



# Common Criteria

## An Introduction

*The CC combines the best aspects of existing criteria for the security evaluation of information technology systems and products.*

This document provides a summary of the principal features of the Common Criteria (CC), and is intended for those readers who do not have either the need or time to study the CC in its entirety.

In this document you will find:

- an overview of the key CC concepts
- an overview of security functionality and the CC component catalogue
- an overview of security assurance and CC evaluation assurance levels
- the relationship between CC, TCSEC and ITSEC assurance levels

# Contents

Background	Page 3
General Model	Page 4
Key Concepts	Page 6
Security Functionality	Page 8
Security Assurance	Page 10
Evaluation Assurance Levels	Page 12
Approach to Evaluations	Page 14
Evaluation	Page 16
CC Protection Profiles	Page 17
For Further information...	Page 18

*The Common Criteria represents the outcome of efforts to develop criteria for evaluation of IT security that are widely useful within the international community. It is an alignment and development of a number of source criteria: the existing European, US and Canadian criteria (ITSEC, TCSEC and CTCPEC respectively). The Common Criteria resolves the conceptual and technical differences between the source criteria. It is a contribution to the development of an international standard, and opens the way to worldwide mutual recognition of evaluation results.*

# Background



Criteria developments in Canada and European ITSEC countries followed the original US TCSEC work (Orange Book). The US Federal Criteria development was an early attempt to combine these other criteria with the TCSEC, and eventually led to the current pooling of resources towards production of the Common Criteria.

A great strength in the CC development is the close involvement of all the parties with experience of creating the original national Criteria documents. The CC benefits from their accumulated wisdom, and their intent for a fully flexible approach to the standardisation of security functionality and evaluation assurance. The CC has been made sufficiently flexible to permit its evolutionary convergence with the numerous existing national schemes for IT security evaluation, certification and accreditation.

The CC structure also provides great flexibility in the specification of secure products. Consumers and other parties can specify the security functionality of a product in terms of standard *protection profiles*, and independently select the evaluation assurance level from a defined set of seven increasing levels of assurance, from EAL1 up to EAL7.

Version 1.0 of the CC was published for comment in January 1996. Version 2.0 takes account of extensive review and trials during the past two years and will be available in early 1998.

The CC presents requirements for the IT security of a product or system under the distinct categories of **functional requirements** (CC Part 2) and **assurance requirements** (CC Part 3). The CC functional requirements define desired security behaviour. Assurance requirements are the basis for gaining confidence that the claimed security measures are effective and implemented correctly.

# General Model

Version 2.0 of the Common Criteria has three parts. A description of the applicability of each part to the three sets of interested parties (Consumers, Developers and Evaluators) is shown below.

	Consumers	Developers	Evaluators
<b>Part 1: Introduction and General Model</b>	For background information and reference purposes	For background information and reference for the development of requirements and formulating security specifications for TOEs	For background information and reference purposes. Guidance structure for PPs and STs
<b>Part 2: Security Functional Requirements</b>	For guidance and reference when formulating statements of requirements for security functions	For reference when interpreting statements of functional requirements and formulating functional specifications of TOEs	Mandatory statement of evaluation criteria when determining whether TOE effectively meets claimed security functions
<b>Part 3: Security Assurance Requirements</b>	For guidance when determining required levels of assurance	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

## Approach

*Confidence in IT security can be gained through actions that may be taken during the process of development, evaluation and operation.*

### Development

The CC defines a set of IT requirements of known validity which can be used in establishing security requirements for prospective products and systems. The CC also defines the **Protection Profile (PP)** construct which allows prospective consumers or developers to create standardised sets of security requirements which will meet their needs.

The Target of Evaluation (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 **Security Target (ST)**, which is used by the evaluators as the basis for evaluation.

