Common Criteria

Common Criteria
for Information Technology
Security Evaluation

User Guide

October 1999

Contents

1. Introduction

1.1 Purpose and Scope

This user guide is intended to help those consumers, product developers and system integrators considering the use of the Common Criteria (CC) to gain a better understanding of its principles, and to help them take practical steps towards using the CC.

1.2 User Guide Structure

This user guide is presented in four main parts:

- Introduction – a description of the background of the CC and the context in which it has been developed;
- What is the CC? – a summary of the contents of the CC and its supporting documentation;
- How is the CC used? – a explanation of how the CC should be used;
- National Schemes – contact information, an outline of the conduct of evaluations, and information about mutual recognition of evaluation results.

There is also a detailed glossary of terms.

1.3 Why you should use the CC

1.3.1 What support does the CC have ?

The CC was developed through a collaboration among national security and standards organisations within Canada, France, Germany, the Netherlands, the United Kingdom and the United States, as a common standard to replace their existing security evaluation criteria. As such, it is strongly supported by each of the organisations involved.

The national organisations have worked with the International Organisation for Standards (ISO) to ensure that the CC is suitable to become a formal standard. As a result, CC version 2.1 is now formally recognised as ISO 15408. Acceptance by ISO will ensure that the CC rapidly becomes the world standard for security specifications and evaluations.

Adoption of the CC as a world standard and wide recognition of evaluation results will provide benefits to all parties:

- A wider choice of evaluated products for consumers;
- Greater understanding of consumer requirements;
- Greater access to markets for developers.

1.3.2 How do I buy products that conform to the CC?

Information about products that have been certified/validated against the CC may be found in evaluation scheme publications or on scheme web sites (see section 4).

When selecting a product from one of these lists care should be taken to ensure that the same version of the product is being used, and that the intended environment is consistent with that evaluated.

1.3.3 What guarantees do CC-certified/validated products provide?

The certification/validation of evaluation results can provide a sound basis for confidence that security measures are appropriate to meet a given threat, and that they are correctly implemented. However, the certification/validation of evaluation results should not be viewed as an absolute guarantee of security. Indeed, the term "security" should always be viewed in relation to a particular set of threats and assumptions about the environment. Confidence in the security of a product, system or service is very much a state of mind. The CC can be used to build such confidence by providing a means of quantifying or measuring the extent to which security has been assessed.

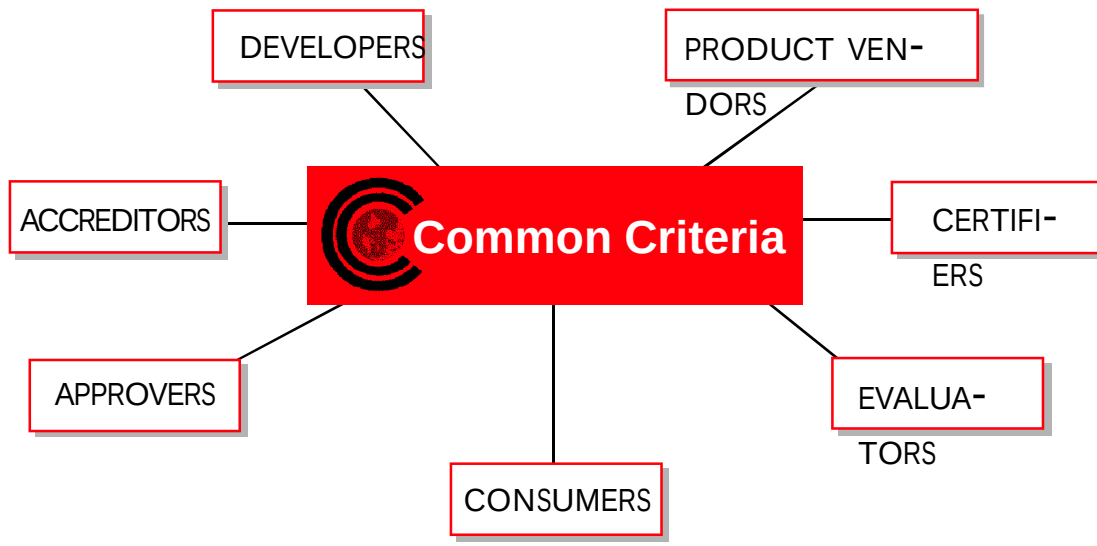
The CC includes an assurance scale (the Evaluation Assurance Levels) that can be applied to help generate different levels of confidence in the security of products. How much confidence is required will be a matter for users to determine, in relation to the value of assets to be protected, the threat environment, and the available budget.

An evaluation carried out under a recognised Scheme does provide confidence that the work is done under an accredited quality system by independent and experienced evaluators.

1.3.4 Where do I start if I want to achieve a CC certification/validation for my security products?

For an organisation or product vendor seeking certification/validation the initial point of contact can be a national scheme, or an evaluation facility (testing laboratory). For those knowing little about the subject it will be most appropriate to contact a national scheme, using the points of contact listed in this guide. National schemes will be able to provide general information on the scheme, together with lists of accredited testing laboratories. The customer may then choose to approach a single laboratory for further information and a quotation, or may invite several to bid for the work.

1.4 Interested Parties



1.4.1 Consumers

The CC is written to ensure that evaluation fulfils the needs of consumers, as this is the fundamental purpose and justification for the evaluation process. Consumers can use the results of evaluations to help decide whether an evaluated product or system fulfils their security needs. The CC gives consumers an implementation independent structure termed the Protection Profile (PP) in which to express their special requirements for IT security measures.

1.4.2 Developers and Product Vendors

Developers of products to meet the requirements of the CC need an understanding of how the processes work. Requirements may be driven by a specific customer need, or vendors may identify a market niche.

This guide refers primarily to the role of developer, but recognises that developers may not be the same organisation as the product vendor, or indeed the sponsor of the evaluation. The term developer is intended to encompass these other organisations.

Developers need to understand how PPs work, since matching a PP is one of the best ways to ensure that a product provides utility.

Developers seeking CC certification/validation need to be aware of the CC approach, and of what an evaluation facility will require from them. The CC requirements can be integrated into the system development process from the very earliest stages of requirements capture and architectural system design. The CC standards are practical and achievable, and can be reached more easily if planned from the outset. Trying to address security concerns near the end of the production process is always more difficult.

1.4.3 Evaluators and Certifiers/Validators/Overseers

The CC model provides for the separation of the roles of evaluator and certifier/validator. Certificates are awarded by national schemes on the basis of evaluations carried out by independent evaluation facilities (testing laboratories). The latter are typically commercial organisations operating testing laboratories accredited to ISO Guide 25. The provision of separate oversight by a certifier/validator helps to ensure technical consistency across all evaluation facilities.

1.4.4 Accreditors and Approvers

It is often the case, for a CC evaluation to be required, that some responsible authority has mandated that certain security standards are to be achieved - by using the CC. These are termed accreditors, or accreditation authorities. Accreditors are sometimes closely involved in the determination of functional and assurance requirements for a system.

Accreditors need to understand how the different Evaluation Assurance Levels or assurance packages can be used as objective measures of risk reduction, when applied to critical security functions in an IT system. They should therefore be familiar with CC Part 3.

It is also important that they understand the system integration concepts associated with building certified/ validated CC products into specific IT systems.

2. What is the CC?

2.1 CC Overview

2.1.1 Roadmap to the Common Criteria

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 Section 6.

Part 1, Introduction and general model, is the introduction to the CC. It 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 usefulness of each part of the CC is described in terms of each of the target audiences.

Part 2, Security functional requirements, establishes a set of security functional components as a standard way of expressing the security functional requirements for TOEs (see Section 6). Part 2 catalogues the set of functional components, families, and classes.

Part 3, Security assurance requirements, 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 and presents evaluation assurance levels that define the predefined CC scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs).

In support of the three parts of the CC listed above, it is anticipated that other types of documents will be published, including technical rationale material and guidance documents.

The following table presents how the parts of the CC will be of interest to the three key CC user groupings.

	Consumers	Developers	Evaluators
Part 1: Introduction and General Model	Use for background information and reference purposes. Guidance structure for PPs.	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.
Part 2: Security Functional Requirements	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.	Use as a mandatory statement of evaluation criteria when determining whether a TOE meets claimed security functions.
Part 3: Security Assurance Requirements	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Use as a mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

2.1.2 How should Consumers use the CC

Consumer use of the CC relates to the specification of the functional and assurance requirements of products and systems under procurement. Part 2 of the CC is used when specifying the security functional requirements, and Part 3 when specifying the assurance requirements. The consumer can then use this statement of requirements as a specification to vendors of products or system integrators.

2.1.3 How should Developers use the CC

Once the developer has recognised that there is a market for a CC evaluated and certified/validated product, the CC should be used to produce deliverables to meet those requirements.

The developer may specify the functional and assurance requirements in a Security Target, or may have them specified by the consumer in the form of a Protection Profile.

The functional requirements, specified using Part 2 of the CC, are those with which the product is required to conform. Part 3 of the CC contains developer actions that are to be followed when formulating deliverables for evaluations to a particular set of assurance requirements.

