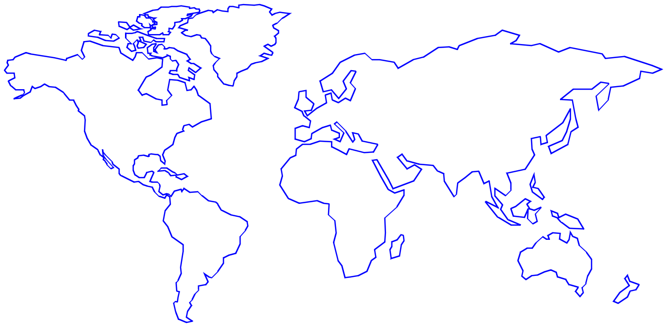
DRAFT



Common Methodology for Information Technology Security Evaluation

CEM-97/052

Part 2 : Evaluation Methodology

Version 0.31

97/09/17

Foreword

This document provides the first version of the Common Evaluation Methodology (CEM) needed to apply the APE (Protection Profile) class requirements of the Common Criteria for Information Technology Security Evaluation (CC).

In general, this CEM is based on Version 1.0 of the CC, although some important and expected changes to version 2.0 have been assumed. Similarly, development of the CEM has proposed changes to the CC. In all cases where the CEM diverges from CC Version 1.0, Annex D describes the deviation.

This document is issued for review by the international security community. Any observation reports should be communicated to the CEM point of contact (cem@cse.dnd.ca) or to one or more of the following points of contact at the sponsoring organisations, using the template for reporting observations included in Annex E:

National Institute of Standards and Technology
Computer Security Division
NIST North Building, Room 426
Gaithersburg, Maryland 20899
U.S.A.
Tel: (+1)(301)975-2934, Fax: (+1)(301)926-2733
E-mail: csd@nist.gov
http://csrc.ncsl.nist.gov

National Security Agency
Attn: V2, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 21122
U.S.A.
Tel: (+1)(410)859-4458, Fax: (+1)(410)684-7512
E-mail: common_criteria@radium.ncsc.mil

Communications Security Establishment
Criteria Coordinator
R2B IT Security Standards and Initiatives
P.O. Box 9703, Terminal
Ottawa, Canada K1G 3Z4
Tel: (+1)(613)991-7409, Fax: (+1)(613)991-7411
E-mail: criteria@cse.dnd.ca
ftp:ftp.cse.dnd.ca
http://www.cse.dnd.ca

Communications Electronic Security Group
Compusec Evaluation Methodology
P.O. Box 144
Cheltenham GL52 5UE
United Kingdom
Tel: (+44) 1242 221 491 ext. 4134
E-mail: criteria@CESG.gov.uk
http://www.cesg.gov.uk/cchtml

Bundesamt für Sicherheit in der Informationstechnik
Abteilung V
Postfach 20 03 63
D-53133 Bonn
Germany
Tel: (+49)228 9582 300, Fax: (+49)228 9582 427
E-mail: cc@bsi.de

Service Central de la Sécurité des Systèmes d'Information
Centre de Certification de la Sécurité des
Technologies de l'Information
18 rue du docteur Zamenhof
92131 Issy les Moulineaux
France
Tel: (+33)(1)41463784, Fax: (+33)(1)41463701
E-mail: ssi20@calva.net

Netherlands National Communications Security Agency
P.O. Box 20061
NL 2500 EB The Hague
The Netherlands
Tel: (+31) 70 3485637, Fax: (+31).70.3486503
E-mail: criteria@nlncsa.minbuza.nl

This document is paginated from i to iv and from 1 to 50

D R A F T

Table of contents

DRAFT

List of figures

D R A F T

Chapter 1

Introduction

1.1 Objective

1 The Common Evaluation Methodology (CEM) is intended to be a companion document to the Common Criteria for Information Technology Security Evaluation (CC). The CEM's purpose is to describe the actions to be performed by an evaluator in order to conduct a CC evaluation.

2 The reader should be familiar with CEM Part 1, Introduction and General Model. CEM Part 1 was released for public review in January 1997 and was written using CCv1.0 as the source material.

1.2 Organisation

3 This part is divided into the following chapters:

4 Chapter 1, Introduction, describes the objective, organisation, document conventions and terminology, and evaluator verdicts.

5 Chapter 2, General evaluation tasks, describes the tasks that are relevant for all evaluation activities. These are the tasks used to manage the inputs and prepare the outputs.

6 Chapter 3, PP evaluation, describes the methodology for the evaluation of Protection Profiles, based on the APE class of CC Part 3.

7 Chapter 4 to 10 *(not included in this version)*, Evaluation methodology for EAL 1 to EAL 7, describes the evaluation methodology for the evaluation assurance levels EAL 1 to EAL 7 defined in CC Part 3 Chapter 4 and Annex D.

8 Chapter 11 *(not included in this version)*, Additional families and components, describes the evaluation methodology for the assurance requirements that are not covered by any EAL such as ADO_IGS.2, ADV_LLD.3, and AVA_CCA.3, and the assurance family ALC_FLR.

9 Annex A, Glossary, defines the terminology used in the CEM.

10 Annex B, PP rationale analysis, provides guidance on the **suitability** and **binding** analysis.

11 Annex C, PP development background, provides information about the derivation of the various requirement abstractions within a PP assumed when drafting the PP evaluation methodology.

12 Annex D, CEM deviations from the CC, summarises all CEM deviations from CCv1.0.

13 Annex E, CEM observation report (CEMOR), details a mechanism by which to comment on the CEM.

1.3 Document conventions and terminology

14 This section describes the terminology and the hierarchical relationship within the CEM structure. It also describes the relationships between the CC and the CEM structures. These relationships are illustrated in Figure 1.1.

15 The term *activity* is used to describe the application of an assurance class of the CC Part 3. This means that every assurance class of the CC is covered by an evaluation activity in the CEM.

16 The term *sub-activity* is related to an assurance component of the CC Part 3. This means that every assurance component is covered by an evaluation sub-activity in the CEM. Assurance families are not explicitly addressed in the CEM because evaluations are conducted on only a single assurance component from each assurance family.

17 The term *action* is related to an evaluator action element of the CC Part 3.

18 The term *work unit* is related to the lowest level of evaluation work. Every CEM action comprises one or more work units, which are grouped within the CEM action by CC content and presentation of evidence element. This means that every content and presentation of evidence element is covered by at least one work unit.

19 All work units and sub-tasks are mandatory and are indicated by prefacing the verb by *shall* and by presenting both verbs in ***bold italic*** type face.

20 The terms *task* and *sub-task* are methodology specific and independent of any CC requirement or terminology.

21 Glossary definitions are presented in bold face type when introduced in this document. The Glossary definitions, presented in Annex A of this part, are provided for only those terms which are used in a specialised way within this document. The majority of terms are used according to their accepted definitions.

22 The verbs **check** and **examine** are used with a special meaning within this part of the CEM and the glossary should be referred to for their definitions.

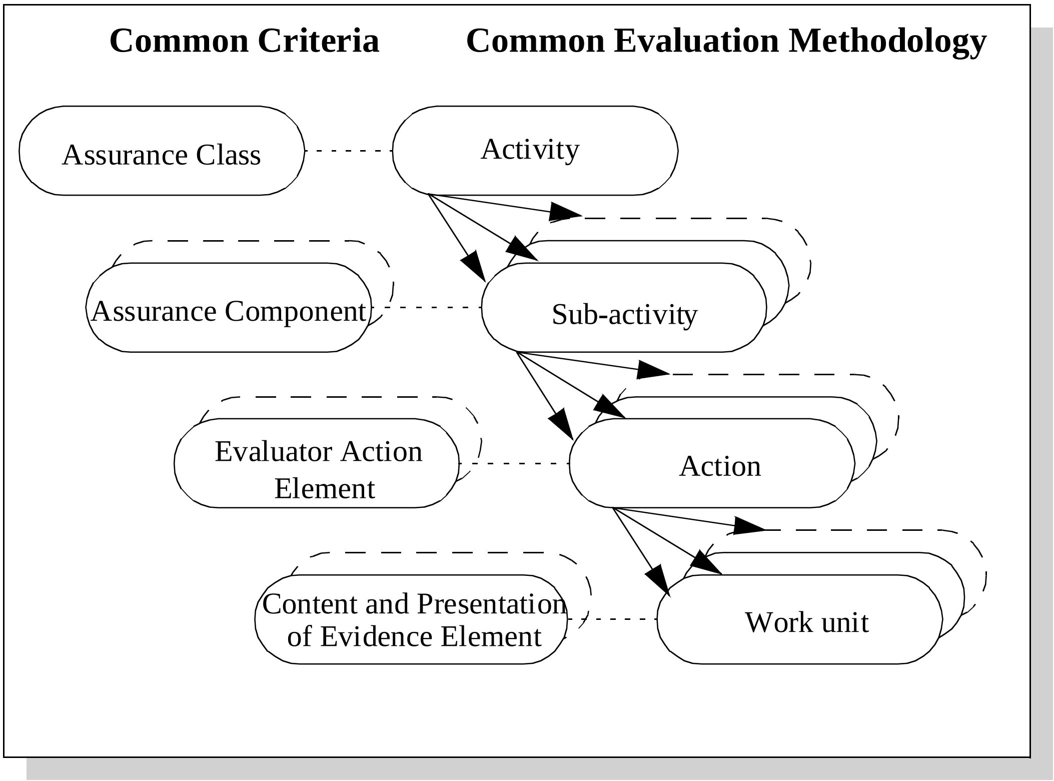


Figure 1.1 - Mapping of the CC and CEM structures

1.4 Evaluator verdicts

23 The evaluator assigns verdicts to the requirement structures of the CC and not to those of the CEM. The most granular CC structure to which a verdict is assigned is the evaluator action element. A verdict is assigned to a CC evaluator action element as a result of performing the corresponding CEM action and its constituent work units.

