INTERNATIONAL STANDARD

ISO/IEC 15408-1

First edition
1999-12-01

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

Part 1:
Introduction and general model

Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI —

Partie 1: Introduction et modèle général

Reference number
ISO/IEC 15408-1:1999(E)

Contents

List of Figures

List of Tables

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, **Part 3.**

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 15408-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in collaboration with Common Criteria Project Sponsoring Organisations. The identical text of ISO/IEC 15408-1 is published by the Common Criteria Project Sponsoring Organisations as *Common Criteria for Information Technology Security Evaluation.* Additional information on the Common Criteria Project and contact information on its Sponsoring Organisations is provided in Annex A of ISO/IEC 15408-1.

ISO/IEC 15408 consists of the following parts, under the general title *Information technology — Security techniques — Evaluation criteria for IT security*:

- *Part 1: Introduction and general model*
- *Part 2: Security functional requirements*
- *Part 3: Security assurance requirements*

Annexes B and C form a normative part of this part of ISO/IEC 15408. Annexes A and D are for information only.

This LEGAL NOTICE has been placed in all Parts of ISO/IEC 15408 by request:
The seven governmental organisations (collectively called "the Common Criteria Project Sponsoring Organisations") identified in ISO/IEC 15408-1 Annex A, as the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluation, Parts 1 through 3 (called the "CC"), hereby grant non-exclusive license to ISO/IEC to use the CC in the development of the ISO/IEC 15408 international standard. However, the Common Criteria Project Sponsoring Organisations retain the right to use, copy, distribute, or modify the CC as they see fit.

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.

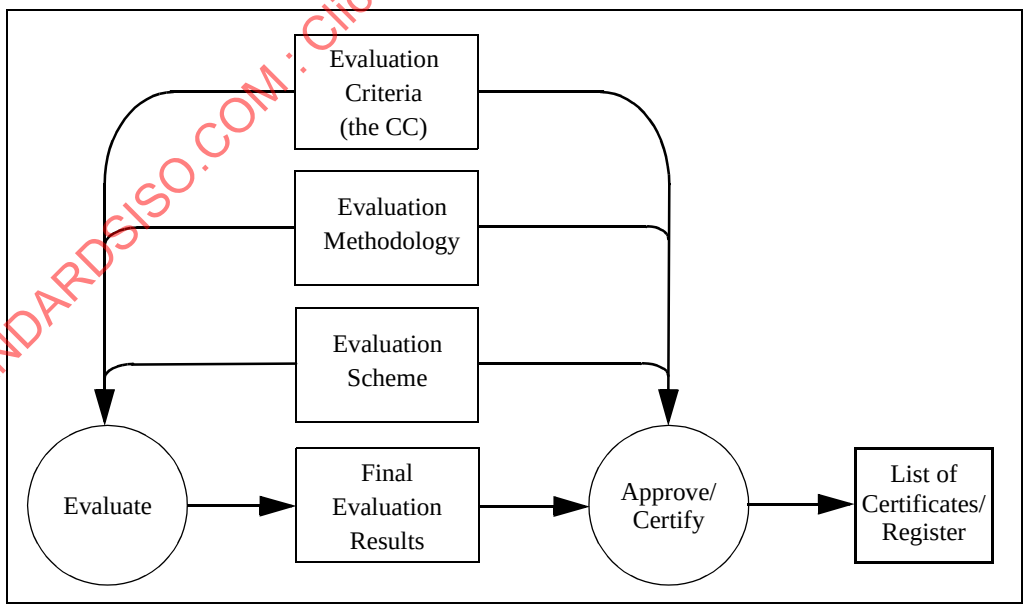

Figure 3.1 - Evaluation context

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.

4 General model

This clause presents the general concepts used throughout the CC, including the context in which the concepts are to be used and the CC approach for applying the concepts. Part 2 and Part 3 expand on the use of these concepts and assume that the approach described is used. This clause assumes some knowledge of IT security and does not propose to act as a tutorial in this area.

