



**Common Criteria  
for Information Technology  
Security Evaluation**

---

**CCEB-96/011**

**Part 1:  
Introduction and general model**

Version 1.0

96/01/31

# Foreword

Following extensive international cooperation to align the source criteria from Canada (CTCPEC), Europe (ITSEC) and the United States of America (TCSEC and Federal Criteria), version 1.0 of the *Common Criteria for Information Technology Security Evaluation* is issued for the purpose of trial evaluations and for review by the international security community. The practical experience acquired through trial evaluations and all the comments received will be used to further develop the criteria.

A template for reporting observations on version 1.0 of the CC is included at the end of this document. Any observation reports should be communicated to one or more of the following points of contact at the sponsoring organisations:

## **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>

## **UK IT Security and Certification Scheme**

Senior Executive  
P.O. Box 152  
Cheltenham GL52 5UF  
United Kingdom  
Tel: (+44) 1242 235739, Fax:(+44)1242 235233  
E-mail: ccv1.0@itsec.gov.uk  
ftp: ftp.itsec.gov.uk  
<http://www.itsec.gov.uk>

## **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**

Bureau Normalisation, Critères Communs  
18 rue du docteur Zamenhof  
92131 Issy les Moulineaux  
France  
Tel: (+33)(1)41463784, Fax:(+33)(1)41463701  
E-mail:ssi28@calvacom.fr

## **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 viii and from 1 to 60

## Table of contents

<b>Chapter 1</b>		
	Introduction .....	1
1.1	Overview .....	1
1.2	Background of the Common Criteria .....	2
1.3	Target audience of the CC .....	2
1.3.1	Consumers .....	3
1.3.2	Developers .....	3
1.3.3	Evaluators .....	3
1.3.4	Others .....	4
1.4	Organisation of Common Criteria .....	4
1.5	Scope and applicability .....	6
 <b>Chapter 2</b>		
	General model .....	9
2.1	Common Criteria approach .....	9
2.1.1	Development .....	9
2.1.2	Evaluation .....	10
2.1.3	Operation .....	11
2.2	Security Framework .....	11
2.3	Common Criteria concepts .....	13
2.3.1	Organisation of Common Criteria requirements .....	13
2.3.2	Construction of TOE requirements .....	14
2.3.3	Construction of TOE specifications .....	17
2.3.4	Sources of requirements .....	17
2.3.5	Stages of evaluation .....	18
 <b>Chapter 3</b>		
	Common Criteria evaluation results .....	19
3.1	Introduction .....	19
3.2	Protection Profile and Security Target evaluation .....	19
3.3	TOE evaluation .....	19
3.4	Expression of security functions and assurance .....	20
3.4.1	Security functions and assurance in Protection Profiles .....	20
3.4.2	Security functions in Security Targets .....	20
3.4.3	Assurance in Security Targets .....	20
3.5	Definition of the CC evaluation results .....	21
 <b>Annex A</b>		
	Glossary of terms (normative) .....	23
A.1	Common abbreviations .....	23
A.2	Scope of glossary .....	23
A.3	Glossary .....	23

	<b>Annex B</b>	
	Specification of Protection Profiles (normative) .....	27
B.1	Overview .....	27
B.2	Content of Protection Profile .....	27
B.2.1	PP introduction .....	27
B.2.2	TOE description .....	28
B.2.3	Security environment .....	29
B.2.4	Security objectives .....	29
B.2.5	IT security requirements .....	30
B.2.6	Application notes .....	30
B.2.7	Rationale .....	31
	<b>Annex C</b>	
	Specification of Security Targets (normative) .....	33
C.1	Overview .....	33
C.2	Content of Security Target .....	33
C.2.1	ST introduction .....	33
C.2.2	TOE description .....	35
C.2.3	Security environment .....	35
C.2.4	Security objectives .....	36
C.2.5	IT security requirements .....	36
C.2.6	TOE summary specification .....	37
C.2.7	PP claims .....	37
C.2.8	Rationale .....	39
	<b>Annex D</b>	
	Security concepts and principles (informative) .....	41
D.1	Introduction .....	41
D.2	General security context .....	41
D.3	Information technology security context .....	43
	<b>Annex E</b>	
	Security development and evaluation model (informative) .....	45
E.1	Introduction .....	45
E.2	Development of security requirements and specifications .....	45
E.3	Development of TOE .....	48
E.4	Evaluation context .....	49
E.5	Use of evaluation results .....	51

	<b>Annex F</b>	
	Bibliography (informative) .....	53
	<b>Annex G</b>	
	CC observation report (CCOR) .....	55
G.1	Introduction .....	55
G.2	Categorisation of observation report .....	55
G.3	Format of observation report .....	56
G.3.1	Tag definitions for observation report .....	56
G.3.2	Example observations: .....	58
G.4	Printed observation report .....	59



**List of figures**

Figure 2.1 - Influence of evaluation .....	10
Figure 2.2 - Organisation and construction of requirements .....	16
Figure B.1 - Protection Profile content .....	28
Figure C.1 - Security target content .....	34
Figure D.1 - Security concepts and relationships .....	41
Figure D.2 - Evaluation concepts and relationships .....	42
Figure E.1 - Derivation of requirements and specifications .....	46
Figure E.2 - TOE development model .....	49
Figure E.3 - Evaluation context .....	50
Figure E.4 - Use of evaluation results .....	51



**List of tables**

Table 1.1 - Roadmap of Common Criteria ..... 5  
Table G.1 - CC observation report ..... 60



## Chapter 1

# Introduction

### 1.1 Overview

1 Information held by IT systems is a critical resource which enables organisations to succeed in their mission. Additionally, individuals whose personal information is contained in IT systems have a reasonable expectation of privacy and protection from harm. Beneficiaries of IT systems have a legitimate expectation that the systems will perform their functions efficiently whilst exercising proper control of the information to ensure it is protected against hazards such as unwanted or unwarranted dissemination, alteration, or loss. The term IT security is used to cover prevention and mitigation of these and similar hazards.

2 Analysis of the threats to an IT system can show what threats are conceivable, and an analysis of the risks can aid selection of security measures to be implemented to reduce risk to an acceptable level and enforce security policies. These security measures can be provided via appropriate combinations of IT system functions and/or external measures.

3 The beneficiaries of an IT system's security and its designers need to be confident that the system's security measures are fit for their intended purpose.

4 Many consumers of IT lack the knowledge and expertise necessary to judge whether their confidence in the security of their IT systems is appropriate, and they may not wish to rely solely on the assertions of the developers. Consumers may therefore choose to increase their confidence in the security measures of an IT system by ordering an analysis of its security and specifying IT products which have undergone a security evaluation.

5 This Common Criteria document (CC) contains criteria for use as the basis for evaluation of IT security properties. The requirements can also be used for the selection of appropriate IT security measures. By establishing a common criteria base, the results of an evaluation will be more meaningful to a wider audience. Common criteria will permit a degree of comparability between the results of otherwise independent security evaluations. The evaluation results are then available to consumers to aid in determining whether an evaluated IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.

6 In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme which sets the standards and monitors the quality of the evaluations. Such evaluation schemes currently exist in several nations and are based on different (though broadly comparable) evaluation criteria.

7 The CC is intended to be compatible with these existing evaluation criteria, and thus to preserve current investment in security evaluations. It also aims to improve on the existing material by introducing new concepts and clarifying current ones.

8 The CC contains the criteria for stating and evaluating security functional and assurance requirements, accompanied by informational material. The purpose of the latter is to provide guidance for using the CC and to make the material accessible to a wider audience.

## 1.2 Background of the Common Criteria

9 The CC represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community. In the early 1980's the Trusted Computer System Evaluation Criteria (TCSEC) was developed in the United States. In the succeeding decade, various countries began initiatives to develop evaluation criteria which built upon the concepts of the TCSEC but were more flexible and adaptable to the evolving nature of IT in general.

10 In Europe, the Information Technology Security Evaluation Criteria (ITSEC) version 1.2 was published in 1991 by the European Commission after joint development by the nations of France, Germany, the Netherlands, and the United Kingdom. In Canada, the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) version 3.1 was published in 1993 as a combination of the ITSEC and TCSEC approaches. In the United States, the draft Federal Criteria for Information Technology Security (FC) version 1 was also published in 1993, as a second approach to combining North American and European concepts for evaluation criteria.

11 Work began in 1990 in the International Organisation for Standardisation (ISO) to develop an international standard evaluation criteria for general use. The new criteria was to be responsive to the need for mutual recognition of standardised security evaluation results in a global IT market. This task was assigned to Working Group 3 (WG3) of subcommittee 27 (SC27).

12 In June 1993, the authors of the CTCPEC, FC, TCSEC, and ITSEC pooled their efforts and began a project to align their criteria and create a single draft CC document. The intent of the project is to resolve the conceptual and technical differences found in the source criteria and then, to deliver the results to ISO as a contribution toward its work in progressing the international standard.

## 1.3 Target audience of the CC

13 IT security evaluations are methodical investigations of the security properties of IT products and systems - referred to in the CC as Targets of Evaluation (TOEs).

14 Three groups with a general interest in these evaluations can be identified. These are TOE consumers, TOE developers, and TOE evaluators. The criteria presented

in this document have been structured to support the needs of all three groups. They are all considered to be the principal users of this CC. The three groups can benefit from the criteria as explained in the following paragraphs.

### 1.3.1 Consumers

15 Consumers can use evaluation to help decide whether an evaluated product or system fulfils their security needs. These security needs are typically identified as a result of both risk analysis and policy direction. The CC plays an important role in supporting techniques for consumer selection of IT security requirements to express their organisational needs. The CC is written to ensure that evaluation fulfils the needs of the consumers as this is the fundamental purpose and justification for the evaluation process.

16 The CC provides a construct for presenting the IT security properties of a product or system that permits a consumer to make an informed decision to use it. Consumers can use evaluation to compare different products or systems. Presentation of the assurance requirements within a hierarchy supports this need.

17 The CC also gives consumers - especially in consumer groups and communities of interest - an implementation-independent structure termed the Protection Profile (PP) in which to express their special requirements for IT security measures in a TOE.

### 1.3.2 Developers

18 The CC supports developers in preparing for and assisting in the evaluation of their products or systems. The CC provides constructs for stating security requirements that support developers in identifying those requirements to be satisfied by their own product or system. They can then use those constructs to make claims that their TOE conforms to those requirements by means of specified security functions and assurances to be evaluated. These requirements are contained in an implementation-dependent construct termed the Security Target (ST).

19 The developers can use the CC to determine their responsibilities and actions in supporting the evaluation of the TOE. The CC describes actions a developer is to carry out and defines the content and presentation of evidence about the TOE a developer is to provide for an evaluation. More detailed developer instructions are also likely to be issued by evaluation authorities.

### 1.3.3 Evaluators

20 The CC contains criteria to be used by evaluators when forming judgements about the conformance of TOEs to their security requirements. The CC describes the set of general actions the evaluator is to carry out. Note that the CC does not specify procedures to be followed in carrying out those actions. An evaluation methodology document with guidance on evaluator actions will supplement the CC in this area.

### 1.3.4 Others

21 Whilst the CC is oriented towards specification and evaluation of the IT security properties of TOEs, it may also be useful as reference material to all parties with an interest in or responsibility for IT security. Some of the additional interest groups that can benefit from information contained in the CC are:

- a) system custodians and system security officers responsible for determining and meeting organisational IT security policies and requirements;
- b) auditors, both internal and external, responsible for assessing the adequacy of the security of a system;
- c) security architects and designers responsible for the specification of the security content of IT systems and products;
- d) accreditors responsible for accepting an IT system for use within a particular environment;
- e) sponsors of evaluation responsible for requesting and supporting an evaluation;
- f) evaluation authorities responsible for the management and oversight of IT security evaluation programmes.

## 1.4 Organisation of Common Criteria

22 The CC is presented as a set of distinct but related parts as identified below. Terms used in the description of the parts are explained in Chapter 2.

- a) **Part 1: Introduction and general model** is the introduction to the CC and defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. In addition, the target audience is described, with pointers to the various parts of the CC where their individual interests with respect to security criteria and evaluation are covered.
- b) **Part 2: Security functional requirements** establishes a set of functional components as a standard way of expressing the functional requirements for TOEs. Part 2 catalogues the set of functional components, families, and classes.
- c) **Part 3: Security assurance requirements** presents evaluation assurance levels that define the CC scale for rating assurance for TOEs. Part 3 establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. Part 3 catalogues the set of assurance

components, families and classes. Part 3 also defines evaluation criteria for PPs and STs.

- d) **Part 4: Predefined Protection Profiles** initially contains examples of PPs that represent functional and assurance requirements which have been identified in source criteria, including ITSEC, CTCPEC, FC, and TCSEC, as well as requirements not represented in the source criteria. Part 4 will ultimately become the registry for PPs which have completed the registration process.
- e) **Part 5: Registration procedures (planned)** will define the procedures necessary to register additional PPs and to maintain them in an international registry.

23 In addition to the five parts of the CC listed above, other types of documents will be published, including technical rationale material and guidance documents.

24 The following table presents, for the three key target audience groupings, how the parts of the CC will be of interest to them.

