evaluations, whether of a PP or TOE (including ST), have two evaluator tasks in common: the input task and the output task. These two tasks, which are related to management of evaluation evidence and to report

generation, are 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).

Although ISO/IEC 15408 does not mandate specific requirements on these evaluation tasks, this International Standard does so where it is necessary. In contrast to the activities described elsewhere in this International Standard, these 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 comply with this International Standard.

7.2 Evaluation input task

7.2.1 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.

7.2.2 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, evaluation evidence pertaining to all products that are part of the TOE is 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 products that are part of the TOE. For example, if a high-level design is required, then the High-level design (ADV_HLD) 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 (ACM_CAP) and Delivery (ADO_DEL)) will also apply to the entire TOE (including any product from 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 documentation (e.g. in the case of a TOE not originally developed to meet the requirements of ISO/IEC 15408).

7.2.3 Management of evaluation evidence sub-task

7.2.3.1 Configuration control

The evaluator shall perform configuration control of the evaluation evidence.

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

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

7.2.3.2 Disposal

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

- a) returning the evaluation evidence;
- b) archiving the evaluation evidence;
- c) destroying the evaluation evidence.

7.2.3.3 Confidentiality

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

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

7.3 Evaluation output task

7.3.1 Objectives

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

Consistent reporting of evaluation results facilitates the achievement of the universal principle of repeatability and reproducibility of results. The consistency covers the type and the amount of information reported in the ETR and OR. ETR and OR consistency among different evaluations is the responsibility of the overseer.

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

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

7.3.2 Application notes

In this version of this International Standard, the requirements for the provision of evaluator evidence to support re-evaluation and re-use have not been explicitly stated. The information resulting from evaluator work to assist in re-evaluation or re-use has not yet been determined by this International Standard under their current work program. 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.

7.3.3 Write OR sub-task

ORs provide the evaluator with a mechanism to request a clarification (e.g. from the overseer 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 additional types, with associated differences in required information and distribution (e.g. evaluation ORs to overseers and sponsors).

7.3.4 Write ETR sub-task

7.3.4.1 Objectives

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

The ETR may contain information proprietary to the developer or the sponsor.

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

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

The ETR supports the overseer in providing the oversight verdict, but it is anticipated that it may not provide all of the information needed for oversight, and the documented results may not provide the evidence necessary for the scheme to confirm that the evaluation was done to the required standard. This aspect is outside the scope of this International Standard and should be met using other oversight methods.

7.3.4.2 ETR for a PP Evaluation

This subclause describes the minimum content of the ETR for a PP evaluation. The contents of the ETR are portrayed in Figure 3; this figure may be used as a guide when constructing the structural outline of the ETR document.

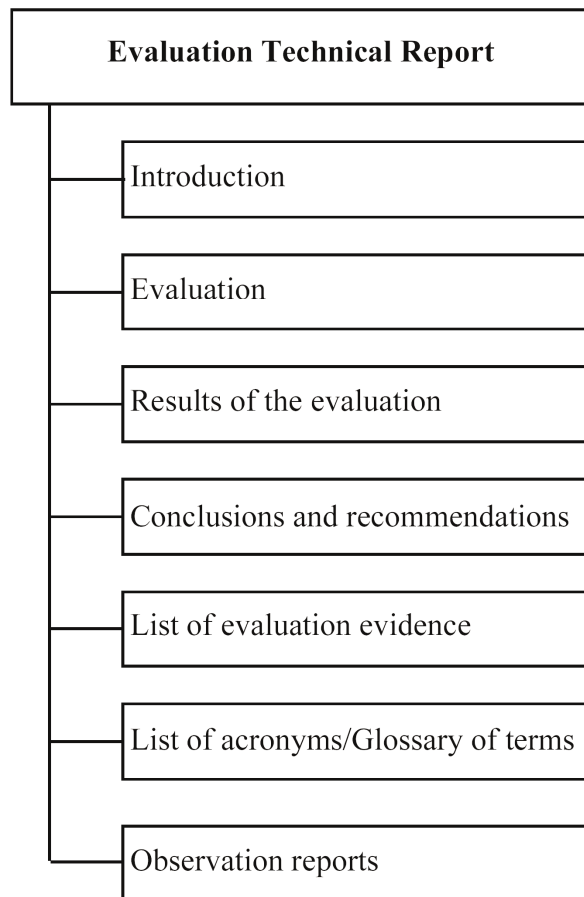


Figure 3 - ETR information content for a PP evaluation

7.3.4.2.1 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 overseer to verify that the verdicts have been assigned correctly by the evaluator.

The evaluator shall report the identity of the developer.

The identity of the PP developer is required to identify the party responsible for producing the PP.

The evaluator shall report the identity of the sponsor.

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

The evaluator shall report the identity of the evaluator.

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

7.3.4.2.2 Evaluation

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

The evaluator references the evaluation criteria, methodology and interpretations used to evaluate the PP.

The evaluator shall report any constraints on the evaluation, constraints on the handling of evaluation results and assumptions made during the evaluation that have an impact on the evaluation results.

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

7.3.4.2.3 Results of the evaluation

The evaluator shall report a verdict and a supporting rationale for each assurance component that constitutes an APE activity, as a result of performing the corresponding evaluation methodology action and its constituent work units.

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

7.3.4.2.4 Conclusions and recommendations

The evaluator shall report the conclusions of the evaluation, in particular the overall verdict as defined in ISO/IEC 15408-1 Clause 6.3, and determined by application of the verdict assignment described in 6.5.

The evaluator provides recommendations that may be useful for the overseer. These recommendations may include shortcomings of the PP discovered during the evaluation or mention of features which are particularly useful.

7.3.4.2.5 List of evaluation evidence

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

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

7.3.4.2.6 List of acronyms/Glossary of terms

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

Terms already defined by ISO/IEC 15408 or by this International Standard need not be repeated in the ETR.

7.3.4.2.7 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.

7.3.4.3 ETR for a TOE Evaluation

This subclause describes the minimum content of the ETR for a TOE 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.

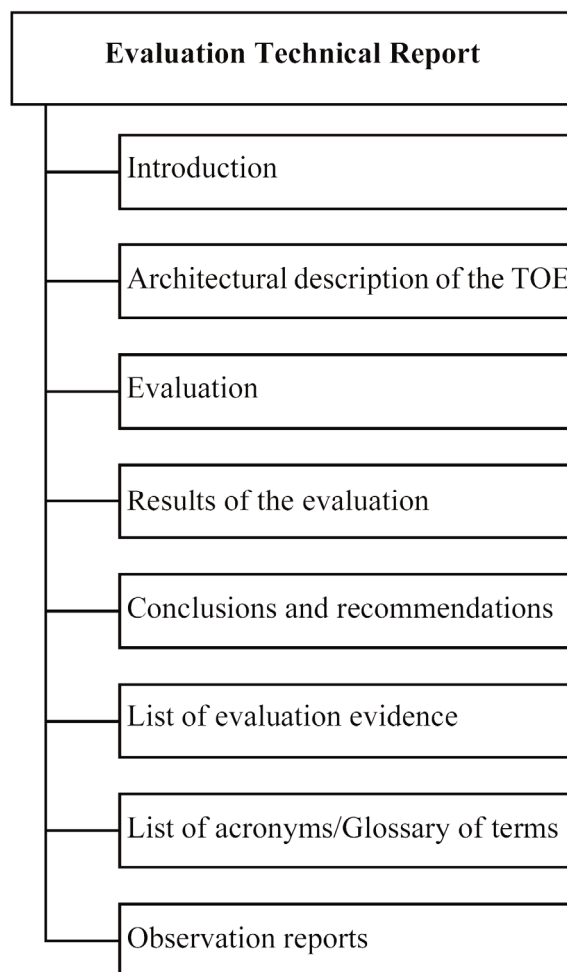


Figure 4 - ETR information content for a TOE evaluation

7.3.4.3.1 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 ST and TOE configuration control identifiers.

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

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

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

The evaluator shall report the identity of the developer.

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

The evaluator shall report the identity of the sponsor.

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

The evaluator shall report the identity of the evaluator.

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

7.3.4.3.2 Architectural description of the TOE

The evaluator shall report a high level description of the TOE and its major components based on the evaluation evidence described in ISO/IEC 15408 assurance family entitled “High-level design (ADV_HLD)”, where applicable.

The intent of this subclause is to characterise the degree of architectural separation of the major components. If there is no High-level design (ADV_HLD) requirement in the ST, this is not applicable and is considered to be satisfied.

7.3.4.3.3 Evaluation

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

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

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

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

7.3.4.3.4 Results of the evaluation

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

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

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

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

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

7.3.4.3.5 Conclusions and recommendations

The evaluator shall report the conclusions of the evaluation, which will relate to whether the TOE has satisfied its associated ST, in particular the overall verdict as defined in ISO/IEC 15408-1 Clause 6.3, and determined by application of the verdict assignment described in 6.5.

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

7.3.4.3.6 List of evaluation evidence

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

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

7.3.4.3.7 List of acronyms/Glossary of terms

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

Terms already defined by ISO/IEC 15408 or by this International Standard need not be repeated in the ETR.