### Evaluation

The principal inputs to evaluation are the Security Target, the set of evidence about the TOE and the TOE itself. **The expected result of the evaluation process is a confirmation that the ST is satisfied for the TOE, with one or more reports documenting the evaluation findings.**

### Operation

Once a TOE is in operation vulnerabilities may surface, or environmental assumptions may require revision. **Reports may then be made to the developer requiring changes to the TOE.** Following such changes re-evaluation may be required.



## Security Framework

*The CC discusses security using a hierarchical framework of security concepts and terminology:*

### Security environment

Laws, organisational security policies etc, which define the context in which the TOE is to be used. Threats present in the environment are also included.

### Security objectives

A statement of intent to counter the identified threats by IT measures.

### TOE security requirements

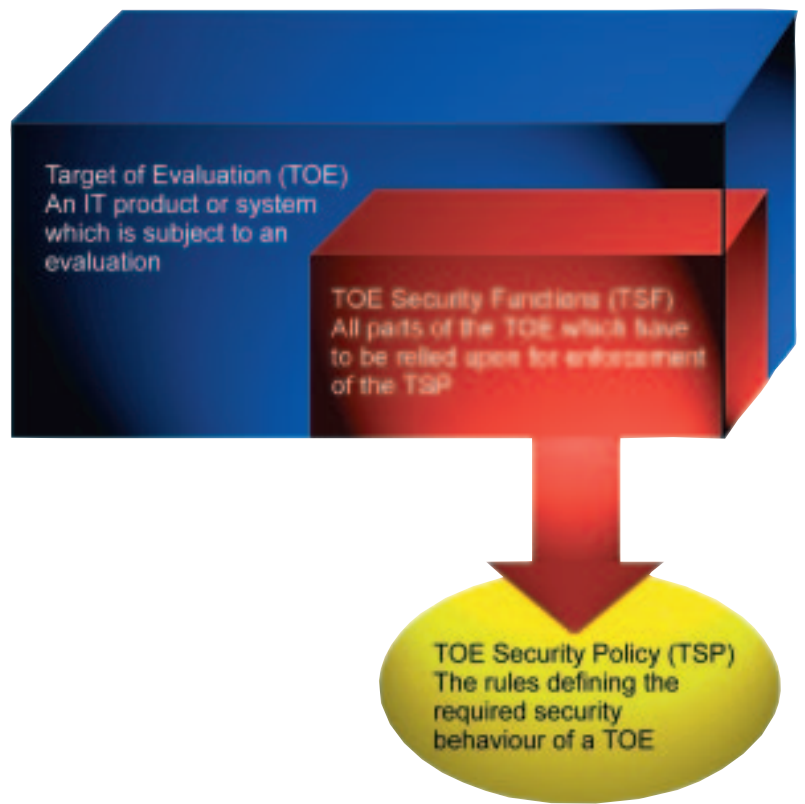
The refinement of the IT security objectives into a set of technical requirements for security functions and assurance.

### TOE security specifications

Define an actual or proposed implementation for the TOE.

### TOE implementation

The realisation of a TOE in accordance with its specification.



# Key concepts

## Protection Profile (PP)

A protection profile defines an implementation-independent set of security requirements and objectives for a category of products or systems which meet similar consumers needs for IT security. A PP is intended to be reusable and to define requirements which are known to be useful and effective in meeting the identified objectives.

The PP concept has been developed to support the definition of functional standards, and as an aid to formulating procurement specifications.

PPs are already under development for firewalls, relational databases, etc, and to enable backwards compatibility with TCSEC B1 and C2 ratings.

## Security Target (ST)

A security target contains the IT security objectives and requirements of a specific identified TOE and defines the functional and assurance measures offered by that TOE to meet stated requirements. The ST may claim conformance to one or more PPs, and forms the basis for an evaluation.