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

4.1 Security context

4.1.1 General security context

Security is concerned with the protection of assets from threats, where threats are categorised as the potential for abuse of protected assets. All categories of threats should be considered; but in the domain of security greater attention is given to those threats that are related to malicious or other human activities. Figure 4.1 illustrates high level concepts and relationships.

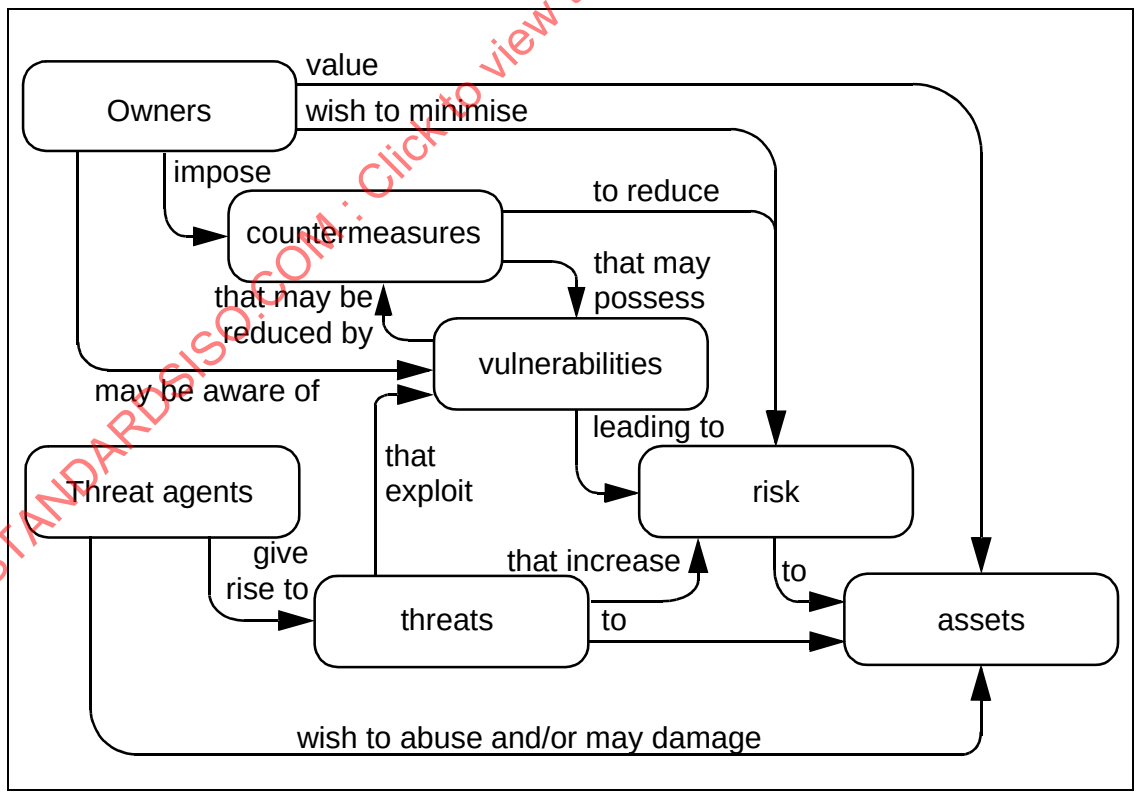

Figure 4.1 - Security concepts and relationships

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

The owners of the assets will analyse the possible threats to determine which ones apply to their environment. The results are known as risks. This analysis can aid in the selection of countermeasures to counter the risks and reduce it to an acceptable level.

Countermeasures are imposed to reduce vulnerabilities and to meet security policies of the owners of the assets (either directly or indirectly by providing direction to other parties). Residual vulnerabilities may remain after the imposition of countermeasures. Such vulnerabilities may be exploited by threat agents representing a residual level of risk to the assets. Owners will seek to minimise that risk given other constraints.