2.1.4 How should Evaluators use the CC

The CC contains mandatory statements of evaluation criteria that are used when determining whether a Target of Evaluation (TOE) meets its claimed security functionality and assurance requirements. Guidance on the application of the CC is given in the Common Evaluation Methodology (see Section 2.5).

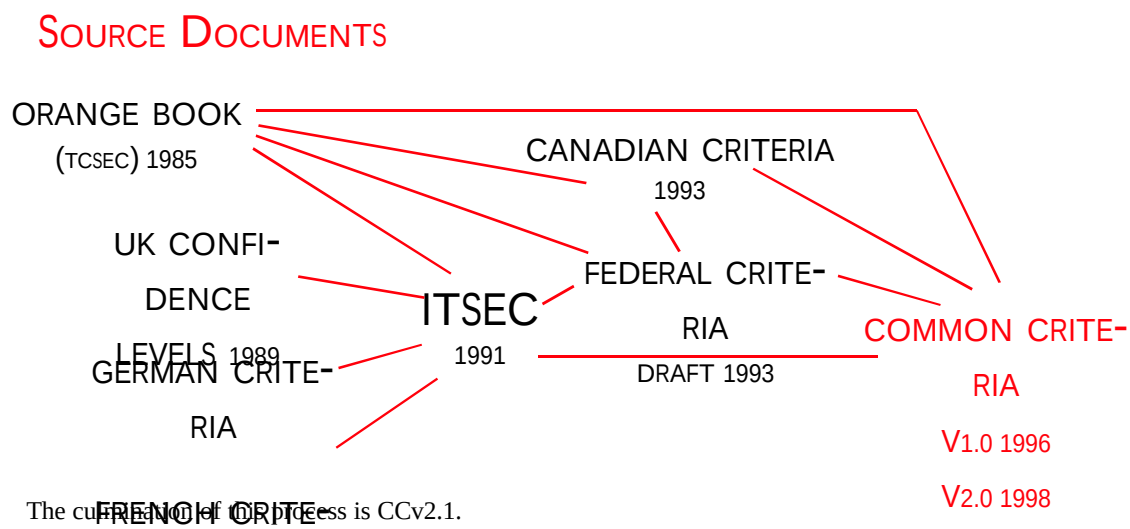
2.1.5 Origins of the CC

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 that built upon the concepts of the TCSEC but were more flexible and adaptable to the evolving nature of IT in general.

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 3.0 was published in early 1993 as a combination of the ITSEC and TCSEC approaches. In the United States, the draft Federal Criteria for Information Technology Security (FC) version 1.0 was also published in early 1993, as a second approach to combining North American and European concepts for evaluation criteria.

Work had begun in 1990 in the International Organisation for Standardisation (ISO) to develop a set of 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.

2.1.5.1 Development of the Common Criteria



The current level of this process is CCv2.1.

For historical and continuity purposes, ISO/IEC JTC 1/SC 27/WG 3 (the ISO body responsible for developing criteria) has accepted the continued use of the term "Common Criteria" (CC), while recognising that its official name in the ISO context is "Evaluation Criteria for Information Technology Security".

2.1.5.2 ISO 15408 v Common Criteria

With the publication of CCv2.1 there are no technical differences between the CC and ISO15408.

2.2 CC Building Blocks

2.2.1 Security Functional Requirements

Security functional requirements are grouped into classes. Classes are the most general grouping of security requirements, and all members of a class share a common focus. Eleven functionality classes are contained within Part 2 of the CC. These are as follows:

- Audit
- Cryptographic Support
- Communications
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TOE Security Functions
- Resource Utilisation
- TOE Access
- Trusted Path/Channels

Each of these classes contains a number of families. The requirements within each family share security objectives, but differ in emphasis or rigour. For example, the Audit class contains six families dealing with various aspects of auditing (e.g. audit data generation, audit analysis and audit event storage).

Each family contains one or more components, and these components may or may not be in a hierarchy. For example, the Audit Data Generation family contains two non-hierarchical components, one dealing with the generation of audit records, and the other dealing with association of a user with an auditable event.

The statement of TOE security functional requirements contained in the ST defines the functional requirements of the TOE and should be drawn from the Part 2 functionality classes where possible.

2.2.2 Security Assurance Requirements

Security assurance requirements are grouped into classes. Classes are the most general grouping of security requirements, and all members of a class share a common focus. Eight assurance classes are contained within Part 3 of the CC. These are as follows:

- Configuration Management
- Delivery and Operation
- Development
- Guidance Documents
- Life Cycle Support
- Tests
- Vulnerability Assessment
- Assurance Maintenance

Two additional classes contain the assurance requirements for PPs and STs.

Each of these classes contains a number of families. The requirements within each family share security objectives, but differ in emphasis or rigour. For example, the Development class contains seven families dealing with various aspects of design documentation (e.g. functional specification, high-level design and representation correspondence).

Each family contains one or more components, and these components are in a strict hierarchy. For example, the Functional Specification family contains four hierarchical components, dealing with increasing completeness and formality in the presentation of the functional specification.

The CC has provided seven predefined assurance packages, on a rising scale of assurance, known as Evaluation Assurance Levels (EALs). These provide balanced groupings of assurance components that are intended to be generally applicable. The seven EALs are as follows:

EAL1 - functionally tested

EAL2 - structurally tested

EAL3 - methodically tested and checked

EAL4 - methodically designed, tested and reviewed

EAL5 - semiformally designed and tested

EAL6 - semiformally verified design and tested

EAL7 - formally verified design and tested

The statement of TOE security assurance requirements in the ST, should state the assurance requirements as one of the EALs optionally augmented by Part 3 assurance components.

Each of the seven Evaluation Assurance Levels is summarised below. EAL1 is the entry level. Up to EAL4 increasing rigour and detail are introduced, but without introducing significant specialised security engineering techniques. EAL1-4 can generally be applied to products and systems not developed with evaluation in mind.

Above EAL4 the increasing application of specialised security engineering techniques is required. TOEs meeting the requirements of these levels of assurance will probably have been designed and developed with that objective. At the top level (EAL7) there are significant limitations on the practicability of meeting the requirements, partly due to substantial cost impact on the developer and evaluation activities, and also because anything other than the simplest of products is likely to be too complex to submit to state of the art techniques for formal analysis.

EAL1 EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

This level provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided.

EAL2 EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

EAL3 EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices. It is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without incurring substantial re-engineering costs.

An EAL3 evaluation provides an analysis supported by “grey box” testing, selective confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. Development environment controls and TOE configuration management are also required.

EAL4 EAL4 permits a developer to maximise assurance gained from positive security engineering based on good commercial development practices. Although rigorous, these practices do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. It is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs, and are prepared to incur additional security-specific engineering costs.

An EAL4 evaluation provides an analysis supported by the low-level design of the modules of the TOE, and a subset of the implementation. Testing is supported by an independent search for vulnerabilities. Development controls are supported by a life-cycle model, identification of tools, and automated configuration management.

EAL5 EAL5 permits a developer to gain maximum assurance from security engineering, based upon rigorous commercial development practices, supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

An EAL5 evaluation provides an analysis that includes all of the implementation. Assurance is supplemented by a formal model and a semiformal presentation of the functional specification and high-level design, and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure resistance to attackers with a moderate attack potential. Covert channel analysis and modular design are also required.

EAL6 EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.

An EAL6 evaluation provides an analysis that is supported by a modular and layered approach to design, and a structured presentation of the implementation. The independent search for vulnerabilities must ensure resistance to attackers with a high attack potential. The search for covert channels must be systematic. Development environment and configuration management controls are further strengthened.

EAL7 EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

For an EAL7 evaluation the formal model is supplemented by a formal presentation of the functional specification and high-level design, showing correspondence. Evidence of developer "white-box" testing and complete independent confirmation of developer test results are required. Complexity of the design must be minimised.

2.2.3 Dependencies and Operations

2.2.3.1 Dependencies

Dependencies may exist between components when a component is not self sufficient, and relies on the presence of another component. Dependencies may exist between functional components, between assurance components, and (rarely) between functional and assurance components.

Component dependency descriptions form part of the CC component definitions. In order to ensure completeness of the requirements description, dependencies should be satisfied when incorporating components into PPs and STs.

An example of a dependency is that user authentication requires that the user is first identified. In CC terms this is expressed as user identification depends on user authentication (or, using component names, FIA_UAU.1 depends on FIA_UID.1).

All assurance dependencies are satisfied when using the predefined EALs.

2.2.3.2 Operations

CC components can be used exactly as defined in the CC, or may be tailored through the use of permitted operations, in order to meet a specific security policy or counter a specific threat. There are four types of operation:

- **Assignment**, which permits the specification of a parameter to be filled in when the component is used
  e.g. FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].
- **Selection**, which permits the specification of items that are to be selected from a list given in the component
  e.g. FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] all objects
- **Iteration**, which permits the use of a component more than once with varying operations. It is likely that iteration will be needed when specifying management operations using functionality class FMT.
- **Refinement**, which permits the addition of extra detail when the component is used
  e.g. FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric specified by the ST author].
  Refinement: The TSF shall enforce a minimum password length of 8 characters.

Each CC component identifies any permitted operations of assignment and selection. These operations are used only in CC Part 2. The operations of iteration and refinement can be performed for any component. Some required operations may be completed (in whole or in part) in the PP, or may be left to be completed in the ST. All operations must be completed in the ST.