24 In addition to CC evaluator action elements, verdicts are assigned to CC assurance components and classes. Finally, an evaluation result is assigned, as described in CCv1.0 Part 1, Chapter 3.

25 The CEM recognises three, mutually exclusive, verdict states:

a) Pass, if the evaluator successfully completes a CC evaluator action element. The conditions for successfully completing a CC evaluator action element are defined by the constituent work units of the related CEM action;

b) Inconclusive, if the evaluator has not completed, for any reason, one or more work units of the CEM action related to the CC evaluator action element;

c) Fail, if the evaluator cannot successfully complete one or more work units of the CEM action related to the CC evaluator action element.

26 All verdicts are initially inconclusive and remain so until either a pass or fail verdict is assigned.

27 For the purposes of assignment, verdicts have a hierarchical relationship within the CEM. Lowest in the hierarchy is fail, next highest is inconclusive and, finally, highest in the hierarchy is pass.

28 The verdict assignment rule is: the verdict for a CC assurance requirement structure at any given point in time is equal to the verdict of a constituent structure which has the lowest verdict in the hierarchy of verdicts. For example and as illustrated in Figure 1.2, if the verdict for one evaluator action element is fail then the verdicts for the corresponding assurance component and assurance class are also fail.

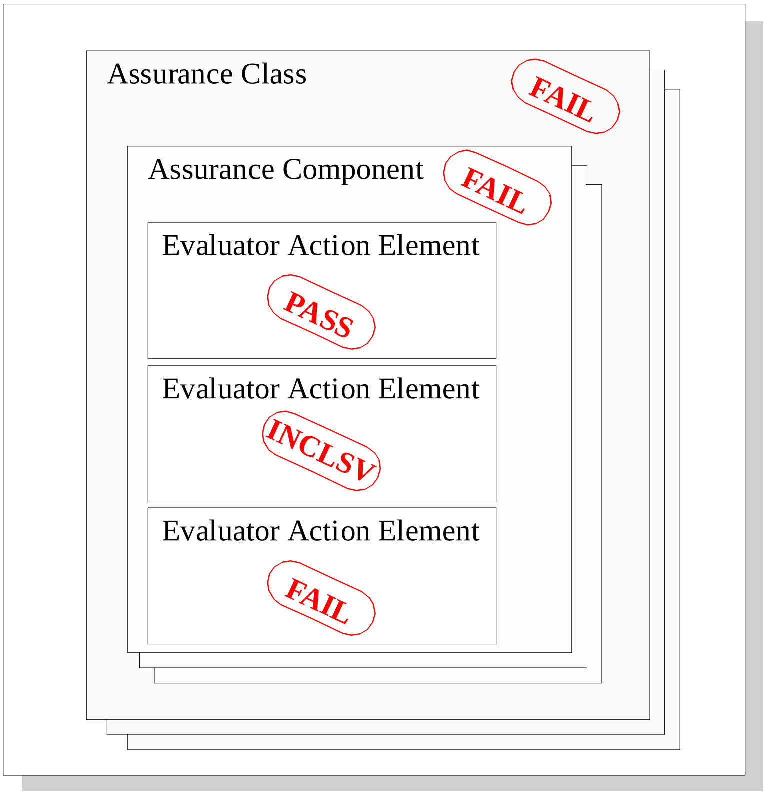


Figure 1.2 - Application example of the verdict assignment rule

Chapter 2

General evaluation tasks

2.1 Introduction

29 All evaluations, whether of a PP or TOE, have two evaluator tasks in common. These two tasks, which are related to management of evaluation evidence and to report generation, are described in this chapter. Each task has associated sub-tasks which apply to, and are normative for, all CC evaluations (evaluation of a PP or a TOE).

30 Although the CC does not mandate specific requirements on these evaluation tasks, the CEM does so where it is necessary to determine conformance with the Universal Principles defined in Part 1 of the CEM. In contrast to the activities described elsewhere in this part of the CEM, these tasks have no verdicts associated with them as they do not map to CC evaluator action elements; they are performed in order to comply with the CEM.

2.2 Evaluation input task

2.2.1 Objective

31 The objective of this task is to ensure that the evaluator has available all necessary evaluation evidence for the evaluation and that it is adequately protected. The sponsor's responsibility is to supply the evaluation evidence, while the evaluator is responsible for the management of the evidence when it is in the evaluator's possession.

2.2.2 Evaluation evidence

32 The management of evaluation evidence is an important aspect in the conduct of an evaluation. The evaluator must be able to determine that the developer's intended evidence is used in the evaluator's analysis; that is, the developer and the evaluator must reference the same version of any item of evidence necessary for the evaluator's analysis. 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. This section describes how the evaluator must manage the evidence in order to maintain cognisance of the correct versions, and to protect them from alteration.

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

34 It is recommended that the evaluator, in conjunction with the sponsor, produces a list of required evaluation evidence. This list of the expected evaluation evidence may be a set of references to the sponsor's documentation.

35 Scheme issues that may need to be covered with a sponsor include national sensitivity and commercial confidentiality of information, access to or requirements for specialist tools, or any limitations imposed on the access of the evaluator to the evaluation evidence and any previous evaluation results.

36 Evaluators require stable and formally-issued versions of evidence. Draft evidence may be provided during an evaluation, for example, to help an evaluator make an early, informal assessment, but are not used as the basis for verdicts. It may be helpful for the evaluator to see draft versions of particular 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.

37 Draft 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 evidence of security which is not provided in the existing documentation (e.g. in the case of a TOE not originally developed to meet the requirements of the CC).

2.2.3 Management of evaluation evidence

2.2.3.1 Configuration control

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

39 The evaluator should be able to identify and locate every item of evaluation evidence after it has been received. The evaluator should be able to determine whether a specific version of a document is in the evaluator’s possession.

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

2.2.3.2 Disposal

41 Following conclusion of an evaluation, the evaluator ***shall dispose*** of the evaluation evidence provided for the conduct of the evaluation in accordance with scheme guidance and consultation with the sponsor.

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

a) returning the evidence;

b) archiving the evidence;

c) destroying the evidence.

2.2.3.3 Confidentiality

43 The evaluator ***shall protect*** the confidentiality of the evaluation evidence provided for the conduct of the evaluation in accordance with the scheme.

44 During their work, evaluators may have access to sponsor and developer commercially-sensitive TOE information, and may have access to nationally-sensitive information. Schemes may wish to impose requirements for the evaluator to maintain the confidentiality of the evaluation evidence. Sponsors and evaluators may mutually agree to additional requirements as long as these are **consistent** with the scheme.

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

2.3 Evaluation output task

2.3.1 Objective

46 The objective of this section is to describe the Evaluation Technical Report (ETR), and the Observation Report (OR). Schemes may require additional evaluator reports such as reports on evaluation methods, reports on individual units of work, or may require additional information to be contained in the ETR and the OR. The CEM does not preclude the addition of information into these reports as the CEM specifies only the minimum information content. For instance, schemes may require that certain introductory material (e.g. disclaimers, scheme logos, and copyright clauses) be recorded in the ETR.

47 In order to achieve the Universal Principle of repeatability and reproducibility and to assure the re-usability of results, evaluation results must be consistently recorded. In order to achieve the CEM requirements for the information content of reports, the evaluator has to perform two sub-tasks:

a) write ETR sub-task;

b) write OR sub-task.

2.3.2 Write ETR sub-task

48 The ETR is written by the evaluator for the overseer. It is intended to support the overseer in providing the oversight verdict. The objective of the ETR is to present all verdicts, their justifications and any findings derived from the work performed during the evaluation. The ETR may contain more details on the PP or TOE and the evaluation process than the Evaluation Summary Report (ESR), and may contain information proprietary to the developer. Secondary audiences of the ETR are the sponsor and any evaluator charged with performing a re-evaluation.

49 Schemes will define the final structure of an ETR. The CEM defines the minimum content requirement.

2.3.2.1 ETR for a PP Evaluation

50 The evaluator ***shall record*** the following information as a minimum:

a) Introduction:

1) all relevant evaluation scheme identifiers;

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

2) ETR configuration control identifiers;

ETR configuration control identifiers (e.g. date and version number) are required to perform the management of evidence sub-task, in particular, configuration control of the ETR.

3) the identity of the developer and the sponsor;

The identity of the PP developer (e.g. individual, organisation, user group or community of interest) is required to identify who is responsible for producing the PP and the identify of the sponsor (e.g., individual, organisation, user group or community of interest) is required to identify who is responsible for providing evaluation deliverables (e.g. new version of the PP implementing changes required to meet failed evaluation requirements) to the evaluator.

4) the identity of the evaluator;

The identity of the evaluator (e.g. individual, team or organisation) is required to identify who performed the evaluation and who is responsible for the evaluation verdicts.

b) PP referred or restated in full:

The PP is required to identify what is being evaluated to the overseer in order for the overseer to verify that the verdicts have been assigned correctly by the evaluator.

c) Results, conclusions and recommendations:

1) for every APE assurance component evaluator action element, as a result of performing the corresponding CEM action and its constituent work units, a verdict and a justification for the verdict (e.g. a description of the work performed) to support the verdict;

2) for every APE assurance component and for the APE assurance class, a verdict based on the application of the verdict assignment rule on constituent CC evaluator action elements;

3) the overall evaluation result, as defined in CCv1.0 Part 1, Chapter 3, and any recommendations relevant to the overall evaluation result;

4) evidence that the CEM tasks and sub-tasks have been completed.

The above information is required in order for overseer to verify that the verdicts have been assigned correctly by the evaluator and to verify that the CEM has been applied by the evaluator.

d) Annex A - Guidance for re-evaluation:

(optional section, can be omitted if the sponsor has stated that re-evaluation information is not required)

1) any way in which the constraints and assumptions of the evaluation would impact re-evaluation or re-use;

2) any lessons regarding evaluation techniques or tools that would be useful for a re-evaluation.

e) Annex B - List of evaluation evidence, acronyms and glossary:

1) a complete list of all observations reports and related correspondence and comments;

2) a complete list of all evaluation evidence and their configuration control identifiers;

3) a list of abbreviations;

4) a glossary of vocabulary.