**Table 1.1 - Roadmap of Common Criteria**

	<b>Consumers</b>	<b>Developers</b>	<b>Evaluators</b>
<b>Part 1</b>	Use for background information and reference purposes.	Use for background information and reference for the development of requirements and formulating security specifications for TOEs.	Use for background information and reference purposes. Guidance structure for PPs and STs.
<b>Part 2</b>	Use for guidance and reference when formulating statements of requirements for security functions.	Use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Mandatory statement of evaluation criteria when determining whether TOE effectively meets claimed security functions.
<b>Part 3</b>	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.
<b>Part 4</b>	Use for guidance and reference when formulating requirements.	Use for reference when interpreting statements of requirements and formulating security specifications for TOEs.	Mandatory reference base when determining claimed conformance of TOEs to PPs.
<b>Part 5</b>	Use for guidance when offering PPs for registration	Use for guidance when offering PPs for registration	Use for guidance when determining whether PPs are eligible for registration

## 1.5 Scope and applicability

- 25 The CC supports the selection and evaluation of IT security properties of TOEs. The CC is useful as a guide for development of products or systems with IT security functions and for procurement of commercial products and systems with such functions. The CC defines a basis for evaluation of a TOE in order to establish the level of confidence that may be held in its IT security. Such TOEs include, for example, operating systems, computer networks, distributed systems, and application services.
- 26 The aspects of IT security addressed by the CC include, but are not limited to, the protection of information from unauthorised disclosure, modification, or loss of use by countering threats to that information arising from human activities whether malicious or otherwise. Resistance to these three types of damage is commonly called confidentiality, integrity, and availability, respectively. The CC is also designed to be applicable to aspects of IT security which do not fall clearly within these three. The CC could be applied in other areas of IT, but makes no claim of competence outside the strict domain of IT security.
- 27 The CC is applicable to IT security measures implemented in hardware or software. Where particular aspects of evaluation are intended only to apply to certain methods of implementation, this will be indicated within the relevant criteria statements.
- 28 Certain topics, because they involve specialised techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the CC. Some of these are identified below.
- a) The CC does not cover evaluation of administrative security measures. A significant part of the security of a TOE can often be achieved through administrative measures such as organisational, personnel, physical, and procedural controls. Administrative security measures in the operating environment of the TOE are considered only where these have an impact on the ability of the IT security measures to counter the identified threats.
  - b) The evaluation of technical physical aspects of IT security such as electromagnetic emanation control is not discussed.
  - c) The organisation-specific evaluation methodology, and any scheme established to use the results generated by evaluation, are matters left up to individual evaluation authorities. The CC provides technical evaluation criteria only and does not address the evaluation methodology or the administrative and legal framework under which the criteria may be applied by the evaluation authorities. However, it is expected that the CC will be used for evaluation purposes in the context of such a framework, and such a methodology, as a requirement for the successful application of its more subjective elements.
  - d) The procedures for use of evaluation results in system accreditation are outside the scope of the CC. System accreditation is the administrative process whereby authority is granted for the operation of an IT system in its

full operational environment. Evaluation focuses on the IT security parts of the system and those parts of the operational environment which may directly affect the IT elements. The results of the evaluation process are consequently a valuable input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related system security properties and their relationship to the IT security parts, accreditors should make separate provision for those aspects.

- e) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms and related techniques is not covered in the CC. Should independent assessment of mathematical properties of cryptography embedded in a TOE be required, the scheme under which the CC is applied must make provision for such assessments.



## Chapter 2

# General model

## 2.1 Common Criteria approach

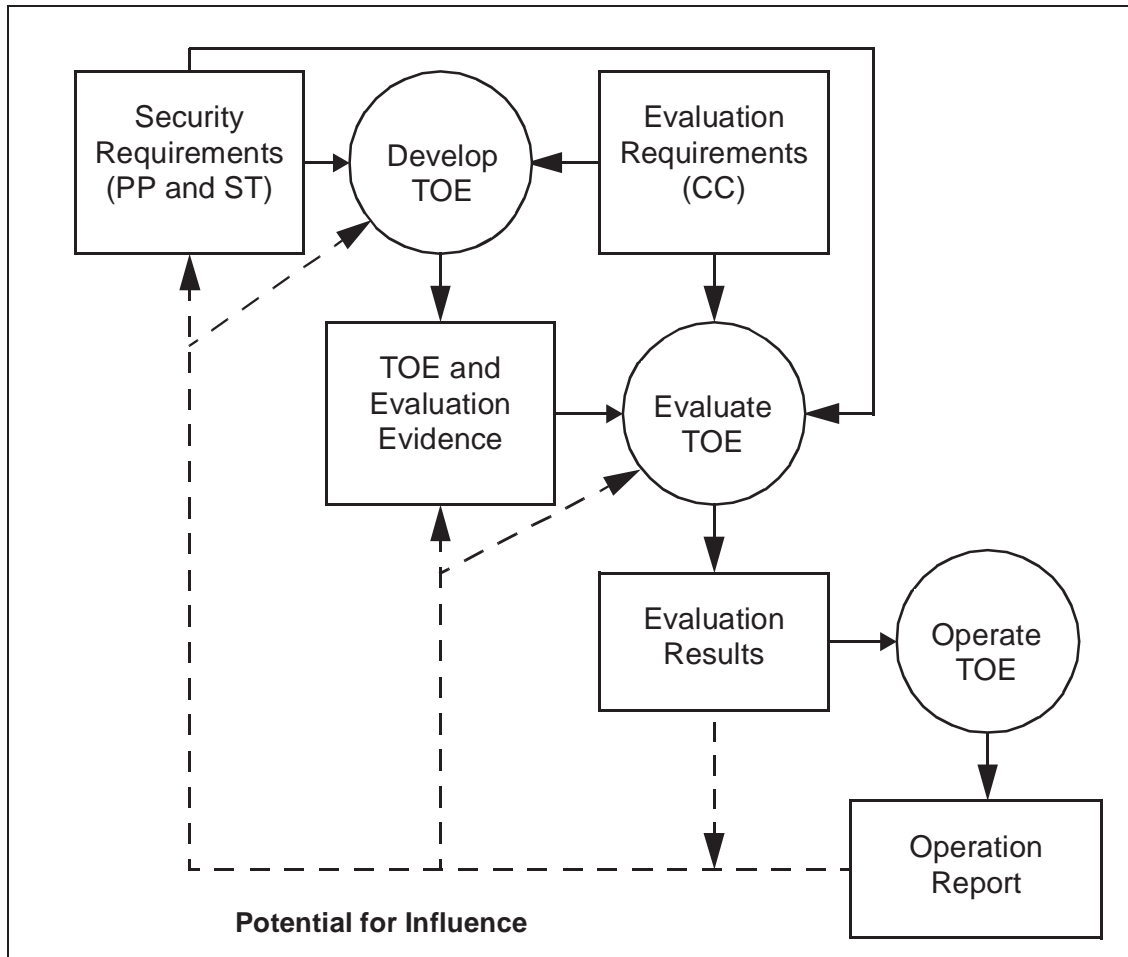
29 Confidence in IT security can be gained through actions that may be taken during the processes of development, evaluation, and operation. Figure 2.1 illustrates the relationships between evaluation and the IT product or system, which are briefly described below (see Annex E for background discussion).

### 2.1.1 Development

30 It is essential that the security requirements imposed on the IT development be effective in contributing to the security objectives of consumers. Unless suitable requirements are established at the start of the development process, the resulting end product, however well engineered, may not meet the objectives of its anticipated consumers.

31 The CC defines a set of IT security requirements of known validity which can be used in establishing security requirements for prospective products and systems. The CC also defines the PP construct which allows prospective consumers or developers to create standardised sets of these security requirements which will meet their needs. Developers should use PPs as the basis for specifying products or systems to be developed.

32 The TOE is that part of the product or system which is subject to evaluation. The TOE security threats, objectives, requirements, and summary specification of security functions and assurance measures together form the primary inputs to the ST, which is used by the evaluators as the basis for evaluation.



**Figure 2.1 - Influence of evaluation**

### 2.1.2 Evaluation

33 The evaluation process may be carried out in parallel with development, or it may follow. The principal inputs to evaluation are:

- a) an ST describing the security functions of the TOE to be evaluated and containing the security requirements, which may be by reference to any PP(s) to which conformance is claimed;
- b) the set of evidence about the TOE;
- c) the TOE for which the security evaluation is required.

34 Additional input comes from application notes of the CC and the IT security expertise of the evaluator and the evaluation community.

35 The expected result of the evaluation process is a confirmation that the ST is satisfied for the TOE with one or more reports documenting, at various levels of detail, the evaluator findings about the TOE as determined by the evaluation criteria. These reports will be useful to actual and potential consumers of the product or system represented by the TOE as well as to the developer.

36 Evaluation leads to more care being taken in product design, development, and operation. Evaluation reduces the probability of errors or vulnerabilities remaining in the TOE and may therefore influence the initial requirements, the development process, the end product, or the operational environment.

### 2.1.3 Operation

37 Consumers may elect to use evaluated products in their particular environment. Once a TOE is in operation, it is possible that previously unknown errors or vulnerabilities may surface or environmental assumptions may need to be revised. As a result, reports could be made which would require the developer to correct the TOE or redefine its security requirements or environmental assumptions. Such changes require the TOE to be re-evaluated or the security of its operational environment to be strengthened. Procedures for re-evaluation, including reuse of evaluation results, are outside the scope of the CC and are expected to be covered by evaluation authorities when developing a standardised methodology.

## 2.2 Security Framework

38 The CC discusses security using a set of security concepts and terminology. An understanding of these concepts and the terminology is a prerequisite to the effective use of the CC. However, the concepts themselves are quite general and are not intended to restrict the class of IT security problems to which the CC is applicable.

39 The CC is applicable when IT is being used and there is concern about the ability of the IT element to safeguard assets. In order to show that the assets are secure, the security concerns must be addressed at all levels from the most abstract to the final IT implementation in its operational environment. The CC layers these levels of abstraction as follows.

- a) The **security environment** includes all the laws, organisational security policies, customs, expertise, and knowledge that are, or may be, relevant. It thus defines the context in which the TOE is used. The security environment also includes the threats to security which are, or are held to be, present in the environment.
- b) The **security objectives** are a statement of intent to counter the identified threats and meet stated organisational security policies. The **IT security**

**objectives** cover those threats and security policies which are to be addressed by IT, and are of particular relevance to the TOE.

- c) The **TOE security requirements** are the refinement of the IT security objectives into a set of technical IT requirements for security functions and assurances which, if met, will ensure that the TOE can meet its security objectives.
- d) The **TOE security specifications** define an actual or proposed implementation for the TOE. If implemented according to the security specification, the TOE will meet its security objectives.
- e) The **TOE implementation** is the realisation of the TOE in accordance with the TOE security specifications.

40 The layers described permit security problems and issues to be characterised and discussed but do not, of themselves, demonstrate that the final IT implementation does actually exhibit the required security behaviour and can, therefore, be trusted.

41 The CC requires, therefore, that certain layers contain a rationale for the representation of the TOE at that level. That is, such a layer must contain a reasoned and convincing argument that shows that it is in conformance with the higher layer and is itself complete, correct, and internally self consistent. Statements of rationale demonstrating compliance with the adjacent higher level representation contribute to the case for TOE correctness. Rationale directly demonstrating compliance with security objectives supports the case that the TOE is effective in countering the threats and enforcing the organisational security policy.

42 Security requirements generally include both requirements for the presence of desired behaviour and requirements for the absence of undesired behaviour. It is normally possible to demonstrate, by use or testing, the presence of the desired behaviour. It is not always possible to perform a conclusive demonstration of absence of undesired behaviour. Testing, design review, and implementation review contribute significantly to reducing the risk that such undesired behaviour is present. The rationale statements provide further support to the claim that such undesired behaviour is absent.

43 Those responsible for security may seek to increase the confidence they have in the TOE by seeking expert analysis (i.e., evaluation) of the TOE and the various statements of rationale.

44 The CC presents the framework in which such evaluation can take place. By presenting the requirements for evidence and analysis, a more objective, and hence useful evaluation result can be achieved. The CC incorporates a common set of constructs and a language in which to express and communicate the relevant aspects of IT security and permits those responsible for IT security to benefit from prior experience and expertise of others.

## 2.3 Common Criteria concepts

45 The CC presents requirements for the IT security of a TOE under the distinct categories of functional requirements and assurance requirements.

46 The CC functional requirements are levied on those functions of the TOE that are specifically in support of IT security and define the desired security behaviour. Part 2 defines the CC functional requirements.

47 Examples of functional requirements include requirements for identification, authentication, security audit, or non-repudiation of origin.

48 Assurance is a property of a TOE which gives grounds for confidence that the claimed security measures of the TOE are effective and implemented correctly. Assurance is derived from knowledge about the definition, construction, and operation of the TOE. Part 3 defines the CC assurance requirements.

49 Examples of assurance requirements include required constraints on the rigour of the development process and requirements to search for, and analyse, the impact of potential security vulnerabilities.

### 2.3.1 Organisation of Common Criteria requirements

50 The CC presents requirements for TOE functions and assurance in the same general style and uses the same organisation and terminology for each.

51 The term class is used for the most general grouping of security requirements. All the members of a class share a common intent, while differing in coverage of security objectives.

52 The members of a class are termed families. A family is a grouping of sets of security requirements which share security objectives but may differ in emphasis or rigour.

53 The members of a family are termed components. A component describes a specific set of security requirements and is the smallest selectable set of security requirements for inclusion in the structures defined in the CC. In most cases, the set of components within a family will be ordered to represent increasing strength or capability of security requirements which share a common purpose.

54 The components are constructed from individual elements. The element is the lowest level expression of security requirements and is the indivisible security requirement which evaluation confirms as satisfied.

55 The organisation of the CC security requirements into the hierarchy of class - family - component - element is provided to help consumers locate the right components once they have identified the threats to the information in their IT environment.

### 2.3.1.1 Dependencies between components

56 Dependencies may exist between components. Dependencies arise when a component is not self sufficient and relies upon the presence of another component. Dependencies may exist between functional components, between assurance components, and between functional and assurance components.

57 Component dependency descriptions are part of the CC component definitions. In order to ensure completeness of the TOE requirements, dependencies must be satisfied when incorporating components into PPs and STs.