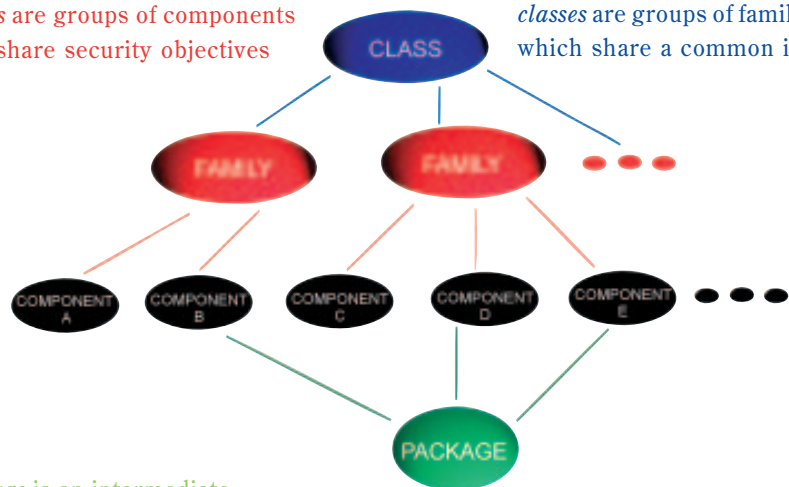


## Components

The CC defines a set of constructs which classify security requirement components into related sets:

families are groups of components which share security objectives

classes are groups of families which share a common intent



a package is an intermediate combination of components

The package permits the expression of a set of requirements which meets 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.

## Component Operations

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. Each component identifies and defines any permitted operations, the circumstances under which it may be applied and the results of the application. Permitted operations are: *assignment*, *selection* and *refinement*.

## Component Dependencies

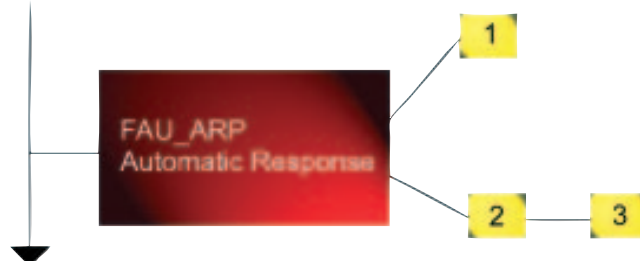
Dependencies may exist between components. Dependencies arise when a component is not self-sufficient and relies upon the presence of another component. Dependencies may exist between functional components, between assurance components and (rarely) between functional and assurance components.

## Component Naming Convention

Requirements for a TOE can be constructed from the hierarchy of specifications. The class name is three characters in length (eg FAU). Families within each class are named by the addition of an underscore and a further 3 characters (eg FAU\_ARP). Components within families are numbered, as are any elements within the components (eg FAU\_ARP2.1).

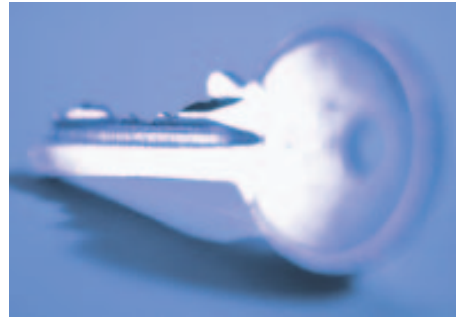
The diagram shows an example family taxonomy for the FAU\_ARP (Security Audit Automatic Response) family. It contains three components, with a hierarchy between components 2 and 3.

Security Audit



## *Aims of the Taxonomy*

*In defining the security requirements for a system the user/developer needs to consider the threats to the IT environment. The CC contains a pool of components, that the developers of PPs and STs can collate to form the security requirements definition of a trusted product or system. The organisation of these components into a hierarchy helps the user to locate the right components to combat threats. The user then presents the security requirements in the PPs and the ST of the TOE.*



# Security functionality

## *Component Catalogue*

*Part 2 of the CC contains the Component Catalogue. A high level overview of the nine functionality classes in CC Version 1.0 is provided here.*

*Version 2.0 of the CC will include a new class for cryptographic services, and significant restructuring and modification of the existing material.*

*There are some inter-class dependencies, such as the reliance the Data Protection class has upon the correct Identification and Authentication of users in order to be effective.*

### **Audit (FAU)**

Security auditing involves recognising, recording, storing and analysing information related to security activities. Audit records are produced by these activities, and can be examined to determine their security relevance. The class is made up of families, which define, amongst other things, requirements for the selection of auditable events, the analysis of audit records, their protection and their storage.