2.3.3 Write OR sub-task

51 ORs provide the evaluator with a mechanism to request a clarification of or identify a problem with an aspect of the evaluation, e.g. to request clarification from the overseer on the application of a requirement. Specifically in the case of a failure or a fail verdict, the OR may be used to reflect this evaluation result.

52 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 identify different types of ORs, with associated differences in required information and procedures for disposition, e.g. evaluation ORs to overseers and sponsors or CC, CEM and scheme ORs.

53 At a minimum, the evaluator ***shall record*** the following:

a) the identifier of the PP or TOE evaluated;

b) the evaluation task/sub-activity during which the observation was found;

c) the observation;

d) the assessment of its severity;

e) the identification of the organisation responsible for resolving the issue;

f) the recommended timetable for resolution;

g) the assessment of the impacts on the evaluation of failure to resolve the observation.

Chapter 3

PP evaluation

3.1 Introduction

54 This chapter describes the evaluation of Protection Profiles (PP). It is based on the CCv1.0, Part 1, Annex B, where the normative specification of a PP is described and on Part 3, class APE where the evaluation requirements for a PP are presented. As the PP evaluation is based on a single CC class, the evaluation comprises the PP evaluation activity, and the general evaluation input and output tasks that are described in Chapter 2.

3.2 Objective

55 The objective of the PP evaluation is to ensure that the PP is complete, consistent, technically sound, and to determine that the PP provides a meaningful basis for a TOE evaluation. Such a PP may be eligible for inclusion within a PP registry.

3.3 PP evaluation relationships

56 To conduct a complete evaluation of a PP the evaluator has to perform the following:

Editor Note : This section contains deviations from CCv1.0; see Annex D.

a) evaluation input task;

b) PP evaluation activity, comprised of the following sub-activities:

   1) evaluation of the TOE description;

   2) evaluation of the security environment;

   3) evaluation of the PP introduction;

   4) evaluation of the security objectives;

   5) evaluation of the security requirements.

c) evaluation output task.

DRAFT

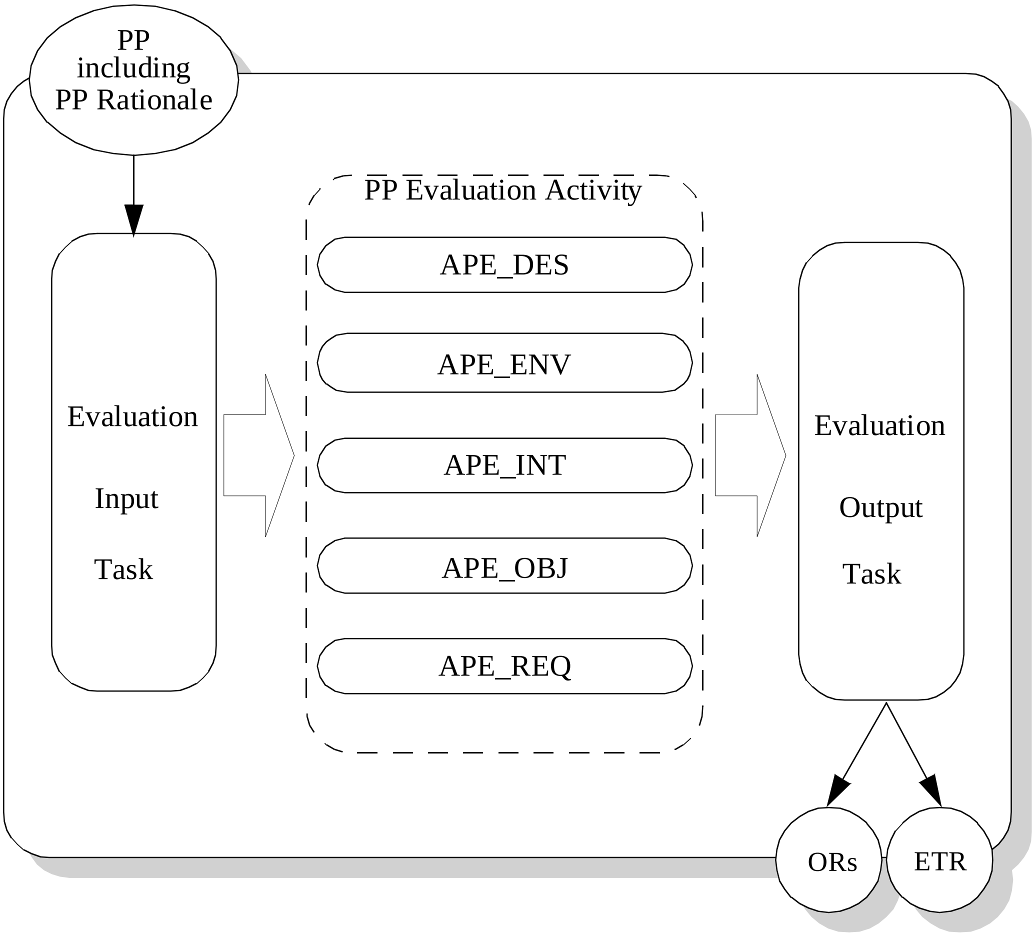


Figure 3.1 - PP evaluation activity and tasks

57 As illustrated in Figure 3.1, the PP evaluation methodology comprises the evaluation input task, the PP evaluation activity, and the evaluation output task. In practice, these tasks and activity will not be performed in sequence but in parallel.

58 The evaluation input task has to be considered and carried out for each family of the APE class. It deals with the organisational and procedural aspects of handling the deliverables for the PP evaluation activity. The evaluation output task describes the record of the evaluation results. This is an ongoing process. During the evaluation the evaluator has to record evaluation results for each evaluator action element. These results will be recorded and justified in the ETR. During the conduct of the evaluation, the evaluator may generate ORs to raise and resolve issues as necessary to progress the evaluation. ORs may be used to support the evaluation results recorded in the ETR, which is the final product of the evaluation output task.

59 The actual evaluation of the PP is described by the PP evaluation activity. For the sequence of these tasks and activity, no order is required. However, it may be the case, that results which are generated by the evaluator during one action are used for performing another action. In general consecutive dependencies are identified for those actions for which output must be completed before any action using that evaluation output can itself complete. Actions for the suitability and binding analysis**,** for example, cannot be completed until the content and presentation checks have been completed. This means that the evaluator has to evaluate the PP rationale after analysing the actual PP.

60 A further dependency occurs in the case of a failure of an evaluator action. If the developer provides an update of the PP, in response to an OR indicating the potential failure, then it may be the case that actions which have been closed before have to be performed again. This case has to be examined carefully by the evaluator.

61 A sub-activity is successfully completed if all its constituent evaluator actions are successfully completed. However, it may be that a future sub-activity will impact a completed sub-activity, requiring previously completed evaluator actions to be re-performed. When determining whether a sub-activity yet to be performed will impact a completed sub-activity, the evaluator must consider whether or not any future sub-activities are dependent upon the completed sub-activity.

62 If dependencies, as defined in the CC, exist between a completed and future sub-activity and, as a result of conducting the future sub-activity a completed sub-activity is deemed to be impacted, then the evaluator must re-perform all impacted evaluator actions.

3.4 PP evaluation activity

3.4.1 Evaluation of the TOE description (APE_DES) sub-activity

Editor Note : This section contains deviations from CCv1.0; see Annex D.

3.4.1.1 Objective

63 The objective of this sub-activity is to ensure that the TOE description contains relevant information to describe the TOE and to aid the understanding of its security requirements and that it is described completely and consistently.

3.4.1.2 Input

64 The evaluation evidence for this sub-activity is the PP and in particular the PP rationale.

3.4.1.3 Evaluator action

65 This sub-activity comprises three CC Part 3 evaluator action elements:

a) APE_DES.1.1E;

b) APE_DES.1.2E;

c) APE_DES.1.3E.

3.4.1.3.1 Action APE_DES.1.1E

APE_DES.1.1C

66 The evaluator ***shall check*** the PP to determine that it contains a TOE description.

67 The evaluator ***shall check*** the TOE description for a description of the product type, the intended usage, IT features, and IT security features of the TOE.

68 The level of detail for the description of the IT features must be commensurate with a CC family requirement description.

3.4.1.3.2 Action APE_DES.1.2E

APE_DES.1.1C

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

70 As a PP does not normally refer to a specific implementation, the described TOE features may be assumptions.

3.4.1.3.3 Action APE_DES.1.3E

APE_DES.1.1C

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

3.4.2 Evaluation of the security environment (APE_ENV) sub-activity

3.4.2.1 Objective

72 The objective of this sub-activity is to ensure that the environment in which the TOE is expected to operate is described completely and consistently.

3.4.2.2 Input

73 The evaluation evidence for this sub-activity is the TOE security environment statements in the PP.

3.4.2.3 Evaluator action

74 This sub-activity comprises two CC Part 3 evaluator action elements:

a) APE_ENV.1.1E;

b) APE_ENV.1.2E.

3.4.2.3.1 Action APE_ENV.1.1E

APE_ENV1.1C

75 If the TOE security objectives are derived from OSP only, the statement of threats may be omitted. Otherwise, the following two evaluator work units are mandatory.

76 The evaluator ***shall check*** the PP to determine that the statement of the TOE security environment clearly identifies and describes the known or presumed threats against which a compliant TOE must provide protection.

77 For informational purposes, it is acceptable for a PP to articulate threats against which a compliant TOE is not intended to provide protection (un-countered threats). In meeting this work unit, such threats will be explicitly delineated from those that a compliant TOE is intended to counter (threats to be countered). Work units in APE_ENV and APE_OBJ will explicitly specify whether requirements apply to threats to be countered by the TOE, threats not to be countered or all threats.

78 The evaluator ***shall check*** the PP environment statements to determine that all threats are described in terms of an identified threat agent, the attack, and the asset which is the subject of the attack.

