

Australian Standard™

**Information technology—Security
techniques—Evaluation criteria for IT
security**

Part 1: Introduction and general model



This Australian Standard was prepared by Committee IT-012, Information systems—Security and identification technology. It was approved on behalf of the Council of Standards Australia on 29 January 2004 and published on 17 March 2004.

The following are represented on Committee IT-012:

Attorney General's Department
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber of Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Australian Information Industry Association
Certification Forum of Australia
Department of Defence (Australia)
Department of Social Welfare New Zealand
Government Communications Security Bureau, New Zealand
Internet Industry Association
NSW Police Service
New Zealand Defence Force
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Web Shop at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Global Standard*, has a full listing of revisions and amendments published each month.

Australian Standards™ and other products and services developed by Standards Australia are published and distributed under contract by SAI Global, which operates the Standards Web Shop.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 03549.

Australian Standard™

Information technology—Security techniques—Evaluation criteria for IT security

Part 1: Introduction and general model

First published as AS ISO/IEC 15408.1—2004.

COPYRIGHT

© Standards Australia International

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 5766 9

 **Documents**
Document Sharing Hub

PREFACE

This Standard was prepared by the Australian members of the Joint Standards Australia/Standards New Zealand Committee IT-012, Information systems—Security and identification technology. After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian, rather than an Australian/New Zealand Standard.

This Standard is identical with, and has been reproduced from ISO/IEC 15408-1:1999, *Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model*.

The objective of this Standard is to define criteria, which for historical and continuity purposes are referred to herein as the Common Criteria (CC), to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience. The CC will permit comparability between the results of independent security evaluations.

This Standard is Part 1 of AS ISO/IEC 15408, *Information technology—Security techniques—Evaluation criteria for IT security*, which is published in parts as follows:

Part 1: Introduction and general model (this Standard)

Part 2: Security functional requirements

Part 3: Security assurance requirements

The terms ‘normative’ and ‘informative’ are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

As this Standard is reproduced from an international standard, the following applies:

- (a) Its number appears on the cover and title page while the international standard number appears only on the cover.
- (b) In the source text ‘ISO/IEC 15408’ should read ‘AS ISO/IEC 15408’.
- (c) A full point substitutes for a comma when referring to a decimal marker.

CONTENTS

Page

1	Scope	1
2	Definitions	3
2.1	Common abbreviations	3
2.2	Scope of glossary	3
2.3	Glossary	4
3	Overview	9
3.1	Introduction	9
3.2	Target audience of the CC	9
3.2.1	Consumers	9
3.2.2	Developers	10
3.2.3	Evaluators	10
3.2.4	Others	10
3.3	Evaluation context	11
3.4	Organisation of Common Criteria	12
4	General model	13
4.1	Security context	13
4.1.1	General security context	13
4.1.2	Information technology security context	15
4.2	Common Criteria approach	15
4.2.1	Development	16
4.2.2	TOE evaluation	18
4.2.3	Operation	18
4.3	Security concepts	18
4.3.1	Security environment	20
4.3.2	Security objectives	21
4.3.3	IT security requirements	22
4.3.4	TOE summary specification	23
4.3.5	TOE implementation	23
4.4	CC descriptive material	23
4.4.1	Expression of security requirements	23
4.4.2	Use of security requirements	25
4.4.3	Sources of security requirements	27
4.5	Types of evaluation	28
4.5.1	PP evaluation	28
4.5.2	ST evaluation	28

4.5.3	TOE evaluation	28
4.6	Assurance maintenance	28
5	Common Criteria requirements and evaluation results	29
5.1	Introduction	29
5.2	Requirements in PPs and STs	30
5.2.1	PP evaluation results	30
5.3	Requirements in TOE	30
5.3.1	TOE evaluation results	31
5.4	Caveats on evaluation results	31
5.5	Use of TOE evaluation results	32
Annex A	The Common Criteria project (informative)	33
A.1	Background to the Common Criteria project	33
A.2	Development of the Common Criteria	33
A.3	Common Criteria project sponsoring organisations	34
Annex B	Specification of Protection Profiles	37
B.1	Overview	37
B.2	Content of Protection Profile	37
B.2.1	Content and presentation	37
B.2.2	PP introduction	37
B.2.3	TOE description	38
B.2.4	TOE security environment	38
B.2.5	Security objectives	39
B.2.6	IT security requirements	40
B.2.7	Application notes	41
B.2.8	Rationale	41
Annex C	Specification of Security Targets	43
C.1	Overview	43
C.2	Content of Security Target	43
C.2.1	Content and presentation	43
C.2.2	ST introduction	43
C.2.3	TOE description	45
C.2.4	TOE security environment	45
C.2.5	Security objectives	46
C.2.6	IT security requirements	46
C.2.7	TOE summary specification	47
C.2.8	PP claims	48
C.2.9	Rationale	49
Annex D	Bibliography (informative)	53