### **Communications (FCO)**

The communications class provides two families concerned with assuring the identity of a party participating in data exchange. The families are concerned with non-repudiation by the originator and by the recipient of data.

### **User Data Protection (FDP)**

This class contains families specifying requirements relating to the protection of user data. These families address user data within the TOE during import, export and storage, in addition to security attributes related to user data.

### **Identification and Authentication (FIA)**

The requirements for identification and authentication ensure the unambiguous identification of authorised users and the correct association of security attributes with users and subjects. Families in this class deal with determining and verifying user identity, determining their authority to interact with the TOE, and with the correct association of security attributes with the authorised user.



### Functional Components

Security functional components are used to express a wide range of security functional requirements within PPs and STs. Components are ordered sets of functional elements, and as discussed on page 7 these sets are grouped into families with common objectives (eg Security Audit Trail Protection) and classes with common intent (eg Audit). Components other than those defined may be used at the discretion of evaluation authorities. A hierarchy may exist between components.

### Component Extensibility

Part 2 of the CC includes procedures for the extension of the functionality classes and the addition of new classes. Note that the use of such extensions may require the prior approval of a certification body.



### Privacy (FPR)

Privacy requirements provide a user with protection against discovery and misuse of his identity by other users. The families in this class are concerned with anonymity, pseudonymity, unlinkability and unobservability.

### Protection of the Trusted Functions (FPT)

This class is focused on protection of TSF (TOE security functions) data, rather than of user data. The class relates to the integrity and management of the TSF mechanisms and data.

### Resource Utilisation (FRU)

Resource utilisation provides three families which support the availability of required resources, such as processing capability and storage capacity. The families detail requirements for fault tolerance, priority of service and resource allocation.

### TOE Access (FTA)

This class specifies functional requirements, in addition to those specified for identification and authentication, for controlling the establishment of a user's session. The requirements for TOE access govern such things as limiting the number and scope of user sessions, displaying the access history and the modification of access parameters.

### Trusted Path/Channels (FTP)

This class is concerned with trusted communications paths between the users and the TSF, and between TSFs. Trusted paths are constructed from trusted channels, which exist for inter-TSF communications; this provides a means for users to perform functions through a direct interaction with the TSF. The user or TSF can initiate the exchange, which is guaranteed to be protected from modification by untrusted applications. Only two families exist in this class, one specifying requirements for trusted channels, the other for trusted paths.

## Taxonomy

*The assurance requirements for the CC are defined in Part 3 of the CC. The taxonomy for assurance requirements is similar to that for functional requirements. Part 3 contains the nine assurance categories from which the assurance requirements for a TOE can be chosen. These requirements should be listed in the PPs and STs along with the functional requirements. The seven assurance classes and two evaluation assurance classes, defined by the CC, are summarised below.*

### Assurance Classes

#### Configuration Management (ACM)

Configuration management requires that the integrity of the TOE is adequately preserved. Specifically, configuration management provides confidence that the TOE and documentation used for evaluation are the ones prepared for distribution. The families in this class are concerned with the capabilities of the CM, its scope and automation.

#### Delivery and Operation (ADO)

This class provides families concerned with the measures, procedures and standards for secure delivery, installation and operational use of the TOE, to ensure that the security protection offered by the TOE is not compromised during these events.