2.2.4 Packages

Sets of functional and assurance components may be grouped together into re-usable packages, which are known to be useful in meeting identified objectives. An example of such a package would be functional components required for Discretionary Access Controls.

2.3 Protection Profiles

2.3.1 What is a Protection Profile (PP)?

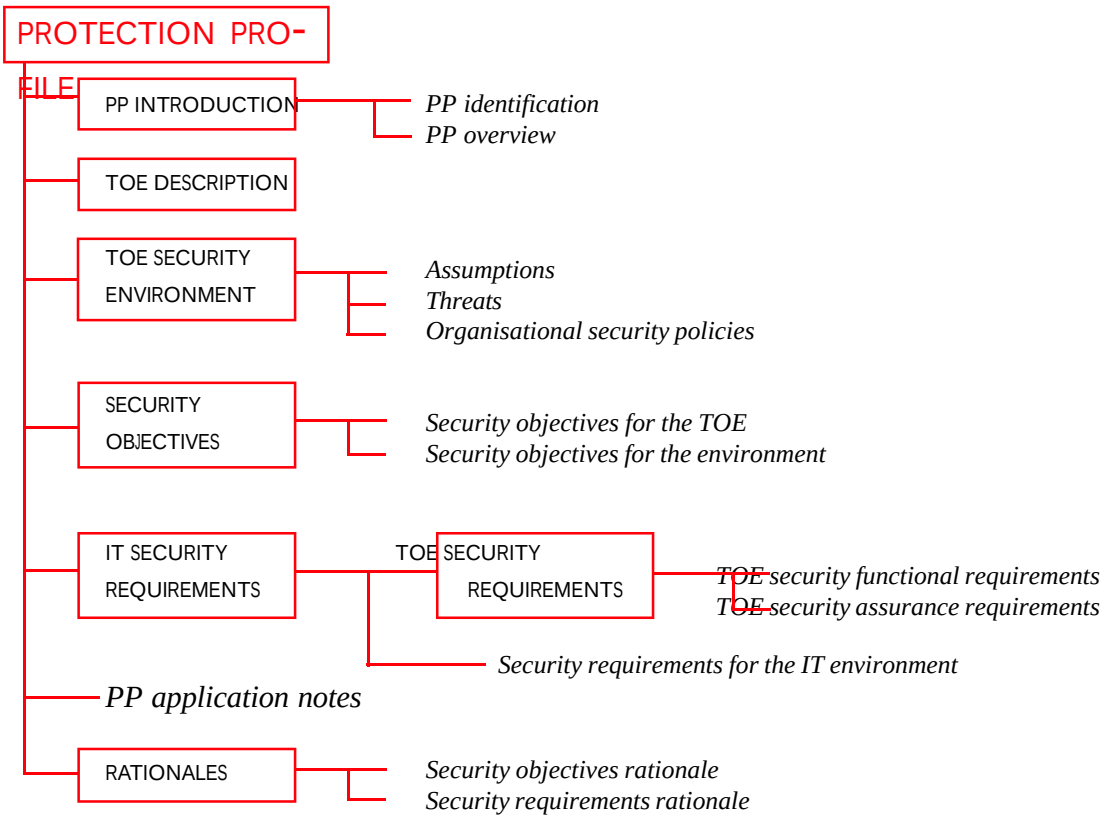
A PP is an implementation independent statement of security requirements that is shown to address threats that exist in a specified environment.

A PP would be appropriate in the following cases:

- A consumer group wishes to specify security requirements for an application type (e.g. electronic funds transfer)
- A government wishes to specify security requirements for a class of security products (e.g. firewalls)
- An organisation wishes to purchase an IT system to address its security requirements (e.g. patient records for a hospital)

2.3.2 Contents of a PP

The required content of a PP is given in CC Part 1 Annex B.



2.3.3 When is a PP Needed?

PPs are needed when setting the standard for a particular product type. These standards can be set by government agencies, consumers or developers.

PPs are also used to create specifications for systems or services, as the basis for a procurement.

2.3.4 How do I match my security requirements with a CC Protection Profile?

Sets of registered PPs exist at the following locations:

- http://www.radium.ncsc.mil/tpep/protection_profiles/index.html
- http://www.cesg.gov.uk/cchtml/ippr/list_by_type.html
- http://csrc.nist.gov/cc/pp/pplist.htm
- http://www.scssi.gouv.fr/present/si/ccsti/pp.html

The consumer who wishes to use one of these PPs should review the set of objectives and security requirements to decide whether to claim this as his product standard.

2.3.5 Registering PPs

Registration of a PP means that it is included in one or more of the current national scheme lists. Some national schemes offer lists for both certified/validated and non-certified/validated PPs. Care should be taken in distinguishing between these.

PPs can be submitted for evaluation to one of the evaluation facilities. Through this process the content of the PP is checked against the CC requirements to ensure that it is technically correct, clear, and internally consistent. For further information on this process, the PP author should contact one of the national schemes.

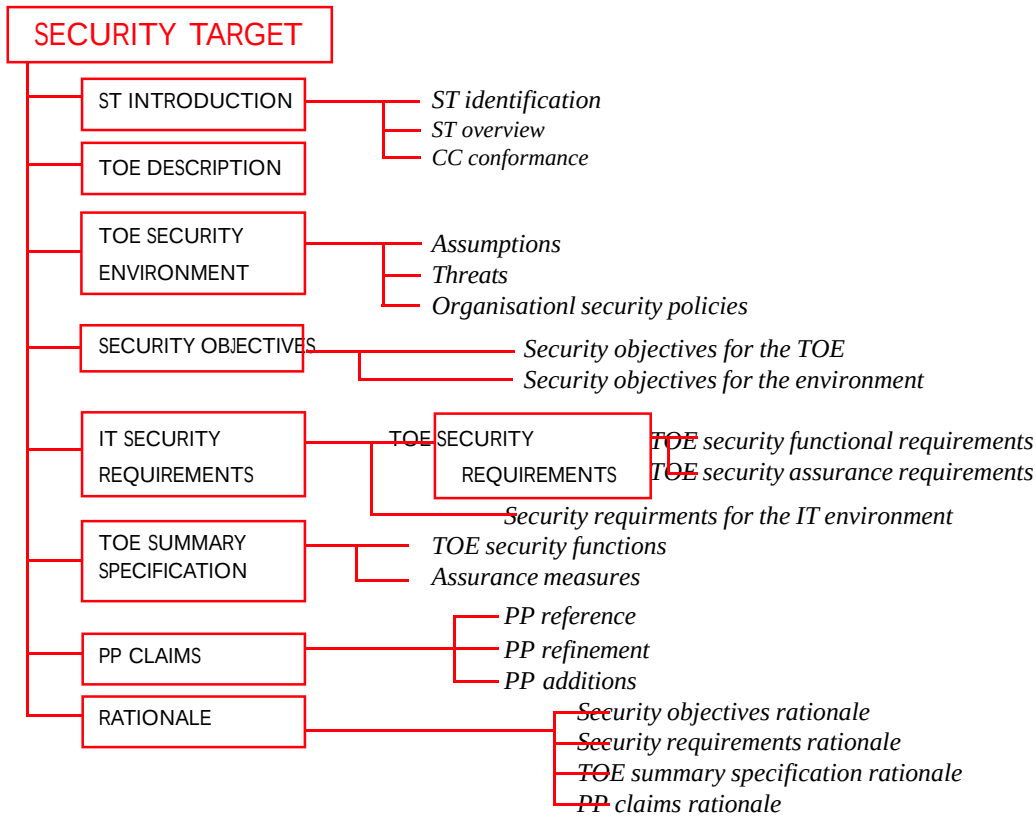
2.4 Security Targets

2.4.1 What is a Security Target (ST)?

Security Targets are the basis against which an evaluation is performed. The ST contains the TOE security threats, objectives, requirements, and summary specification of security functions and assurance measures.

2.4.2 Contents of an ST

The required content of an ST is given in CC Part 1 Annex C.



2.4.3 When is an ST Needed?

An ST is required when submitting a product for evaluation, or when submitting a product to a consumer as a statement of the TOE's security functionality and evaluated configuration.

2.4.4 How to use an ST

The consumer of a TOE should use the ST to check whether the security functionality of the TOE and its assurance package are consistent with his requirements and whether the evaluated configuration is consistent with the proposed environment.

The evaluator is required to evaluate the ST, and to use it as the basis against which the product is evaluated.

2.5 Supporting CC-Related Documentation

2.5.1 Common Evaluation Methodology (CEM)

The CEM is a companion document to the CC that explains in detail the principles and processes whereby evaluations are conducted using the CC criteria. Part 1 contains a statement of the fundamental principles behind CC evaluations, and defines various roles. Part 2 currently provides a detailed methodology for evaluations at EAL1 to EAL4. This document is currently at version 1.0, and its application is mandatory for mutual recognition of results. Future expansion of the scope, and possible reorganisation of the CEM is under consideration. The CEM describes the activities to be carried out by an evaluator in conducting a CC evaluation.