7.3.4.3.8 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.

7.3.5 Evaluation sub-activities

Figure 5 provides an overview of the work to be performed for an evaluation.

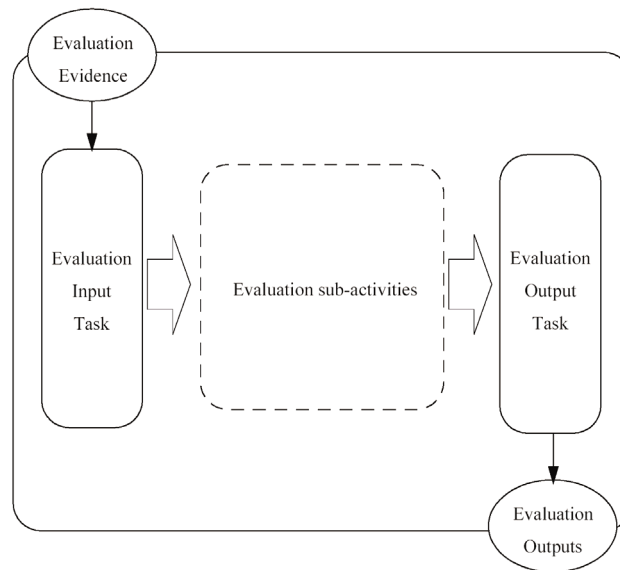


Figure 5 - Generic evaluation model

The evaluation evidence may vary depending upon the type of evaluation (PP evaluations require merely the PP, while TOE evaluations require TOE-specific evidence). Evaluation outputs result in an ETR and possibly ORs. The evaluation sub-activities vary and, in the case of TOE evaluations, depend upon the assurance requirements in ISO/IEC 15408-3.

Each of the Clauses 8 through 13 is organised similarly based on the evaluation work required for an evaluation. Clause 8 addresses the work necessary for reaching an evaluation result on a PP. Clause 9 addresses the work necessary on an ST, although there is no separate evaluation result for this work. Clauses 10 through 13 address the work necessary for reaching an evaluation result on EAL1 through EAL4 (in combination with the ST). Each of these clauses is meant to stand alone and hence may contain some repetition of text that is included in other clauses.

8 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 criteria) that is claimed in the PP. While further clauses in this International Standard are targeted at performing evaluations at specific EALs, this clause is applicable to any PP that is evaluated.

The evaluation methodology in this clause is based on the requirements of the PP as specified in ISO/IEC 15408-1 especially Annex A, and ISO/IEC 15408-3 class APE.

8.2 PP evaluation relationships

The activities to conduct a complete PP evaluation cover the following:

- a) evaluation input task (Clause 7);
- b) PP evaluation activity, comprising the following sub-activities:
 - 1) evaluation of the TOE description (Subclause 8.3.1);
 - 2) evaluation of the security environment (Subclause 8.3.2);
 - 3) evaluation of the PP introduction (Subclause 8.3.3);

- 4) evaluation of the security objectives (Subclause 8.3.4);
 - 5) evaluation of the IT security requirements (Subclause 8.3.5);
 - 6) evaluation of the explicitly stated IT security requirements (Subclause 8.3.6);
- c) evaluation output task (Clause 7).

The evaluation input and evaluation output tasks are described in Clause 7. The evaluation activities are derived from the APE assurance requirements contained in ISO/IEC 15408-3.

The sub-activities comprising a PP evaluation are described in this clause. Although the sub-activities can, in general, be started more or less coincidentally, some dependencies between sub-activities have to be considered by the evaluator. For guidance on dependencies see A.4, Dependencies.

The evaluation of the explicitly stated IT security requirements sub-activity applies only if security requirements not taken from ISO/IEC 15408-2 or ISO/IEC 15408-3 are included in the IT security requirements statement.

8.3 Protection Profile evaluation activity

8.3.1 Evaluation of TOE description (APE_DES.1)

8.3.1.1 Objectives

The objective of this sub-activity is to determine whether the TOE description contains relevant information to aid the understanding of the purpose of the TOE and its functionality, and to determine whether the description is complete and consistent.

8.3.1.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP.

8.3.1.3 Action APE_DES.1.1E

8.3.1.3.1 Work unit APE_DES.1-1

ISO/IEC 15408-3 APE_DES.1.1C: *The TOE description shall describe the product type and the general IT features of the TOE.*

The evaluator shall examine the TOE description to determine that it describes the product or system type of the TOE.

The evaluator determines that the TOE description is sufficient to give the reader a general understanding of the intended usage of the product or system, thus providing a context for the evaluation. Some examples of product or system types are: firewall, smartcard, crypto-modem, web server, intranet.

There are situations where it is clear that some functionality is expected of the TOE because of its product or system type. If this functionality is absent, the evaluator determines whether the TOE description adequately discusses this absence. An example of this is a firewall-type TOE, whose TOE description states that it cannot be connected to networks.

8.3.1.3.2 Work unit APE_DES.1-2

The evaluator shall examine the TOE description to determine that it describes the IT features of the TOE in general terms.

The evaluator determines that the TOE description discusses the IT, and in particular the security features offered by the TOE at a level of detail that is sufficient to give the reader a general understanding of those features.

8.3.1.4 Action APE_DES.1.2E

8.3.1.4.1 Work unit APE_DES.1-3

The evaluator shall examine the PP to determine that the TOE description is coherent.

The statement of the TOE description is coherent if the text and structure of the statement are understandable by its target audience (i.e. developers, evaluators, and consumers).

8.3.1.4.2 Work unit APE_DES.1-4

The evaluator shall examine the PP to determine that the TOE description is internally consistent.

The evaluator is reminded that this subclause of the PP is only intended to define the general intent of the TOE.

For guidance on consistency analysis see A.3, Consistency analysis.

8.3.1.5 Action APE_DES.1.3E

8.3.1.5.1 Work unit APE_DES.1-5

The evaluator shall examine the PP to determine that the TOE description is consistent with the other parts of the PP.

The evaluator determines in particular that the TOE description does not describe threats, security features or configurations of the TOE that are not considered elsewhere in the PP.

For guidance on consistency analysis see A.3, Consistency analysis.

8.3.2 Evaluation of Security environment (APE_ENV.1)

8.3.2.1 Objectives

The objective of this sub-activity is to determine whether the statement of TOE security environment in the PP provides a clear and consistent definition of the security problem that the TOE and its environment is intended to address.

8.3.2.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP.

8.3.2.3 Action APE_ENV.1.1E

8.3.2.3.1 Work unit APE_ENV.1-1

ISO/IEC 15408-3 APE_ENV.1.1C: *The statement of TOE security environment shall identify and explain any assumptions about the intended usage of the TOE and the environment of use of the TOE.*

The evaluator shall examine the statement of TOE security environment to determine that it identifies and explains any assumptions.

The assumptions can be partitioned into assumptions about the intended usage of the TOE, and assumptions about the environment of use of the TOE.

The evaluator determines that the assumptions about the intended usage of the TOE address aspects such as the intended application of the TOE, the potential value of the assets requiring protection by the TOE, and possible limitations of use of the TOE.

The evaluator determines that each assumption about the intended usage of the TOE is explained in sufficient detail to enable consumers to determine that their intended usage matches the assumption. If the assumptions are not clearly understood, the end result may be that consumers will use the TOE in an environment for which it is not intended.

The evaluator determines that the assumptions about the environment of use of the TOE cover the physical, personnel, and connectivity aspects of the environment:

- a) Physical aspects include any assumptions that need to be made about the physical location of the TOE or attached peripheral devices in order for the TOE to function in a secure way. Some examples:
 - it is assumed that administrator consoles are in an area restricted to only administrator personnel;
 - it is assumed that all file storage for the TOE is done on the workstation that the TOE runs on.
- b) Personnel aspects include any assumptions that need to be made about users and administrators of the TOE, or other individuals (including potential threat agents) within the environment of the TOE in order for the TOE to function in a secure way. Some examples:
 - it is assumed that users have particular skills or expertise;
 - it is assumed that users have a certain minimum clearance;
 - it is assumed that administrators will update the anti-virus database monthly.
- c) Connectivity aspects include any assumptions that need to be made regarding connections between the TOE and other IT systems or products (hardware, software, firmware or a combination thereof) that are external to the TOE in order for the TOE to function in a secure way. Some examples:
 - it is assumed that at least 100MB of external disk space is available to store logging files generated by a TOE;
 - the TOE is assumed to be the only non-operating system application being executed at a particular workstation;
 - the floppy drive of the TOE is assumed to be disabled;
 - it is assumed that the TOE will not be connected to an untrusted network.

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

8.3.2.3.2 Work unit APE_ENV.1-2

ISO/IEC 15408-3 APE_ENV.1.2C: *The statement of TOE security environment shall identify and explain any known or presumed threats to the assets against which protection will be required, either by the TOE or by its environment.*

The evaluator shall examine the statement of TOE security environment to determine that it identifies and explains any threats.