### Evaluation of PPs and STs

*Assurance classes are provided for the evaluation of PPs (Class APE) and STs (Class ASE). All of the requirements in the relevant class need to be applied for a PP or ST evaluation. The criteria need to be applied in order to find out whether the PP or ST is a meaningful basis for a TOE evaluation.*

#### Development (ADV)

The families of this class are concerned with the refinement of the TSF from the specification defined in the ST to the implementation, and a mapping from the requirements to the lowest level representation.

#### Guidance Documents (AGD)

Guidance documents are concerned with the secure operational use of the TOE, by the users and administrators.

#### Life Cycle Support (ALC)

The requirements of the families concerned with the life-cycle of the TOE include life-cycle definition, tools and techniques, the developers security and the remediation of flaws found by TOE consumers.

#### Protection Profile Evaluation (APE)

The goal here is to demonstrate that the PP is complete, consistent and technically sound. Further, the PP needs to be a statement of the requirements for an evaluable TOE. The families in this class are concerned with the Security Environment, the Security Objectives and the TOE Security Requirements.

#### Tests (ATE)

This class is concerned with demonstrating that the TOE meets its functional requirements. The families address issues of coverage, depth, TOE requirements and independent testing.

#### Vulnerability Assessment (AVA)

This class defines requirements directed at the identification of exploitable vulnerabilities, which could be introduced by construction, operation, misuse or incorrect configuration of the TOE. The families identified here are concerned with identifying vulnerabilities through covert channel analysis, analysis of the configuration of the TOE, examining the strength of mechanisms of the security functions, and identifying flaws introduced during development of the TOE.

#### Security Target Evaluation (ASE)

The goal here is to demonstrate that the ST is complete, consistent and technically sound, and is a suitable basis for the TOE evaluation. The requirements for the families of this class are concerned with the Security Environment, the Security Objectives, any PP Claims, the TOE Security Requirements and the TOE Summary Specification.

## Evaluation Assurance Levels

*The CC contains a set of defined assurance levels constructed using components from the assurance families. These levels are intended partly to provide backward compatibility to source criteria and to provide internally consistent general purpose assurance packages. Other groupings of components are not excluded. To meet specific objectives an assurance level can be augmented by one or more additional components.*



# Security Assurance

Assurance levels define a scale for measuring the criteria for the evaluation of PPs and STs. Evaluation Assurance Levels (EALs) are constructed from the assurance components detailed opposite. Every assurance family (except Delivery and Flaw Remediation) contributes directly to the assurance that a TOE meets its security claims. EALs provide a uniformly increasing scale which balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. There are seven hierarchically ordered EALs. The increase in assurance across the levels is accomplished by substituting hierarchically higher assurance components from the same assurance family, and by the addition of assurance components from other assurance families.

### 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

Further details are provided overleaf, of the meaning and applicability of each EAL.

### Backwards Compatibility Objective

The CC EALs have been developed with the goal of preserving the assurance and results of previous evaluations performed using the source criteria. Comparisons are possible by design, but should be made with caution. This table can be used to assist in making such comparisons, though it is by no means intended to assert exact equivalence, since the levels do not derive assurance in exactly the same manner.

Common Criteria	US TCSEC	European ITSEC
EAL0	D: Minimal Protection	E0
EAL1		
EAL2	C1: Discretionary Security Protection	E1
EAL3	C2: Controlled Access Protection	E2
EAL4	B1: Labeled Security Protection	E3
EAL5	B2: Structured Protection	E4
EAL6	B3: Security Domains	E5
EAL7	A1: Verified Design	E6

*Each of the seven CC Evaluation Assurance Levels is summarised here. EAL1 is the entry level. As we step up to EAL4 increasing rigour and detail are introduced, but without introducing significantly specialised security engineering techniques. These lower four levels can generally be retrofitted to pre-existing products and systems.*

#### **EAL1 - functionally tested**

This is the lowest assurance level for which evaluation is meaningful and economically justified. It is intended to detect obvious errors for a minimum outlay, but is unlikely to result in the detection of subtle security weaknesses. It is applicable where the requirement is for a low level of independently assured security. An EAL1 rating could support the contention that due care has been exercised with respect to systems handling personal or similar information.