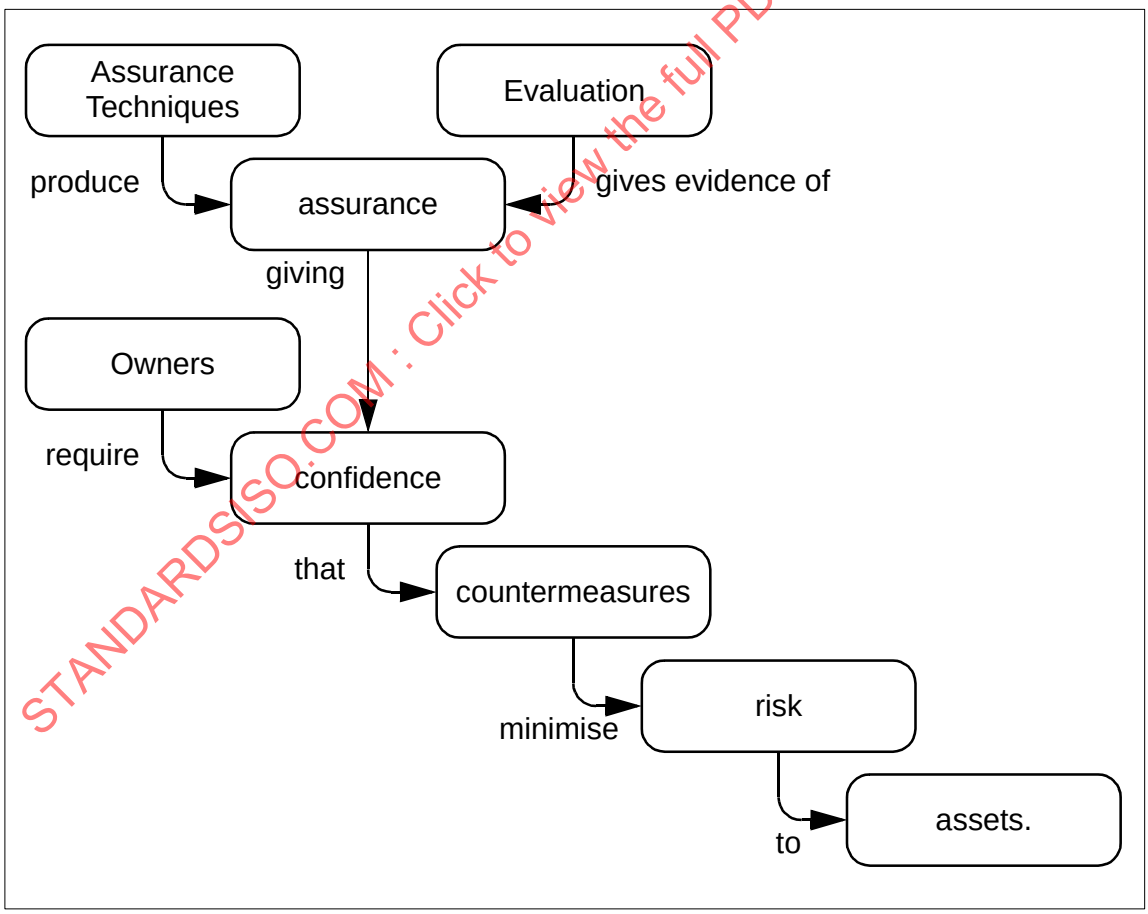

Figure 4.2 - Evaluation concepts and relationships

Owners will need to be confident that the countermeasures are adequate to counter the threats to assets before they will allow exposure of their assets to the specified threats. Owners may not themselves possess the capability to judge all aspects of the countermeasures, and may therefore seek evaluation of the countermeasures. The outcome of evaluation is a statement about the extent to which assurance is gained that the countermeasures can be trusted to reduce the risks to the protected assets. The statement assigns an assurance rating of the countermeasures, assurance being that property of the countermeasures that gives grounds for confidence in their proper operation. This statement can be used by the owner of the assets in deciding whether to accept the risk of exposing the assets to the threats. Figure 4.2 illustrates these relationships.

Owners of assets will normally be held responsible for those assets and should be able to defend the decision to accept the risks of exposing the assets to the threats. This requires that the statements resulting from evaluation are defensible. Thus, evaluation should lead to objective and repeatable results that can be cited as evidence.