### 2.3.1.2 Permitted operations on components

58 CC components may be used exactly as defined in the CC, or they may be tailored through the use of permitted operations in order to meet a specific security policy or counter a specific threat. Not all operations are permissible on all components. Each CC component identifies and defines any permitted operations, the circumstances under which the operation may be applied to the component, and the results of the application of the operation. The permitted operations are:

- a) **assignment** which permits the specification of a parameter to be filled in when the component is used;
- b) **selection** which permits the specification of elements which are to be selected from a list given in the component;
- c) **refinement** which permits the addition of extra detail when the component is used.

### 2.3.2 Construction of TOE requirements

59 The CC defines a set of constructs which combine security requirement components into meaningful assemblies. The relationships among the various concepts for requirements expression are described below and illustrated in figure 2.2.

60 An intermediate combination of components is termed a package. The package permits the expression of a set of requirements which meet an identifiable subset of security objectives. A package is intended to be reusable and to define requirements which are known to be useful and effective in meeting the identified objectives. A package may be used in the construction of larger packages, PPs, and STs.

61 The evaluation assurance levels (EALs) are predefined assurance packages contained in Part 3. An EAL is the baseline set of assurance requirements for evaluation. EALs each define a complete set of assurance requirements. Together, the EALs form an ordered set which defines the assurance scale of the CC.

62 The PP contains a set of CC functional and assurance requirements components which include an EAL. The PP permits the implementation independent expression of security requirements for a set of TOEs which will comply fully with a set of security objectives. A PP is intended to be reusable and to define TOE requirements

which are known to be useful and effective in meeting the identified objectives, both for functions and assurance.

- 63 The ST contains a set of security requirements which may be made by reference to a PP, directly by reference to the CC, or stated explicitly. The ST permits the expression of security requirements for a specific TOE which are shown, by evaluation, to be useful and effective in meeting the identified objectives.

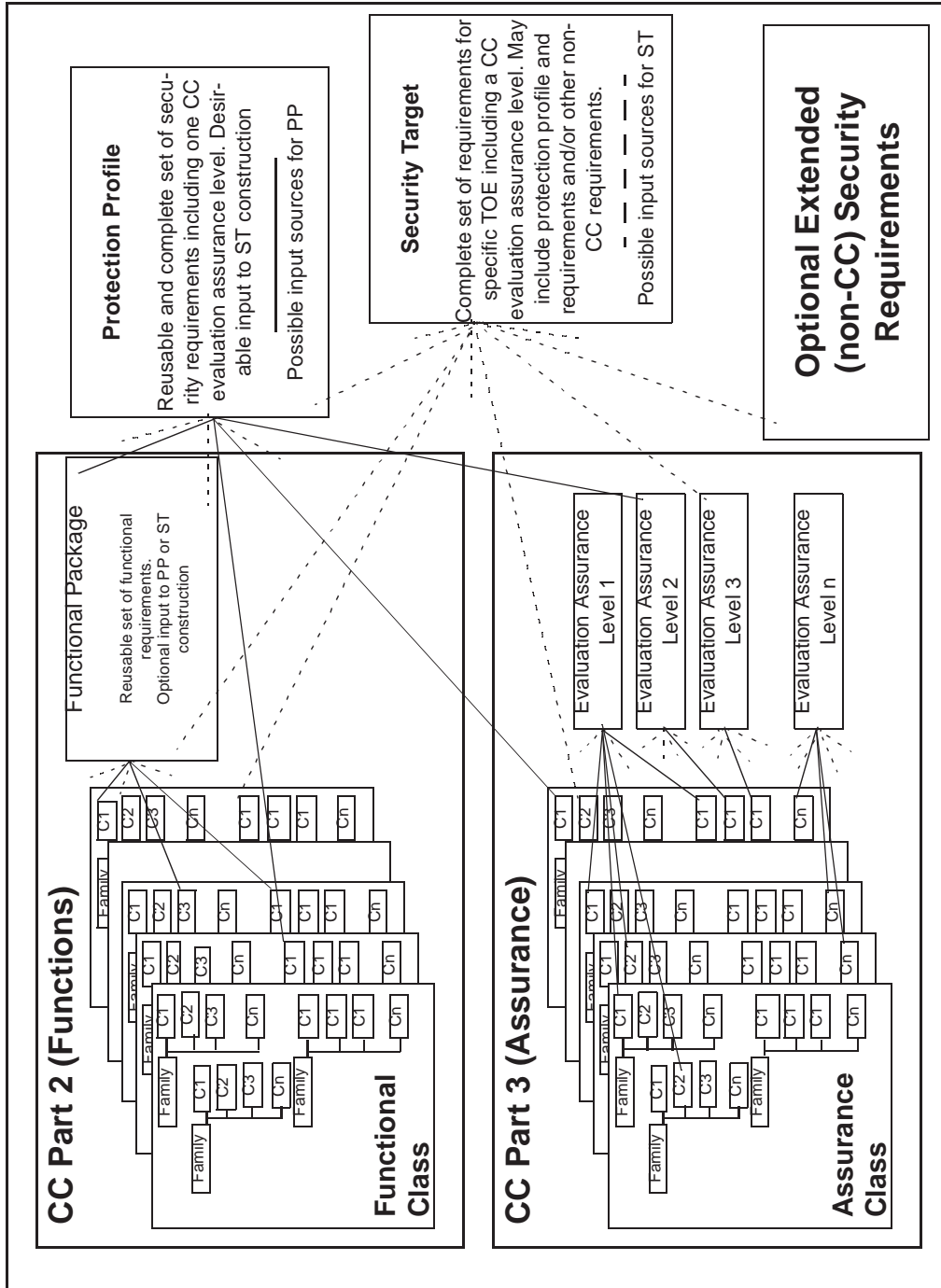


Figure 2.2 - Organisation and construction of requirements

### 2.3.3 Construction of TOE specifications

64 The TOE specifications are derived by refining the security requirements through a process of applying security and IT engineering skills and knowledge.

65 The **TOE summary specification** provides a high-level definition of the TOE security functions and assurance measures to a sufficient depth to scope the evaluation.

66 The ST contains the TOE summary specification for the TOE, together with the security requirements and objectives and the rationale for each. The ST is the basis for the agreement between the TOE developers, consumers, evaluators, and evaluation authorities as to what security the TOE offers.

### 2.3.4 Sources of requirements

67 TOE security requirements can be constructed by using the following inputs:

a) Existing PPs

The TOE security requirements in an ST may be adequately expressed by, or are intended to comply with, a pre-existing statement of requirements contained in an existing PP.

b) Existing packages

Part of the TOE security requirements in a PP or ST may have already been expressed in a package which may be used.

c) Existing EALs

The TOE assurance requirements in a PP or ST shall include an EAL from Part 3.

d) Existing functional or assurance requirements components

The TOE functional or assurance requirements in a PP or ST may be expressed directly, using the components in Part 2 or 3.

e) Extended requirements

Additional functional requirements not contained in Part 2 and/or additional assurance requirements not contained in Part 3 may be used in an ST.

68 Existing requirements material from Parts 2 and 3 should be used where available. The use of an existing PP will ensure that the TOE will meet a well known set of needs of known utility and thus be more widely recognised.

69 The PP might be developed by user communities, IT product developers, or other parties interested in defining such a common set of requirements. A PP gives

consumers a means of referring to a specific set of needs and facilitates future evaluation against those needs.

### 2.3.5 Stages of evaluation

70 Distinct stages of evaluation are identified corresponding to the principal layers of TOE representation, that is requirements, specifications, and implementation. These evaluations are:

- a) the **PP evaluation** carried out against the evaluation criteria for PPs contained in Part 3. The goal of such an evaluation is to demonstrate that the PP is complete, consistent, and technically sound and suitable for use as a statement of requirements for an evaluatable TOE. Such a PP is eligible for inclusion within a PP registry.
- b) the **TOE evaluation** carried out in two phases:
  - 1) the **ST evaluation** carried out against the evaluation criteria for STs contained in Part 3. The goal of such an evaluation is to demonstrate that the ST properly meets the requirements of the PP and is complete, consistent, and technically sound and hence suitable for use as the basis for the corresponding TOE evaluation.
  - 2) the **TOE evaluation** carried out against the evaluation criteria contained in Part 3 using an evaluated ST as the basis. The goal of such an evaluation is to demonstrate that the TOE meets the security requirements contained in the ST.

## Chapter 3

# Common Criteria evaluation results

### 3.1 Introduction

71 There is no totally objective scale for representing the results of an IT security evaluation. The results arise from the application of criteria which contain both objective and subjective elements. Precise and universal ratings for IT security are not, therefore, feasible.

72 A rating made relative to the CC represents the findings of a specific type of investigation of the security properties of a TOE. Such a rating does not guarantee fitness for use in any particular application environment. The decision to accept a TOE for use in a specific application environment is based on consideration of many security issues including the evaluation findings.

### 3.2 Protection Profile and Security Target evaluation

73 The CC contains the evaluation criteria which permit an evaluator to state whether a PP or ST is complete, consistent, and technically sound and hence suitable for use as a statement of requirements for an evaluatable TOE. Criteria are also provided to evaluate any ST claims of compliance with any PPs. Evaluation of the PP or ST will result in a pass/fail statement.

### 3.3 TOE evaluation

74 The CC contains the evaluation criteria which permit an evaluator to determine whether the TOE satisfies the security requirements expressed in the ST. By using the CC in evaluation of the TOE, the evaluator will be able to make statements about:

- a) whether the specified security functions of the TOE meet the functional requirements and are thereby effective in meeting the security objectives of the TOE;
- b) whether the specified security functions of the TOE are correctly implemented.

75 The security requirements expressed in the CC define the known working domain of applicability of IT security evaluation criteria. A TOE for which the security requirements are expressed only in terms of the functional and assurance requirements drawn from the CC will be evaluatable against the CC. However there may be a need for a TOE to meet security requirements not directly expressed in the CC. The CC recognises the necessity to evaluate such a TOE but, as the additional

requirements lie outside the known domain of applicability of the CC, the results of such an evaluation must be qualified accordingly and may place at risk universal acceptance of the evaluation results.

76 The results of an evaluation will include a statement of conformance to the CC. Describing the security of a TOE in CC terms permits comparison of the security characteristics of TOEs in general.

### **3.4 Expression of security functions and assurance**

77 The CC defines a single set of IT security criteria that can address the needs of many communities and thus serve as a major expert input to the production of an international standard for IT security. The CC has been developed around the central notion that use only of the security functional components and packages contained in Part 2, and the EALs and components contained in Part 3, represents the preferred course of action for expression of TOE requirements, as they represent a well-known and understood domain.

78 The following caveats apply to the expression of security functions and assurance in PPs and STs.

#### **3.4.1 Security functions and assurance in Protection Profiles**

79 A PP is a successfully evaluated set of functional and assurance requirements. A PP is defined as a set of requirements that consists only of functional requirement components contained in Part 2 and an EAL (possibly augmented by additional assurance components) contained in Part 3.

#### **3.4.2 Security functions in Security Targets**

80 The CC provides for the articulation in STs of functional requirements not contained in Part 2. However, the following caveats apply to the inclusion of these novel functional components in STs.

- a) Any functional requirements presented in an ST shall comply with annex C of Part 1.
- b) Evaluation results obtained using functional components not drawn from Part 2 of the CC are qualified as such. The incorporation of novel functional requirements into STs requires more than conformance to the CC structure and rules and does not guarantee the universal acceptance of the evaluation results by the involved evaluation authorities.

#### **3.4.3 Assurance in Security Targets**

81 ST assurance requirements shall consist of at least an EAL (possibly augmented by additional assurance components) contained in Part 3. Assurance components other than those contained in Part 3 may be included in STs. However, the following caveats apply to the inclusion of these novel assurance components in STs:

- a) Any assurance requirements presented in an ST shall comply with annex C of Part 1.
- b) Evaluation results obtained using assurance requirements not drawn from Part 3 of the CC are qualified as such. Use of such extended assurance requirements does not guarantee universal acceptance of the evaluation results by the involved evaluation authorities.

### 3.5 Definition of the CC evaluation results

82 The result of the evaluation shall be a statement which describes the extent to which the TOE can be trusted to conform to the requirements. The results shall be stated with respect to both Part 2 (functional requirements) and Part 3 (assurance requirements) or directly to a PP, as listed below.

- a) A TOE is **Conformant to Part 2** if and only if it is based upon functional components contained in Part 2.
- b) A TOE is **Part 2 extended** if it is based upon functional components contained in Part 2 plus additional functional requirements not contained in Part 2.
- c) A TOE is **Conformant to Part 3** if and only if it is based upon an EAL contained in Part 3.
- d) A TOE is **Part 3 augmented** if and only if it is based upon an EAL and other assurance components contained in Part 3.
- e) A TOE is **Part 3 extended** if it is based upon an EAL and optionally other assurance components contained in Part 3 plus additional assurance requirements not contained in Part 3.
- f) A TOE is **Conformant to PP** if and only if it is conformant to all parts of the PP.

83 Although the evaluation results 'Part 2 Extended' and 'Part 3 Extended' are defined, it is recommended that these options only be used after very careful consideration of the preferred alternative of being conformant with the requirements presented in the CC.



## Annex A

# Glossary of terms (normative)

### A.1 Common abbreviations

84 The following abbreviations are common to more than one part of the CC:

<b>CC</b>	Common Criteria for Information Technology Security Evaluation
<b>EAL</b>	Evaluation Assurance Level
<b>IT</b>	Information Technology
<b>PP</b>	Protection Profile
<b>SF</b>	Security Function
<b>SFP</b>	Security Function Policy
<b>ST</b>	Security Target
<b>TOE</b>	Target of Evaluation
<b>TSC</b>	TSF Scope of Control
<b>TSF</b>	TOE Security Functions
<b>TSFI</b>	TSF Interface
<b>TSP</b>	TOE Security Policy

### A.2 Scope of glossary

85 This glossary contains only those terms which are used in a specialised way in the CC. The majority of terms in the CC are used either according to their accepted dictionary definitions or according to commonly accepted definitions that may be found in ISO security glossaries or other well-known collections of security terms. Some combinations of common terms used in the CC, while not meriting glossary definition, are explained for clarity in the context where they are used. For an important example of in-context explanation, the reader is referred to the Part 2 and Part 3 'paradigm' sections.