APE_ENV.1.2C

Editor Note : This section contains a deviation from CCv1.0; see Annex D.

79 If the TOE security objectives are derived only from threats to be countered, the statement of the OSPs may be omitted. Otherwise, the following two evaluator work units are required.

80 The evaluator ***shall check*** the security environment statements to determine that they identify the subset of the OSPs with which the TOE must comply.

81 The evaluator ***shall check*** that the statement of OSPs with which the TOE must comply with consists of rules, procedures, practices or guidelines.

APE_ENV.1.3C

82 The evaluator ***shall check*** the security environment statements to determine that they identify the secure usage assumptions of the TOE in its anticipated or actual environment of use.

83 The evaluator ***shall examine*** the secure usage assumptions to determine that it describes security aspects of the environment in which the compliant TOEs are intended to be used.

84 Security aspects may include physical, personnel and connectivity information about the intended environment.

3.4.2.3.2 Action APE_ENV.1.2E

APE_ENV.1.1C

85 The evaluator ***shall examine*** all threat statements to determine that they are stated in a manner which is consistent.

86 Two threat statements are inconsistent if either of them can be interpreted in a manner which could possibly lead to contradictory policies, objectives, security requirements or mechanisms associated with the other. For example, in a telephone, a threat of anonymous calling could be expressed and countered by mandating a policy that the originating phone be required to convey its telephone number to the receiver where it would then be displayed. A PP which also identifies an invasion of privacy threat linked with the lack of anonymity of the caller (i.e., mandating anonymous calling as is the case with crisis centres) would offer an inconsistent threat as the former threat explicitly results in a policy which requires identification of the caller where the latter would explicitly prohibit such a policy. The threat statements could be made consistent if they were modified to articulate which types of callers should be allowed anonymous services and which types should not.

87 The evaluator ***shall examine*** each threat to determine that it does or could exist in the actual or intended environment.

88 The evaluator ***shall examine*** each attack to determine that it does or could exist in the actual or intended environment.

89 The evaluator ***shall examine*** the assets at risk to determine that they are relevant (i.e., could be present) in the types of products/systems which the PP is intended to address.

90 Threat agents should be characterised by addressing aspects such as expertise and available resources. Attacks should be characterised by addressing aspects such as attack methods, any vulnerabilities exploited, and opportunity.

APE_ENV.1.2C

91 If the PP contains both threat and OSP statements, the evaluator ***shall examine*** the OSPs to determine that they are consistent with the to be countered threats.

92 The evaluator ***shall examine*** the OSPs to determine that they are consistent and, where appropriate, mutually supportive.

93 Two (or more) OSPs are consistent if, when considered together, neither statement becomes invalid because of the presence of the others. For example, in many systems and products, the policy mandate for identification and authentication is consistent with the policy mandate to protect against scavenging for data (object re-use) or to require access control. This is because the OSP statements are made such that each of these policies can be implemented in a manner that does not invalidate the others.

94 Two (or more) OSPs are mutually supportive if they achieve together what neither can achieve individually. For example, a policy mandating the auditing of individual actions is supported by a OSP mandating the identification and authentication of users before they access the system. The argument is that to audit individuals with accuracy and confidence they must be identified and authenticated. It is not expected that all OSPs be mutually supportive; however, binding analysis (see Annex B) should be performed in the context of this requirement to ascertain which statements should be considered mutually supportive in an effort to identify flawed or missing OSPs.

APE_ENV.1.3C

95 The evaluator ***shall examine*** the secure usage assumptions to determine that they do not contradict one another.

96 If the TOE is physically distributed, the evaluator ***shall examine*** the secure usage assumptions to determine that they apply consistently to all components of the TOE.

97 If physical components have different secure usage assumptions, the evaluator ***shall examine*** the secure usage assumptions for each component to determine that they are consistent and mutually supportive of the secure usage assumptions of the other components.

98 The evaluator ***shall examine*** each secure usage assumption to determine that it is reasonable in the context of any compliant TOE's intended usage.

99 A reasonable secure usage assumption is one that can be assumed in most applications of a compliant TOE. For example, it may not be reasonable for a firewall PP which enforces an access control policy for Internet services to have a secure usage assumption which assumes the firewall is not connected to the Internet.

100 The evaluator ***shall examine*** each secure usage assumption statement to determine that it is detailed enough to allow its verification by a consumer upon installation of a compliant TOE.

3.4.3 Evaluation of the PP introduction (APE_INT) sub-activity

Editor Note : This section contains deviations from CCv1.0; see Annex D.

3.4.3.1 Objective

101 The objective of this sub-activity is to ensure that the PP introduction is described completely and consistently.

3.4.3.2 Input

102 The evaluation evidence for this sub-activity is the PP and in particular the PP rationale.

3.4.3.3 Evaluator action

103 This sub-activity comprises three CC Part 3 evaluator action elements:

a) APE_INT.1.1E;

b) APE_INT.1.2E;

c) APE_INT.1.3E.

3.4.3.3.1 Action APE_INT.1.1E

APE_INT.1.1C

104 The evaluator ***shall check*** the PP to determine that it contains a PP introduction.

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

106 Since this requirement is largely for the benefit of schemes, it is the responsibility of the scheme to determine the specific identification information.

107 PP identification information may include:

a) an identifier of the PP together with version number/release number;

b) the identity of the PP author (including subcontractors as applicable);

c) registration identification, if the PP has been registered before evaluation.

APE_INT.1.2C

108 The evaluator ***shall check*** the PP to determine that the PP introduction provides a PP overview in narrative form.

109 The PP overview is intended to be a summary of the TOE description.

3.4.3.3.2 Action APE_INT.1.2E

110 The evaluator ***shall examine*** the PP introduction to determine that the PP overview is internally consistent so that no contradictions exist.

111 The level of detail for the description of the IT features must be commensurate with a CC class requirement description.

3.4.3.3.3 Action APE_INT.1.3E

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

113 The overview should characterise the features and assurances of a compliant TOE.

3.4.4 Evaluation of the security objectives (APE_OBJ) sub-activity

3.4.4.1 Objective

114 The objective of this sub-activity is to ensure that the security objectives are described completely and consistently, and to ensure that the security objectives counter the identified threats and achieve the identified OSPs.

3.4.4.2 Input

115 The evaluation evidence for this sub-activity is the:

a) TOE security environment statements in the PP;

b) security objective statements in the PP;

c) rationale section of the PP.

3.4.4.3 Evaluator action

116 This sub-activity comprises two CC Part 3 evaluator action elements:

a) APE_OBJ.1.1E;

b) APE_OBJ.1.2E.

3.4.4.3.1 Action APE_OBJ.1.1E

APE_OBJ.1.1C

117 The evaluator ***shall check*** the PP to determine that it contains a description of the security objectives.

118 The evaluator ***shall check*** the security objectives to determine that every security objective is unambiguously identified as either an IT or a non-IT security objective, but not both.

119 IT and non-IT security objectives are distinct in that the former is achieved by technology and the latter by secure usage assumptions. Annex C provides background information which may be useful for completing this work unit.

APE_OBJ.1.2C

120 The evaluator ***shall check*** that each security objective identified as an IT security objective is unambiguously mapped to at least one to be countered threat or OSP or both.

121 This work unit is not satisfied if an IT security objective exists to which no to be countered threats or OSPs are mapped. Annex C provides background information that may be useful for completing this work unit as it describes the derivation of IT security objectives from to be countered threats and OSPs.

APE_OBJ.1.3C

122 The evaluator ***shall check*** that each security objective identified as a non-IT security objective is unambiguously mapped to at least one to be countered threat or OSP or both.

123 This action is not satisfied if a non-IT security objective exists to which no to be countered threats or OSPs are mapped. Annex C provides background information which may be useful for completing this work unit as it describes the derivation of non-IT security objectives from to be countered threats and OSPs.

APE_OBJ.1.4C

Editor Note : This section contains deviations from CCv1.0, see Annex D.

124 The evaluator ***shall check*** that each to be countered threat is unambiguously mapped to at least one security objective.

125 The evaluator ***shall check*** that, for each to be countered threat, a rationale is provided to explain why the security objectives counter the threat.

126 The evaluator ***shall check*** that each OSP statement is unambiguously mapped to at least one security objective.

127 The evaluator ***shall check*** that, for each OSP, a rationale is provided to explain why the security objectives achieve the OSP.

3.4.4.3.2 Action APE_OBJ.1.2E

Editor Note : This section contains deviations from CCv1.0, see Annex D.

APE_OBJ.1.4C

128 The evaluator ***shall examine***, for every to be countered threat, the mapping to the security objective(s) and the rationale to determine that the threat is countered by the security objective(s).

129 A security objective contributes towards countering a threat if, as a result of the objective, the threat agent has no attack method, has less opportunity or if the threat agent must have greater expertise or expend greater resources. The evaluator should refer to Annex B for guidance in conducting this suitability analysis.

130 The evaluator ***shall examine***, for every OSP, the mapping to security objectives and the rationale to determine that the OSP is achieved by the security objectives.

131 A single security objective contributes towards achieving an OSP if, as a result of the objective, all or some of the policy may be administered.

132 The evaluator ***shall examine*** all security objectives to determine that no security objective conflicts with any other security objective and that the security objectives are mutually supportive, where applicable.

133 The evaluator should refer to Annex B for guidance in conducting this binding analysis.

3.4.5 Evaluation of the IT security requirements (APE_REQ) sub-activity

3.4.5.1 Objective

134 The objective of this sub-activity is to ensure that the TOE IT security requirements (both the TOE IT functional requirements and the TOE IT 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.

3.4.5.2 Input

135 The evaluation evidence for this sub-activity is the:

a) IT security objective statements in the PP;

b) TOE IT security requirements statements in the PP;

c) IT security requirements for the IT environment statements in the PP;

d) rationale section of the PP.