If the security objectives for the TOE and its environment are derived from assumptions and organisational security policies only, the statement of threats need not be present in the PP. In this case, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that all identified threats are clearly explained in terms of an identified threat agent, the attack, and the asset that is the subject of the attack.

The evaluator also determines that threat agents are characterised by addressing expertise, resources, and motivation and that attacks are characterised by attack methods, any vulnerabilities exploited, and opportunity.

8.3.2.3.3 Work unit APE_ENV.1-3

ISO/IEC 15408-3 APE_ENV.1.3C: *The statement of TOE security environment shall identify and explain any organisational security policies with which the TOE must comply.*

The evaluator shall examine the statement of TOE security environment to determine that it identifies and explains any organisational security policies.

If the security objectives for the TOE and its environment are derived from assumptions and threats only, organisational security policies need not be present in the PP. In this case, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that organisational security policy statements are made in terms of rules, practices or guidelines that must be followed by the TOE or its environment, as laid down by the organisation controlling the environment in which the TOE is to be used. An example organisational security policy is a requirement for password generation and encryption to conform to a standard stipulated by a national government.

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

8.3.2.4 Action APE_ENV.1.2E

8.3.2.4.1 Work unit APE_ENV.1-4

The evaluator shall examine the statement of TOE security environment to determine that it is coherent.

The statement of the TOE security environment is coherent if the text and structure of the statement are understandable by its target audience (i.e. evaluators and consumers).

8.3.2.4.2 Work unit APE_ENV.1-5

The evaluator shall examine the statement of TOE security environment to determine that it is internally consistent.

Examples of internally inconsistent statements of TOE security environment are:

- a) a statement of TOE security environment that contains a threat where the attack method is not within the capability of its threat agent;
- b) a statement of TOE security environment that contains an organisational security policy "The TOE shall not be connected to the Internet" and a threat where the threat agent is an intruder from the Internet.

For guidance on consistency analysis see A.3, Consistency analysis.

8.3.3 Evaluation of PP introduction (APE_INT.1)

8.3.3.1 Objectives

The objective of this sub-activity is to determine whether the PP introduction is complete and consistent with all parts of the PP and whether it correctly identifies the PP.

8.3.3.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP.

8.3.3.3 Action APE_INT.1.1E

8.3.3.3.1 Work unit APE_INT.1-1

ISO/IEC 15408-3 APE_INT.1.1C: *The PP introduction shall contain a PP identification that provides the labelling and descriptive information necessary to identify, catalogue, register, and cross reference the PP.*

The evaluator shall check that the PP introduction provides PP identification information necessary to identify, catalogue, register and cross reference the PP.

The evaluator determines that the PP identification information includes:

- a) information necessary to control and uniquely identify the PP (e.g. title of the PP, version number, publication date, authors, sponsoring organisation);
- b) indication of the version of ISO/IEC 15408 used to develop the PP;
- c) registration information, if the PP has been registered before evaluation;
- d) cross references, if the PP is compared to other PP(s);
- e) additional information, as required by the scheme.

8.3.3.3.2 Work unit APE_INT.1-2

ISO/IEC 15408-3 APE_INT.1.2C: *The PP introduction shall contain a PP overview which summarises the PP in narrative form.*

The evaluator shall check that the PP introduction provides a PP overview in narrative form.

The PP overview is intended to provide a brief summary of the content of the PP (a more detailed description is provided in the TOE description) that is sufficiently detailed to enable a potential user of the PP to determine whether the PP is of interest.

8.3.3.4 Action APE_INT.1.2E

8.3.3.4.1 Work unit APE_INT.1-3

The evaluator shall examine the PP introduction to determine that it is coherent.

The PP introduction is coherent if the text and structure of the statement are understandable by its target audience (i.e. developers, evaluators and consumers).

8.3.3.4.2 Work unit APE_INT.1-4

The evaluator shall examine the PP introduction to determine that it is internally consistent.

The internal consistency analysis will naturally focus on the PP overview that provides a summary of the content of the PP.

For guidance on consistency analysis see A.3, Consistency analysis.

8.3.3.5 Action APE_INT.1.3E

8.3.3.5.1 Work unit APE_INT.1-5

The evaluator shall examine the PP to determine that the PP introduction is consistent with the other parts of the PP.

The evaluator determines that the PP overview provides an accurate summary of the TOE. In particular, the evaluator determines that the PP overview is consistent with the TOE description, and that it does not state or imply the presence of security features that are not in the scope of evaluation.

The evaluator also determines that ISO/IEC 15408 conformance claim is consistent with the rest of the PP.

For guidance on consistency analysis see A.3, Consistency analysis.

8.3.4 Evaluation of Security objectives (APE_OBJ.1)

8.3.4.1 Objectives

The objective of this sub-activity is to determine whether the security objectives are described completely and consistently, and to determine whether the security objectives counter the identified threats, achieve the identified organisational security policies and are consistent with the stated assumptions.

8.3.4.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP.

8.3.4.3 Action APE_OBJ.1.1E

8.3.4.3.1 Work unit APE_OBJ.1-1

ISO/IEC 15408-3 APE_OBJ.1.1C: *The statement of security objectives shall define the security objectives for the TOE and its environment.*

The evaluator shall check that the statement of security objectives defines the security objectives for the TOE and its environment.

The evaluator determines that for each security objective it is clearly specified whether it is intended to apply to the TOE, to the environment, or both.

8.3.4.3.2 Work unit APE_OBJ.1-2

ISO/IEC 15408-3 APE_OBJ.1.2C: *The security objectives for the TOE shall be traced back to aspects of the identified threats to be countered by the TOE and/or organisational security policies to be met by the TOE.*

The evaluator shall examine the security objectives rationale to determine that all security objectives for the TOE are traced back to aspects of the identified threats to be countered and/or aspects of the organisational security policies to be met by the TOE.

The evaluator determines that each security objective for the TOE is traced back to at least one threat or organisational security policy.

Failure to trace implies that either the security objectives rationale is incomplete, the threats or organisational security policy statements are incomplete, or the security objective for the TOE has no useful purpose.

A threat may therefore be addressed entirely by one or more objectives for the environment. An extreme case would be where there are no security objectives for the TOE. Whilst this remains a valid use of the PP/ST construct, a TOE for which all threats and OSPs are addressed by the environment would be of questionable utility, as for such a TOE there would be no security functional requirements for the TOE. Certification/validation of such a TOE is a scheme issue.

8.3.4.3.3 Work unit APE_OBJ.1-3

ISO/IEC 15408-3 APE_OBJ.1.3C: *The security objectives for the environment shall be traced back to aspects of identified threats not completely countered by the TOE and/or organisational security policies or assumptions not completely met by the TOE.*

The evaluator shall examine the security objectives rationale to determine that the security objectives for the environment are traced back to aspects of the identified threats to be countered by the TOE's environment and/or aspects of the organisational security policies to be met by the TOE's environment and/or assumptions to be met in the TOE's environment.

The evaluator determines that each security objective for the environment is traced back to at least one assumption, threat or organisational security policy.

Failure to trace implies that either the security objectives rationale is incomplete, the threats, assumptions or organisational security policy statements are incomplete, or the security objective for the environment has no useful purpose.

8.3.4.3.4 Work unit APE_OBJ.1-4

ISO/IEC 15408-3 APE_OBJ.1.4C: *The security objectives rationale shall demonstrate that the stated security objectives are suitable to counter the identified threats to security.*

The evaluator shall examine the security objectives rationale to determine that for each threat it contains an appropriate justification that the security objectives are suitable to counter that threat.

If no security objectives trace back to the threat, this work unit fails.

The evaluator determines that the justification for a threat demonstrates that if all security objectives that trace back to the threat are achieved, the threat is removed, the threat is diminished to an acceptable level, or the effects of the threat are sufficiently mitigated.

The evaluator also determines that each security objective that traces back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat.

Examples of removing a threat are:

- removing the ability to use an attack method from an agent;
- removing the motivation of a threat agent by deterrence;
- removing the threat agent (e.g. removing machines from a network that frequently crash that network).

Examples of diminishing a threat are:

- restricting the threat agent in attack methods;
- restricting the threat agents in opportunity;
- reducing the likelihood of a launched attack being successful;
- requiring greater expertise or greater resources from the threat agent.

Examples of mitigating the effects of a threat are:

- making frequent back-ups of the asset;
- having spare copies of a TOE;
- frequent changing of keys used in a communication session, so that the effects of breaking one key are relatively minor.

Note that the tracings from security objectives to threats provided in the security objectives rationale may be a part of a justification, but do not constitute a justification by themselves. Even in the case that a security objective is merely a statement reflecting the intent to prevent a particular threat from being realised, a justification is required, but this justification could be quite minimal in this case.

8.3.4.3.5 Work unit APE_OBJ.1-5

ISO/IEC 15408-3 APE_OBJ.1.5C: *The security objectives rationale shall demonstrate that the stated security objectives are suitable to cover all of the identified organisational security policies and assumptions.*

The evaluator shall examine the security objectives rationale to determine that for each organisational security policy it contains an appropriate justification that the security objectives are suitable to cover that organisational security policy.