### A.3 Glossary

86 **Assurance** — Property of a TOE giving grounds for confidence that its security functions enforce the TSP.

87 **Augmentation** — The addition of one or more assurance component(s) from Part 3 to an EAL.

88 **Authentication Data** — Information used to verify the claimed identity of a user.

- 89        **Authorised Administrator** — A Human User to whom authorisation has been granted to perform administrative operations which may affect the enforcement of the TSP.
- 90        **Authorised User** — A User who may, in accordance with the TSP, perform an operation.
- 91        **Class** — A grouping of Families which share a common intent.
- 92        **Component** — The smallest selectable set of elements that may be included in a PP, an ST, an EAL or a Package.
- 93        **Dependency** — A relationship between requirements such that one will not meet its objectives unless the other is also satisfied.
- 94        **Element** — An indivisible security requirement.
- 95        **Evaluation Assurance Level (EAL)** — A predefined set of assurance components from Part 3 that represents a point on the CC assurance scale.
- 96        **Extension** — The addition to an ST of functional requirements not contained in Part 2 and/or additional assurance requirements not contained in Part 3.
- 97        **Family** — A grouping of components which share security objectives or threats addressed but may differ in emphasis or rigour.
- 98        **Formal** — Expressed in a notation based on well established mathematical concepts.
- 99        **Human User** — Any person who interacts with the TOE.
- 100       **Informal** — Expressed in natural language.
- 101       **Machine User** — Any IT entity outside of the TOE which interacts with the TOE.
- 102       **Object** — An entity within the TSF Scope of Control (TSC) that contains or receives information and upon which subjects perform operations. Objects are visible through the TSF interface and are composed of one or more TOE resources encapsulated with security attributes.
- 103       **Organisational Security Policy** — A set of security rules, procedures, practices, and guidelines imposed by an organisation upon its operations.
- 104       **Package** — A reusable set of functional or assurance Components combined together to satisfy a set of identified Security Objectives.
- 105       **Protection Profile (PP)** — A reusable and complete combination of Security Objectives, functional and assurance requirements with associated rationale.

- 106        **Reference Monitor** — A concept of an abstract machine that enforces TOE access control policies.
- 107        **Reference Validation Mechanism** — An implementation of the Reference Monitor concept that possesses the following properties: it is tamperproof, always invoked, and small enough to be subjected to thorough analysis and testing.
- 108        **Resource** — Anything usable or consumable in the TOE not directly visible through the TSF interface.
- 109        **Role** — The authorisation to perform a TOE-defined set of functionally related operations that may be granted to Users.
- 110        **Secret** — Information which must be known only to authorised users and/or the TSF in order to enforce a specific SFP.
- 111        **Security Attribute** — Information associated with subjects and/or objects which is used for the enforcement of the TSP.
- 112        **Security Function (SF)** — A part or parts of the TOE which have to be relied upon for enforcing a closely related subset of the rules from the TSP.
- 113        **Security Function Policy (SFP)** — The Security Policy enforced by a SF.
- 114        **Security Objective** — A statement of intent to counter a given threat or enforce a given Organisational Security Policy.
- 115        **Security Policy** — A set of rules designed to meet a set of Security Objectives.
- 116        **Security Target (ST)** — 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.
- 117        **Semiformal** — Expressed in a restricted syntax language with defined semantics.
- 118        **Subject** — An entity within the TSC that causes operations to be performed.
- 119        **Target of Evaluation (TOE)** — An IT product or system that is the subject of an evaluation.
- 120        **TOE Security Functions (TSF)** — All parts of the TOE which have to be relied upon for enforcement of the TSP.
- 121        **TOE Security Policy (TSP)** — The rules defining the security behaviour of a TOE.
- 122        **Trusted Channel** — A means by which two TSFs can communicate directly with necessary confidence to support the TSPs of each TSF.
- 123        **Trusted Path** — A means by which a User and a TSF can communicate directly with necessary confidence to support the TSP of the TSF.

- 124        **TSF Scope of Control (TSC)** — The domain over which the TSF enforces the TSP.
- 125        **User** — Any entity (human or machine) outside the TOE that interacts with the TOE.

## Annex B

# Specification of Protection Profiles (normative)

### B.1 Overview

126 A PP defines an implementation-independent set of IT security requirements and objectives for a category of TOEs. Such TOEs are intended to meet common consumer needs for IT security. Consumers can therefore construct or cite a PP to express their IT security needs without reference to any specific TOE.

127 A PP shall conform to the content requirements described in this annex. A PP should be presented as a user oriented document that minimises reference to other material which might not be readily available to the PP user. Evaluation evidence, such as the rationale, may be supplied separately if that is appropriate.

128 The contents of the PP are portrayed in figure B.1 which should be used as guidance when constructing the structural outline of the PP document. Bolding is used to indicate those parts of the PP which, if present, are subject to evaluation.

### B.2 Content of Protection Profile

#### B.2.1 PP introduction

129 The PP introduction shall contain document management and overview information necessary to operate a PP registry as follows:

- a) The **PP identification** provides the labelling and descriptive information necessary to identify, catalogue, register, and cross reference a PP.
- b) The **PP overview** summarises the PP in narrative form. The overview should be detailed enough for a potential user of the PP to determine whether the PP is of interest. The overview should also be usable as a stand alone abstract for use in PP catalogues and registers.

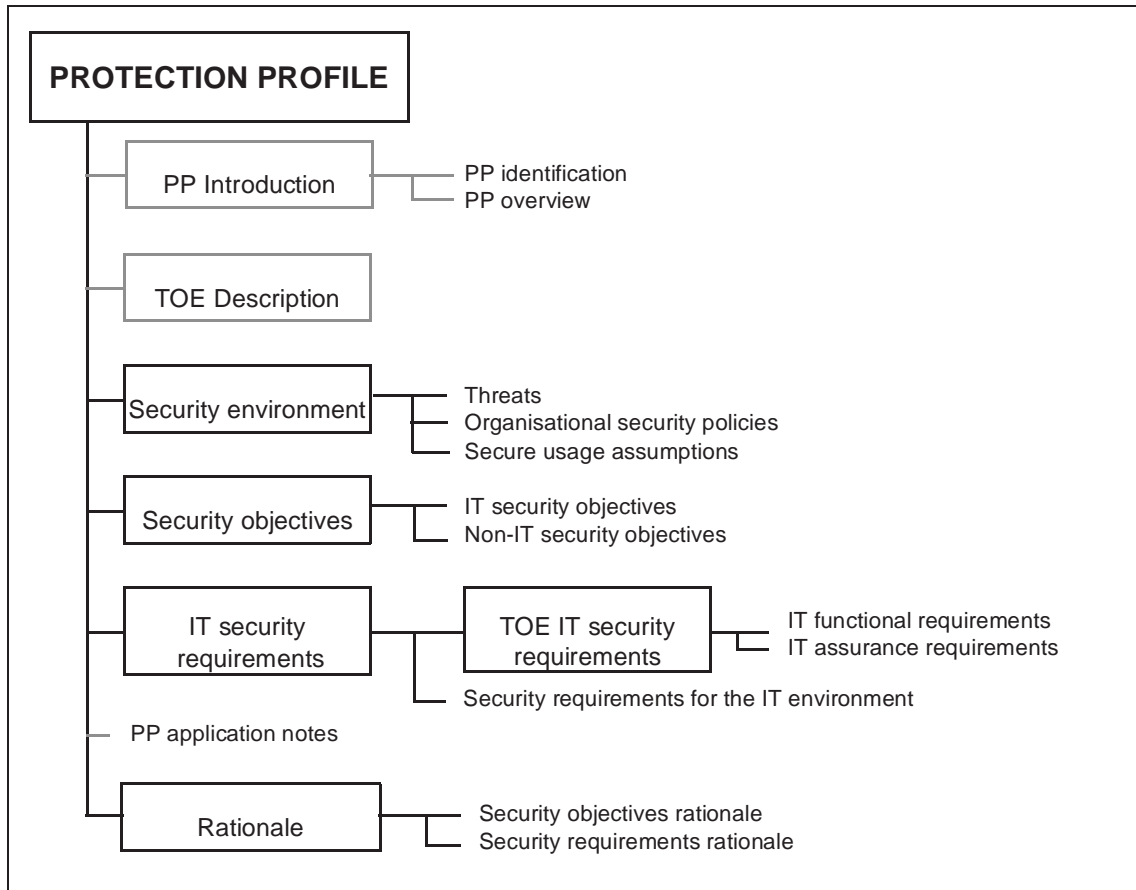


Figure B.1 - Protection Profile content

**B.2.2 TOE description**

130 This part of the PP should describe the TOE as an aid to the understanding of its security requirements and should address the product type, the intended usage, and the general IT features of the TOE. Aspects of usage that may be addressed include the intended application and possible limitations of use.

131 The TOE description provides context for the evaluation but is not itself evaluated. The information presented in the TOE description may be used in the course of the evaluation to identify inconsistencies. As a PP does not normally refer to a specific implementation, the described TOE features may be assumptions. If the TOE is a product or system whose primary function is security, this section may be used to describe the wider application context into which such a TOE will fit.

### B.2.3 Security environment

132 The statement of TOE security environment shall describe the security aspects of the environment in which the TOE is intended to be used and shall address the following:

- a) A description of **Threats** shall describe any known or presumed threats to the IT assets against which protection will, or should, be required. Note that all such threats should be identified even though some may not be countered by the TOE.

A threat shall be described in terms of an identified threat agent, the attack, and the asset which is the subject of the attack. Threat agents should be described by addressing aspects such as expertise, available resources, and motivation. Attacks should be described by addressing aspects such as attack methods, any vulnerabilities exploited, and opportunity.

Should TOE security objectives be derived from organisational security policy only, then the statement of threats may be omitted.

- b) A description of **Organisational security policies** shall identify, and if necessary explain, any organisational security policies or rules with which the TOE must comply. Explanation and interpretation may be necessary to present each policy in a manner that permits it to be used to set clear IT security objectives.

Should TOE security objectives be derived from threat assumptions only, then the statement of organisational security policy may be omitted.

- c) A description of **Secure usage assumptions** shall describe the security aspects of the environment in which the TOE will be, or is intended to be used. This includes information about the physical, personnel, and connectivity aspects of the environment.

133 Where the TOE is physically distributed, it may be necessary to discuss the security environment separately for distinct domains of the TOE environment.

### B.2.4 Security objectives

134 The security objectives of the TOE and its supporting environment shall be defined. Security objectives reflect the stated intent to counter identified threats and/or comply with any organisational security policies identified. The following categories of objectives shall be identified.

- a) The **IT security objectives** shall be clearly stated and traced back to identified threats to be countered and/or policies which are to be met by the IT.

- b) The **Non-IT security objectives** shall be clearly stated and traced back to identified threats to be countered and/or policies which are to be met by the non-IT environmental measures.

135 All of the identified threats and organisational policies shall be addressed under one of the categories above.

### B.2.5 IT security requirements

136 This section defines the detailed IT security requirements which shall be satisfied. The IT security requirements are stated as follows:

- a) The statement of **TOE IT security requirements** defines the IT security requirements which the TOE shall satisfy in order to meet its security objectives. The TOE security requirements are stated as follows:

- 1) The statement of **TOE IT functional requirements** shall define the functional requirements for the TOE using only functional requirements components drawn from Part 2. Pre-existing functional requirements packages may be used providing such packages use only CC functional components. Any required operations shall be used to amplify the requirements to the level of detail necessary to demonstrate that the security objectives are met.

Any required operations which are not performed within the profile shall be clearly identified and described such that they can be correctly performed at the point the PP is instantiated in an ST.

By using the permitted operations, the IT functional requirements statement may optionally prescribe or forbid the use of particular security mechanisms and techniques where necessary.

- 2) The statement of **TOE IT assurance requirements** shall state the assurance requirements as one of the EALs optionally augmented by additional Part 3 assurance components.

- b) The optional statement of **Security requirements for the IT environment** shall identify the functional and assurance IT security requirements which are asserted as being met by the IT environment of the TOE. The requirements should, if possible, be stated by reference to security requirements from the CC. If the TOE is a complete TSF with no assertions on the IT environment, this section is omitted.

### B.2.6 Application notes

137 This optional section may contain additional supporting information which is considered relevant or useful for the construction, evaluation, or use of the TOE.

**B.2.7 Rationale**

138 This section presents the rationale which demonstrates that the PP states a complete and cohesive set of requirements and that a conformant TOE would constitute an effective set of IT security countermeasures within the security environment. The rationale should contain the following:

- a) The **Security objectives rationale** shall demonstrate that the stated security objectives address all of the security environment aspects identified. The following shall be demonstrated:
  - 1) that the stated security objectives would lead to effective countermeasures to all of the identified threats to security;
  - 2) that the stated security objectives provide for complete coverage of all of the organisational security policies.
- b) The **Security requirements rationale** shall demonstrate that the set of IT security requirements (TOE and environment) is suitable to meet the IT security objectives. The following shall be demonstrated:
  - 1) that the combination of the objectives of the individual functional requirements components of the TOE together meet the stated security objectives of the TOE;
  - 2) that the set of security requirements together forms a mutually supportive and internally consistent whole;
  - 3) that all of the dependencies of the requirements components of the TOE are satisfied. Dependencies may be satisfied by the inclusion of the relevant component within the TOE security requirements, or as a requirement which is asserted as being met by the IT environment of the TOE;
  - 4) that the choice of the EAL and augmenting assurance requirements components, if any, can be justified.