3.4.5.3 Evaluator action

136 This sub-activity comprises two CC Part 3 evaluator action elements:

a) APE_REQ.1.1E;

b) APE_REQ.1.2E.

3.4.5.3.1 Action APE_REQ.1.1E

APE_REQ.1.1C

137 The evaluator ***shall check*** that the statement of TOE IT functional requirements uses functional requirement components drawn from CC Part 2 only.

138 The evaluator ***shall check*** that every element of each functional component used is included and is correctly transcribed into the PP.

139 The evaluator ***shall check*** that if functional packages from Chapter 3 of CC Part 2 are used they are transcribed correctly.

APE_REQ.1.3C

Editor Note : This section contains deviations from CCv1.0; see Annex D.

140 The evaluator ***shall check*** that the PP specifies an EAL as defined in CC Part 3.

141 The evaluator ***shall check*** that all CC Part 3 assurance requirements that are included in the specified EAL are included in the PP.

142 The PP may contain assurance requirements in addition to the ones specified as part of the CC Part 3 EAL.

APE_REQ.1.2C

Editor Note : This section contains deviations from CCv1.0; see Annex D.

143 The evaluator ***shall check*** that the statement of TOE IT assurance requirements uses assurance requirement components drawn from CC Part 3 only.

144 The evaluator ***shall check*** that every element of each assurance component used is included and is correctly transcribed into the PP.

145 In performing this check, the evaluator is reminded that no operations on CC Part 3 assurance requirements are permitted by the CC.

APE_REQ.1.4C

146 If the TOE is a complete TSF with no assertions on the IT environment, the following work unit will be omitted.

147 The evaluator ***shall check*** that security requirements for the IT environment are identified and defined.

148 The security requirements for the IT environment should be distinguished from the TOE IT security requirements (i.e., “identified”) and should be correct statements of security requirements (i.e., “defined”).

APE_REQ.1.5C

Editor Note : This section contains deviations from CCv1.0; see Annex D.

APE_REQ.1.6C

Editor Note : This section contains deviations from CCv1.0; see Annex D.

149 The evaluator ***shall check*** that all operations on CC Part 2 functional requirements included in the PP are identified and explained.

150 The permitted operations for CC Part 2 functional components are assignment, selection and refinement. The assignment and selection operations are permitted

only where specifically indicated in an element. Refinement, that is, the addition of additional detail, is permitted for all functional elements.

151 The PP should identify all operations in each element where such an operation is used. Identification can be achieved by typographical distinctions, or by explicit identification in the surrounding text, or by any other distinctive means. The rationale for the choice of operation should appear in the text following the requirement that uses it.

152 The evaluator ***shall examine*** the PP to determine that all operations are performed correctly.

153 In performing this analysis, the evaluator should compare each statement with the CC Part 2 element from which it is derived to determine that:

a) for an assignment or refinement, the item or items 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.

154 The evaluator should also determine that the items chosen are appropriate for the requirement.

155 The evaluator ***shall examine*** the rationale for each operation accompanying each requirement for completeness and clarity.

156 The evaluator ***shall examine*** each use of refinement to determine that the refinement does not levy new requirements nor does it lessen the strength of the requirement.

157 The refinement operation is intended to provide a means of limiting the set of acceptable implementations by specifying additional technical detail. It does not allow new requirements to be created or existing requirements to be deleted.

APE_REQ.1.7C

158 The evaluator ***shall check*** that any uncompleted operations within the PP are clearly identified and described.

159 It is permissible for a PP to contain elements with uncompleted operations. That is, the PP can contain requirement statements that include choices for assignment, selection or refinement. The operations can then be completed in an ST based on the PP. This gives the ST developer more flexibility in producing an ST that is compliant to a particular PP.

160 The PP should identify uncompleted operations in each element where one appears. Identification can be achieved by typographical distinctions, or by explicit identification in the surrounding text, or by any other distinctive means. The

description of the uncompleted operation should appear in the text following the requirement that uses it.

161 The evaluator ***shall examine*** the PP to determine that any required operations which are not applied within the PP are described such that they can be correctly applied at the point that the PP is used as the basis for an ST.

APE_REQ.1.8C

Editor Note : This section contains deviations from CCv1.0; see Annex D.

162 The evaluator ***shall examine*** the PP to determine that all dependencies required by the CC components used in the security requirement statement are accounted for and satisfied.

163 If the PP contains assurance requirement statements in addition to those that are included in the specified EAL for the PP, the evaluator ***shall check*** that the dependencies are satisfied for these additional requirements.

164 The evaluator ***shall check*** the PP to determine that a rationale is provided in cases where security requirement dependencies is not explicitly satisfied.

165 Dependencies may be satisfied by the inclusion of the relevant component within the TOE security requirement statements, or as a requirement which is asserted as being met by the IT environment of the TOE. This means that if a component is included, all the components indicated in the dependency section should also be included. In the case of assurance components, a component which is hierarchical (higher in the hierarchy) to the component requiring the dependency could be selected. A dependency may be satisfied without the explicit inclusion of the relevant component if a rational is provided explaining why the inclusion of the dependency is unnecessary.

APE_REQ.1.9C

166 The evaluator ***shall check*** that, for each security objective, a rationale is provided to explain why the security requirements achieve the security objective.

APE_REQ.1.10C

167 The evaluator ***shall check*** that the PP includes a rationale that explains how the security requirements together form a consistent whole.

3.4.5.3.2 Action APE_REQ.1.2E

APE_REQ.1.9C

168 The evaluator ***shall examine*** the rationale to determine that the articulated IT security requirements for the TOE and for the environment of the TOE are suitable to meet all of the stated IT security objectives of the TOE.

169 The evaluator may use mappings from objectives to security requirements to assist in conducting this examination. The evaluator should refer to Annex B for guidance in conducting this suitability analysis.

170 The evaluator ***shall examine*** the rationale to determine that, for the security requirements, there are no instances of conflict that could result in a failure to satisfy a security objective.

171 Each security objective will be achieved if the security requirements are correctly implemented. The intent is that all threats are countered and the OSPs are implemented, as required by a compliant TOE when the security objectives are met. It is the purpose of the evaluation of the security objectives (APE_OBJ) sub-activity to provide the assurance that the security objectives counter the threats and enforce the OSP. In contrast, it is the purpose of the present sub-activity to provide assurance that the requirements are suitable for meeting the TOE IT security objectives.

APE_REQ.1.10C

172 The evaluator ***shall examine*** the rationale statement to determine that the set of security requirements together forms a **mutually supportive** and internally consistent whole.

173 As part of this binding analysis, the evaluator should determine that the choice of functional requirements, EAL and augmenting assurance requirements is consistent. In particular, if augmented assurance requirements are included, the evaluator should determine that they are consistent with each other. The evaluator should refer to Annex B for guidance in conducting this binding analysis.

Annex A

Glossary

174 This annex presents, abbreviations and acronyms, vocabulary and references used in the CEM.

A.1 Abbreviations and acronyms

175	CC	Common Criteria
176	CEM	Common Evaluation Methodology
177	EAL	Evaluation Assurance Level
178	ESR	Evaluation Summary Report
179	ETR	Evaluation Technical Report
180	IT	Information Technology
181	OSP	Organisational Security Policy
182	PP	Protection Profile
183	ST	Security Target
184	TOE	Target of Evaluation

A.2 Vocabulary

185 Vocabulary which are presented in bold faced type are themselves defined in this section. If the vocabulary is defined in another document (e.g. the CC), the definition is quoted verbatim unless otherwise noted, and the source is noted in brackets at the end of the definition. The number in parentheses beside the term indicates in which CEM part the vocabulary is first used: for instance, (2) indicates that this term is first used in Part 2 of the CEM.

186 Binding analysis(2):

> the determination of the appropriateness of the collection of security objectives, security requirements, TOE security functions or mechanisms to work together in a way which is **mutually supportive** to provide security as an integrated and effective whole.

187 Check(2):

to generate a **verdict** by a simple comparison performed by mapping which does not require **evaluator** expertise. The statement which uses this verb describes what is mapped.

188 Consistent(2):

entities, such as statements, functions or mechanisms are consistent if, when considered together, no entity becomes less valid or, in fact, invalid.

189 Deliverable(1):

see **evaluation deliverable** and **oversight deliverable**.

190 Developer(1):

a party to an **evaluation** with responsibilities specified in CEM Part 1, Section 3.1.2.

191 Element(1):

an indivisible security requirement. [CCv1.0]

192 Evaluation(1):

the assessment of a **PP** or **TOE** against defined evaluation criteria.

193 Evaluation Assurance Level(1):

a pre-defined set of assurance components from Part 3 (of the CC) that represent a point on the CC assurance scale. [CCv1.0]

194 Evaluation Authority(1):

the body responsible for the business application of the **evaluation** results. Its activities are outside the scope of the CEM, but include such things as issuing “certificates”, making mutual recognition agreements and defining scheme rules such as “licensing” commercial facilities.

195 Evaluation Deliverable(1):

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

196 Evaluation Evidence(1):

a tangible **evaluation deliverable**.

197 Evaluation Process(1):

a set of actions performed by the parties in order to conduct an IT security **evaluation**.

198 Evaluation Result(1):

this term is used in a generic sense only.

199 Evaluation Summary Report(1):

a report issued by an **overseer** and submitted to an **evaluation authority** that documents the **oversight verdict** and its justification.

200 Evaluation Technical Report(1):

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

201 Evaluator(1):

a party to an **evaluation** with responsibilities specified in CEM Part 1, Section 3.1.3.

202 Evaluator Action Element(1):

an assurance requirement stated in the CC that represents an **evaluator's** responsibilities in performing a **PP** or **TOE evaluation**.

203 Examine(2):

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

204 Interpretation(1):

a clarification or amplification of a CC, CEM or **scheme** requirement.

205 Methodology(1):

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

206 Mutually Supportive(2):

entities, such as statements, functions or mechanisms are mutually supportive if they achieve together what they cannot each individually achieve.