If no security objectives trace back to the organisational security policy, this work unit fails.

The evaluator determines that the justification for an organisational security policy demonstrates that if all security objectives that trace back to that organisational security policy are achieved, the organisational security policy is implemented.

The evaluator also determines that each security objective that traces back to an organisational security policy, when achieved, actually contributes to the implementation of the organisational security policy.

Note that the tracings from security objectives to organisational security policies provided in the security objectives rationale may be a part of a justification, but do not constitute a justification by themselves. Even in the case that a security objective is merely a statement reflecting the intent to implement a particular organisational security policy, a justification is required, but this justification could be quite minimal in this case.

8.3.4.3.6 Work unit APE_OBJ.1-6

The evaluator shall examine the security objectives rationale to determine that for each assumption it contains an appropriate justification that the security objectives for the environment are suitable to cover that assumption.

If no security objectives for the environment trace back to the assumption, this work unit fails.

An assumption is either an assumption about the intended usage of the TOE, or an assumption about the environment of use of the TOE.

The evaluator determines that the justification for an assumption about the intended usage of the TOE demonstrates that if all security objectives for the environment that trace back to that assumption are achieved, the intended usage is supported.

The evaluator also determines that each security objective for the environment that traces back to an assumption about the intended usage of the TOE, when achieved, actually contributes to the support of the intended usage.

The evaluator determines that the justification for an assumption about the environment of use of the TOE demonstrates that if all security objectives for the environment that trace back to that assumption are achieved, the environment is consistent with the assumption.

The evaluator also determines that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption.

Note that the tracings from security objectives for the environment to assumptions provided in the security objectives rationale may be a part of a justification, but do not constitute a justification by themselves. Even in the case that a security objective of the environment is merely a restatement of an assumption, a justification is required, but this justification could be quite minimal in this case.

8.3.4.4 Action APE_OBJ.1.2E

8.3.4.4.1 Work unit APE_OBJ.1-7

The evaluator shall examine the statement of security objectives to determine that it is coherent.

The statement of security objectives is coherent if the text and structure of the statement are understandable by its target audience (i.e. evaluators and consumers).

8.3.4.4.2 Work unit APE_OBJ.1-8

The evaluator shall examine the statement of security objectives to determine that it is complete.

The statement of security objectives is complete if the security objectives are sufficient to counter all identified threats, and cover all identified organisational security policies and assumptions. This work unit may be performed in conjunction with the APE_OBJ.1-4, APE_OBJ.1-5 and APE_OBJ.1-6 work units.

8.3.4.4.3 Work unit APE_OBJ.1-9

The evaluator shall examine the statement of security objectives to determine that it is internally consistent.

The statement of security objectives is internally consistent if the security objectives do not contradict each other. An example of such a contradiction could be two security objectives as “a user's identity shall never be released”, and “a user's identity shall be available to the other users”.

For guidance on consistency analysis see A.3, Consistency analysis.

8.3.5 Evaluation of IT security requirements (APE_REQ.1)

8.3.5.1 Objectives

The objective of this sub-activity is to determine whether the TOE security requirements (both the TOE security functional requirements and the TOE security assurance requirements) and the security requirements for the IT environment are described completely and consistently, and that they provide an adequate basis for development of a TOE that will achieve its security objectives.

8.3.5.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP.

8.3.5.3 Action APE_REQ.1.1E

8.3.5.3.1 Work unit APE_REQ.1-1

ISO/IEC 15408-3 APE_REQ.1.1C: *The statement of TOE security functional requirements shall identify the TOE security functional requirements drawn from ISO/IEC 15408-2 functional requirements components.*

The evaluator shall check the statement of TOE security functional requirements to determine that it identifies the TOE security functional requirements drawn from ISO/IEC 15408-2 functional requirements components.

The evaluator determines that all TOE security functional requirements components drawn from ISO/IEC 15408-2 are identified, either by reference to an individual component in ISO/IEC 15408-2, or by reproduction in the PP.

8.3.5.3.2 Work unit APE_REQ.1-2

The evaluator shall check that each reference to a TOE security functional requirement component is correct.

The evaluator determines for each reference to a ISO/IEC 15408-2 TOE security functional requirement component whether the referenced component exists in ISO/IEC 15408-2.

8.3.5.3.3 Work unit APE_REQ.1-3

The evaluator shall check that each TOE security functional requirement component that was drawn from ISO/IEC 15408-2 that was reproduced in the PP, is correctly reproduced.

The evaluator determines that the requirements are correctly reproduced in the statement of TOE security functional requirements without examination for permitted operations. The examination for correctness of component operations will be performed in the APE_REQ.1-11 work unit.

8.3.5.3.4 Work unit APE_REQ.1-4

ISO/IEC 15408-3 APE_REQ.1.2C: *The statement of TOE security assurance requirements shall identify the TOE security assurance requirements drawn from ISO/IEC 15408-3 assurance requirements components.*

The evaluator shall check the statement of TOE security assurance requirements to determine that it identifies the TOE security assurance requirements drawn from ISO/IEC 15408-3 assurance requirements components.

The evaluator determines that all TOE security assurance requirements components drawn from ISO/IEC 15408-3 are identified, either by reference to an EAL, or by reference to an individual component in ISO/IEC 15408-3, or by reproduction in the PP.

8.3.5.3.5 Work unit APE_REQ.1-5

The evaluator shall check that each reference to a TOE security assurance requirement component is correct.

The evaluator determines for each reference to a ISO/IEC 15408-3 TOE security assurance requirement component whether the referenced component exists in ISO/IEC 15408-3.

8.3.5.3.6 Work unit APE_REQ.1-6

The evaluator shall check that each TOE security assurance requirement component that was drawn from ISO/IEC 15408-3 that was reproduced in the PP, is correctly reproduced.

The evaluator determines that the requirements are correctly reproduced in the statement of TOE security assurance requirements without examination for permitted operations. The examination for correctness of component operations will be performed in the APE_REQ.1-11 work unit.

8.3.5.3.7 Work unit APE_REQ.1-7

ISO/IEC 15408-3 APE_REQ.1.3C: *The statement of TOE security assurance requirements should include an Evaluation Assurance Level (EAL) as defined in ISO/IEC 15408-3.*

The evaluator shall examine the statement of TOE security assurance requirements to determine that either it includes an EAL as defined in ISO/IEC 15408-3 or appropriately justifies that it does not include an EAL.

If no EAL is included, the evaluator determines that the justification addresses why the statement of TOE assurance requirements contains no EAL. This justification may address the reason why it was impossible, undesirable or inappropriate to include an EAL, or it may address why it was impossible, undesirable or inappropriate to include particular components of the families that constitute EAL1 (CM capabilities (ACM_CAP), Installation, generation and start-up (ADO_IGS), Functional specification (ADV_FSP), Representation correspondence (ADV_RCR), Administrator guidance (AGD_ADM), User guidance (AGD_USR), and Independent testing (ATE_IND)).

8.3.5.3.8 Work unit APE_REQ.1-8

ISO/IEC 15408-3 APE_REQ.1.4C: *The evidence shall justify that the statement of TOE security assurance requirements is appropriate.*

The evaluator shall examine the security requirements rationale to determine that it sufficiently justifies that the statement of TOE security assurance requirements is appropriate.

If the assurance requirements contain an EAL, the justification is allowed to address the choice of that EAL as a whole, rather than addressing all individual components of that EAL. If the assurance requirements contain augmented components to that EAL, the evaluator determines that each augmentation is individually justified. If the assurance requirements contain explicitly stated assurance requirements, the evaluator determines that the use of each explicitly stated assurance requirement is individually justified.

The evaluator determines that the security requirements rationale sufficiently justifies that the assurance requirements are sufficient given the statement of security environment and security objectives. For example, if defence against knowledgeable attackers is required, then it would be inappropriate to specify AVA_VLA.1 Developer vulnerability analysis which is unlikely to detect other than obvious security weaknesses.

The justification may also include reasons such as:

- a) specific requirements imposed by the scheme, national government, or other organisations;
- b) assurance requirements that were dependencies from TOE security functional requirement;
- c) assurance requirements of systems and/or products that are to be used in conjunction with a TOE;
- d) consumer requirements.

An overview of the intent and goals of each EAL is provided in ISO/IEC 15408-3 subclause 10.2.

The evaluator is reminded that determining whether the assurance requirements are appropriate may be subjective and that the analysis of sufficiency of the justification should therefore not be overly rigorous.

If the assurance requirements do not contain an EAL, this work unit may be performed in conjunction with the APE_REQ.1-7 work unit.

8.3.5.3.9 Work unit APE_REQ.1-9

ISO/IEC 15408-3 APE_REQ.1.5C: *The PP shall, if appropriate, identify any security requirements for the IT environment.*

The evaluator shall check that security requirements for the IT environment are identified, if appropriate.

If the PP does not contain security requirements for the IT environment, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that any dependencies of the TOE on other IT in its environment to provide any security functionality in order for the TOE to achieve its security objectives are clearly identified in the PP as security requirements for the IT environment.