139 These rationale statements are of primary value as PP evaluation deliverables by providing the justification for the selection of the security objectives and the functional and assurance requirements. This potentially bulky material may be distributed separately as it may not be of interest to all PP users.



## Annex C

# Specification of Security Targets (normative)

### C.1 Overview

140 An ST contains the IT security objectives and requirements of an identified TOE and specifies the functional and assurance security measures offered by that TOE to meet stated requirements.

141 The ST for a TOE is a basis for agreement between the developers, evaluators and, where appropriate, consumers on the security properties of the TOE and the scope of the evaluation. The audience for the ST is not confined to those responsible for the production of the TOE and its evaluation, but may also include those responsible for managing, marketing, purchasing, installing, configuring, operating, and using the TOE.

142 The ST may incorporate the requirements of, or claim conformance to, one or more PPs. The impact of such a PP conformance claim is not considered when initially defining the required ST content in Section C.2. Section C.2.7 addresses the impact of a PP conformance claim on the required ST content.

143 The contents of the ST are portrayed in figure C.1 which may be used as guidance when constructing the structural outline of the ST. Bolding is used to indicate those parts of the ST which, if present, are subject to evaluation.

### C.2 Content of Security Target

#### C.2.1 ST introduction

144 The following identification and indexing material shall be incorporated in the ST introduction.

- a) The **ST identification** provides the labelling and descriptive information necessary to control and identify the ST and the TOE to which it refers.
- b) The **ST overview** summarises the ST in narrative form. The overview should be sufficiently detailed for a potential consumer of the TOE to determine whether the TOE is of interest. The overview should also be usable as a stand alone abstract for incorporation in evaluated products lists.
- c) A **CC conformance claim** shall state any evaluatable claim of CC conformance for the TOE. Conformance claims shall be made to at least one registered CC compliant PP or EAL.

A strength of function rating may be claimed for appropriate TOE security functions, or an assertion that a strength claim is inappropriate for that function may be made.

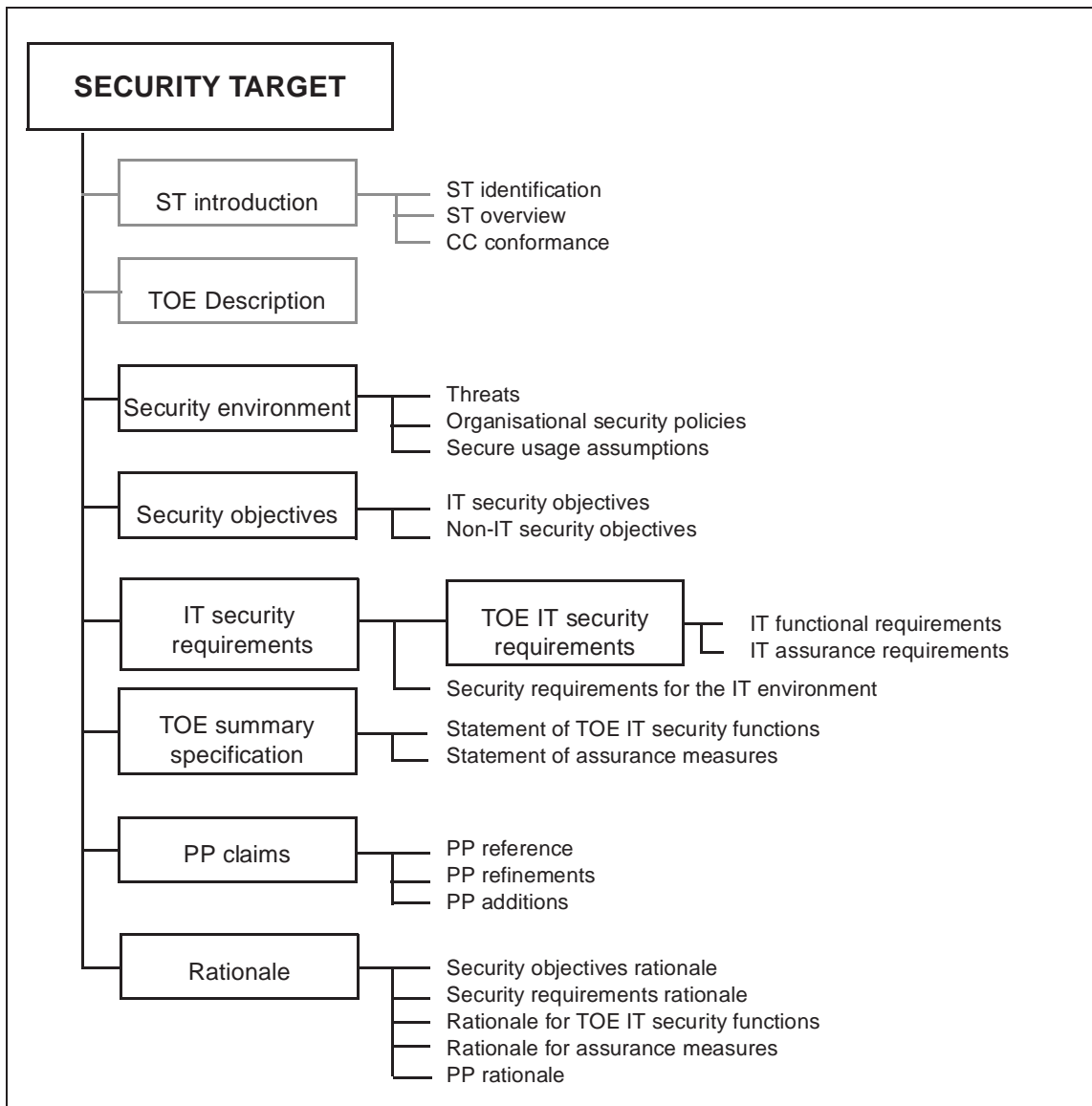


Figure C.1 - Security target content

### C.2.2 TOE description

145 This part of the ST should describe the TOE as an aid to the understanding of its security requirements and should address the product type, the intended usage, and the general IT features of the TOE. Aspects of usage that may be addressed include the intended application and possible limitations of use.

146 The TOE description provides context for the evaluation but is not itself evaluated. The information presented in the TOE description may be used in the course of the evaluation to identify inconsistencies. If the TOE is a product or system whose primary function is security, this section may be used to describe the wider application context into which such a TOE will fit.

### C.2.3 Security environment

147 The ST shall include a statement of the security environment of the TOE which addresses the following:

- a) A description of **Threats** shall describe any known or presumed threats to the IT assets against which protection will, or should, be required. Note that all such threats should be identified even though some may not be countered by the TOE.

A threat shall be described in terms of an identified threat agent, the attack, and the asset which is the subject of the attack. Threat agents should be described by addressing aspects such as expertise, available resources, and motivation. Attacks should be described by addressing aspects such as attack methods, any vulnerabilities exploited, and opportunity.

Should TOE security objectives be derived from organisational security policy only, then the statement of threats may be omitted.

- b) A description of **Organisational security policies** shall identify, and if necessary explain, any organisational security policies with which the TOE must comply. Explanation and interpretation may be necessary to present each policy in a manner that permits it to be used to set clear IT security objectives.

Should TOE security objectives be derived from threat assumptions only, then the statement of organisational security policy may be omitted.

- c) A description of **Secure usage assumptions** shall describe the security aspects of the environment in which the TOE will be, or is intended to be used. This includes information about the physical, personnel, and connectivity aspects of the environment.

148 Where the TOE is physically distributed, it may be necessary to discuss the security environment separately for distinct domains of the TOE environment.

#### C.2.4 Security objectives

149 The security objectives of the TOE and its supporting environment shall be defined. Security objectives reflect the stated intent to counter identified threats and/or comply with any organisational security policies identified. The following categories of objectives shall be identified.

- a) The **IT security objectives** shall be clearly stated and traced back to identified threats to be countered and/or policies which are to be met by the TOE.
- b) The **Non-IT security objectives** shall be clearly stated and traced back to identified threats to be countered and/or policies which are to be met by the environment.

150 All of the identified threats and organisational policies shall be addressed under one of the categories above.

#### C.2.5 IT security requirements

151 This section defines the IT security requirements which must be satisfied. The IT security requirements are stated as follows:

- a) The statement of **TOE IT security requirements** defines the IT security requirements which the TOE must satisfy in order to meet its security objectives. The TOE security requirements are stated as follows:

- 1) The statement of **TOE IT functional requirements** should define the functional requirements for the TOE as functional components and/or packages drawn from Part 2 where applicable. Any required operations shall be used to amplify the requirements to the level of detail necessary to demonstrate that the security objectives are met. All operations on the functional requirements components shall be performed.

Should none of the Part 2 functional requirements components be readily applicable to all or part of the TOE security requirements, the ST may state those functional requirements explicitly without reference to the CC.

Any explicit statements of functional requirements shall be clearly and unambiguously expressed such that evaluation and demonstration of compliance is feasible. The level of detail and manner of expression of existing CC functional requirements shall be used as a model.

- 2) The statement of **TOE IT assurance requirements** shall state the assurance requirements as one of the EALs optionally augmented by Part 3 assurance components.

The ST may also extend the EAL by stating additional assurance requirements not taken from Part 3. Any such explicit statements of assurance requirements shall be clearly and unambiguously expressed such that evaluation and demonstration of compliance is feasible. The level of detail and manner of expression of existing CC assurance requirements shall be used as a model.

- b) The optional statement of **Security requirements for the IT environment** shall identify the functional and assurance IT security requirements which are asserted as being met by the IT environment of the TOE. The requirements shall be stated by reference to security requirements from the CC where feasible, otherwise they should be stated explicitly. If the TOE is a complete TSF with no assertions on the IT environment, this section may be omitted.

### C.2.6 TOE summary specification

152 The TOE summary specification defines the instantiation of the security requirements for the TOE by providing a high level definition of the security functions claimed to meet the functional requirements and of the assurance measures taken to meet the assurance requirements. It contains the following:

- a) The **Statement of TOE IT security functions** specifies the IT security functions which are claimed to satisfy the stated requirements. The security functions shall be mapped to the security requirements so that it can be seen which functions satisfy which requirements. Every security function shall, as a minimum, contribute to the satisfaction of at least one security requirement.

The IT security functions shall be defined in an informal style to a level of detail necessary for an understanding of the intent and behaviour of the function.

All references to security mechanisms and techniques included in the ST shall be traced to the relevant security functions so that it can be seen which required mechanisms or techniques are used in the implementation of each function.

- b) The **Statement of assurance measures** specifies the assurance measures of the TOE which are claimed to satisfy the stated assurance requirements. The assurance measures shall be traced to the assurance requirements so that it can be seen which measures satisfy which requirements.

If appropriate, the definition of assurance measures may be made by reference to relevant quality plans, life cycle plans, or management plans.

### C.2.7 PP claims

153 The ST may make a claim that the TOE conforms with the requirements of one (or possibly more than one) PP. The optional **PP claims** part of the ST contains the

explanation, justification, and any other supporting material necessary to substantiate the claims.

154 The presentation and content of the statements of TOE objectives and requirements within the ST may be affected by a PP claim made for the TOE. The impact on the ST can be summarised by considering the following cases.

- a) If there is no claim of PP compliance made, then the full presentation of the TOE objectives and requirements should be made as described in this annex. No PP claims are included.
- b) If the ST claims only compliance with the requirements of a PP without need for further qualification, then reference to the PP is sufficient to define and justify the TOE objectives and requirements. Restatement of the PP contents is unnecessary.
- c) If the ST claims compliance with the requirements of a PP, and that PP requires further qualification, then the ST shall show that the PP requirements for qualification have been met. Such a situation would typically arise where the PP contains uncompleted operations. In such a situation, the ST may refer to the specific requirements but complete the operations within the ST. In some circumstances, where the requirements to complete operations are substantial, it may be preferable to restate the PP contents within the ST as an aid to clarity.
- d) If the ST claims compliance with the requirements of a PP but extends that PP by the addition of further objectives and requirements, then the ST shall define the additions, whereas a PP reference may be sufficient to define the PP objectives and requirements. In some circumstances, where the additions are substantial, it may be preferable to restate the PP contents within the ST as an aid to clarity.
- e) The case where an ST claims to be partially conformant to a PP is not admissible for CC evaluation.

155 The CC is not prescriptive with respect to the choice of restating or referencing PP objectives and requirements. The fundamental requirement is that the ST content be complete, clear, and unambiguous such that evaluation of the ST is possible, the ST is an acceptable basis for the TOE evaluation, and the traceability to any claimed PP is clear.

156 The PP claims part of the ST should, for each PP claimed, contain the following material.

- a) The **PP reference** statement will identify the PP for which compliance is being claimed plus any amplification which may be needed with respect to that claim. A valid claim implies that the TOE meets all the requirements of the PP.

- b) The **PP refinements** statement will identify the TOE objectives and requirements statements which satisfy the permitted operations of the PP or otherwise further qualify the PP objectives and requirements.
- c) The **PP additions** statement will identify the TOE objectives and requirements statements which are additional to the PP objectives and requirements.