4.1.2 Information technology security context

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

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

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

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

4.2 Common Criteria approach

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

4.2.1 Development

The CC does not mandate any specific development methodology or life cycle model. Figure 4.3 depicts underlying assumptions about the relationship between the security requirements and the TOE. The figure is used to provide a context for discussion and should not be construed as advocating a preference for one methodology (e.g. waterfall) over another (e.g. prototyping).

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

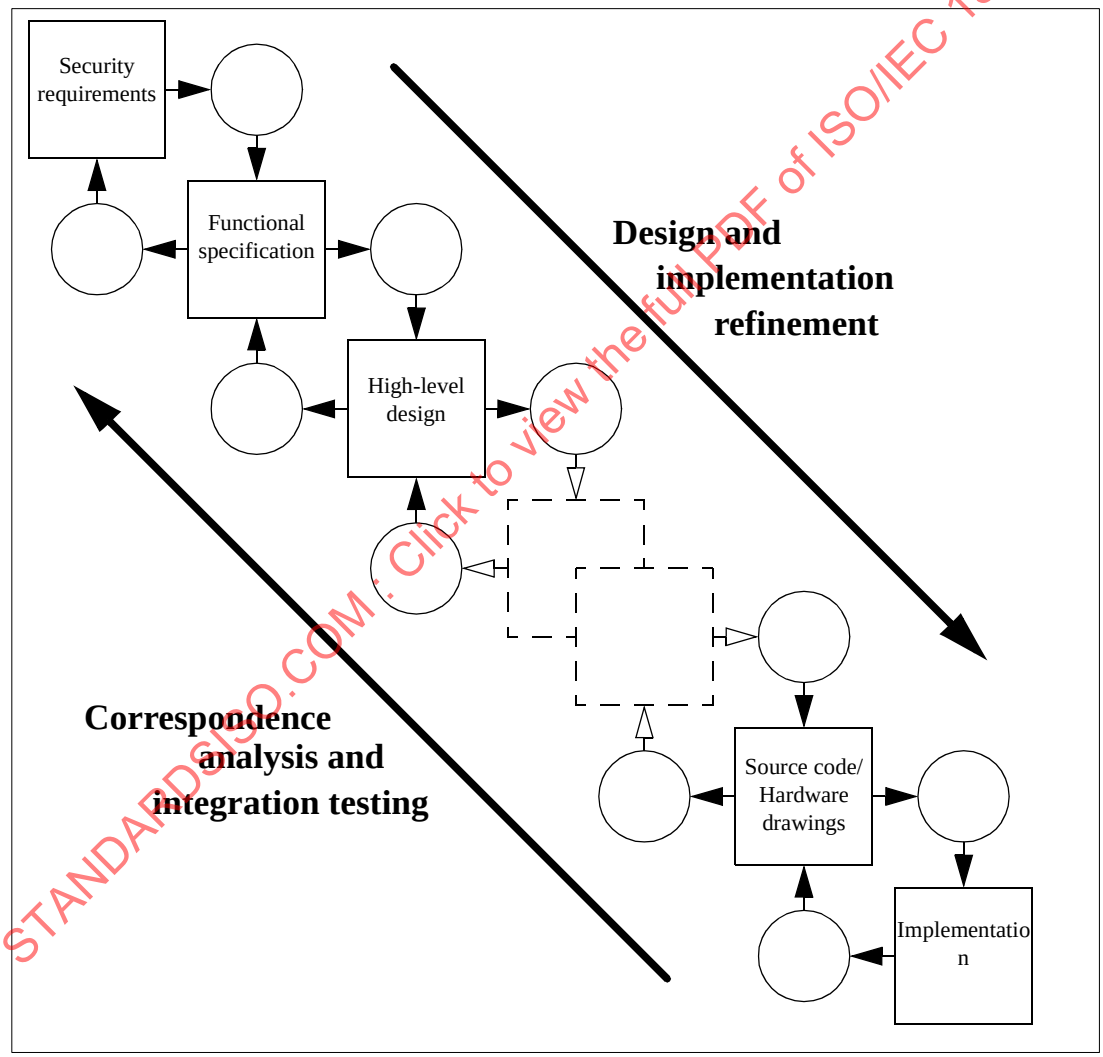

Figure 4.3 - TOE development model

The process is based on the refinement of the security requirements into a TOE summary specification expressed in the security target. Each lower level of refinement represents a design

decomposition with additional design detail. The least abstract representation is the TOE implementation itself.