2.5.2 ISO Guide to Writing PPs and STs

ISO has produced a guide to the construction of Protection Profiles (PPs) and Security Targets (STs) that is consistent with version 2.1 of the Common Criteria. As such, the document is primarily aimed at those who are involved in the development of PPs and STs. However, it is also likely to be useful to evaluators of PPs and STs, and to those who are responsible for defining and monitoring the application of the methodology for PP and ST evaluations.

2.5.3 CC Brochure

The CC sponsoring organisations have published an introductory brochure that provides a factual summary of the CC in about 20 pages. Copies of this brochure should be available from national schemes.

2.5.4 Additional information

A useful set of links to websites containing CC information can be found at:

http://csrc.nist.gov/cc/linklist.htm

3. How is the CC Used?

3.1 Application of the CC

The CC is especially useful for:

- Specifying security features in a product or system
- Assisting in the building of security features into a product or system
- Evaluating the security features of products or systems
- Supporting the procurement of products or systems with security features

A common theme is applicable in each of these areas. The CC is highly modular, and its application makes use of this feature. The CC employs structures (e.g. PP, ST and package) that can be used whole, or be divided into useful pieces to make new structures. This idea will be introduced here, and revisited later in the chapter.

3.1.1 How to construct Protection Profiles

3.1.1.1 Basic approach to Protection Profile development

The PP provides a framework within which to specify security requirements.

The steps are as follows:

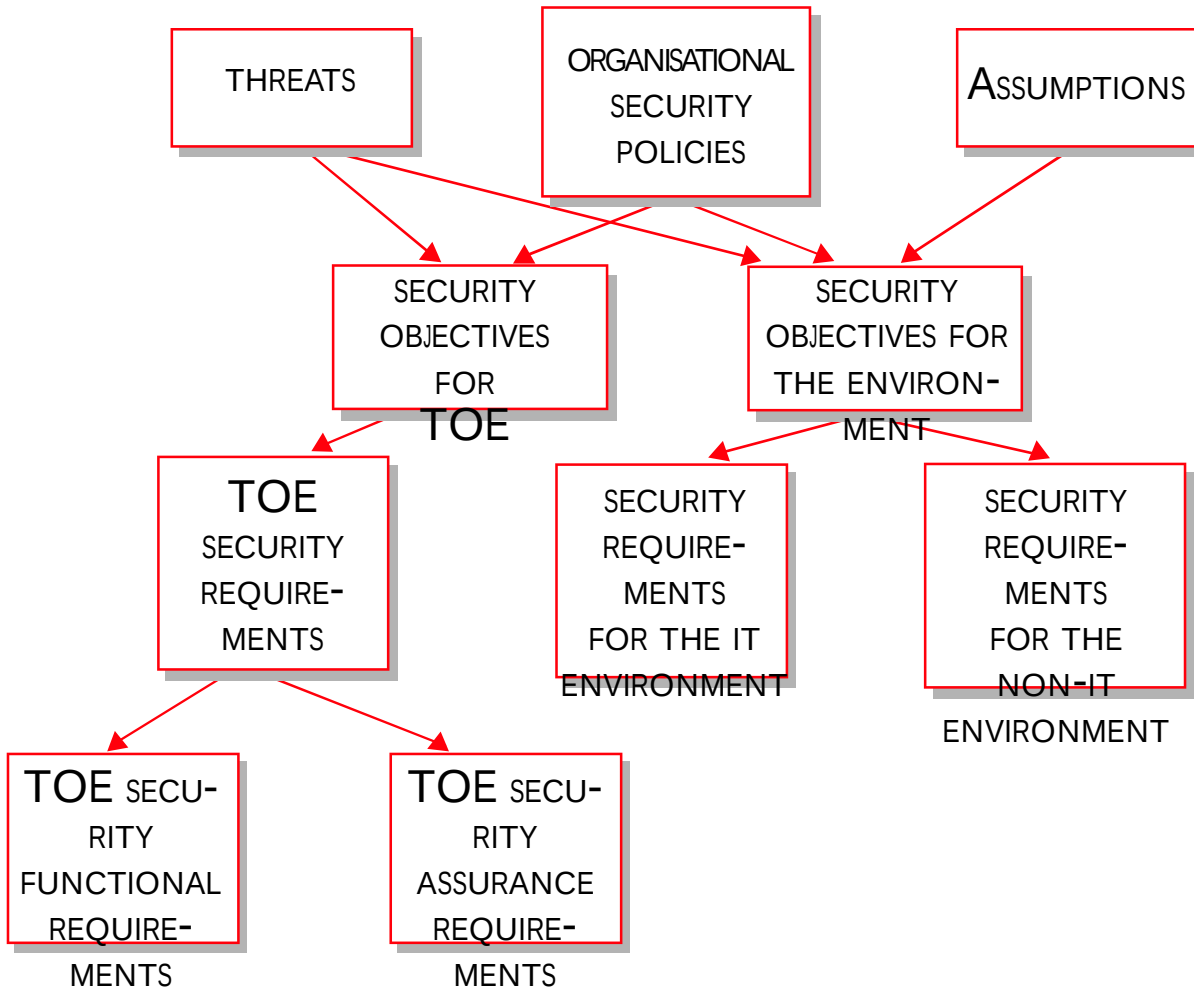
1. Describe the environment in which the product or system will reside. What are the threats against which the product or system has to provide protection? What assumptions are made about that environment? What policies exist in the environment (e.g. laws, organisational policies) to which the system must conform?

2. Determine what it is that you want to achieve in relation to the threat, and establish a set of specific objectives. The objectives should not be simply a negation of the threat, and should be realistic and achievable. The scope of the PP is determined at this stage. The objectives should be separated into those that are to be achieved by the TOE, those that are to be achieved in the environment (IT or otherwise), and those that are to be achieved by a combination of the two.

3. Use the CC Part 2 security functional requirements catalogue to specify functionality that will meet each objective identified for the product or system, and each objective for other IT within the environment. Operations should be completed where there is a need to be more specific than the generalised requirement in Part 2. Where appropriate components cannot be identified from Part 2, new ones may be devised in a similar format.

4. Use the CC Part 3 security assurance requirements catalogue to specify components that will be used to provide assurance that the objectives have been met. You can devise an assurance package that meets your explicit needs, choose from a set of predefined assurance packages (the EALs), or select some combination of these two approaches.

5. The final step is to provide a rationale that shows how the selected functional and assurance components are suitable to counter the threats in the intended environment.



3.1.1.2 Building on existing work[1]

The CC model is founded on the principles of modularity and reuse. The functional and assurance requirements catalogues are provided with this end in mind. It is intended that users should take advantage of the efforts of others when using the CC, and this approach is well illustrated by the process of system specification.

In the simplest case an existing PP may be found that addresses the entire requirement. This will be uncommon, particularly early on in the life of the CC, before a substantial set of case histories becomes available. It may be that two or more existing PPs are needed to meet a requirement. This case is almost as straightforward, although it will be necessary to demonstrate that the PPs are consistent and do not conflict.

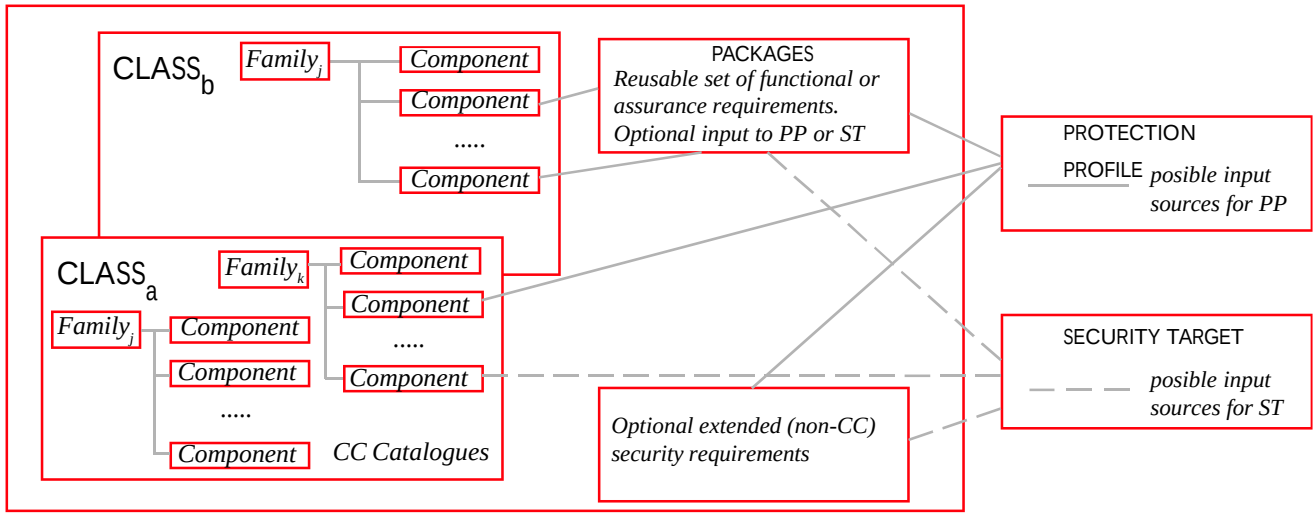
Failing this, it may be possible to take an existing PP, and adapt it to meet modified requirements. This modification may take the form of a change to the intended environment (threats, assumptions, organisational security policies), with consequential:

- Inserted or deleted functional requirements
- Inserted or deleted assurance requirements
- Modified completion of operations

It is in the process of modifying an existing PP that the benefits of the rationale become evident. Through examination of the rationale, the impact on satisfaction of objectives of any change in the functional requirements can be determined. Similarly, if an objective is no longer required it can be seen which requirements can safely be removed.