### C.2.8 Rationale

157

This section presents the rationale which demonstrates that the ST states a complete and cohesive set of requirements, that a conformant TOE would constitute an effective set of IT security countermeasures within the security environment, and that the summary specification addresses the requirements. The rationale also demonstrates that any PP conformance claims are valid. The rationale should contain the following:

- a) The **Security objectives rationale** shall demonstrate that the stated security objectives address all of the security environment aspects identified. The following shall be demonstrated:
  - 1) that the stated security objectives lead to effective countermeasures to all of the identified threats to security;
  - 2) that the stated security objectives provide for complete coverage of all of the organisational security policies and rules.
- b) The statement of **Security requirements rationale** shall demonstrate that the set of IT security requirements (TOE and environmental) is suitable to meet the objectives. The following shall be demonstrated:
  - 1) that explicitly stated functional requirements identify the objectives which they are intended to meet;
  - 2) that explicitly stated functional requirements are suitable to meet the objectives identified for the TOE;
  - 3) that the assurance requirements are applicable and appropriate to support all explicitly stated functional requirements;
  - 4) that the combination of the individual CC functional requirements components together with any explicitly stated functional requirements for the TOE meet the stated security objectives of the TOE;
  - 5) that all of the dependencies of the CC requirements components of the TOE are satisfied. Dependencies may be satisfied by the inclusion of the relevant component within the TOE security requirements, or as a requirement which is asserted as being met by the IT environment of the TOE. Any dependencies which are not

satisfied by the relevant CC requirement shall be shown to be satisfied by other identified requirements. The claim that such dependencies can be satisfied by other explicitly stated requirements shall be supported by a justification.

- 6) that all of the operations of the CC requirements components have been satisfactorily performed;
  - 7) that the choice of the EAL and augmenting assurance requirements components, if any, are justified.
- c) The **Rationale for TOE IT security functions** shows that the TOE IT security functions address all functional requirements of the TOE and are suitable to meet the TOE objectives. The following shall be demonstrated:
- 1) that the specified TOE IT security functions meet the security objectives claimed for them;
  - 2) that the combination of specified TOE IT security functions work together so as to satisfy the TOE security objectives;
  - 3) that the strength of TOE function claims made are valid, or that assertions that such claims are unnecessary are valid.

The statement of rationale shall be presented at a level of detail which matches the level of detail of the definition of the security functions.

- d) The **Rationale for assurance measures** justifies the claim that the stated assurance measures are compliant with the assurance requirements.
- e) The **PP rationale** statement shows that the totality of the TOE requirements statements include, and support, any PP requirements. The following shall be demonstrated:
- 1) that any refinements of PP objectives result in valid interpretations of the more abstract statements of objectives within the PP;
  - 2) that any refinements of and operations on PP requirements result in valid interpretations of the more abstract statements of requirement within the PP;
  - 3) that all of the PP objectives are met and all PP requirements are satisfied;
  - 4) that no additional objectives and requirements contradict those of the PP itself.

This section may be omitted if no claims of PP conformance are made.

Annex D

**Security concepts and principles (informative)**

**D.1 Introduction**

158 The CC is based upon a set of assumptions about the general domain of security and IT security in particular. This annex provides a top level description of the CC principles of security and should be considered as introductory material only.

**D.2 General security context**

159 Security is concerned with the protection of assets from threats where threat is categorised as the potential for abuse of protected assets. All categories of threat should be considered, but in the domain of security greater attention is given to those threats which are related to malicious or other human activities. Figure D.1 illustrates high level concepts and relationships.

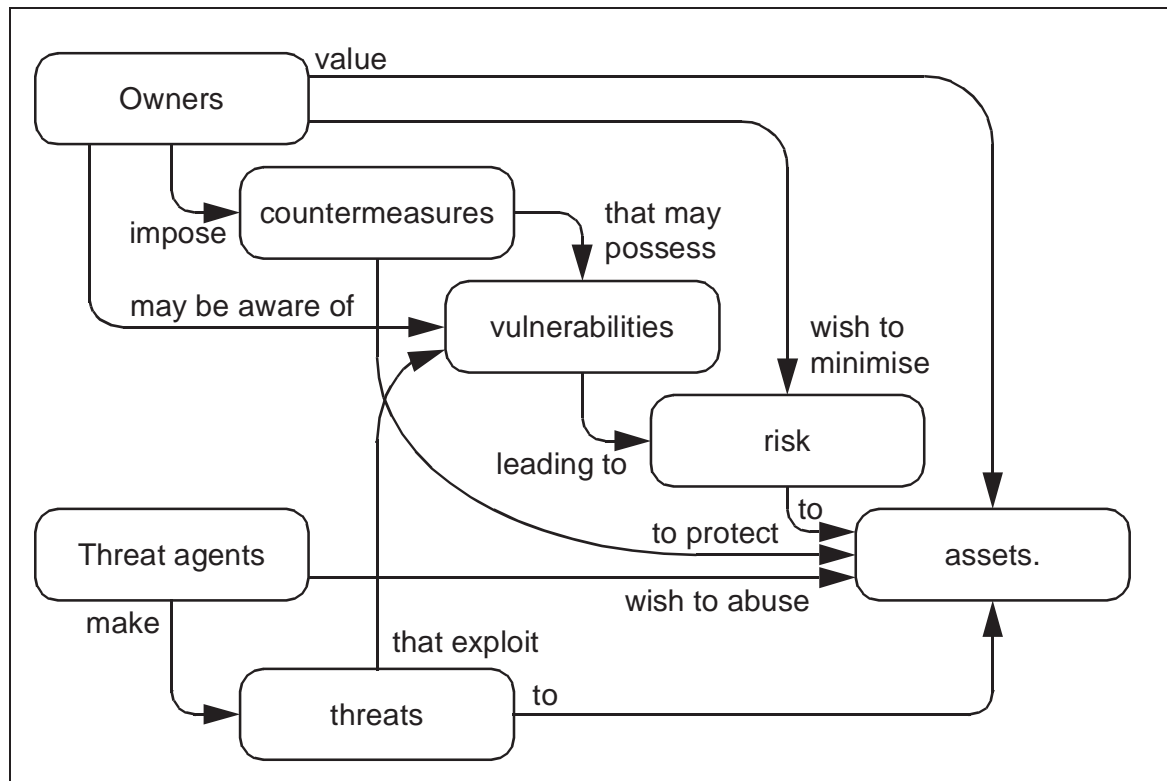


Figure D.1 - Security concepts and relationships

160 Safeguarding assets of interest is the responsibility of owners who place value on those assets. Actual or presumed threat agents may also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner. Owners will perceive such threats as potential for impairment of the assets such that the value of the assets to the owners would be reduced. Security specific impairment commonly includes, but is not limited to, damaging disclosure of the asset to unauthorised recipients (loss of confidentiality), damage to the asset through unauthorised modification (loss of integrity), or unauthorised deprivation of access to the asset (loss of availability).

161 Owners impose countermeasures which seek to mitigate the threat of asset impairment. Residual vulnerabilities will remain after the imposition of countermeasures. Such vulnerabilities may be exploited by threat agents resulting in a residual level of risk to the assets. Owners will seek to minimise that risk.

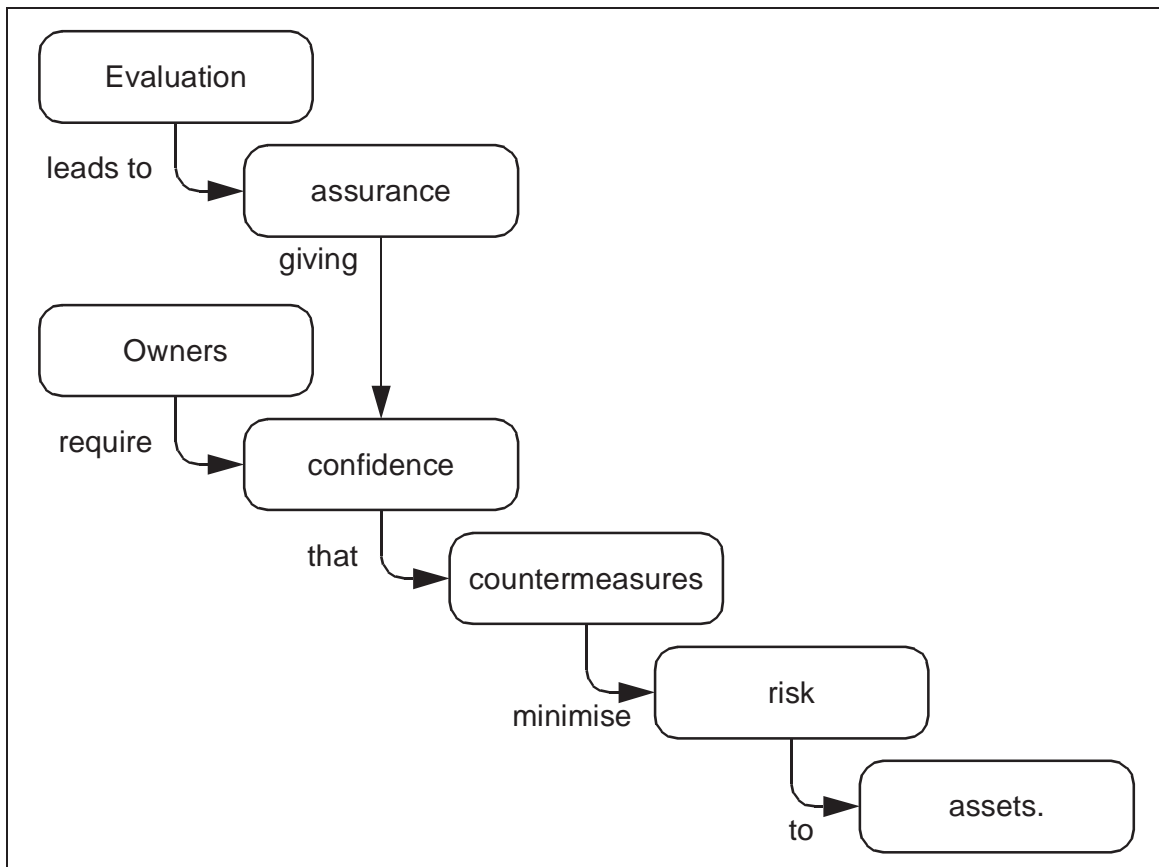


Figure D.2 - Evaluation concepts and relationships

162 Owners will need to be confident that the countermeasures are adequate to counter the threats to assets before they will allow exposure of their assets to the specified threats. Owners may not themselves possess the capability to judge all aspects of the countermeasures and may therefore seek evaluation of the countermeasures. The outcome of evaluation is a statement about the extent to which the countermeasures can be trusted to reduce the risks to the protected assets. The statement

assigns assurance to the countermeasures, assurance being that property of the countermeasures which gives grounds for confidence in their proper operation. This statement can be used by the owner of the assets in deciding whether to accept the risk of exposing the assets to the threats. Figure D.2 illustrates these relationships.

163 Owners of assets will normally be held responsible for those assets and should, therefore, be able to defend the decision to accept the risks of exposing the assets to the threats. This, in turn, requires that the statements resulting from evaluation are themselves defensible. Thus evaluation should lead to objective and repeatable results that can be cited as evidence. The existence of a set of evaluation criteria is a necessary pre-condition for evaluation to lead to a meaningful result and to provide a technical basis for mutual recognition of evaluation results between evaluation authorities.

### D.3 Information technology security context

164 Many assets are in the form of information which is stored, processed and transmitted by IT systems to meet requirements laid down by owners of the information. Information owners may require that dissemination and modification of any such information representations (data) be strictly controlled. They may demand that the IT system implement IT specific security controls as part of the overall set of security countermeasures put in place to counteract the threats to the data.

165 IT systems are procured and constructed to meet user-specific requirements and may, for economic reasons, make maximum use of existing commodity IT products such as operating systems, general purpose application components, and hardware platforms. IT security countermeasures implemented by a system may use functions of the underlying IT products and depend upon the correct operation of IT product security functions. The IT products may, therefore, be subject to evaluation as part of the IT system security evaluation.

166 Where an IT product is incorporated or being considered for incorporation in multiple IT systems, there are cost advantages in evaluating the security aspects of such a product independently and building a catalogue of evaluated products. The results of such an evaluation should be expressed in a manner which supports incorporation of the product in multiple IT systems without unnecessary repetition of work required to examine the product's security.

167 An IT system accreditor has the authority of the owner of the information to determine whether the combination of IT and non-IT security countermeasures furnishes adequate protection for the data and thus to decide whether to permit the operation of the system. The accreditor may call for evaluation of the IT countermeasures in order to determine whether the IT countermeasures provide adequate protection and whether the specified countermeasures are properly implemented by the IT system. This evaluation may take various forms and degrees of rigour, depending upon the rules imposed upon, or by, the accreditor.

168 The CC provides a basis for evaluation of the technical IT security properties of either products or systems.



## Annex E

# Security development and evaluation model (informative)

### E.1 Introduction

169 Evaluation criteria are most useful in the context of the engineering processes and regulatory frameworks which are supportive of secure TOE development and evaluation. This annex discusses frameworks within which the CC might be employed. It is provided for illustration and guidance purposes only and is not intended to constrain the analysis processes, development approaches, or evaluation schemes within which the CC might be employed.

### E.2 Development of security requirements and specifications

170 Development and evaluation of a secure TOE presupposes the existence of a demonstrably sound and internally consistent set of security requirements and specifications. Figure E.1 illustrates the means by which the security requirements and specifications might be derived when developing a PP or ST. This chart is not intended to constrain the means by which PPs and STs are developed but illustrates how the results of some analytic approaches relate to the content of PPs and STs.

171 All TOE security requirements ultimately arise from consideration of the purpose and context of the TOE. The TOE environment is presumed to include relevant security specific information such as physical, personnel, and IT security policies. Through the requirements capture or formulation activities, a statement of IT requirements will be developed.

172 The statement of IT requirements is the foundation for TOE or PP development. Investigation of the security policies, threats, and risks should permit the following security specific statements to be made about the TOE.