*An EAL1 evaluation provides analysis of the security functions, using a functional and interface specification of the TOE, to understand the TOE's security behaviour. The analysis is supported by independent testing of the security functions.*

# Evaluation Assurance Levels

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

#### **EAL5 - semiformal designed and tested**

EAL5 permits a developer to gain maximum assurance from security engineering based on rigorous commercial development practices, supported by moderate application of specialised security engineering techniques. Such a TOE will be designed and developed with the intent of meeting EAL5 requirements. EAL5 is applicable where the requirement is for a high level of independently assured security in a planned development, with a rigorous development approach but without incurring unreasonable costs for specialised security engineering techniques.

*An EAL5 evaluation provides an analysis of all 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 relative resistance to penetration attack. Modular design is required, and covert channel analysis may also be required.*

### **EAL2 - structurally tested**

This is the highest assurance level that can be used without imposing other than minimal additional tasks on the developer. If the developer applies reasonable standards of care, EAL2 may be feasible with no developer involvement other than support for security functional testing. It is applicable where the requirement is for a low to moderate level of independently assured security, but the complete TOE development record is not readily available. This may arise when securing legacy systems, or where access to the developer is limited.

*An EAL2 evaluation provides analysis of the TOE security functions, using its functional and interface specification as well as the high-level design of the subsystems of the TOE. Independent testing of the security functions is performed, and the evaluators review the developer's evidence of "black box" testing, and a search for obvious vulnerabilities.*

### **EAL3 - methodically tested and checked**

This assurance level 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 where the requirement is for a moderate level of independently assured security, with 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 independent 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 - methodically designed, tested and reviewed**

This is the highest assurance level which it is likely to be economically feasible to retrofit to an existing product line. EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices, which are rigorous but not overly specialised. It is applicable where the requirement is for a moderate to high level of independently assured security in conventional commodity products, and there is willingness to incur some 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 obvious vulnerabilities. Development controls are supported by a life-cycle model, identification of tools, and automated configuration management.*



### **EAL6 - semiformally verified design and tested**

EAL6 permits a developer to gain high assurance from application of specialised security engineering techniques in a rigorous development environment, to produce a premium product for protecting high value assets against significant risks. EAL6 is applicable to the development of specialised security products, for application in high risk situations which justify the additional costs.

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

### **EAL7 - formally verified design and tested**

EAL7 represents an achievable upper bound on evaluation assurance for practically useful products. It should only be considered for experimental application to all but conceptually simple and well understood products. EAL7 is applicable to the development of specialised security products, for application in extraordinarily high risk situations which justify the extraordinary additional costs. Practical application of this level is currently limited to products with tightly focused security functionality which is amenable to 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.*



## Approach to Evaluation

*The evaluation process may be carried out in parallel with or after the development of the TOE. The principal input to evaluation is an ST describing the security functions of the TOE, which may reference any PPs to which conformance is claimed. The approach to describing the security functionality of the TOE, in PPs and STs, is defined here.*

## Protection Profile

The PP describes implementation-independent sets of security requirements for categories of TOEs, and contains a statement of the security problem that a compliant product is intended to solve. It specifies CC functional and assurance requirements components (including an EAL), and provides a rationale for the selected functional and assurance components. The PP is structured into the following sections:

### Introduction

This contains information necessary to operate a PP registry. It holds the identification and stand-alone abstract of the PP.

### Security Objectives

These reflect the stated intent to counter identified threats and/or comply with any organisational security policies. Both IT and non-IT security objectives are included, and traced back to threats or policies.

### TOE Description

This provides context for the evaluation. As the description relates to a category of TOEs, the description may be a set of assumptions, and may describe the application context into which the TOE will fit.