1 When reusing existing Protection Profiles care should be taken to avoid any infringement of copyright.

It may be the case for a system that more than one PP is required to address the overall requirement. These PPs may be taken on board in their entirety, or may be modified to suit. In the former case, a PP may claim conformance to one or more existing PPs (e.g. operating system PP, database PP, secure data exchange PP). In the latter it may be necessary to modify the content of a PP, in which case it may no longer possible to claim conformance. In all cases it will need to be shown that the incorporated material is consistent, and meets the objectives of the overall PP.



3.1.1.3 Protection Profiles for classes of product

Many organisations have now produced PPs that specify requirements for a class of products. Examples of this include operating systems, firewalls and smart cards (see Section 2.3.4 for sources). The purpose of such a PP is to provide a set of functional and assurance requirements that the organisation considers appropriate for the use of a particular type of product in a specific threat environment.

A product that has been certified/validated against a PP in effect receives an endorsement from the organisation that originates the PP. Firstly, the product has been found to provide the security functions that the originating organisation considers appropriate for a particular environment. Secondly, the correct operation of these functions has been independently verified using a package of assurance measures that the organisation considers appropriate for that environment.

3.1.2 How to specify a system based on CC evaluated products

A common approach when specifying security features for systems is to assemble every relevant security requirement the individual can think of. This approach is often borne out of a lack of experience, or the absence of any structured method for deriving requirements. The inevitable outcome of this process is that no evaluated product, or set of products, is able to meet all requirements, leading to non-compliant solutions, use of unevaluated products, or demands for expensive, specially produced solutions

An alternative and pragmatic approach is to use existing product specifications (STs) to help prepare a PP. The advantage of this approach is that it should be much easier to address the resulting system specification from available certified/validated products.

A suggested method is to begin by identifying the security environment for the system (threats, assumptions and organisational security policies), and to derive a set of objectives. A review of product security targets should then be conducted to identify similar objectives. The related security requirements can then be drawn out (using the rationales) and assembled into a PP. An iterative approach should be adopted, trying out various products, or combinations of products, to find the best match and reassessing risks each time. It should be considered whether moving objectives from TOE to environment might provide a more cost-effective solution for any objectives not met by an existing product, substituting procedural measures for IT.

It may thus be possible to construct a system PP that both meets the system objectives, and can be implemented using evaluated products.

Evaluation of such a system will be much simpler, given the opportunity to reuse results of the component product evaluations. However, the system evaluation needs to ensure that product dependencies on the environment are met, and that no conflicting requirements are introduced.

3.1.3 How to procure products and systems using the CC

Where a candidate product exists to address a security requirement the following checklist may be applied.

Checklist for procuring CC products

Certification/validation requirement

Certified/validated product required by organisational policy?

Certification/validation status

Product certified/validated?

Certified/validated against a PP?

PP endorsed by a relevant organisation?

Product in evaluation?

What stage has the product reached?

Can vendor claim be independently verified (e.g. by eval. facility)

Product not in evaluation?

Are there plans to enter?

Are plans credible?

Does the vendor have any incentive to achieve certification/ validation?

Does vendor have other evaluated products?

Does the PP address the relevant risks?

Is the intended environment consistent?

Hardware platform?

IT environment available?

Are risks countered sufficiently?

Are the assurance measures adequate?

Is the vendor committed to maintaining certification/validation for future releases of the product ?

3.2 Understanding Evaluation

3.2.1 What should I look for in an evaluated product?

A number of questions need to be addressed when considering use of an evaluated product:

- Does the product provide the functionality and assurance that you need ?
- Does the ST for the product claim conformance to a PP?
- Has the PP been endorsed as useful by relevant organisations?
- Is the intended environment consistent with that assumed for the evaluation?
- What are the implications for using the product in a manner not consistent with the evaluation?

National schemes undertake to make public certain information about the products that they certify/validate. This information is intended to assist consumers in determining whether the product is appropriate for their needs. The following sources are available:

- **Certificate**

  This provides the highest level of information. It is useful for checking version numbers, hardware/software platforms and assurance levels.

- **Certified/Validated Product List entry**

  This will provide a high level description of the product and the scope of the evaluation. This should be sufficient to determine whether a product is of interest, but will not provide sufficient detail to assess its suitability for use.

- **Security Target**

  This provides the basis for the evaluation, describing in detail the intended environment, objectives, requirements and top level specification. The ST alone does not provide evidence of certification/validation.

- **Certification/validation report**

  This is published by the national scheme, and provides details about the product and the results of the evaluation. The ST should be attached to the report.

These documents should be consulted as appropriate.

Where a product claims conformance to a PP, this is normally an indication that the product conforms to an industry standard. If the PP is produced or endorsed by a government agency, then the product is likely to be recommended for use in government. If the product does not claim conformance to a PP, then the ST will need to be examined carefully, to make sure that it is appropriate for the application.

An evaluation is usually based on a very limited range of hardware/software platforms. The ideal case would be that the intended platform is that covered by the evaluation. Where this is not the case, the results of the evaluation may be invalid. The certification/validation report should contain information that may be useful in assessing the impact of using alternative platforms.

It is important to check that all of the security functionality required from the product has been included in the evaluation. Some STs will contain assumptions that certain functionality is not used, as it has not been covered by the evaluation. If these assumptions are invalid for the consumer's environment, then vulnerabilities may be exploitable. For example, evaluations of network firewalls typically exclude VPN functionality. If this functionality is used, then assurance gained from the evaluation is lost.

3.2.2 What to look for in Certificates and Certification/Validation Reports

A certificate should provide the following information:

- Scheme identification
- Product name and version
- Hardware/software platform
- Assurance package (EAL)
- PP claims
- Date certified/validated

The Certification/Validation Report is the source of detailed security information about the product for any interested parties. It is intended to provide practical information to consumers. The contents of the report are specified in the Mutual Recognition Arrangement, as follows:

- Executive summary
- Identification of the product
- Product security policy
- Assumptions and scope of the evaluation
- Architectural information
- List of product documentation
- Outline of testing approach and results
- Description of the evaluated configuration
- Results of the evaluation
- Evaluator comments and recommendations
- Security Target

3.2.3 What assurance do I need?

This is a much more significant question under the CC than under preceding documents. The CC's modular design allows much more discretion in the specification of individual assurance requirements, and therefore demands more attention when it comes to the selection of an assurance package.

The simple approach is to follow the sample EALs provided in CC Part 3. These are constructed from the Part 3 components to provide a graded scale of assurance requirements. The content of each of these levels has been chosen to provide some backwards compatibility with assurance scales from previous criteria, and to give a balanced set of measures.

There is nothing sacred or magic about the EALs, and the PP or ST author is free to specify alternative approaches, either by augmenting an existing EAL, or by developing an entirely new assurance package.

This flexibility creates the opportunity to think carefully about building a cost-effective approach to evaluations, selecting components to address threats that exist for particular types of products.

Common augmentations –

For products subject to sophisticated penetration attacks ----------Vulnerability analysis (AVA_VLA)

For products that need to evolve rapidly to meet changing threats ----- Flaw remediation (ALC_FLR)

For products where high confidence is required,
but little documentation is available ----------Testing (ATE_COV, ATE_DPT)

3.2.4 What does "evaluated" mean to the Consumer?

To say that a product has been "evaluated" is to say that a defined methodology has been applied to its assessment. This of itself carries no information about the verdict of the evaluation, but merely states that a verdict has been obtained. Evaluations are conducted by the commercial testing laboratories.

Consumers should therefore look for use of the terms "certified" (Europe) and "validated " (USA). This status is conferred by the national schemes, following a successful evaluation.

Purchasing a product that merely claims to be evaluated is at your own risk!

3.2.5 What does "evaluated" mean to the Developer?

For a developer the knowledge that a product is evaluated and certified/validated imposes certain obligations for conformance to evaluated procedures. As part of the evaluation, subject to the specific assurance measures claimed, the evaluators will have ensured that procedures are in place for configuration control, distribution and developer security. The developer is expected to maintain these procedures to ensure that the assurance gained in the certified/validated product is not compromised.

3.2.6 Certification/Validation of PPs

One of the advantages of the PP approach is that a product claiming conformance to a PP can reuse the results of a PP to reduce the effort required on evaluating the product's ST. In order to take advantage of this efficiency the PP needs to be evaluated and certified/validated. The process is broadly the same as for a product evaluation, with a certificate and a certification/validation report. Certified/validated PPs should be identified as such on national registers.

3.2.7 What are Certified/Validated Products Lists?

The UK Certification Body publishes UKSP06 the Certified Products List twice each year. This document gives information on all products and PPs holding current certificates. It also identifies certified/validated products and PPs from the other organisations covered by the Mutual Recognition Arrangement. This document is also available on the U.K Scheme web site.