An example of a security requirement for the IT environment is a firewall that relies on an underlying operating system to provide authentication of administrators and permanent storage of audit data. In this case, the security requirements for the IT environment would contain components from the FAU: Security audit and FIA: Identification and authentication classes.

Note that the security requirements for the IT environment can contain both functional and assurance requirements.

An example of a dependency on the IT environment is a software crypto-module, which periodically inspects its own code, and disables itself when the code has been tampered with. To allow for recovery, it has the requirement FPT_RCV.2 Automated recovery (automated recovery). As it cannot recover itself once it has disabled itself, this becomes a requirement on the IT environment. One of the dependencies of FPT_RCV.2 Automated recovery is AGD_ADM.1 Administrator guidance (administrator guidance). This assurance requirement therefore becomes an assurance requirement for the IT environment.

The evaluator is reminded that where security requirements for the IT environment refer to the TSF, they refer to the security functions of the environment, rather than security functions of the TOE.

8.3.5.3.10 Work unit APE_REQ.1-10

ISO/IEC 15408-3 APE_REQ.1.6C: *All completed operations on IT security requirements included in the PP shall be identified.*

The evaluator shall check that all completed operations on IT security requirements are identified.

It is permissible for a PP to contain elements with uncompleted operations. That is, the PP can contain IT security requirement statements that include uncompleted operations for assignment or selection. The operations have then to be completed in an ST instantiating the PP. This gives the ST developer more flexibility in developing the TOE and the corresponding ST that claims compliance to a particular PP.

The permitted operations for ISO/IEC 15408-2 and ISO/IEC 15408-3 components are assignment, iteration, selection and refinement. The assignment and selection operations are permitted only where specifically indicated in a component. Iteration and refinement are permitted for all components.

The evaluator determines that all operations are identified in each component where such an operation is used. Completed and uncompleted operations need to be identified in such a way, that they can be distinguished, and that it is clear whether the operation is completed or not. Identification can be achieved by typographical distinctions, or by explicit identification in the surrounding text, or by any other distinctive means.

8.3.5.3.11 Work unit APE_REQ.1-11

The evaluator shall examine the statement of IT security requirements to determine that operations are performed correctly.

The evaluator is reminded that operations on security requirements need not be performed and completed in a PP.

The evaluator compares each statement with the element from which it is derived to determine that:

- a) for an assignment, the values of the parameters or variables chosen comply with the indicated type required by the assignment;

- b) for a selection, the selected item or items are one or more of the items indicated within the selection portion of the element. The evaluator also determines that the number of items chosen is appropriate for the requirement. Some requirements require a selection of just one item (e.g. FAU_GEN.1.1.b), in other cases multiple items (e.g. FDP_ITT.1.1 second operation) are acceptable;
- c) for a refinement, the component is refined in such manner that a TOE meeting the refined requirement also meets the unrefined requirement. If the refined requirement exceeds this boundary it is considered to be an extended requirement;

Example: ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modelled. Refinement: The TSP model need cover only access control. If the access control policy is the only policy of the TSP this is a valid refinement. If there are also identification and authentication policies in the TSP, and the refinement is meant to state that only access control needs to be modeled, then this is not a valid refinement.

A special case of refinement is an editorial refinement, where a small change is made in a requirement, i.e. rephrasing a sentence due to adherence to proper English grammar. This change is not allowed to modify the meaning of the requirement in any way.

An example of an editorial refinement is FAU_ARP.1 with a single action. Instead of writing: "The TSF shall take inform the operator upon detection of a potential security violation" the PP author is allowed to write: "The TSF shall inform the operator upon detection of a potential security violation".

The evaluator is reminded that editorial refinements have to be clearly identified (see work unit APE_REQ.1-10).

- d) for an iteration, that each iteration of a component is different from each other iteration of that component (at least one element of a component is different from the corresponding element of the other component), or that the component applies to a different part of the TOE.

8.3.5.3.12 Work unit APE_REQ.1-12

ISO/IEC 15408-3 APE_REQ.1.7C: *Any uncompleted operations on IT security requirements included in the PP shall be identified.*

The evaluator shall examine the statement of IT security requirements to determine that all uncompleted operations are identified.

The evaluator determines that all operations are identified in each component where such an operation is used. Completed and uncompleted operations need to be identified in such a way, that they can be distinguished, and that it is clear whether the operation is completed or not. Identification can be achieved by typographical distinctions, or by explicit identification in the surrounding text, or by any other distinctive means.

8.3.5.3.13 Work unit APE_REQ.1-13

ISO/IEC 15408-3 APE_REQ.1.8C: *Dependencies among the IT security requirements included in the PP should be satisfied.*

The evaluator shall examine the statement of IT security requirements to determine that dependencies required by the components used in the IT security requirements statement are satisfied.

Dependencies may be satisfied by the inclusion of the relevant component (or one that is hierarchical to it) within the statement of TOE security requirements, or as a requirement that is asserted as being met by the IT environment of the TOE.

Although ISO/IEC 15408 provides support for dependency analysis by inclusion of dependency, this is not a justification that no other dependencies exist. An example of such other dependencies is an element that refers to "all objects" or "all subjects", where a dependency could exist to a refinement in another element or set of elements where the objects or subjects are enumerated.

Dependencies of security requirements necessary in the IT environment should be stated and satisfied in the PP.

The evaluator is reminded that ISO/IEC 15408 does not require all dependencies to be satisfied: see the following work-unit.

8.3.5.3.14 Work unit APE_REQ.1-14

ISO/IEC 15408-3 APE_REQ.1.9C: *The evidence shall justify why any non-satisfaction of dependencies is appropriate.*

The evaluator shall examine the security requirements rationale to determine that an appropriate justification is given for each case where security requirement dependencies are not satisfied.

The evaluator determines that the justification explains why the dependency is unnecessary, given the identified security objectives.

The evaluator confirms that any non-satisfaction of a dependency does not prevent the set of security requirements adequately addressing the security objectives. This analysis is addressed by APE_REQ.1.13C.

An example of an appropriate justification is when a software TOE has the security objective: “failed authentications shall be logged with user identity, time and date” and uses FAU_GEN.1 Audit data generation (audit data generation) as a functional requirement to satisfy this security objective. FAU_GEN.1 Audit data generation contains a dependency on FPT_STM.1 Reliable time stamps (reliable time stamps). As the TOE does not contain a clock mechanism, FPT_STM.1 Reliable time stamps is defined by the PP author as a requirement on the IT environment. The PP author indicates that this requirement will not be satisfied with the justification: “there are attacks possible on the time-stamping mechanism in this particular environment, the environment can therefore not deliver a reliable time-stamp. Yet, some threat agents are incapable of executing attacks against the time-stamping mechanisms, and some attacks by these threat agents may be analysed by logging time and date of their attacks.”

8.3.5.3.15 Work unit APE_REQ.1-15

ISO/IEC 15408-3 APE_REQ.1.10C: *The PP shall include a statement of the minimum strength of function level for the TOE security functional requirements, either SOF-basic, SOF-medium or SOF-high, as appropriate.*

The evaluator shall check that the PP includes a statement of the minimum strength of function level for the TOE security functional requirements, and that this level is either SOF-basic, SOF-medium or SOF-high.

If the TOE security assurance requirements do not include AVA_SOF.1 Strength of TOE security function evaluation, this work unit is not applicable and is therefore considered to be satisfied.

The strength of cryptographic algorithms is outside the scope of ISO/IEC 15408. Strength of function only applies to probabilistic or permutational mechanisms that are non-cryptographic. Therefore, where an PP contains a minimum SOF claim this claim does not apply to any cryptographic mechanisms with respect to an ISO/IEC 15408 evaluation. Where such cryptographic mechanisms are included in a TOE the evaluator determines that the PP includes a clear statement that the assessment of algorithmic strength does not form part of the evaluation.

The TOE may contain multiple distinct domains, where the PP writer deems it to be more applicable to have a minimum strength of function level for each domain, rather than having one overall minimum strength of function level for the entire TOE. In this case it is allowed to partition the TOE security functional requirements in distinct sets, and have different minimum strength of function levels associated with each set.

An example of this is a distributed terminal system which has user terminals that are in a public space, and administrator terminals that are in a physically secure place. The authentication requirements for the user terminals have SOF-medium associated with them, and the authentication requirements for the administrative terminals have SOF-basic associated with them. Rather than stating that the TOE has a minimum strength of

function level of SOF-basic, which might lead potential consumers of the TOE to believe that it would be relatively easy to successfully attack the authentication mechanisms on user terminals, the PP writer divides the TOE into a user domain and an administrative domain, partitions the TOE security functional requirements into sets belonging to those domains, assigns a minimum strength of function level of SOF-basic to the set belonging to the administrative domain, and assigns a minimum strength of function level of SOF-medium to the set belonging to the user domain.

8.3.5.3.16 Work unit APE_REQ.1-16

ISO/IEC 15408-3 APE_REQ.1.11C: *The statement of security requirements shall identify all security functional requirements for which an explicit strength of function claim is required, together with the explicit strength of function claim for each such security functional requirement.*

The evaluator shall check that the PP identifies any specific TOE security functional requirements for which an explicit strength of function is appropriate, together with the specific strength of function or metric as applicable.