- a) A statement of the **TOE physical environment** would identify all aspects of the TOE operating environment relevant to TOE security. This would include known physical and personnel security arrangements.
- b) A statement of the **IT assets requiring protection** would identify all assets which are under the control of the IT element of the TOE to which security requirements or policies will apply. This may include assets which are directly referred to such as files and databases plus assets which are indirectly subject to security requirements such as authorisation credentials and the IT implementation itself.

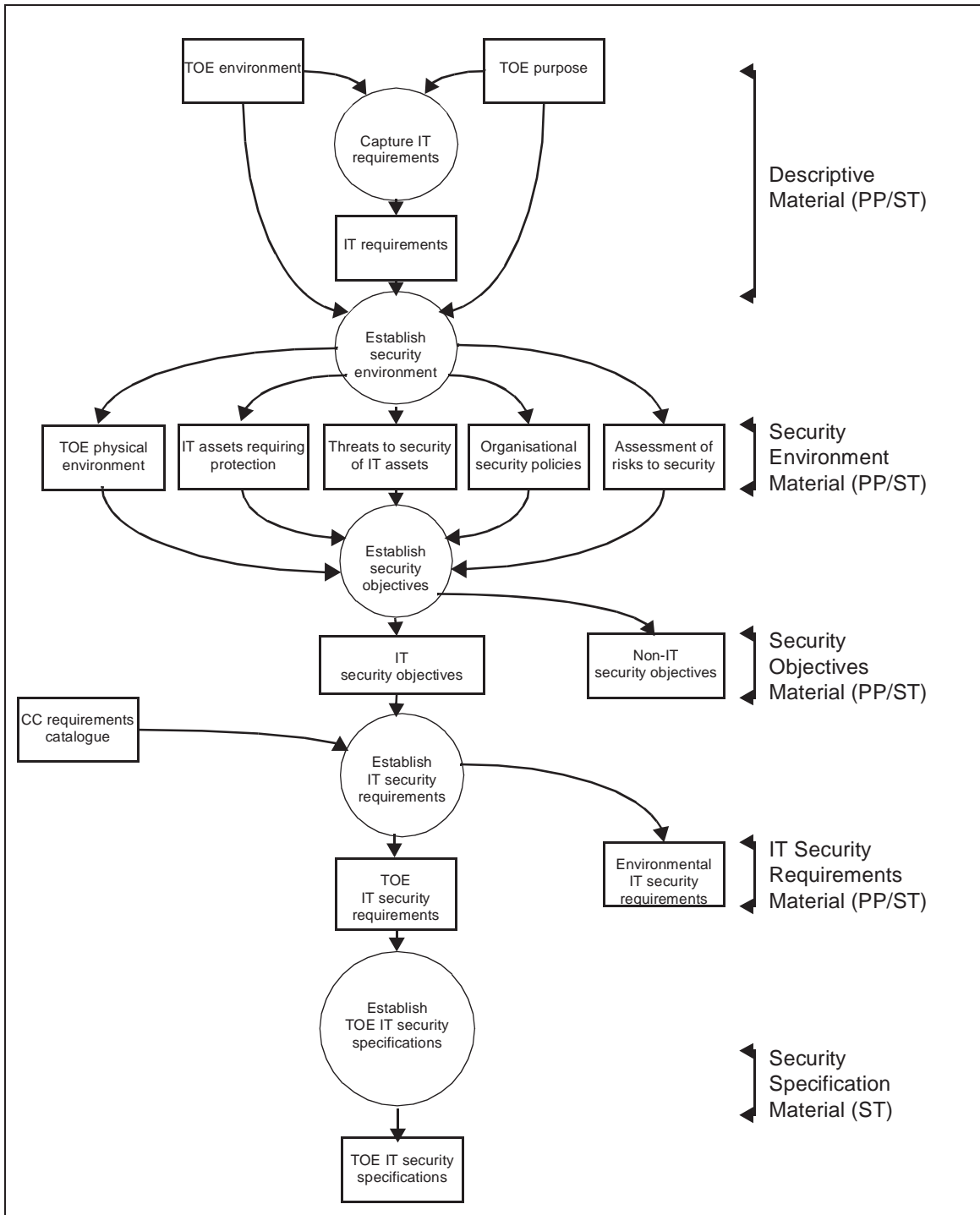


Figure E.1 - Derivation of requirements and specifications

- a) A statement of **Threats to security of the IT assets** would identify all the threats perceived by the security analyst as relevant to the TOE. The CC characterises a threat in terms of a threat agent, a presumed attack method, any vulnerabilities which are the foundation for the attack, and identification of the asset under attack.
- b) A statement of applicable **Organisational security policies** would identify relevant policies and rules. For an IT system, such policies may be explicitly referenced whereas, for a general purpose IT product or product class, working assumptions about organisational security policy may need to be made.
- c) An **Assessment of risks to security** would qualify each threat with an assessment of the likelihood of such a threat developing into an actual attack, the likelihood of such an attack proving successful, and the consequences of any damage that may be caused.

173 The object of the analysis of the security environment is to determine and characterise all of the security concerns that are, or may be, relevant to the TOE.

174 The results of the analysis of the security environment could then be used to decide which threats and policy objectives will be addressed by countermeasures, which of those countermeasures would be implemented within the IT domain, and which would be implemented by non-technical or procedural means. The countermeasures must be consistent with the stated operational aim or product purpose of the TOE, any knowledge about the physical environment of the TOE, and any organisational security policies which are to be enforced by the TOE.

175 The decision as to whether a threat or policy requires a corresponding countermeasure, and whether that countermeasure will form part of the IT security requirements, is based on a process incorporating engineering judgement, security policy, economic factors, and risk acceptance decisions. Criteria for making such decisions are outside the scope of the CC. The results should include:

- a) A statement of **TOE IT security objectives** which covers the threats and policy objectives which are covered by the IT resources of the TOE.
- b) A statement of relevant **Non-IT security objectives** will cover those non-IT measures which are necessarily taken to ensure that the identified IT assets are protected against the balance of the threats not covered by the IT security objectives - or are otherwise necessary to ensure that the IT security policy objectives can be met effectively.

176 The intent of determining security objectives is to lay down responsibility for addressing all of the security concerns and to declare which security concerns are addressed directly by the IT and which are addressed externally. Proper allocation of security objectives to the IT is a matter of judgement, engineering skill, and willingness to accept a measure of residual risk. The criteria for making such judgements are outside the scope of the CC.

177 The security objectives of the TOE IT may then be refined into a set of **TOE IT security requirements**. The requirements catalogue of the CC should be used as a source of security requirements expression. For a PP, use of the CC requirements components is mandatory if the PP is to be registered for general use by CC-based schemes.

178 In order to permit the evaluation of TOEs which are not complete TSFs, it may be necessary to define IT security requirements which are to be met by the IT environment of the TOE in order for the TOE to be considered secure. Such requirements can be stated in an optional statement of **Environmental IT security requirements** which can be accepted as axiomatic for the TOE evaluation.

179 Through a further process of design refinement, the **TOE IT security specifications** will be developed from the security requirements and used as the basis for the implementation of the TOE security features.

### E.3 Development of TOE

180 The CC does not mandate any specific development methodology or life cycle model. Figure E.2 depicts underlying assumptions about the relationship between the security requirements and the TOE. The figure is used to provide a context for discussion and should not be construed as advocating a preference for one methodology (e.g., waterfall) over another (e.g., prototyping).

181 The process commences with the refinement of the security requirements into a set of summary specifications expressed in the security target. Each lower level of refinement represents a design decomposition with additional design detail. The least abstract representation is the TOE implementation itself.

182 The CC does not mandate a specific set of design representations. The CC requirement is that there should be sufficient design representations presented at a sufficient level of granularity to demonstrate where required:

- a) that the refinement level is a complete instantiation of the higher levels. Thus all security functions, properties, and behaviour defined at the higher level of abstraction must be demonstrably present in the lower level;
- b) that the refinement level is an accurate instantiation of the higher levels. Thus there should be no security functions, properties, and behaviour defined at the lower level of abstraction which are not required by the higher level.

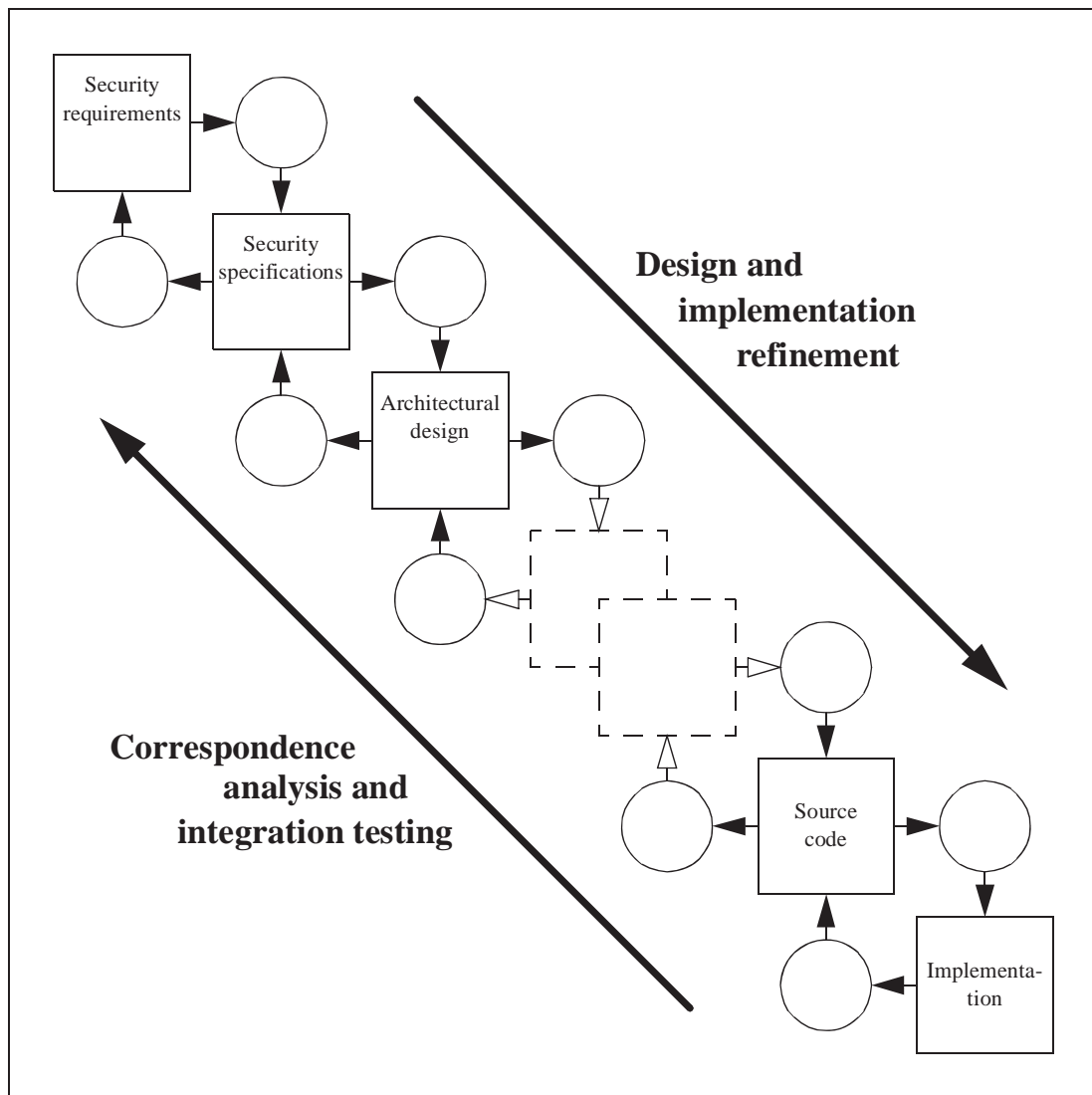


Figure E.2 - TOE development model

183 The CC assurance criteria identify the design abstraction levels of architectural design, detailed design, and implementation. Developers will be required to show how the proposed development methodology meets the CC assurance requirements.

#### E.4 Evaluation context

184 The CC is the basis for the evaluation of the security properties of a TOE and presupposes the existence of a controlled framework in which to conduct evaluations. The CC does not state requirements for the regulatory framework. However, consistency between the regulatory frameworks of different evaluation

authorities will be necessary to achieve the goal of mutual recognition of the results of such evaluations. Figure E.3 depicts the major elements which form the context for evaluations.

185 The IT security evaluation process analyses the TOE representations in accordance with the CC. Representations are evaluated to determine whether they are self consistent, comprehensible, and correctly interpret the higher level requirements. Representations will be evaluated to determine their compliance with security requirements.

186 The evaluation process operates on evidence from the developer and evaluates the TOE using technical methods and techniques prescribed in the evaluation methodology and the standards laid down in the evaluation criteria.