List of Figures

Figure 3.1 - Evaluation context	11
Figure 4.1 - Security concepts and relationships	13
Figure 4.2 - Evaluation concepts and relationships	14
Figure 4.3 - TOE development model	16
Figure 4.4 - TOE evaluation process	17
Figure 4.5 - Derivation of requirements and specifications	20
Figure 4.6 - Organisation and construction of requirements	24
Figure 4.7 - Use of security requirements	26
Figure 5.1 - Evaluation results	29
Figure 5.2 - Use of TOE evaluation results	32
Figure B.1 - Protection Profile content	38
Figure C.1 - Security Target content	44

List of Tables

Table 3.1 - Roadmap to the Common Criteria	12
--	----

AUSTRALIAN STANDARD

Information technology — Security techniques — Evaluation criteria for IT security —**Part 1:****Introduction and general model****1 Scope**

This multipart standard ISO/IEC 15408 defines criteria, which for historical and continuity purposes are referred to herein as the Common Criteria (CC), to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience.

The CC will permit comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.

The CC is useful as a guide for the development of products or systems with IT security functions and for the procurement of commercial products and systems with such functions. During evaluation, such an IT product or system is known as a Target of Evaluation (TOE). Such TOEs include, for example, operating systems, computer networks, distributed systems, and applications.

The CC addresses protection of information from unauthorised disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The CC may also be applicable to aspects of IT security outside of these three. The CC concentrates on threats to that information arising from human activities, whether malicious or otherwise, but may be applicable to some non-human threats as well. In addition, the CC may be applied in other areas of IT, but makes no claim of competence outside the strict domain of IT security.

The CC is applicable to IT security measures implemented in hardware, firmware or software. Where particular aspects of evaluation are intended only to apply to certain methods of implementation, this will be indicated within the relevant criteria statements.

Certain topics, because they involve specialised techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the CC. Some of these are identified below.

- a) The CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security measures. However, it is recognised that a significant part of the security of a TOE can often be achieved through administrative measures such as organisational, personnel, physical, and procedural controls. Administrative security measures in the operating environment of

the TOE are treated as secure usage assumptions where these have an impact on the ability of the IT security measures to counter the identified threats.

- b) The evaluation of technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area. In particular, the CC addresses some aspects of physical protection of the TOE.
- c) The CC addresses neither the evaluation methodology nor the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that the CC will be used for evaluation purposes in the context of such a framework and such a methodology.
- d) The procedures for use of evaluation results in product or system accreditation are outside the scope of the CC. Product or system accreditation is the administrative process whereby authority is granted for the operation of an IT product or system in its full operational environment. Evaluation focuses on the IT security parts of the product or system and those parts of the operational environment that may directly affect the secure use of IT elements. The results of the evaluation process are consequently a valuable input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related product or system security properties and their relationship to the IT security parts, accreditors should make separate provision for those aspects.
- e) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. Should independent assessment of mathematical properties of cryptography embedded in a TOE be required, the evaluation scheme under which the CC is applied must make provision for such assessments.

2 Definitions

2.1 Common abbreviations

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

CC	Common Criteria, the name used historically for this multipart standard ISO/IEC 15408 in lieu of its official ISO name of “Evaluation criteria for information technology security”
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

2.2 Scope of glossary

This subclause 2.2 contains only those terms which are used in a specialised way throughout 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. Explanations of the use of terms and concepts used in a specialised way in ISO/IEC 15408-2 and ISO/IEC 15408-3 can be found in their respective “paradigm” subclauses.

2.3 Glossary

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.

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.

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.

Element — An indivisible security requirement.

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

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.

Extension — The addition to an ST or PP of functional requirements not contained in Part 2 and/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 TOE.

Internal TOE transfer — Communicating data between separated parts of the TOE.

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

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.

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.

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.

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-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.

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.

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 resource — Anything useable 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.

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.

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

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

3 Overview

This clause introduces the main concepts of the CC. It identifies the target audience, evaluation context, and the approach taken to present the material.

3.1 Introduction

Information held by IT products or systems is a critical resource that enables organisations to succeed in their mission. Additionally, individuals have a reasonable expectation that their personal information contained in IT products or systems remain private, be available to them as needed, and not be subject to unauthorised modification. IT products or systems should perform their functions while exercising proper control of the information to ensure it is protected against hazards such as unwanted or unwarranted dissemination, alteration, or loss. The term IT security is used to cover prevention and mitigation of these and similar hazards.

Many consumers of IT lack the knowledge, expertise or resources necessary to judge whether their confidence in the security of their IT products or systems is appropriate, and they may not wish to rely solely on the assertions of the developers. Consumers may therefore choose to increase their confidence in the security measures of an IT product or system by ordering an analysis of its security (i.e. a security evaluation).

The CC can be used to select the appropriate IT security measures and it contains criteria for evaluation of security requirements.

3.2 Target audience of the CC

There are three groups with a general interest in evaluation of the security properties of IT products and systems: TOE consumers, TOE developers, and TOE evaluators. The criteria presented in this document have been structured to support the needs of all three groups. They are all considered to be the principal users of this CC. The three groups can benefit from the criteria as explained in the following paragraphs.