207 Observation Report(1):

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

208 Overall Verdict(1):

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

209 Overseer(1):

a party to an **evaluation** with responsibilities specified in CEM Part 1, Section 3.1.4.

210 Oversight Deliverable(1):

any resource required from the **evaluator** to perform one or more **evaluation** oversight activities.

211 Oversight Verdict(1):

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

212 Protection Profile(1):

a re-usable and complete combination of security objectives, functional and assurance requirements with associated rationale. [CCv1.0]

213 Scheme(1):

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

214 Security Target(1):

a complete combination of security objectives, functional and assurance requirements, summary specifications and rationale to be used as the basis for **evaluation** of an identified **TOE**. [CCv1.0]

215 Sponsor(1):

a party to an **evaluation** with responsibilities specified in CEM Part 1, Section 3.1.1.

216 Suitability analysis(2):

an examination of the appropriateness of a particular security objective, security requirement, **TOE** security function or mechanism in its intended security context.

217 Target of Evaluation(1):

an IT product or system that is the subject of an **evaluation**. [CCv1.0]

218 Verdict(1):

a “pass”, “fail” or “inconclusive” statement issued by an **evaluator** with respect to a CC evaluator action element, assurance component, or class. Also see **overall verdict.**

A.3 References

CCv1.0 Common Criteria for Information Technology Security Evaluation, Version 1.0, January 1996.

COD Concise Oxford Dictionary, Oxford University Press, Ninth edition, 1995.

Annex B

PP rationale analysis

Editor Note: *This annex is currently incomplete and will continue to evolve with subsequent drafts of the CEM. Future drafts will include more description for direct and indirect attacks as well as the application of suitability and binding analysis to ST and TOE evaluation.*

B.1 PP suitability and binding analysis

219 PP Suitability and Binding Analysis includes an effort by the developer and the evaluator to justify the collection of requirements that have been chosen.

B.1.1 Suitability analysis

220 The goal of suitability analysis is to build an argument that each functional security requirement of the PP counters the intended threat or achieves an OSP requirement. It is performed in a step-wise manner. That is, the evaluator must first determine if the security objectives are suitable to counter the threats and achieve the OSPs. Then the evaluator must determine if the security requirements are suitable to achieve the IT security objectives. Finally the evaluator must determine if the secure usage assumptions are suitable to achieve the non-IT security objectives.

221 A security requirement is suitable to counter a threat if, as a result of the security requirement, one or more of the following conditions exist:

a) the threat agent is removed from the environment;

b) the vulnerability by which the attack is carried out is removed.

222 A security requirement contributes towards countering a threat if, as a result of the requirement, one or more of the following conditions exist:

a) fewer vulnerabilities and, hence, attack options exist;

b) the threat agent has less opportunity to perform an attack;

c) the threat agent must have greater expertise to perform an attack;

d) the threat agent must expend greater resources to perform an attack.

223 A security requirement is suitable to achieve an OSP statement if, as a result of the security requirement, the policy may be implemented (achieved).

B.1.2 Binding analysis

224 Like suitability analysis, binding analysis is performed in a step-wise manner. The goal of binding analysis is to ascertain that the collection of security objectives, security requirements, TOE security functions or mechanisms work together in a way which is mutually supportive to counter the threats. The binding analysis provides an analysis of the interrelationships between a compliant TOE's security objectives, security requirements, and TOE security functions or mechanisms and shows that there is no contradiction. For example, binding analysis addresses the question of whether a threat is countered by the security objectives when all security objectives are considered.

225 When performing a binding analysis, as a minimum an evaluator should consider the following:

a) for IT security requirements, are there dependencies which have not been satisfied that introduce a vulnerability?

b) have refinement operations rendered the requirements to be non-mutually supportive?

c) for IT security requirements, is there a clear delineation between those requirements for the TOE and those for the environment and are they mutually supportive?

d) are the IT security requirements and the secure usage assumptions mutually supportive?

e) is the set of functional requirements for the TOE sufficient for the protection of the trusted security functions?

B.1.3 Suitability and binding analysis example

226 An example, based on threats, which illustrates suitability and binding for a PP is illustrated in Figure B.1. This Figure represents:

a) the assets as a bag valuables;

b) attacks by nails with a length proportional to the level of expertise, opportunity and resource available to the attacker;

c) the countermeasures (e.g. security functions) by a wall which has a thickness proportional to the countermeasure's ability to defend against direct attack;

d) indirect attacks by a hand entering through holes in the countermeasure design or implementation.

227 A TOE specified to meet the PP is deemed to be secure (implying that the PP requirements are suitable and bind appropriately) if the assets are completely

surrounded by a wall which has a minimum thickness equal to or greater than the length of any nail. Figure B.1 illustrates the case where the selected security functions are sufficient to counter direct attacks (i.e. suitable), but the collection of chosen security functions leaves a hole for indirect attacks (i.e. does not bind). Consider, for example, the design of a secure operating system where the developer has neglected to include the necessary functions to protect the traditional security functions (e.g. Identification and Authentication, Access Control etc.) from external interference and tampering. As a result, the chosen mechanisms can counter direct attack (e.g. password guessing, direct attempts to access information) but because they do not protect against tampering, indirect attacks (e.g. modifying the security enforcing functions to allow access) can allow a violation of the security policy. The evaluator could argue that this solution does not bind, because it does not form an integrated whole to enforce the security policy even though the mechanisms that are articulated may prevent direct attacks.

228 Figure B.1 illustrates the concepts of suitability and binding based on threats only. A CC evaluation requires that this analysis be performed to show that a TOE compliant with the PP under analysis achieves the stated security objectives and, ultimately counters threats and enforces the OSPs.

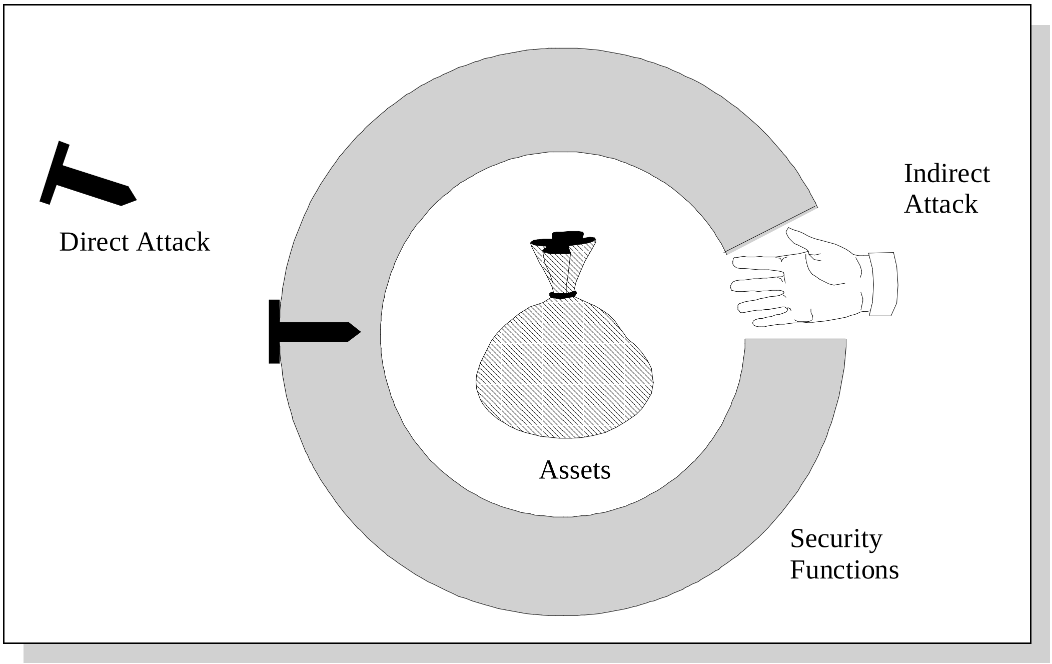


Figure B.1 - The failure of binding

Annex C

PP development background

229 In writing the methodology for evaluating a PP, assumptions were made regarding the development of a PP. Since these assumptions may be helpful to a PP evaluator, a description of these assumption ensues.

230 Figure C.1 illustrates the parts of a PP which are grouped into one of the three levels of PP abstraction: security environment, security objectives and security requirements.

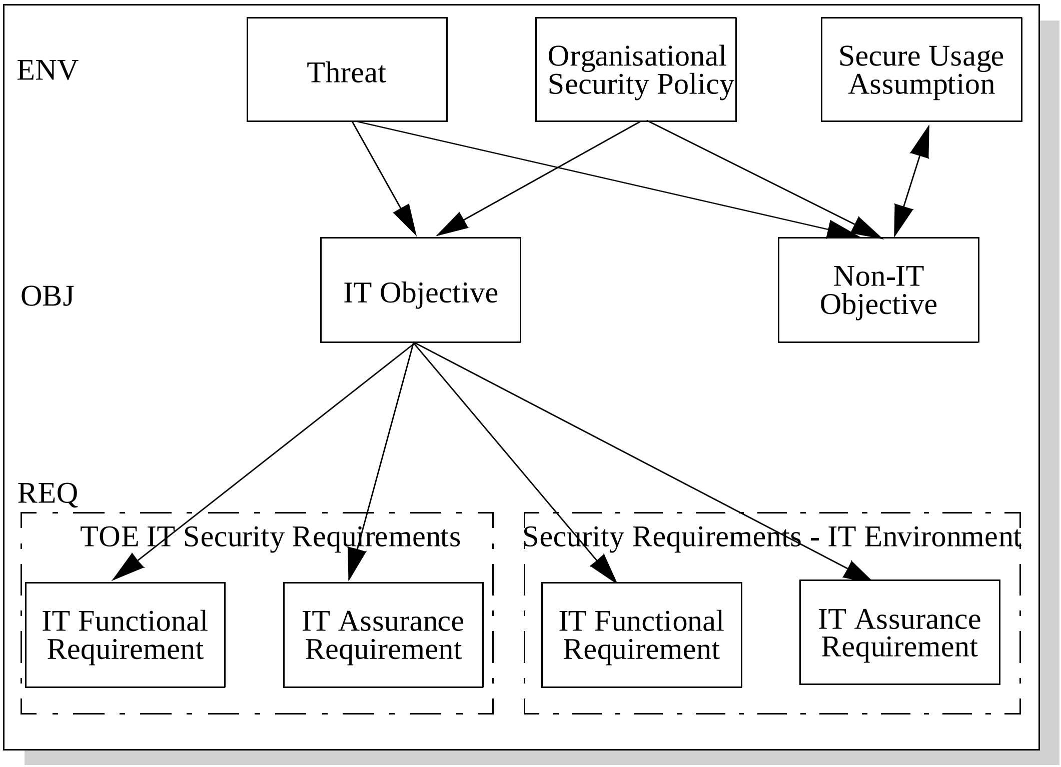

ENV
Threat
Organisational Security Policy
Secure Usage Assumption
OBJ
IT Objective
Non-IT Objective
REQ
TOE IT Security Requirements
Security Requirements - IT Environment
IT Functional Requirement
IT Assurance Requirement
IT Functional Requirement
IT Assurance Requirement

Figure C.1 - Derivation of PP security requirements

231 From the perspective of developing a PP, security requirements are derived, in brief, by performing analyses in a step-wise refinement manner. Analysis begins with the security environment to derive the security objectives, and then with the security objective to derive the security requirements. The security requirements

form the basis of the TOE security services, the TOE development, and the TOE evaluation.