If the TOE security assurance requirements do not include AVA_SOF.1 Strength of TOE security function evaluation, this work unit is not applicable and is therefore considered to be satisfied.

The explicit strength of function claim can be either SOF-basic, SOF-medium, SOF-high, or a defined specific metric. Where a specific metric is used, the evaluator determines that these are appropriate for the type of functional requirement specified, and that the metric specified is evaluatable as a strength claim. This work unit refers to the case where a PP author requires to set specific SOF requirements (i.e. higher than the overall SOF claim of the PP) or by using a metric. A specific SOF claim for a TOE security functional requirement may be specified by a PP author. In the absence of any specific claim, the overall claim for the PP applies for all TOE security functional requirements stated in the PP. The evaluator should confirm the presence or absence of explicit SOF claims is consistent with other parts of the PP.

A PP could potentially have varying specifications of SOF claims. There can be an overall SOF claim for a PP and within a PP the TOE security functional requirements could have a SOF claim specified for it.

Further guidance on appropriateness and suitability of strength of function metrics may be provided by the scheme.

8.3.5.3.17 Work unit APE_REQ.1-17

ISO/IEC 15408-3 APE_REQ.1.12C: *The security requirements rationale shall demonstrate that the minimum strength of function level for the PP, together with any explicit strength of function claim, is consistent with the security objectives for the TOE.*

The evaluator shall examine the security requirements rationale to determine that it demonstrates that the minimum strength of function level, together with any explicit strength of function claim, is consistent with the security objectives for the TOE.

If the TOE security assurance requirements do not include AVA_SOF.1 Strength of TOE security function evaluation, this work unit is not applicable and is therefore considered to be satisfied.

The evaluator determines that the rationale takes into account details about the likely expertise, resources, and motivation of attackers as described in the statement of TOE security environment. For example, a claim of SOF-basic is inappropriate if the TOE is required to provide defence against attackers who possess a high attack potential.

The evaluator also determines that the rationale takes into account any specific strength-related properties of security objectives. The evaluator can use the tracings from requirements to objectives to determine that requirements that trace towards objectives with specific strength related properties, if appropriate, have a suitable strength of function claim associated with them.

8.3.5.3.18 Work unit APE_REQ.1-18

ISO/IEC 15408-3 APE_REQ.1.13C: *The security requirements rationale shall demonstrate that the IT security requirements are suitable to meet the security objectives.*

The evaluator shall examine the security requirements rationale to determine that the TOE security requirements are traced back to the security objectives for the TOE.

The evaluator determines that each TOE security functional requirement is traced back to at least one security objective for the TOE.

Failure to trace implies that either the security requirements rationale is incomplete, the security objectives are incomplete, or that the TOE security functional requirement has no useful purpose.

It is also allowed, but not mandatory, for some or all TOE security assurance requirements to trace back to security objectives for the TOE.

An example of a TOE security assurance requirement tracing back to a security objective for the TOE is a PP containing the threat "A user unwittingly discloses information by using a device thinking it to be the TOE" and the security objective for the TOE "The TOE shall be clearly labelled with its version number" to counter that threat. This security objective for the TOE can be achieved by satisfying ACM_CAP.1 Version numbers and the PP author therefore traces ACM_CAP.1 Version numbers back to that security objective for the TOE.

8.3.5.3.19 Work unit APE_REQ.1-19

The evaluator shall examine the security requirements rationale to determine that the security requirements for the IT environment are traced back to the security objectives for the environment.

The evaluator determines that each functional security requirement for the IT environment is traced back to at least one security objective for the environment.

Failure to trace implies that either the security requirements rationale is incomplete, the security objectives for the environment are incomplete, or that the functional security requirement for the IT environment has no useful purpose.

It is also allowed, but not mandatory, for some or all security assurance requirements for the IT environment to trace back to security objectives for the environment.

8.3.5.3.20 Work unit APE_REQ.1-20

The evaluator shall examine the security requirements rationale to determine that for each security objective for the TOE it contains an appropriate justification that the TOE security requirements are suitable to meet that security objective for the TOE.

If no TOE security requirements trace back to the security objective for the TOE, this work unit fails.

The evaluator determines that the justification for a security objective for the TOE demonstrates that if all TOE security requirements that trace back to the objective are satisfied, the security objective for the TOE is achieved.

The evaluator also determines that each TOE security requirement that traces back to a security objective for the TOE, when satisfied, actually contributes to achieving the security objective.

Note that the tracings from TOE security requirements to security objectives for the TOE provided in the security requirements rationale may be a part of the justification, but do not constitute a justification by themselves.

8.3.5.3.21 Work unit APE_REQ.1-21

The evaluator shall examine the security requirements rationale to determine that for each security objective for the IT environment it contains an appropriate justification that the security requirements for the IT environment are suitable to meet that security objective for the IT environment.

If no security requirements for the IT environment trace back to the security objective for the IT environment, this work unit fails.

The evaluator determines that the justification for a security objective for the environment demonstrates that if all security requirements for the IT environment that trace back to the security objective for the IT environment are satisfied, the security objective for the IT environment is achieved.

The evaluator also determines that each security requirement for the IT environment that traces back to a security objective for the IT environment, when satisfied, actually contributes to achieving the security objective.

Note that the tracings from security requirements for the IT environment to security objectives for the IT environment provided in the security requirements rationale may be a part of a justification, but do not constitute a justification by themselves.

8.3.5.3.22 Work unit APE_REQ.1-22

ISO/IEC 15408-3 APE_REQ.1.14C: *The security requirements rationale shall demonstrate that the set of IT security requirements together forms a mutually supportive and internally consistent whole.*

The evaluator shall examine the security requirements rationale to determine that it demonstrates that the set of IT security requirements is internally consistent.

The evaluator determines that on all occasions where different IT security requirements apply to the same types of events, operations, data, tests to be performed etc., and these requirements might conflict, an appropriate justification is provided that this is not the case.

For example, if the PP contains requirements for individual accountability of users as well as requirements for user anonymity, it needs to be shown that these requirements do not conflict. This might involve showing that none of the auditable events requiring individual user accountability relate to operations for which user anonymity is required.

For guidance on consistency analysis see A.3, Consistency analysis.

8.3.5.3.23 Work unit APE_REQ.1-23

The evaluator shall examine the security requirements rationale to determine that it demonstrates that the set of IT security requirements together forms a mutually supportive whole.

This work unit builds on the determination performed in work units APE_REQ.1-18 and APE_REQ.1-19, which examine the tracing from IT security requirements to security objectives and work units APE_REQ.1-20 and APE_REQ.1-21 which examine whether the IT security requirements are suitable to meet the security objectives. This work unit requires the evaluator to consider the possibility that a security objective might in fact not be achieved because of lack of support from other IT security requirements.

This work unit also builds on the dependency analysis addressed by previous work units, because if functional requirement A has a dependency on functional requirement B, B supports A by definition.

The evaluator determines that the security requirements rationale demonstrates that functional requirements support each other where necessary, even when no dependency between these requirements is indicated. This demonstration should address security functional requirements that:

- a) prevent bypass of other security functional requirements, such as FPT_RVM.1 Non-bypassability of the TSP;

- b) prevent tampering with other security functional requirements, such as Domain separation (FPT_SEP);
- c) prevent de-activation of other security functional requirements, such as FMT_MOF.1 Management of security functions behaviour;
- d) enable detection of attacks aimed at defeating other security functional requirements, such as components of the FAU: Security audit class.

The evaluator takes the performed operations into account in his analysis to determine whether they affect the mutual support between the requirements.

8.3.5.4 Action APE_REQ.1.2E

8.3.5.4.1 Work unit APE_REQ.1-24

The evaluator shall examine the statement of IT security requirements to determine that it is coherent.

The statement of IT security requirements is coherent if the text and structure of the statement are understandable by its target audience (i.e. evaluators and consumers).

8.3.5.4.2 Work unit APE_REQ.1-25

The evaluator shall examine the statement of IT security requirements to determine that it is complete.

This work unit draws on the results from the work units required by APE_REQ.1.1E and APE_SRE.1.1E, and in particular the evaluator's examination of the security requirements rationale.

The statement of security requirements is complete if the evaluator judges the security requirements to be sufficient to ensure that all security objectives for the TOE are satisfied.

8.3.5.4.3 Work unit APE_REQ.1-26

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

This work unit draws on the results from the work units required by APE_REQ.1.1E and APE_SRE.1.1E, and in particular the evaluator's examination of the security requirements rationale.

The statement of security requirements is internally consistent if the evaluator determines that no security requirement conflicts with any other security requirement, such that a security objective will not be fully satisfied.

For guidance on consistency analysis see A.3, Consistency analysis.

8.3.6 Evaluation of Explicitly stated IT security requirements (APE_SRE.1)

8.3.6.1 Objectives

The objective of this sub-activity is to determine whether the security functional requirements or security assurance requirements that are stated without reference to ISO/IEC 15408 are appropriate and adequate.