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

a) that each refinement level is a complete instantiation of the higher levels (i.e. all TOE security functions, properties, and behaviour defined at the higher level of abstraction must be demonstrably present in the lower level);

b) that each refinement level is an accurate instantiation of the higher levels (i.e. there should be no TOE security functions, properties, and behaviour defined at the lower level of abstraction that are not required by the higher level).

The CC assurance criteria identify the design abstraction levels of functional specification, high-level design, low-level design, and implementation. Depending upon the assurance level specified, developers may be required to show how the development methodology meets the CC assurance requirements.

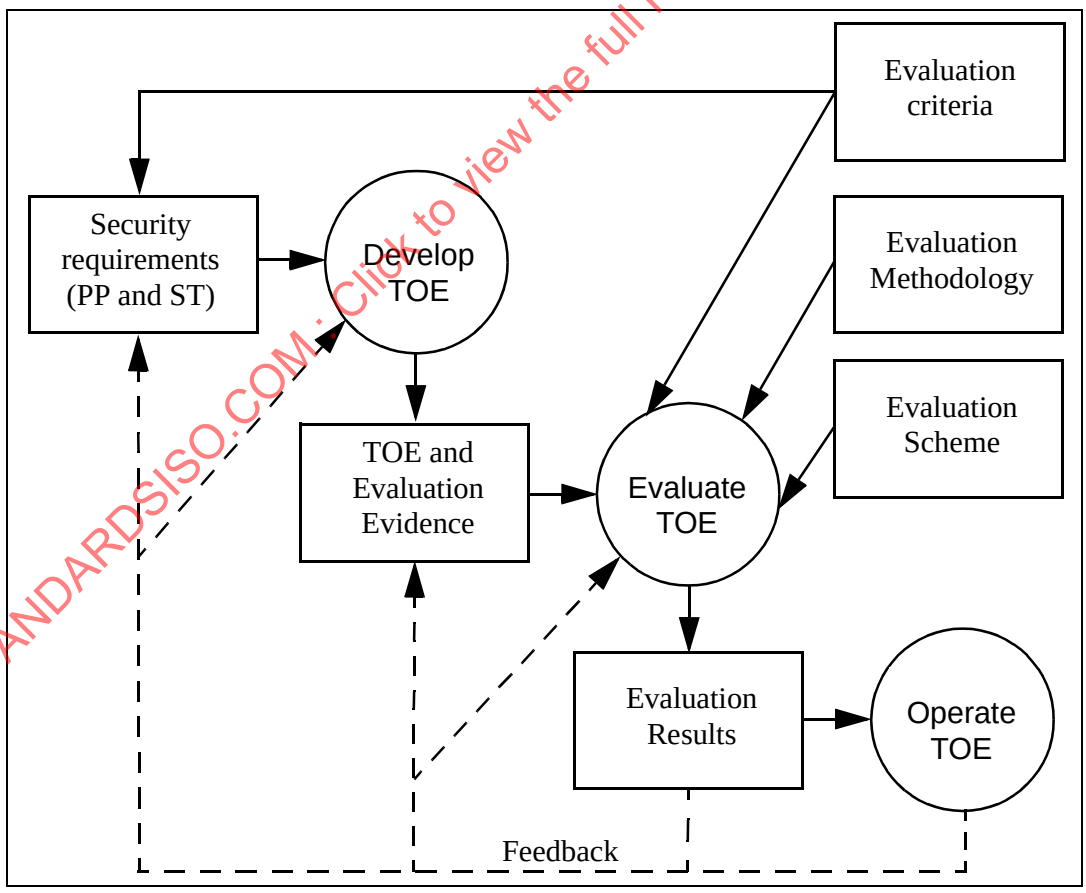

Figure 4.4 - TOE evaluation process

4.2.2 TOE evaluation

The TOE evaluation process as described in Figure 4.4 may be carried out in parallel with development, or it may follow. The principal inputs to TOE evaluation are:

a) the set of TOE evidence, which includes the evaluated ST as the basis for TOE evaluation;

b) the TOE for which the evaluation is required;

c) the evaluation criteria, methodology and scheme.