3.2.1 Consumers

The CC plays an important role in supporting techniques for consumer selection of IT security requirements to express their organisational needs. The CC is written to ensure that evaluation fulfils the needs of the consumers as this is the fundamental purpose and justification for the evaluation process.

Consumers can use the results of evaluations to help decide whether an evaluated product or system fulfils their security needs. These security needs are typically identified as a result of both risk analysis and policy direction. Consumers can also use the evaluation results to compare different products or systems. Presentation of the assurance requirements within a hierarchy supports this need.

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

3.2.2 Developers

The CC is intended to support developers in preparing for and assisting in the evaluation of their products or systems and in identifying security requirements to be satisfied by each of their products or systems. It is also quite possible that an associated evaluation methodology, potentially accompanied by a mutual recognition agreement for evaluation results, would further permit the CC to support someone, other than the TOE developer, in preparing for and assisting in the evaluation of a developer's TOE.

The CC constructs can then be used to make claims that the TOE conforms to its identified requirements by means of specified security functions and assurances to be evaluated. Each TOE's requirements are contained in an implementation-dependent construct termed the Security Target (ST). One or more PPs may provide the requirements of a broad consumer base.

The CC describes security functions that a developer could include in the TOE. The CC can be used to determine the responsibilities and actions to support evidence that is necessary to support the evaluation of the TOE. It also defines the content and presentation of that evidence.

3.2.3 Evaluators

The CC contains criteria to be used by evaluators when forming judgements about the conformance of TOEs to their security requirements. The CC describes the set of general actions the evaluator is to carry out and the security functions on which to perform these actions. Note that the CC does not specify procedures to be followed in carrying out those actions.

3.2.4 Others

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

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

- f) evaluation authorities responsible for the management and oversight of IT security evaluation programmes.

3.3 Evaluation context

In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme that sets the standards, monitors the quality of the evaluations and administers the regulations to which the evaluation facilities and evaluators must conform.

The CC does not state requirements for the regulatory framework. However, consistency between the regulatory frameworks of different evaluation authorities will be necessary to achieve the goal of mutual recognition of the results of such evaluations. Figure 3.1 depicts the major elements that form the context for evaluations.

Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve. In order to enhance the consistency of the evaluation findings, the final evaluation results could be submitted to a certification process. The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval. The certificate is normally publicly available. It is noted that the certification process is a means of gaining greater consistency in the application of IT security criteria.

The evaluation scheme, methodology, and certification processes are the responsibility of the evaluation authorities that run evaluation schemes and are outside the scope of the CC.

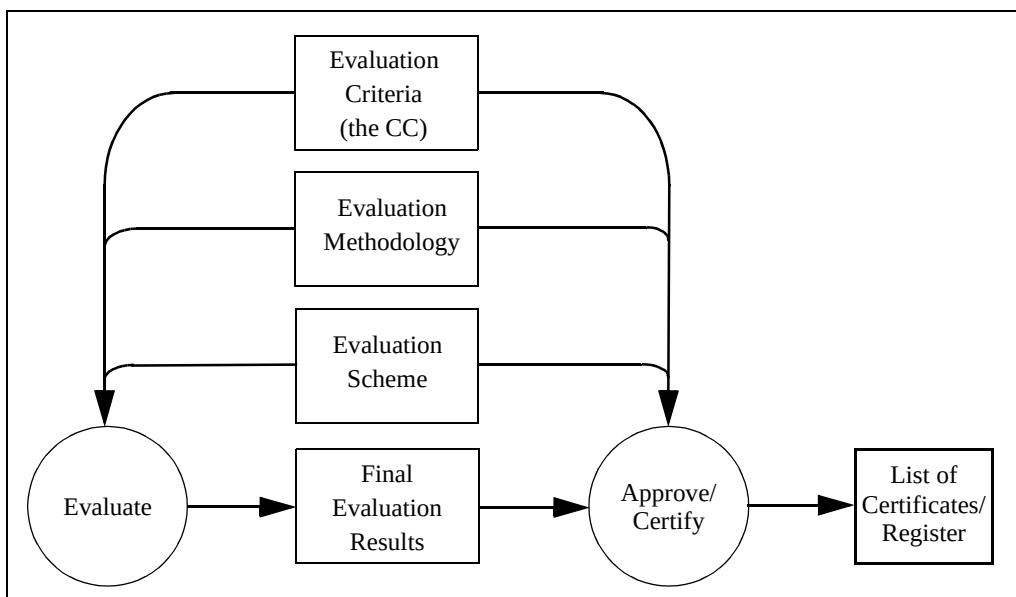


Figure 3.1 - Evaluation context

3.4 Organisation of 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 clause 4.

- a) **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.
- b) **Part 2, Security functional requirements**, establishes a set of functional components as a standard way of expressing the functional requirements for TOEs. Part 2 catalogues the set of functional components, families, and classes.
- c) **Part 3, Security assurance requirements**, 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, for the three key target audience groupings, how the parts of the CC will be of interest.

Table 3.1 - Roadmap to the Common Criteria

	Consumers	Developers	Evaluators
Part 1	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	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 mandatory statement of evaluation criteria when determining whether a TOE effectively meets claimed security functions.
Part 3	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 mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.