8.3.6.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP.

8.3.6.3 Application notes

This subclause is only applicable if the PP contains IT security requirements that are explicitly stated without reference to either ISO/IEC 15408-2 or ISO/IEC 15408-3. If this is not the case, all work units in this subclause are not applicable, and therefore considered to be satisfied.

The Explicitly stated IT security requirements (APE_SRE) requirements do not replace the IT security requirements (APE_REQ) requirements, but are additional to them. This means that IT security requirements that are explicitly stated without reference to either ISO/IEC 15408-2 or ISO/IEC 15408-3 must be evaluated with the Explicitly stated IT security requirements (APE_SRE) criteria, and also, in combination with all other security requirements, with the IT security requirements (APE_REQ) criteria.

8.3.6.4 Action APE_SRE.1.1E

8.3.6.4.1 Work unit APE_SRE.1-1

ISO/IEC 15408-3 APE_SRE.1.1C: *All TOE security requirements that are explicitly stated without reference to ISO/IEC 15408 shall be identified.*

The evaluator shall check that the statement of the IT security requirements identifies all TOE security requirements that are explicitly stated without reference to ISO/IEC 15408.

Any TOE security functional requirements that are not specified using ISO/IEC 15408-2 functional components are required to be clearly identified as such. Similarly, any TOE security assurance requirements that are not specified using ISO/IEC 15408-3 assurance components are also required to be clearly identified as such.

8.3.6.4.2 Work unit APE_SRE.1-2

ISO/IEC 15408-3 APE_SRE.1.2C: *All security requirements for the IT environment that are explicitly stated without reference to ISO/IEC 15408 shall be identified.*

The evaluator shall check that the statement of IT security requirements identifies all security requirements for the IT environment that are explicitly stated without reference to ISO/IEC 15408.

Any security functional requirements for the IT environment that are not specified using ISO/IEC 15408-2 functional components are required to be clearly identified as such. Similarly, any security assurance requirements for the IT environment that are not specified using ISO/IEC 15408-3 assurance components are also required to be clearly identified as such.

8.3.6.4.3 Work unit APE_SRE.1-3

ISO/IEC 15408-3 APE_SRE.1.3C: *The evidence shall justify why the security requirements had to be explicitly stated.*

The evaluator shall examine the security requirements rationale to determine that it appropriately justifies why each explicitly stated IT security requirement had to be explicitly stated.

The evaluator determines for each explicitly stated IT security requirement that the justification explains why existing functional or assurance components (from ISO/IEC 15408-2 and ISO/IEC 15408-3, respectively) could not be used to express the explicitly stated security requirement in question. The evaluator takes the possibility of performing operations (i.e. assignment, iteration, selection or refinement) on these existing components into account in this determination.

8.3.6.4.4 Work unit APE_SRE.1-4

ISO/IEC 15408-3 APE_SRE.1.4C: *The explicitly stated IT security requirements shall use ISO/IEC 15408 requirements components, families and classes as a model for presentation.*

The evaluator shall examine each explicitly stated IT security requirement to determine that the requirement uses ISO/IEC 15408 requirements components, families and classes as a model for presentation.

The evaluator determines that explicitly stated IT security requirements are presented in the same style as ISO/IEC 15408-2 or ISO/IEC 15408-3 components and to a comparable level of detail. The evaluator also determines that the functional requirements are broken down into individual functional elements and that the assurance requirements specify the developer action, content and presentation of evidence, and evaluator action elements.

8.3.6.4.5 Work unit APE_SRE.1-5

ISO/IEC 15408-3 APE_SRE.1.5C: *The explicitly stated IT security requirements shall be measurable and state objective evaluation requirements such that compliance or noncompliance of a TOE can be determined and systematically demonstrated.*

The evaluator shall examine each explicitly stated IT security requirement to determine that it is measurable and states objective evaluation requirements, such that compliance or noncompliance of a TOE can be determined and systematically demonstrated.

The evaluator determines that functional requirements are stated in such a way that they are testable, and traceable through the appropriate TSF representations. The evaluator also determines that assurance requirements avoid the need for subjective evaluator judgement.

The existing ISO/IEC 15408 functional and assurance requirements are to be used as models for compliance with this requirement.

8.3.6.4.6 Work unit APE_SRE.1-6

ISO/IEC 15408-3 APE_SRE.1.6C: *The explicitly stated IT security requirements shall be clearly and unambiguously expressed.*

The evaluator shall examine each explicitly stated IT security requirement to determine that it is clearly and unambiguously expressed.

The existing ISO/IEC 15408 functional and assurance requirements are to be used as models for compliance with this requirement.

8.3.6.4.7 Work unit APE_SRE.1-7

ISO/IEC 15408-3 APE_SRE.1.7C: *The security requirements rationale shall demonstrate that the assurance requirements are applicable and appropriate to support any explicitly stated TOE security functional requirements.*

The evaluator shall examine the security requirements rationale to determine that it demonstrates that the assurance requirements are applicable and appropriate to support any explicitly stated TOE security functional requirements.

The evaluator determines whether application of the specified assurance requirements will yield a meaningful evaluation result for each explicitly stated security functional requirement, or whether other assurance requirements should have been specified. For example, an explicitly stated functional requirement may imply the need for particular documentary evidence (such as a TSP model), depth of testing, or analysis (such as strength of TOE security functions analysis or covert channel analysis).

8.3.6.5 Action APE_SRE.1.2E

8.3.6.5.1 Work unit APE_SRE.1-8

The evaluator shall examine the statement of IT security requirements to determine that all of the dependencies of any explicitly stated IT security requirement have been identified.

The evaluator confirms that no applicable dependencies have been overlooked by the PP author.

Examples of possible dependencies are: components of the FAU: Security audit class if an explicitly stated functional requirement mentions auditing and Implementation representation (ADV_IMP) if an explicitly stated assurance requirement mentions the source code or implementation representation of the TOE.

9 Security Target evaluation

9.1 Introduction

This clause describes the evaluation of an ST. The ST evaluation is started prior to any TOE evaluation sub-activities since the ST provides the basis and context to perform these sub-activities. A final verdict on the ST may not be possible until the TOE evaluation is complete, since changes to the ST may result from sub-activity findings in the TOE evaluation.

The requirements and methodology for ST evaluation are identical for each ST evaluation, regardless of the EAL (or other set of assurance criteria) that is claimed in the ST. While further clauses in this International Standard are targeted at performing evaluations at specific EALs, this clause is applicable to any ST that is evaluated.

The evaluation methodology in this clause is based on the requirements of the ST as specified in ISO/IEC 15408-1 especially Annex B, and ISO/IEC 15408-3 class ASE.

9.2 ST evaluation relationships

The activities to conduct a complete ST evaluation cover the following:

- a) evaluation input task (Clause 7);
- b) ST evaluation activity, comprising the following sub-activities:
 - 1) evaluation of the TOE description (Subclause 9.3.1);
 - 2) evaluation of the security environment (Subclause 9.3.2);
 - 3) evaluation of the ST introduction (Subclause 9.3.3);
 - 4) evaluation of the security objectives (Subclause 9.3.4);
 - 5) evaluation of the PP claims (Subclause 9.3.5);
 - 6) evaluation of the IT security requirements (Subclause 9.3.6);
 - 7) evaluation of the explicitly stated IT security requirements (Subclause 9.3.7);
 - 8) evaluation of the TOE summary specification (Subclause 9.3.8).
- c) evaluation output task (Clause 7).

The evaluation input and evaluation output tasks are described in Clause 7. The evaluation activities are derived from the ASE assurance requirements contained in ISO/IEC 15408-3.

The sub-activities comprising an ST evaluation are described in this clause. Although the sub-activities can, in general, be started more or less coincidentally, some dependencies between sub-activities have to be considered by the evaluator. For guidance on dependencies see A.4, Dependencies.

The evaluation of the PP claims and the evaluation of the explicitly stated IT security requirements sub-activities do not always have to be performed: the evaluation of the PP claims sub-activity applies only if a PP claim is made, and the evaluation of the explicitly stated IT security requirements sub-activity applies only if

security requirements not taken from ISO/IEC 15408-2 or ISO/IEC 15408-3 are included in the IT security requirements statement.

Some of the information required for the ST may be included by reference. For example if compliance to a PP is claimed, the information in the PP such as the information about the environment and threats is considered to be part of the ST and should conform to the criteria for the ST.

If the ST claims compliance with an evaluated PP, and is largely based on the content of that PP, then it may be possible to reuse the PP evaluation results in performing many of the sub-activities listed above. In particular, reuse may be possible when evaluating the statement of security environment, the security objectives and IT security requirements. It is allowed for an ST to claim compliance with multiple PPs.

9.3 Security Target evaluation activity

9.3.1 Evaluation of TOE description (ASE_DES.1)

9.3.1.1 Objectives

The objective of this sub-activity is to determine whether the TOE description contains relevant information to aid the understanding of the purpose of the TOE and its functionality, and to determine whether the description is complete and consistent.

9.3.1.2 Input

The evaluation evidence for this sub-activity is:

- a) the ST.