In addition, informative material (such as application notes of the CC) and the IT security expertise of the evaluator and the evaluation community are likely to be used as inputs to the evaluation.

The expected result of the evaluation process is a confirmation that the TOE satisfies its security requirements as stated in the ST with one or more reports documenting the evaluator findings about the TOE as determined by the evaluation criteria. These reports will be useful to actual and potential consumers of the product or system represented by the TOE as well as to the developer.

The degree of confidence gained through an evaluation depends on the assurance requirements (e.g. Evaluation Assurance Level) met.

Evaluation can lead to better IT security products in two ways. Evaluation is intended to identify errors or vulnerabilities in the TOE that the developer may correct, thereby reducing the probability of security failures in future operation. Also in preparing for the rigours of evaluation, the developer may take more care in TOE design and development. Therefore, the evaluation process can exert a strong, though indirect, positive effect on the initial requirements, the development process, the end product, and the operational environment.

4.2.3 Operation

Consumers may elect to use evaluated TOEs in their environments. Once a TOE is in operation, it is possible that previously unknown errors or vulnerabilities may surface or environmental assumptions may need to be revised. As a result of operation, feedback could be given that would require the developer to correct the TOE or redefine its security requirements or environmental assumptions. Such changes may require the TOE to be re-evaluated or the security of its operational environment to be strengthened. In some instances this may only require that the needed updates are evaluated in order to regain confidence in the TOE. Although the CC contains criteria to cover assurance maintenance, detailed procedures for re-evaluation, including reuse of evaluation results, are outside the scope of the CC.

4.3 Security concepts

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

The CC is applicable when IT is being used and there is concern about the ability of the IT element to safeguard assets. In order to show that the assets are secure, the security concerns must be addressed at all levels from the most abstract to the final IT implementation in its operational environment. These levels of representation, as described in the following subclauses, permit security problems and issues to be characterised and discussed but do not, of themselves, demonstrate that the final IT implementation actually exhibits the required security behaviour and can, therefore, be trusted.

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

The CC layers the different levels of representation as described in Figure 4.5, which illustrates the means by which the security requirements and specifications might be derived when developing a PP or ST. All TOE security requirements ultimately arise from consideration of the purpose and context of the TOE. This chart is not intended to constrain the means by which PPs and STs are developed, but illustrates how the results of some analytic approaches relate to the content of PPs and STs.