The US NIAP Validation Body publishes a Validated Products List on its web site. The NIAP web site contains information on all products and PPs holding current certificates. It also identifies certified/validated products and PPs from the other organisations covered by the Mutual Recognition Arrangement.

3.2.8 What are the types of evaluation result and what do they mean?

3.2.8.1 PP evaluation results

Application of the CC Part 3 evaluation criteria for PPs permits an evaluator to determine whether a PP is complete, consistent and technically sound, and hence suitable for use as a statement of requirements for an evaluatable TOE. These criteria are given in Class APE.

Evaluation of a PP results in a pass/fail statement.

3.2.8.2 TOE evaluation results

Application of the CC Part 3 evaluation criteria for TOEs permits an evaluator to determine whether the TOE satisfies the security requirements expressed in the ST.

Evaluation of a TOE results in a pass/fail statement.

3.2.8.3 Caveats on evaluation results

The results of PP and TOE evaluations are caveated with respect to the functional requirements in Part 2, the assurance requirements in Part 3, or directly to a PP. The various terms used are identified below:

- **Part 2 conformant** – where the functional requirements are based only upon functional components in Part 2
- **Part 2 extended** – where the functional requirements include functional components not in Part 2
- **Part 3 conformant** – where the assurance requirements are in the form of an EAL or assurance package that is based only on assurance components in Part 3
- **Part 3 augmented** – where the assurance requirements are in the form of an EAL or assurance package plus other components in Part 3
- **Part 3 extended** – where the assurance requirements are in the form of an EAL and additional assurance components not in Part 3, or an assurance package that includes assurance components not in Part 3
- **Conformant to a PP** – A TOE is conformant to a PP only if it is compliant with all parts of the PP

3.2.9 Accreditation vs. Certification/Validation

The accreditor is the agent that approves security measures for an organisation. The accreditor establishes the requirement for certification/validation as a means of ensuring that security requirements are addressed and threats are adequately countered.

In many system evaluations, the need arises to make judgements concerning the scope of the evaluator's work. This is to ensure that resources, which are often limited, are expended in a cost-effective manner. The developer or evaluator may propose that an accreditor grants such waivers, but the accreditor will have the final say.

Where certification/validation is a prerequisite to accreditation, the accreditor will take the certification/validation report as an input to the accreditation process. Where interim accreditation is required before certification/validation, to allow for early operation of a system, the accreditor may seek evidence from the certification/validation body or from the evaluator.

The approach to system accreditation varies significantly between countries.

3.3 Performing an Evaluation

3.3.1 Who does the work?

Evaluations are carried out by accredited evaluation facilities (testing laboratories). Lists of such facilities may be obtained from national schemes.

3.3.2 What is done during an evaluation?

The process outlined here is that for a typical evaluation, and for ease of presentation is divided into three phases. In practice there are a number of options, in particular when the evaluation is performed in parallel with the development process.

- Phase 1 – Preparation
- Phase 2 – Conduct of Evaluation
- Phase 3 – Conclusion

3.3.2.1 Phase 1

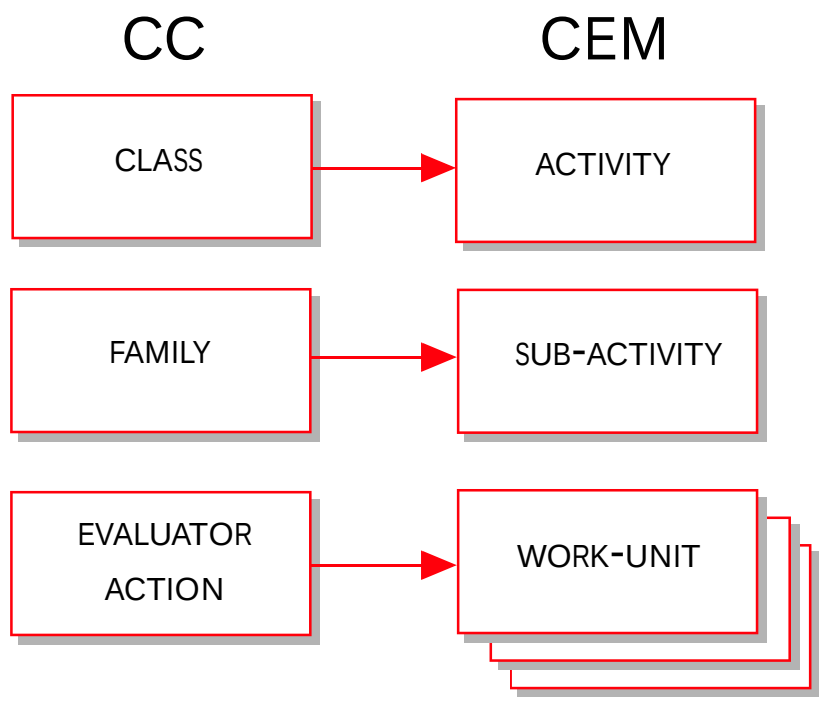
Phase 1 includes the initial contact between the sponsor of the evaluation and the evaluation facility, any initial consultancy to determine readiness for evaluation, and preparation for the evaluation itself. Initial consultancy is particularly recommended for sponsors and developers without prior evaluation experience. Consultancy will confirm that the sponsor and developer are well prepared for the conduct of an evaluation, and will include at least a review of the ST, and probably some of the other evaluation deliverables.

When a successful evaluation seems feasible, a list of the required evaluation deliverables, a plan for their delivery, and a project plan for the evaluation are established.

Liaison is arranged between the certification/validation body, the evaluation facility, the developer and sponsor. Contracts are established as appropriate.

3.3.2.2 Phase 2

The conduct of evaluation is a structured and formal process during which the evaluators carry out a series of activities derived from the CC. The Common Evaluation Methodology (CEM) has documented in detail the work required for evaluations conducted against EAL1-4. The correspondence between the CC and CEM entities is shown in the diagram below:



The evaluators carry out the CEM activities and their associated work-units. These activities encompass all of the evaluator actions defined in the CC. Problem reports are raised to identify any deficiencies in the deliverables, and the Evaluation Technical Report (ETR) is prepared during this phase.

3.3.2.3 Phase 3

In Phase 3 the evaluation facility provides the final output of the evaluation process, the ETR, to the certification/validation body. The ETR will contain sensitive information, and is therefore not intended as a public document. The certification/validation body uses information from the ETR to prepare a certification/validation report for publication.

3.3.3 What kind of oversight exists?

3.3.3.1 Quality

International and European standards (ISO Guide 25 and EN45001) have been established to provide general guidance for accreditation and operation of test laboratories. These standards create a framework for the objective testing of all types of products, not only those in the IT field. Where security evaluation and certification/validation are concerned, compliance with these standards is a worthwhile goal, and is an essential prerequisite of mutual recognition.

National laboratory testing organisations (UKAS in the UK and NVLAP in the USA) have developed their own interpretations of these standards for accreditation purposes. Evaluation facilities seeking to carry out evaluations under a national scheme are required to obtain laboratory accreditation from these organisations.

3.3.3.2 Technical

Each national scheme has its own approach to technical oversight of evaluation facilities, based on a combination of evaluator qualifications, monitoring of activities and review of final outputs. Although no specific approach is mandated, the organisations participating in the Mutual Recognition Arrangement have confidence in the technical standards maintained by the other organisations.

3.3.4 Rapid Development Cycles and Lengthy Evaluation

A problem identified by many developers is the length of time required for an evaluation compared to the product development lifecycle. In some cases the evaluation is not completed until a new version has been produced, and the old one is obsolescent.

Consumers may take different views of this situation. Some may have no confidence in the product following any change, since the impact of the change is unknown. Others may consider that their confidence declines progressively as the product changes. This may be an example of the difference between confidence and assurance: confidence being a state of mind, and assurance being the direct consequence of an evaluation.

Irrespective of the speed of evaluations, developers will wish to have a cost-effective approach to maintain the assurance in their evaluated products, and therefore to ensure the continued confidence held by consumers.

3.3.5 Assurance Maintenance

Two approaches are available:

- **Re-evaluation** – During re-evaluation the evaluation facility will consider the impact of changes made to the product, and will reuse results of the original evaluation where possible. Re-evaluation will again be specific to a single version of the product. Substantial savings on the original evaluation costs should be possible, although the assurance achieved should be the same.

- **Certificate Maintenance Schemes** (CMS) – Some countries have developed alternative schemes that allow their certification/validation status to be maintained. The objective here is to define an approach that will ensure that assurance is maintained, even in the face of a rapidly evolving product. The UK scheme achieves this by placing greater trust in the work of the developer, while at the same time ensuring that this trust can be justified, and that the developer's work is audited.

As the Mutual Recognition Arrangement does not yet cover CMS, re-evaluation is the only alternative currently available to a developer requiring international acceptance of certification/validation status.

3.3.6 ITSEC/TCSEC to CC

Many developers already have a significant investment in evaluations against the source criteria (particularly ITSEC and TCSEC). This investment can be protected through special arrangements made by national schemes that allow conversion to the CC at the time of a re-evaluation.

The UK has produced a set of work programme supplements that identify the work required to migrate from ITSEC E1-E3 to CC EAL2-EAL4.

In the USA, PPs have been produced to express TCSEC C2 and B1 requirements in CC format, although the logistics for conversion have not yet been identified.