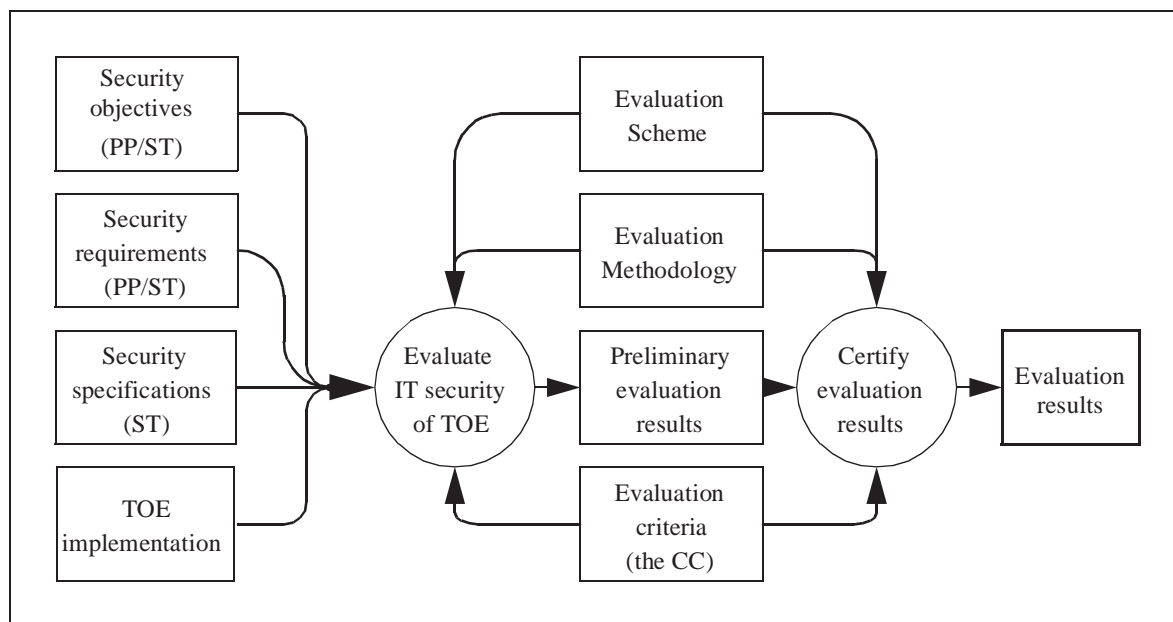


Figure E.3 - Evaluation context

187 Use of a standard evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve. In order to enhance the consistency of the evaluation findings, the preliminary evaluation results should be submitted to a certification process. Certification is the independent inspection of the results of the evaluation leading to an authoritative statement of the results. The certified results and associated qualifying material are the external output of the evaluation and are available to parties with an interest in the security properties of the TOE. The certification activity is outside the scope of the CC and is shown as a means of demonstrating how greater consistency in the application of the more subjective criteria might be achieved.

188 The evaluation methodology is applied within the administrative and legal framework laid down by the evaluation scheme which sets the standards and administers the regulations to which the evaluation facilities and evaluators must conform. The evaluation scheme, methodology, and certification processes are the responsibility of the bodies that run national schemes and are outside the scope of the CC.

### E.5 Use of evaluation results

189 IT products and systems differ in respect to the use of the results of the evaluation. Figure E.4 shows options for processing the results of evaluation. Products can be evaluated and catalogued at successively higher levels of aggregation until operational systems are achieved, at which time they may be subject to evaluation in connection with system accreditation.

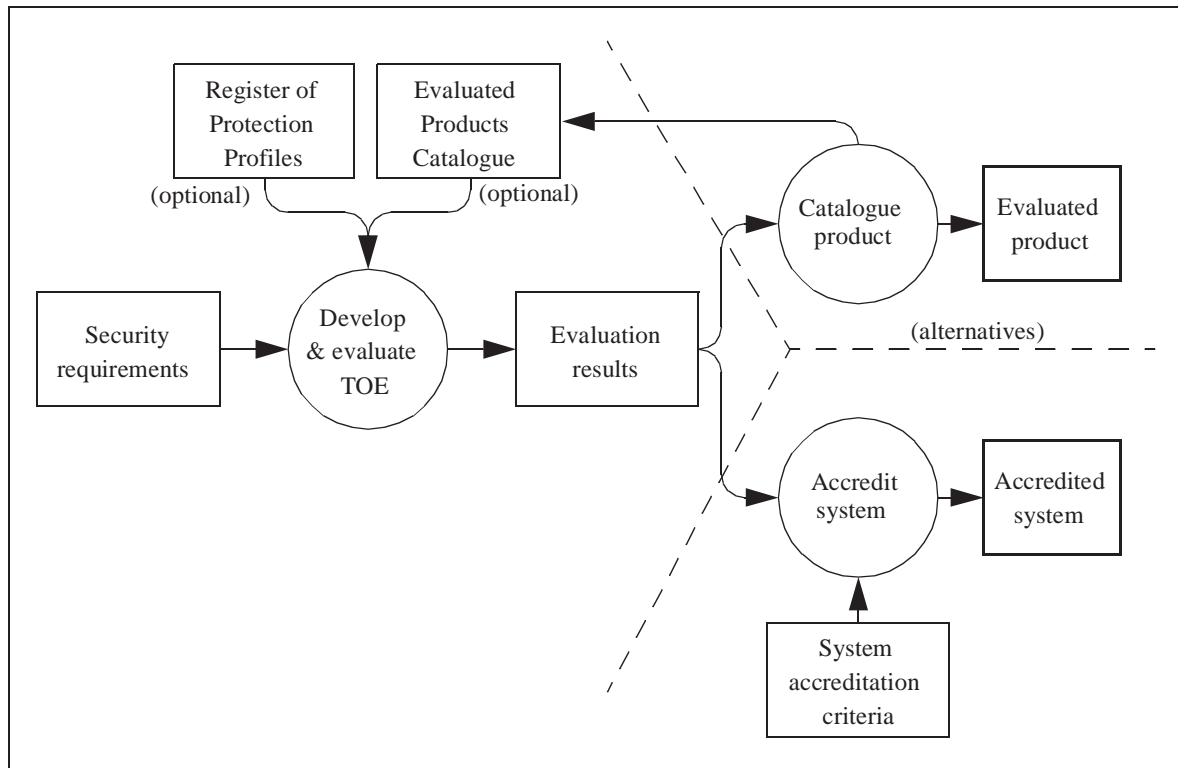


Figure E.4 - Use of evaluation results

190 The TOE is developed in response to requirements which may take account of the security properties of any evaluated products incorporated and PPs referenced. Subsequent evaluation of the TOE leads to a set of evaluation results documenting the findings of the evaluation.

191 Following an evaluation of an IT product intended for wider use, a summary of the evaluation findings might be entered in a catalogue of evaluated products so that it becomes available to a wider market seeking to use secure IT products.

192 Where the TOE is, or will be included in, an installed IT system which has been subject to evaluation, the evaluation results will be available to the system accreditor. The CC evaluation results may then be considered by the accreditor when applying organisation specific accreditation criteria which call for CC evaluation. CC evaluation results are one of the inputs to the accreditation process leading to a decision on accepting the risk of system operation.

## Annex F

### Bibliography (informative)

- a) Trusted Computer Systems Evaluation Criteria (TCSEC), US DoD 5200.28-STD, December 1985.
- b) Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, Office for Official Publications of the European Communities, June 1991.
- c) Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993.
- d) Federal Criteria for Information Technology Security (FC), Draft Version 1.0, (Volumes I and II), jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993.
- e) Evaluation Criteria for IT Security, Part 1: General model of security evaluation, Working Draft, ISO/IEC/JTC1 SC27/WG3.
- f) Evaluation Criteria for IT Security, Part 2: Functionality of IT systems, products and components, Working Draft, ISO/IEC/JTC1 SC27/WG3.
- g) Evaluation Criteria for IT Security, Part 3: Assurance of IT systems, products and components, Working Draft, ISO/IEC/JTC1 SC27/WG3.
- h) ISO Directive 3: Style guide.
- i) ISO Guide 2: 1991. General terms and their definitions concerning standardisation and related activities.
- j) ISO 7498-2: 1989. Information processing systems - Open Systems Interconnection - Basic Reference Model, Part 2: Security Architecture.



## Annex G

# CC observation report (CCOR)

### G.1 Introduction

193 The CC sponsoring organisations welcome feedback from the community and are particularly interested in observations and comments arising out of trial application of the criteria.

194 The CC sponsoring organisations have set up a body, the Common Criteria Implementation Board (CCIB), to coordinate and learn from the community experience and to ensure that future issues of the CC can benefit from that experience.

195 Comments, observations, and requests for interpretations should be sent to one of the addresses listed inside the front cover of the CC. If you require feedback on a specific evaluation matter, you should use the contact address which corresponds to the evaluation authority concerned.

### G.2 Categorisation of observation report

196 In order to allow automated categorisation of the observations, a standard observation format is needed. Each observation should include an identifier as to whether the comment pertains to the *approach* in the CC, the technical *detail* of any specific portion of the CC, or *editorial* work that needs to be done. Additionally, for comments on technical detail, an indication of the scope of the comment (e.g., *local*, *global*) should be provided.

197 The following provides a description of each of these terms:

- a) *Approach*: observations requesting further guidance relating to the approach of the CC which the author of the observation report considers to be fundamental to the further progress of the CC or trial application of the criteria should be marked with this identifier.
- b) *Detail*: Specific observations on technical details of the CC should be marked with this identifier. These comments should be further categorised as either local or global.

*Local*: is applicable to a single specific class, family, component, or element.

*Global*: is applicable to multiple classes, families, components, or elements.

- c) *Editorial*: typographical and grammatical errors, as well as comments on presentation style.

*Local*: is applicable to a single specific class, family, component, or element.

*Global*: is applicable to multiple classes, families, components, or elements.

### G.3 Format of observation report

198 The following provides a description of each of the structure of the required  
comment format and an example of a comment in the required format.

199 If you are submitting one or more observations by electronic mail or other machine  
readable format, please insert the tags defined below starting in the first column as  
this will greatly assist in any automated handling of your input.

200 Each observation report should consist of three parts.

- a) The first part consists of a tags **\$1:** to **\$4:**, which includes the information to allow the unique identification of the originator. This first set of tags is required only once per single observation or batch of observations.
- b) The second part consists of tags **\$5:** to **\$9:**, which includes the information to allow the unique identification and categorisation of the observation, the actual observation itself and suggested solution. The text of each observation should extend to as many lines as are needed to fully express the observation. There can be one or more observations in an observation report.

The set of tags **\$5:** to **\$9:**, comprising this second part of the observation report, should be repeated for each observation being submitted.

- c) The third part consists of a single terminating tag **\$\$:**. This final tag is required only once per single observation or batch of observations.

#### G.3.1 Tag definitions for observation report

##### **\$1: Originator name**

201 Name of commenter (only required once per message).

##### **\$2: Originator organisation**

202 Originator organisation/affiliation (only required once per message).

##### **\$3: Return address**

203 Electronic mail or other address for response (only required once per message).

**\$4: Date**

204 Submission date of observation YY/MM/DD (only required once per message).

**\$5: Originator report reference identification**

205 Reference for observation which is unique to originator. Please include your initials or similar unique discriminator, e.g., ABC1234.

**\$6: One line summary/title of observation**

206 Short summary/title for problem (up to 60 characters).

**\$7: CC document reference**

207 Single reference to the affected area of the CC as detailed as appropriate. Where possible, part number, section, paragraph, class, family, component, or requirement reference should be provided.

208 The template for CC document reference is as follows:

**\$7: Part / Section / Paragraph / [Approach / Detail - [Local / Global] / Editorial] - [Local / Global] / [Keyword]**

209 The CC document reference template should be completed as follows (see below for completed example):

- a) The characters “\$7:”, to indicate the start of an observation.
- b) Identification of the CC part, section, and paragraph to which the comment applies in the CC. All 3 pieces of identifying information should be provided, each separated by a slash character (/).

Valid identifiers for the CC Part are e.g., part 1 or 1, part 2 or 2, part 3 or 3, and profiles or PP.

Identification for the CC section should be either a section number (e.g., 1.3.2), if applicable, or, for requirement classes, families, or components, the name of the class (e.g., FIA), family (e.g., FIA\_ATD), or component (e.g., FIA\_ATD.1).

- c) Identification of the reviewer’s categorisation of the observation. Brackets “[.]” indicate that the reviewer should choose *one* of the options contained within the brackets, these can be abbreviated to the initial character only (e.g., “A”, “D - L”, or “E - G”).
- d) An optional keyword.

210 Any identification field should be left blank or be filled with an asterisk (\*) to indicate that the field is not applicable or necessary for the comment.

**\$8: Statement of observation**

211 Comprehensive statement of observation or query, contains the actual text of the observation. Should include specific reference to examples of the observation, where appropriate.

**\$9: Suggested solution**

212 Proposed solution or solution approach.

**\$\$: Terminating tag.**

213 This enables any automated handling to determine the end of the batch of observations (only required once per batch of observations).

**G.3.2 Example observations:**

\$1: A. N. Other

\$2: PPs 'R' US

\$3: another@ppsrus.com

\$4: 960131

\$5: ano.comment.1

\$6: Presentation comment.

\$7: 1 / 8.1 / 90 / Editorial - Local /

\$8: The word "global" at the end of the first line should be italicised.

\$9: Italicise "global".

\$5: ano.comment.2

\$6: Missing requirement for audit.

\$7: 2 / FAU / 336 / Detail - Local /

\$8: The first sentence of this paragraph is incomplete.

\$9: The first sentence should include "imminent" violations.

\$5: ano.comment.3

\$6: Problems in navigating the document.

\$7: 2 / \* / \* / Approach / threats

\$8: The statements of threat in the functional families are largely re-statements of the family behaviour from the threat viewpoint. Does this material need to be re-stated twice within the functional families?

\$9: Could all threat information be described in a separate section with a table mapping the various functional components to the threats they address?

\$\$: This is the end tag, the contents are immaterial.

#### **G.4 Printed observation report**

214 An example of a printed observation report is provided in Table G.1.

<b>COMMON CRITERIA OBSERVATION REPORT</b>	
<b>\$1:</b>	<b>Originator Name</b>
<b>\$2:</b>	<b>Originator organisation</b>
<b>\$3:</b>	<b>Return address</b>
<b>\$4:</b>	<b>Date</b>
<b>\$5:</b>	<b>Originator report reference identification</b>
<b>\$6:</b>	<b>One line summary/title of observation</b>
<b>\$7:</b>	<b>CC document reference</b>
<b>\$8:</b>	<b>Statement of observation</b>
<b>\$9:</b>	<b>Suggested solution</b>
<b>\$\$:</b>	

Table G.1 - CC observation report