### Functional and Assurance Requirements



These describe the TOE's IT security requirements. The assurance requirements consist of an assurance package, which is normally an EAL augmented by additional assurance components from Part 3 where necessary. An optional statement can be included to identify the security requirements for the IT environment. [Where the TOE is a complete TSF with no assertions on the IT environment this last section can be omitted.]

### Security Environment

This is a narrative statement of the security problem to be solved by the TOE. It describes the security aspects of the environment in which the TOE is intended to be used. It will address:

**threats:** the anticipated threats to the IT assets, even those not encountered by the TOE. The threat is described in terms of the agent, the attack and the subject of the attack

**organisational security policies:** identify any rules with which the TOE must comply

**usage assumptions:** describe the security aspects of the environment in which the TOE is intended to be used, including physical, personnel and connectivity aspects of the environment.

### Rationale

In two parts, the *objectives rationale* demonstrates that the security objectives address all of the environmental aspects identified, and that the objectives are effective and provide complete coverage. The *requirements rationale* demonstrates that the security requirements are suitable to meet the IT security objectives.

## ***Security Target***

The ST is the basis for the agreement between the TOE developers, consumers, evaluators and evaluation authorities as to what security the TOE offers, and on the scope of the evaluation. The audience for an ST may also include those managing, marketing, purchasing, installing, configuring, operating and using the TOE. The ST is structured into the following sections:

### **Introduction**

This contains the ST identification (and the TOE to which it refers), the ST overview and the CC conformance claim. The overview is aimed at the potential user of the TOE, and suitable for inclusion in the evaluated products lists. The conformance claim states any evaluable claim of the TOE, and includes at least one registered PP or EAL. An optional strength of function rating can be included.

### **Security Objectives**

These address the IT and non-IT security objectives of the TOE and its supporting environment. These objectives counter the identified threats and comply with any organisational security policies.

### **TOE Description**

This provides context for the evaluation. It is an aid to understanding the security requirements of the TOE and should address the TOE type, its intended usage and its general IT features.

### **Security Requirements**

This identifies the TOE IT security requirements, and includes the functional and assurance requirements. An optional statement of the security requirements of the IT environment can be included.

### **TOE Summary Specification**

This provides a high-level definition of the security functions claimed to meet the functional requirements, and the assurance measures taken to meet the assurance requirements.

### **Security Environment**

As with the PP, this addresses the threats to the environment, the organisational security policies with which the TOE must comply and the security aspects for the environment in which the TOE will be used (the usage assumptions).

### **PP Claims**

Where the ST claims that the TOE conforms with the requirements of one or more PPs, an explanation justification and supporting material is presented here. This includes reference to the PP, a PP refinements statement, and a PP additions statement.

### **Rationale**

This demonstrates that the ST contains an effective and suitable set of countermeasures, which is complete and cohesive.



# Evaluation

An evaluation is an assessment of an IT product or system against defined criteria. A CC evaluation is one using the CC as the basis for evaluating the IT security properties. Evaluations against a common standard facilitate comparability of evaluation outcomes. In order to enhance comparability between evaluation results yet further, evaluations should be performed within the framework of an authoritative evaluation scheme, which sets standards and monitors the quality of evaluations. Such schemes currently exist in several nations, using differing though related evaluation criteria.

Distinct stages of evaluation are identified, corresponding to the principal layers of TOE representation:

- **PP evaluation** - carried out against the evaluation criteria for PPs (CC Part 3)
- **ST evaluation** - carried out against the evaluation criteria for STs (CC Part 3)
- **TOE evaluation** - carried out against the evaluation criteria in Part 3 using an evaluated ST as the basis.

Testing, design review and implementation review contribute significantly to reducing the risk that undesired behaviour is present in the TOE. The CC presents a framework in which expert analysis (evaluation) in these areas can take place.