232 Environmental analysis yields statements about aspects of the environment in which the TOE is intended to operate and which are relevant to the secure operation of the TOE, including:

a) threats, specifically those threats from which protection is required (to be countered threats) and, optionally, other threats which are present in the environment but from which no protection is provided (un-countered threats);

b) OSP;

c) secure usage assumptions.

233 The security objectives provide an intermediate stage in the logical link between the security environment and security requirements. This step-wise refinement facilitates an analysis by the PP developer to ascertain that the security requirements counter the threats or achieve the OSP. A single threat or OSP statement is countered or achieved respectively by at least one security objective.

234 A security objective is often met by employing information technology and, when this is the case, is categorised as being an IT security objective. However, a security objective can be met by other means which do not employ information technology, and is so categorised as a non-IT security objective. As a consequence of security objective categorisation:

a) all requirements (or constraints) of a non-IT nature can be clearly derived from the non-IT security objectives;

b) all requirements of an IT nature can be derived from the IT security objectives.

235 The requirements for the environment to which the non-IT security objectives are mapped are referred to as the secure usage assumptions. Secure usage assumptions are defined in the PP as part of the description of the environment even though they may be thought of as being similar to security requirements, but for the non-IT environment. Secure usage assumptions support the IT requirements and may include, but are not limited to, such non-IT aspects as:

a) personnel security, such as user security clearances;

b) physical security, such as access restrictions for users versus administrators;

c) procedural security, such as network security rules for users;

d) connectivity, such as constraints on the configuration, operation, etc., of the IT that are not addressed by the IT security objectives.

236 The non-IT environment is illustrated in Figure C.2. The secure usage assumptions is the subset of those non-IT environmental requirements necessary to satisfy the non-IT security objectives.

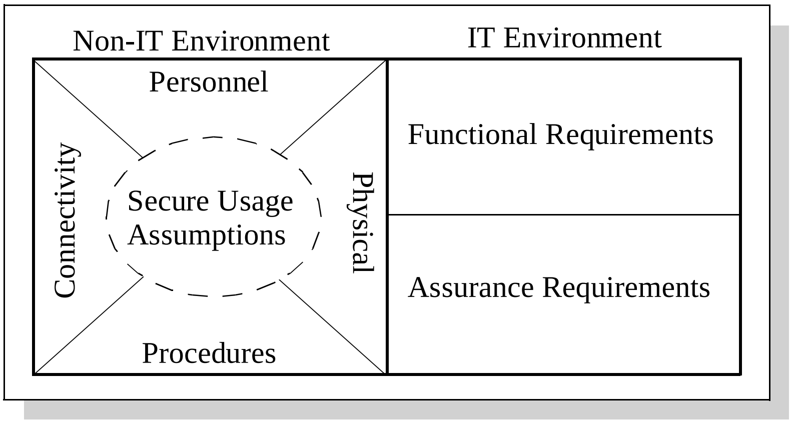


Figure C.2 - TOE environment

237 The IT security objectives are mapped to and satisfied by the IT security requirements. IT security requirements include functional and assurance requirements for the TOE and may include functional and assurance requirements for the IT environment, in cases where the TOE is not a complete TSF.

Annex D

CEM deviations from the CC

Introduction

238 This annex details all CEM deviations from CCv1.0.

239 Reasons for deviation include such things as (1) necessary to write a viable methodology or (2) CC editor's decisions for changes to version 1.0 which were deemed by the CEMEB as useful to facilitating the writing of the methodology. Note that CCIB decisions were considered on a case-by-case basis - not all CCIB decisions were implemented if deem volatile or if insufficient details were known to the CEMEB.

Normative nature of CC Part 2 and Part 3

Problem

240 The developer entries in Table 1.1 state that CC Parts 2 and 3 should be used as a reference when interpreting statements of functional and assurance requirements. This implies that Parts 2 and 3 are not normative (mandatory) for developers, which is inconsistent with the use of "shall" in the Developer Action elements.

Resolution

241 The developer entries in Table 1.1 should be modified to indicate that these are mandatory statements.

Impact on the CEM

242 Part 1 of the CEM assumes that the CC makes mandatory statements of the developer.

Evaluation of the PP introduction and TOE description

Problem

243 The description of content and presentation of a PP described in Part 1, Annex B which provide the normative specification of a PP, requests for the PP to conform to the content requirements described in that annex.

244 This annex includes requirements for "non mandatory" information, such as the PP introduction, the TOE description, or the Application notes.

245 This annex states that the information provided should be used for the evaluation of the PP or the TOE (although it does not have to be evaluated by itself).

246 The criteria in CC Part 3 Class APE which describe the normative content and presentation of evidences to be provided for a PP evaluation does not reflect those requirements for evidences, and if provided the APE class does not provide requirements to use those evidences in the conduct of the evaluation.

Resolution

247 The APE class of Part 3 should be expanded by two more families to satisfy the PP evaluation objectives.

248 One family should contain requirements to examine the suitability for inclusion in the registry i.e. that the PP contains document management and overview information necessary to operate a PP registry. The description of information to be provided about this shall be provided within the PP introduction (see Part 1, Annex B).

249 This includes the PP identification (provides the labelling and descriptive information necessary to identify, catalogue, register, and cross reference a PP) and the PP overview (summarises the PP in narrative form).

250 The new family shall describe the content and presentation of the evidences using the requirements provided in Part 1 Annex B, and provide evaluator action requirements to validate those evidences.

251 Another family should contain requirements to examine the meaning of the TOE i.e. to verify for consistency. Information about relevant information to describe the TOE and to aid to the understanding of its security requirements shall be provided within the TOE description (see Part 1, Annex B).

252 The TOE description shall provide information about the product type, the intended usage including the intended application and possible limitations of use, and the general features of the TOE. If provided, this information shall be used in the course of an evaluation to identify inconsistencies and possible limitation of use of the TOE.

253 The new family shall describe the content and presentation of the evidences using the requirements provided in Part 1 Annex B, and provide evaluator action requirements to validate those evidences.

254 The Application notes should also be considered during an evaluation. If provided, the application notes may contain additional supporting information for the construction, evaluation, or use of the TOE.

255 The evaluator action elements shall be updated to include the information provided in the Application Notes in the conduct of the evaluation.

Impact on the CEM

256 For the evaluation of the PP introduction and the TOE description the CCIB decided to develop two new families, APE_INT and APE_DES (CCIB-97-031). The actual version of the CEM is based on these families as stated in the alpha version of the CC, delivered in July 1997.

Ambiguity of CC terminology

Problem

257 The terminology used in the elements of Part 3, APE class is difficult to handle by the evaluator and the developer. Use of different terms with a similar meaning is subject of interpretation.

258 For example,

a) the developer shall provide “a statement”, “an argument”, or “a description”;

b) this evidence shall “explain”, or “demonstrate”;

c) the evaluator shall “confirm” that the information provided meets all requirements for content and presentation (objective requirement), and also “confirm” that the statement of TOE security environment is complete (but what is the metric for this completeness), coherent, and internally consistent (subjective requirement).

Resolution

259 The terminology used in the Part 3 criteria shall be cleaned up for simplification.

260 The terms used for the definition of the type of evidence to be provided shall be explicit (the term shall reflect the work to be performed by the developer to prepare the evidence).

261 The verbs used in the developer or evaluator actions shall reflect the level of effort to be provided and the objectivity or subjectivity of the decision to be made.

262 To help in the understanding of those terms (name and verbs), a list shall be provided (in the Paradigm Section of the Part 3) to explain the hierarchy of effort to produce and verify the evidences.

Impact on the CEM

263 In writing the CEM for requirements with ambiguous terminology, a small set of verbs for methodology work units will be used to address any ambiguity.

Redundant requirements in APE_OBJ

Problem

264 This CCOR is related to CCORs 277 and 258. The delineation between APE_OBJ.1.4C and APE_OBJ.1.5C is unclear and appears redundant. This CEMEB CCOR is raised in order to accurately track any deviation between the CEM and the CC.

Resolution

265 Delete the current requirements APE_OBJ.1.4C and APE_OBJ.1.5C. Create a new APE_OBJ.1.4C to read: ‘The PP shall demonstrate that all security objectives counter identified threats and/or enforce organisational security policies, and that all threats and policies have been addressed.”