You are encouraged to contact your scheme representatives for additional information in this area.

4. National Schemes

4.1 What are the National Schemes?

The UK,
represented by CESG

Canada,
represented by
the CSE

The Netherlands,
represented by NLNCSA
(No scheme)

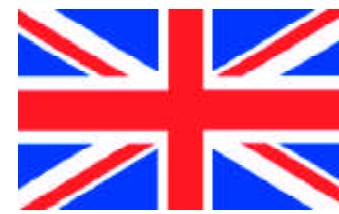
The USA,
represented by
NIST and NSA

Germany,
represented by BSI

France,
represented by SCSSI

The seven European and North American governmental organisations listed above constitute the CC Project Sponsoring Organisations. These organisations have provided nearly all of the effort that went into developing the CC from its inception to its completion. These organisations are also "evaluation authorities" for their respective national governments. They have committed themselves to replacing their respective evaluation criteria with the CC version 2.1 now that its technical development has been completed and it is an international standard.

4.1.1 In the United Kingdom



The Communications-Electronics Security Group (CESG) and the Department of Trade and Industry (DTI) operate the UK IT Security Evaluation and Certification Scheme.

Contact details are:

Certification Body Secretariat
UK IT Security Evaluation and Certification Scheme
PO Box 152
Cheltenham GL52 5UF
United Kingdom

Tel: +44.1242.238739

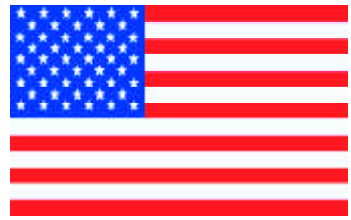
Fax: +44.1242.235233

E-mail: info@itsec.gov.uk

WWW: http://www.itsec.gov.uk

FTP:ftp://ftp.cesg.gov.uk/pub

4.1.2 In the United States



The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) operate the Common Criteria Evaluation and Validation Scheme (CCEVS) under the National Information Assurance Partnership (NIAP).

Contact details are:

National Information Assurance Partnership
100 Bureau Drive (Mailstop 8930)
Gaithersburg, MD 20899-8930
U.S.A.

Tel: +1.301.975.2934, Fax: +1.301.948.0279

E-mail: scheme-comments@nist.gov

WWW: http://niap.nist.gov/cc-scheme

4.1.3 In Canada

The Communications Security Establishment (CSE) operates the Canadian Common Criteria Scheme.

Contact details are:

Communications Security Establishment
Criteria Co-ordinator
Computer and Network Security
P.O. Box 9703, Terminal
Ottawa, Canada K1G 3Z4

Tel: +1.613.991.7882, Fax: +1.613.991.7455

E-mail: criteria@cse-cst.gc.ca

WWW: http://www.cse-cst.gc.ca/cse/english/cc.html

FTP: ftp://ftp.cse-cst.gc.ca/pub/criteria/CC2.0

4.1.4 In the Netherlands (no scheme)

The Netherlands National Communications Security Agency (NLNCSA) participates in Common Criteria development.

Contact details are:

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

WWW: http://www.tno.nl/instit/fel/refs/cc.html

4.1.5 In Germany

The Bundesamt für Sicherheit in der Informationstechnik (BSI) operates the German Evaluation and Certification Scheme.

Contact details are:

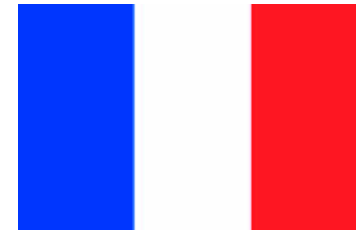
Bundesamt für Sicherheit in der Informationstechnik (BSI)
German Information Security Agency (GISA)
Abteilung V
Postfach 20 03 63
D-53133 Bonn
Germany

Tel: +49.228.9582.300, Fax: +49.228.9582.427

E-mail: cc@bsi.de

WWW: http://www.bsi.bund.de/cc

4.1.6 In France



The Service Central de la Sécurité des Systèmes d'Information (SCSSI) operates the French Evaluation and Certification Scheme.

Contact details are:

Service Central de la Sécurité des Systèmes d'Information (SCSSI)

Centre de Certification de la Sécurité des Technologies de l'Information
18, rue du docteur Zamenhof
F-92131 Issy les Moulineaux
France

Tel: +33.1.41463784, Fax: +33.1.41463701

E-mail: ssi20@calva.net

4.2 How much do evaluations typically cost?

Obviously a guide like this cannot provide prices, but some indication can be given of the things that will typically need to be paid for, and some pointers to how budgets should be set.

4.2.1 What you pay for

4.2.1.1 Pre-evaluation

The amount spent on pre-evaluation activities will vary according to how much experience of the evaluation process the developer has. With little experience it is a good idea to seek (at least) assistance with preparation of the ST, and a review of the proposed evaluation deliverables. Pre-evaluation consultancy may be taken either from an evaluation facility or from an independent consultant.

Developers are often reluctant to spend money in this area, preferring to use the evaluation process itself to reveal problems. This is usually a mistake, since an evaluation is a very formal exercise, with strictly controlled channels of communication, and it is much easier to address such issues in an informal manner, and before large sums are committed to the formal evaluation process.

4.2.1.2 Evaluation

National schemes will differ in the approach that is taken to charges for formal evaluation. A typical approach would be to offer a fixed price for the evaluation, with a further sum requested for any re-work that has to be carried out following the identification of problems.

4.2.1.3 Certification/Validation

Some schemes make a charge for oversight of the evaluation, and a separate contract is necessary to cover these costs. These charges will add to the price of an evaluation.

4.2.1.4 Internal costs

It is easy to underestimate the internal costs to an organisation of the evaluation process. At low assurance levels these may be minimal, but moving up the assurance scale, especially beyond EAL3, can incur significant internal costs. These costs will be associated with:

- Production of evaluation deliverables not normally associated with the developer's production process
- Additional testing
- Additional analysis
- Addressing issues raised by the evaluators

4.2.2 Factors that influence the price

The price of an evaluation will be closely related to the amount of work that the evaluators need to do and to the quality of the evaluation deliverables.

The amount of work that the evaluators need to do is influenced by:

- **The assurance profile** – the more assurance that is required the more work that the evaluators are required to do. Some idea of the work to be performed at EALs 1-4 can be gained from an inspection of the work units for each level given in the Common Evaluation Methodology.
- **The scope of evaluated functionality** – There is a temptation in a functionally rich product to include everything in the ST, when in fact consumers require only a subset to be evaluated. Developers can help to control costs by limiting the functionality claimed, and thus limiting the portion of the product that must be examined.
- **The design of the product** – If the product is designed using a modular approach, with the security functions performed by a small number of modules, it may be possible to limit the portion of the product that must be examined.

- **Problems encountered** – Where the evaluators encounter problems, either with the evaluation deliverables or with the product itself, there will be a need for remedial action, and some of the evaluation activities will need to be revisited. If the developer is not well prepared for the evaluation, or the design of the product itself is poor, then the amount of rework may be substantial.

4.2.3 Factors that affect duration of evaluations

The duration of an evaluation is directly affected by:

- The assurance package claimed
- The extent of security functionality
- Product development timescales
- The quality of evaluation deliverables
- The availability of developer and evaluator resources
- The quality of communication between developer and evaluator

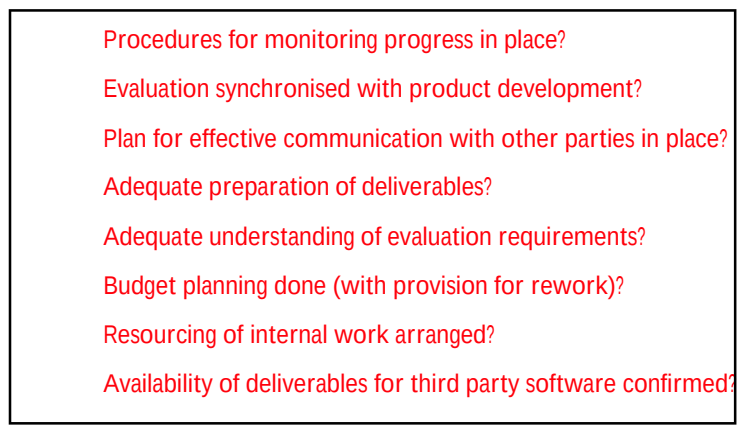
The ST plays a significant role in determining the duration (and cost) of an evaluation. The assurance components that are chosen will determine the activities the evaluator has to perform, and additional functional components affect the work done for many of these assurance components (e.g. those for development). Developers wishing to operate within a limited budget or timescale should consider both the minimum assurance package that is needed for their market, and the security functionality that their market considers essential.

The duration of many evaluations is affected by the timing of product releases. Developers may wish to delay an evaluation in order to take account of a new product release, or indeed because resources are not available to handle both.

Duration is also affected by the quality of evaluation deliverables. If the documentation is clear, and conforms to requirements, then the evaluation will progress smoothly. If not, then significant delays may be encountered as a developer seeks to remedy deficiencies. At worst this can lead to the evaluation being suspended for several months.

The importance of communication should not be underestimated. Both sides have a great deal to learn during an evaluation, and the effective transfer of information and understanding is vital.