*Early versions of the CC contained examples of PPs which had been identified in source criteria, and proposed procedures to establish and control a CC registry of approved PPs. The CC now contains no PP registry - instead a system of linked national registries will be implemented. PPs may be defined by developers when formulating security specifications for TOEs, or by user communities.*

# CC Protection Profiles



## Example PPs

Examples of PPs found in CC (Version 1.0) Part 4 are:

- **Commercial Security 1 (CS1)**  
consisting of security requirements and evaluation interpretations for products providing basic controlled access protection.
- **Commercial Security 3 (CS3)**  
specifying requirements for multi-user operating systems, database management environments, and calls for access controls based on individual user roles with respect to data objects and permitted operations.
- **Packet Filter Firewall (PFFW)**  
specifying security functions and assurances applicable to most packet filter firewalls.

## CC Extensibility

The CC is defined to be extensible and it is possible to define functional and assurance requirements not contained in the CC. Extended functional and assurance requirements must be compliant with extensibility criteria in the CC. However, it is recommended that the components defined in the CC are carefully considered before defining such extensions, as use of extended requirements may require the prior approval of a certification body.



For further  
information...

## Contact the Sponsoring Organisations:



Communications Security Establishment  
Criteria Coordinator  
R2B IT Security Standards and Initiatives  
PO Box 9703, Terminal  
Ottawa, Canada, K1G 3Z4



+1 (613) 991-7409



[criteria@cse-cst.gc.ca](mailto:criteria@cse-cst.gc.ca)



<http://www.cse.dnd.ca>



Service Central de la Sécurité des Systèmes d'Information  
Bureau Normalisation, Critères Communs  
18 rue du docteur Zamenhof  
92131 Issy les Moulineaux  
France



+33 (1) 41 46 37 84



[ssi20@calva.net](mailto:ssi20@calva.net)



Bundesamt für Sicherheit in der Informationstechnik  
Abteilung V  
Postfach 20 03 63  
D-53133 Bonn  
Germany



+49 228 9582 300



[cc@bsi.de](mailto:cc@bsi.de)



Netherlands National Communications Security Agency  
Postbus 20061  
NL 2500 EB Den Haag  
Netherlands



+31 70 348 5637



[criteria@nlncsa.minbuza.nl](mailto:criteria@nlncsa.minbuza.nl)



Communications-Electronics Security Group  
Compusec Evaluation Methodology  
PO Box 144  
Cheltenham, GL52 5UE  
United Kingdom



+44 1242 221 491 ext 4134



[criteria@cesg.gov.uk](mailto:criteria@cesg.gov.uk)



<http://www.cesg.gov.uk/cchtml>



National Institute of Standards and Technology  
Computer Security Division  
NIST North Building, Room 426  
Gaithersburg, Maryland 20899  
USA



+1 (301) 975-2934



[criteria@nist.gov](mailto:criteria@nist.gov)



<http://csrc.nist.gov/cc>

National Security Agency  
Attn: V2, Common Criteria Technical Advisor  
Fort George G Meade  
Maryland 21122  
USA



+1 (410) 859-4458



[common\\_criteria@radium.ncsc.mil](mailto:common_criteria@radium.ncsc.mil)



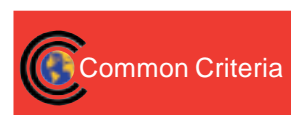
<http://www.radium.ncsc.mil/tpep>

## Interim PP registries may be found on the following Internet Web pages:

[http://www.radium.ncsc.mil/tpep/library/protection\\_profiles/index.html](http://www.radium.ncsc.mil/tpep/library/protection_profiles/index.html)

[http://www.cesg.gov.uk/cchtml/ippr/list\\_by\\_type.html](http://www.cesg.gov.uk/cchtml/ippr/list_by_type.html)

<http://csrc.nist.gov/cc/pp/pplist.htm>





*This brochure was produced by  
Syntegra on behalf of the  
Common Criteria  
Implementation Board*

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