Impact on the CEM

266 The CEM action APE_OBJ.1.2E has been written assuming the change will be implemented in a future version of the CC.

Definition of OSP

Problem

267 In the Glossary of the CC (Part 1) the Organisational Security Policy is defined as “A set of security rules, procedures, practices, and guidelines imposed by an organisation upon its operation.”. The CEMEB questions whether this definition is correct, in other words does an Organisational Security Policy necessarily identify the rules, procedures, practices and guidelines or can it be any combination of this type of information?

268 Furthermore, APE_ENV.1.2C states that “the statement of TOE security environment shall identify and explain any organisational security policies that the TOE must comply with”. This can be interpreted as that all the security rules, procedures, practices, and guidelines of the organisational security policy that the TOE must adhere to are explained. Although some of this information may not have a bearing on the evaluation of the TOE.

269 In order to reduce the amount of work performed by the evaluator and the PP developer, only the part of the organisational security policy that is applicable to the TOE must be explained.

Resolution

270 Change the definition in the Glossary of Part 1 to indicate that this information could be present. A suggestion for the wording is: “A set of security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.”

271 Change APE_ENV.1.2C such that only the relevant information should be identified and explained. A suggestion for the wording is: “The statement of TOE security environment shall identify and explain any subset of the organisational security policy that the TOE must comply with.”

Impact on the CEM

272 The CEM action APE_ENV.1.1E has been written assuming that the proposed definition change will be implemented in a future version of the CC. The work units of this CEM action explicitly use the words of the proposed definition and require that the subset of OSPs with which the TOE must comply be explicitly identified.

Wrong order of requirements

Problem

273 As the assurance requirements in a PP shall be expressed by using an EAL from Part 3, and may be augmented with other components from Part 3, the elements APE_REQ.1.2C and APE_REQ.1.3C are in the wrong order for the evaluator actions.

Resolution

274 Change the order of those two components (APE_REQ.1.3C first to check the use of the mandatory EAL), and APE_REQ.1.2C after (to verify that the components used to augment the level are from Part 3).

Impact on the CEM

275 CEM Part 2 has been written as if the order of the identified requirements is changed.

Ambiguity between CC Part 1 and Part 2 regarding refinement to Part 2 requirements

Problem

276 An interpretation of Part 1, Section 2.3.1.2 is that operations may only be performed on requirements which explicitly state that a particular operation is permitted. In particular, the second and third sentences of paragraph 58 give this impression. Although this is generally accepted for the assignment and selection operations, does it also apply to the refinement operation? Some Part 2 requirement specifically state that a refinement is permitted (for, instance, FIA_UAU.5.2, FIA_UAU.6.3, FPT_ITA.1, etc.,); does this, by default, preclude refinements to requirements which do not explicitly state that the refinement operation is permitted?

Resolution

277 If the CEMEB's assumption is correct, suggest the following changes to the CC:

a) Part 2/Section 2.1.4/ Paragraph 72/ to be changed to add the statement that refinement is permitted for all functional components.

b) Part 1/Section 2.3.1.2/ Paragraph 58/ to be changed in a similar way to add the statement that refinement is permitted for all functional requirements.

Impact on the CEM

278 The CEM has been written assuming that CC Part 2 is correct, that is, refinement may be permitted on any functional requirement.

Missing requirements for the analysis of the IT environment

Problem

279 CC Part 1 paragraph 138 bullet b 3) claims that all dependencies of the requirements components of the TOE shall be satisfied. This statement is clearly related only on the TOE IT security requirements and not to the security requirements for the IT environment.

280 CC Part 1 paragraph 136 bullet b) claims that the security requirements for the IT environment should, if possible, be stated by reference to security requirements from the CC. However, Part 1 does not claim that the dependencies for the security requirements for the IT environment, if they are stated by reference to the CC, shall also be satisfied.

281 CC Part 3 paragraph 120 APE_REQ.1.5C claims that security requirements for the IT environment shall be stated by reference to the CC where feasible. And APE_REQ.1.8C claims that dependencies of CC security requirements shall be accounted for and shown to be satisfied. This statement is not limited to the TOE IT security requirements but relates to all CC security requirements, also to the requirements for the IT environment if they are stated by reference to the CC.

282 There seems to be an inconsistency between Part 1 and Part 3 of the CC and it is unclear whether the dependencies of the requirements for the IT environment have also to be satisfied.

Resolution

283 Please clarify in Part 1 and Part 3 whether the dependencies of the requirements for the IT environment shall be satisfied or not, if they are stated by reference to the CC.

Impact on the CEM

284 The APE_REQ section is possibly incomplete with respect to the dependency analysis of the requirements for the IT environment.

Dependencies

Problem

285 Regarding the issue of requirement dependencies, the CCIB has determined that dependencies may be waived with appropriate rationale.

Resolution

286 Requirement dependencies need not be satisfied as long as a rationale is provided by the ST/PP author as to why the dependency does not need to evaluate. This is further described in document CCIB-97-023, Issue 12, dependencies.

Impact on the CEM

287 The work units associated APE_REQ.1.8C reflect that dependencies may be softened with appropriate rationale.

Suitability of security objectives

Problem

288 Although a goal of evaluation is to determine that the security requirements specified in the PP/ST counter the identified threats and achieve the OSP statements, this determination is achieved using a process of step-wise refinement. That is to say that, if the security objectives counter/achieve the threats/OSPs, and the security requirements satisfy the security objectives, then the security requirements should counter/achieve the threats/OSPs.

289 REQ.1.2E correctly requires that the evaluator determine if the security requirements are suitable to meet the security objectives. The problem is that a similar requirement to determine if the SOs are suitable to counter/achieve the threats/OSPs is not clearly nor consistently (with REQ.1.2E) specified; or could be more clearly and consistently specified.

290 Content and presentation requirement APE_OBJ.1.4C, modified as proposed by CCOR 277, does require that the "PP demonstrate that all security objectives counter identified threats and/or enforce OSP, and that all threats and policies have been addressed", but the only evaluator action associated with any kind of "goodness" check of this evidence is OBJ.1.1E, confirmation of content and presentation.

291 This same type of approach is taken for the APE_REQ. However, APE_REQ.1.2E correctly requires the evaluator to perform a suitability analysis, albeit, using the evidence provided by the developer. Because REQ.1.2E asks for a suitability analysis to be performed on "the set of" requirements, a binding analysis is also implied by REQ.1.2E. This is correct. But, this concept of evaluator analysis for OBJ is not expressed clearly or consistently with APE_REQ.1.2E.

Resolution

292 Reword APE_OBJ.1.2E in a way consistent with APE_REQ.1.2E, that is: "The evaluator shall confirm that the set of security objectives is suitable to counter all of the identified threats and achieve all of the identified OSP statements" Note that the concern for "complete and consistent security objectives" addressed in the current APE_OBJ.1.2E is still addressed by the proposed change since the evaluator is asked to consider the suitability of the set of SOs. This is also the case for APE_REQ, which also employs the requirement APE_REQ.1.10C, demonstrate mutual support and internal consistency.

293 Please note that this CCOR equally applies to the ASE class.

Impact on the CEM

294 The CEM action APE_OBJ.1.2E has be written assuming the change will be implemented in a future version of the CC.

APE_REQ.1.5C inappropriate for cost effective evaluations

Problem

295 Requirements for the IT environment may be selected, at the developer’s discretion, from criteria other than the CC. Since this is allowed by the CC providing no basis for the evaluator to influence the developer, writing CEM work units to verify this content and presentation of evidence element is of no evaluation benefit.

Resolution

296 Delete APE_REQ.1.5C on the grounds that it detracts from the cost effectiveness of evaluations.

Impact on the CEM

297 No work units related APE_REQ.1.5C have written on the assumption that it will be deleted.

Annex E

CEM observation report (CEMOR)

E.1 Introduction

298 This annex details a mechanism by which to comment on the CEM.

299 This mechanism consists of a report format to be used to articulate the observation as well as a mailing address to which a CEMOR should be sent.

E.2 Forwarding a CEMOR

300 A CEMOR may be sent directly to the Internet mail address “cem@cse.dnd.ca”. The CEMOR may be sent to this Internet address directly by the originator or, alternatively, through one of the organisations listed in the foreword of this part. An acknowledgement will normally be sent to the originator of a CEMOR.

E.3 Format of a CEMOR

301 A CEMOR shall be forwarded in a text (ASCII) format only.

302 A separate CEMOR shall be created for each observation. A single CEMOR shall not address two or more unrelated observations.

303 A CEMOR shall contain all of the following fields, although one or more fields may be empty. Each field shall begin with the ASCII character “**$**”, followed by an arabic number, followed by the ASCII character “**:**”

$1: Originator’s name

304 Full name of the originator.

$2: Originator organisation

305 The originator’s organisation/affiliation.

$3: Return address

306 Electronic mail or other address to acknowledge receipt of the CEMOR and request clarification, if necessary.

$4: Date

307 Submission date of observation YY/MM/DD.

$5: Originator's CEMOR identifier

308 This identifier is assigned to the CEMOR by the originator. There are two requirements for this identifier. Firstly, that it be unique to the originator and, secondly, that it be prefixed with "**CEMOR.**".

$6: Title of the CEMOR

309 A short descriptive title for this CEMOR.

$7: CEM document reference

310 Single reference to the affected area of the CEM. This field shall identify the CEM part number and Section number and. Additionally, a paragraph number (or, if no paragraph number is relevant, the table or figure number) shall also be identified in this field.

$8: Statement of observation

311 Comprehensive description of the observation. There is no restriction regarding the length of this field. However, it shall contain text only; no figures or tables other than what can be achieved within the realm of ASCII shall be used.

$9: Suggested solution(s)

312 Proposed solution(s) for addressing the observation.

$$ End of CEMOR

313 Required to mark the end of CEMOR relevant information.

E.3.1 Example observation:

$1: A. N. Other

$2: PPs 'R' US

$3: another@ppsrus.com

$4: 96/01/31

$5: CEMOR.ano.comment.1

$6: Spelling Error

$7: Part 1, Section 3.1.5, Paragraph 49

$8: "Summarizes"

$9: If the intent is to use UK English, use "summarises".$$