The following checklist may be useful as you prepare to enter an evaluation.



4.3 Mutual Recognition

A Mutual Recognition Arrangement (MRA) was signed in 1998 by the government agencies in Canada, France, Germany, the UK and the USA. By this arrangement the parties mean to recognise that evaluations carried out in the other countries conform to acceptable technical standards.

Key features of the MRA are that it is a non-binding arrangement, and that it allows for the admission of new organisations.

Products that are certified/validated and mutually recognised by the participating agencies are entitled to use the identifying mark shown right.

4.3.1 What the arrangement covers

- Assurance levels EAL1 to EAL4
- Any other package using EAL2 to EAL4 assurance components
- CC Part 2 functional components
- Extended functional components

4.3.2 What the arrangement does not cover

- Any CC Part 3 assurance components not used in EAL1 to EAL4
- Any extended assurance components
- Assurance maintenance schemes

4.3.3 Different countries' assurance requirements

The existence of MRA will be beneficial to developers in limiting the number of different criteria to which their products need to conform, and to consumers in widening their choice of certified/validated products. However, it is important to note that national considerations will still have a strong bearing upon the nature of the evaluation that is required.

Governments and private sector organisations in many countries are now developing PPs that identify national or industry requirements, and these often differ significantly. It is important therefore, that the developer considers to those aspects of functionality and assurance that help to ensure that evaluation results have utility in a range of countries.

5. Index to functional components

This index is designed to help identify the appropriate functional component to be used to express requirements in specified areas.

6. Understanding the terms

This section contains only those terms that 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.

Assets Information or resources to be protected by the countermeasures of a TOE.

Assignment The specification of an identified parameter in a component.

Assurance Grounds for confidence that an entity meets its security objectives.

Attack potential The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Augmentation The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package. *Augmentations are used when the PP or ST author*

considers This is a much more significant question under the CC than under preceding documents. The CC's modular design allows much more discretion in the specification of individual assurance requirements, and therefore demands more attention when it comes to the selection of a profile.

The simple approach is to follow the sample EALs provided in CC Part 3. These are constructed from the Part 3 components to provide a graded scale of assurance requirements. The content of each of these levels has been chosen to provide some backwards compatibility with earlier assurance scales, and to give a balanced set of measures.

Authentication data Information used to verify the claimed identity of a user.

Authorised user A user who may, in accordance with the TSP, perform an operation.

CC Common Criteria, the name used historically for the standard in lieu of its official ISO name of "Evaluation Criteria for Information Technology Security"

Class A grouping of families that share a common focus.

Component The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Connectivity The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any

distance in any environment or configuration.

Dependency A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet

their objectives.

EAL Evaluation Assurance Level.

Element An indivisible security requirement.

Evaluation Assurance Level (EAL) A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

Evaluation authority A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.

Evaluation scheme The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

Evaluation Assessment of a PP, an ST or a TOE, against defined criteria.

Extension and/ The addition to an ST or PP of functional requirements not contained in Part 2 or assurance requirements not contained in Part 3 of the CC.

External IT entity Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Family A grouping of components that share security objectives but may differ in emphasis or rigour.

Formal Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Human user Any person who interacts with the TOE.

Identity A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

Informal Expressed in natural language.

Internal communication channel A communication channel between separated parts of a TOE.

Internal TOE transfer Communicating data between separated parts of a TOE.

Inter-TSF transfers Communicating data between the TOE and the security functions of other trusted IT products.

IT Information Technology.

Iteration The use of a component more than once with varying operations.

Object An entity within the TSC that contains or receives information and upon which subjects perform operations.

Organisational security policies One or more security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

Package A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

PP see **Protection Profile**.

Product A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Protection Profile (PP) An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Reference monitor The concept of an abstract machine that enforces TOE access control policies.

Reference validation mechanism An implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing.

Refinement The addition of details to a component.

Role A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

Security attribute Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

Security Function (SF) A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Function Policy (SFP) The security policy enforced by an SF.

Security objective A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.

Security Target (ST) A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Selection The specification of one or more items from a list in a component.

Semiformal Expressed in a restricted syntax language with defined semantics.

SF see **Security Function**.

SFP see **Security Function Policy**.

SOF see **Strength of Function**.

SOF-basic A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-high A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

SOF-medium A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

ST see Security Target

Strength of Function (SOF) A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

Subject An entity within the TSC that causes operations to be performed.

System A specific IT installation, with a particular purpose and operational environment.

Target of Evaluation (TOE) An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE see Target of Evaluation

TOE resource Anything usable or consumable in the TOE.

TOE Security Functions (TSF) A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Functions Interface (TSFI) A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.

TOE Security Policy (TSP) A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TOE security policy model A structured representation of the security policy to be enforced by the TOE.

Transfers outside TSF control Communicating data to entities not under control of the TSF.

Trusted channel A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

Trusted path A means by which a user and a TSF can communicate with necessary confidence to support the TSP.

TSC see **TSF Scope of Control**.

TSF see **TOE Security Functions**.

TSF data Data created by and for the TOE, that might affect the operation of the TOE.

TSF Scope of Control (TSC) The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

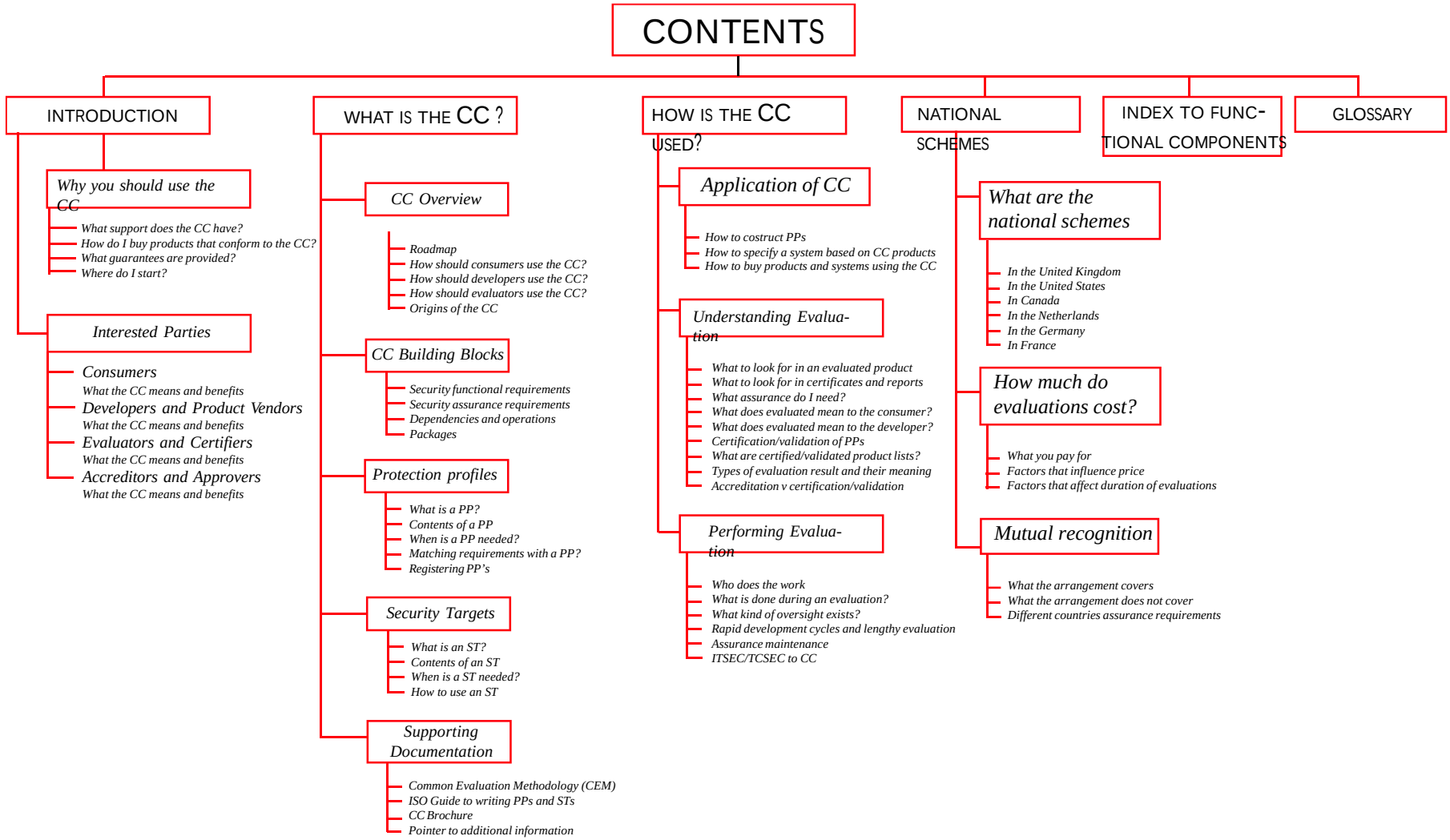
TSFI see **TOE Security Functions Interface**.

TSP see **TOE Security Policy**.

User data Data created by and for the user, that does not affect the operation of the TSF.

User Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Appendix 1 - User Guide Road map



This guide was produced by Syntegra

Its development was sponsored by CESG
in the UK and NIST in the USA