9.3.1.3 Application notes

There may be a difference between a TOE and a product that a consumer might purchase. A discussion on this subject can be found in A.6, TOE Boundary.

9.3.1.4 Action ASE_DES.1.1E

9.3.1.4.1 Work unit ASE_DES.1-1

ISO/IEC 15408-3 ASE_DES.1.1C: *The TOE description shall describe the product or system type, and the scope and boundaries of the TOE in general terms both in a physical and a logical way .*

The evaluator shall examine the TOE description to determine that it describes the product or system type of the TOE.

The evaluator determines that the TOE description is sufficient to give the reader a general understanding of the intended usage of the product or system, thus providing a context for the evaluation. Some examples of product or system types are: firewall, smartcard, crypto-modem, web server, intranet.

There are situations where it is clear that some functionality is expected of the TOE because of its product or system type. If this functionality is absent, the evaluator determines whether the TOE description adequately discusses this absence. An example of this is a firewall-type TOE, whose TOE description states that it cannot be connected to networks.

9.3.1.4.2 Work unit ASE_DES.1-2

The evaluator shall examine the TOE description to determine that it describes the physical scope and boundaries of the TOE in general terms.

The evaluator determines that the TOE description discusses the hardware, firmware and software components and/or modules that constitute the TOE at a level of detail that is sufficient to give the reader a general understanding of those components and/or modules.

If the TOE is not identical to a product, the evaluator determines that the TOE description adequately describes the physical relationship between the TOE and the product.

9.3.1.4.3 Work unit ASE_DES.1-3

The evaluator shall examine the TOE description to determine that it describes the logical scope and boundaries of the TOE in general terms.

The evaluator determines that the TOE description discusses the IT, and in particular the security features offered by the TOE at a level of detail that is sufficient to give the reader a general understanding of those features.

If the TOE is not identical to a product, the evaluator determines that the TOE description adequately describes the logical relationship between the TOE and the product.

9.3.1.5 Action ASE_DES.1.2E

9.3.1.5.1 Work unit ASE_DES.1-4

The evaluator shall examine the ST to determine that the TOE description is coherent.

The statement of the TOE description is coherent if the text and structure of the statement are understandable by its target audience (i.e. evaluators and consumers).

9.3.1.5.2 Work unit ASE_DES.1-5

The evaluator shall examine the ST to determine that the TOE description is internally consistent.

The evaluator is reminded that this subclause of the ST is only intended to define the general intent of the TOE.

For guidance on consistency analysis see A.3, Consistency analysis.

9.3.1.6 Action ASE_DES.1.3E

9.3.1.6.1 Work unit ASE_DES.1-6

The evaluator shall examine the ST to determine that the TOE description is consistent with the other parts of the ST.

The evaluator determines in particular that the TOE description does not describe threats, security features or configurations of the TOE that are not considered elsewhere in the ST.

For guidance on consistency analysis see A.3, Consistency analysis.

9.3.2 Evaluation of Security environment (ASE_ENV.1)

9.3.2.1 Objectives

The objective of this sub-activity is to determine whether the statement of TOE security environment in the ST provides a clear and consistent definition of the security problem that the TOE and its environment is intended to address.

9.3.2.2 Input

The evaluation evidence for this sub-activity is:

- a) the ST.

9.3.2.3 Action ASE_ENV.1.1E

9.3.2.3.1 Work unit ASE_ENV.1-1

ISO/IEC 15408-3 ASE_ENV.1.1C: *The statement of TOE security environment shall identify and explain any assumptions about the intended usage of the TOE and the environment of use of the TOE.*

The evaluator shall examine the statement of TOE security environment to determine that it identifies and explains any assumptions.

The assumptions can be partitioned into assumptions about the intended usage of the TOE, and assumptions about the environment of use of the TOE.

The evaluator determines that the assumptions about the intended usage of the TOE address aspects such as the intended application of the TOE, the potential value of the assets requiring protection by the TOE, and possible limitations of use of the TOE.

The evaluator determines that each assumption about the intended usage of the TOE is explained in sufficient detail to enable consumers to determine that their intended usage matches the assumption. If the assumptions are not clearly understood, the end result may be that consumers will use the TOE in an environment for which it is not intended.

The evaluator determines that the assumptions about the environment of use of the TOE cover the physical, personnel, and connectivity aspects of the environment:

- a) Physical aspects include any assumptions that need to be made about the physical location of the TOE or attached peripheral devices in order for the TOE to function in a secure way. Some examples:
 - it is assumed that administrator consoles are in an area restricted to only administrator personnel;
 - it is assumed that all file storage for the TOE is done on the workstation that the TOE runs on.
- b) Personnel aspects include any assumptions that need to be made about users and administrators of the TOE, or other individuals (including potential threat agents) within the environment of the TOE in order for the TOE to function in a secure way. Some examples:
 - it is assumed that users have particular skills or expertise;
 - it is assumed that users have a certain minimum clearance;
 - it is assumed that administrators will update the anti-virus database monthly.
- c) Connectivity aspects include any assumptions that need to be made regarding connections between the TOE and other IT systems or products (hardware, software, firmware or a combination thereof) that are external to the TOE in order for the TOE to function in a secure way. Some examples:
 - it is assumed that at least 100MB of external disk space is available to store logging files generated by a TOE;
 - the TOE is assumed to be the only non-operating system application being executed at a particular workstation;
 - the floppy drive of the TOE is assumed to be disabled;
 - it is assumed that the TOE will not be connected to an untrusted network.

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

9.3.2.3.2 Work unit ASE_ENV.1-2

ISO/IEC 15408-3 ASE_ENV.1.2C: *The statement of TOE security environment shall identify and explain any known or presumed threats to the assets against which protection will be required, either by the TOE or by its environment.*

The evaluator shall examine the statement of TOE security environment to determine that it identifies and explains any threats.

If the security objectives for the TOE and its environment are derived from assumptions and organisational security policies only, the statement of threats need not be present in the ST. In this case, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that all identified threats are clearly explained in terms of an identified threat agent, the attack, and the asset that is the subject of the attack.

The evaluator also determines that threat agents are characterised by addressing expertise, resources, and motivation and that attacks are characterised by attack methods, any vulnerabilities exploited, and opportunity.

9.3.2.3.3 Work unit ASE_ENV.1-3

ISO/IEC 15408-3 ASE_ENV.1.3C: *The statement of TOE security environment shall identify and explain any organisational security policies with which the TOE must comply.*

The evaluator shall examine the statement of TOE security environment to determine that it identifies and explains any organisational security policies.

If the security objectives for the TOE and its environment are derived from assumptions and threats only, organisational security policies need not be present in the ST. In this case, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that organisational security policy statements are made in terms of rules, practices or guidelines that must be followed by the TOE or its environment, as laid down by the organisation controlling the environment in which the TOE is to be used. An example organisational security policy is a requirement for password generation and encryption to conform to a standard stipulated by a national government.

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

9.3.2.4 Action ASE_ENV.1.2E

9.3.2.4.1 Work unit ASE_ENV.1-4

The evaluator shall examine the statement of TOE security environment to determine that it is coherent.

The statement of the TOE security environment is coherent if the text and structure of the statement are understandable by its target audience (i.e. evaluators and consumers).

9.3.2.4.2 Work unit ASE_ENV.1-5

The evaluator shall examine the statement of TOE security environment to determine that it is internally consistent.

Examples of internally inconsistent statements of TOE security environment are:

- a statement of TOE security environment that contains a threat where the attack method is not within the capability of its threat agent;
- a statement of TOE security environment that contains an organisational security policy “The TOE shall not be connected to the Internet” and a threat where the threat agent is an intruder from the Internet.

For guidance on consistency analysis see A.3, Consistency analysis.

9.3.3 Evaluation of ST introduction (ASE_INT.1)

9.3.3.1 Objectives

The objective of this sub-activity is to determine whether the ST introduction is complete and consistent with all parts of the ST and whether it correctly identifies the ST.

9.3.3.2 Input

The evaluation evidence for this sub-activity is:

- a) the ST.

9.3.3.3 Action ASE_INT.1.1E

9.3.3.3.1 Work unit ASE_INT.1-1

ISO/IEC 15408-3 ASE_INT.1.1C: *The ST introduction shall contain an ST identification that provides the labelling and descriptive information necessary to control and identify the ST and the TOE to which it refers.*

The evaluator shall check that the ST introduction provides ST identification information necessary to control and identify the ST and the TOE to which it refers.

The evaluator determines that the ST identification information includes:

- a) information necessary to control and uniquely identify the ST (e.g. title of the ST, version number, publication date, authors);
- b) information necessary to control and uniquely identify the TOE to which the ST refers (e.g. identity of the TOE, version number of the TOE);
- c) indication of the version of ISO/IEC 15408 used to develop the ST;
- d) additional information, as required by the scheme.

9.3.3.3.2 Work unit ASE_INT.1-2

ISO/IEC 15408-3 ASE_INT.1.2C: *The ST introduction shall contain an ST overview which summarises the ST in narrative form.*

The evaluator shall check that the ST introduction provides an ST overview in narrative form.