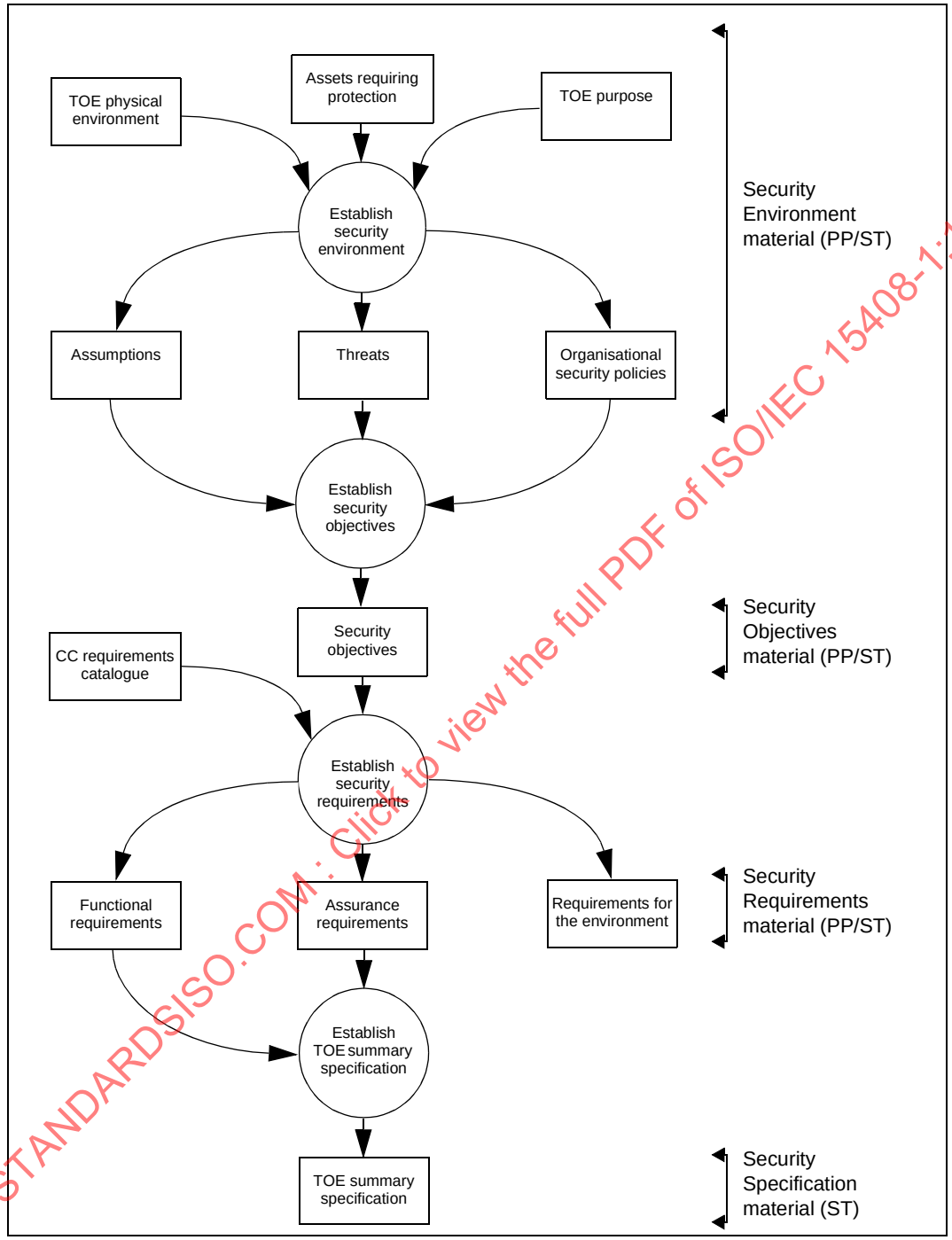

Figure 4.5 - Derivation of requirements and specifications

4.3.1 Security environment

The security environment includes all the laws, organisational security policies, customs, expertise and knowledge that are determined to be relevant. It thus defines the context in which the TOE is

intended to be used. The security environment also includes the threats to security that are, or are held to be, present in the environment.

To establish the security environment, the PP or ST writer has to take into account:

a) the TOE physical environment which identifies all aspects of the TOE operating environment relevant to TOE security, including known physical and personnel security arrangements;

b) the assets requiring protection by the element of the TOE to which security requirements or policies will apply; this may include assets that are directly referred to, such as files and databases, as well as assets that are indirectly subject to security requirements, such as authorisation credentials and the IT implementation itself;

c) the TOE purpose, which would address the product type and the intended usage of the TOE.

Investigation of the security policies, threats and risks should permit the following security specific statements to be made about the TOE:

a) A statement of assumptions which are to be met by the environment of the TOE in order for the TOE to be considered secure. This statement can be accepted as axiomatic for the TOE evaluation.

b) A statement of threats to security of the assets would identify all the threats perceived by the security analysis as relevant to the TOE. The CC characterises a threat in terms of a threat agent, a presumed attack method, any vulnerabilities that are the foundation for the attack, and identification of the asset under attack. An assessment of risks to security would qualify each threat with an assessment of the likelihood of such a threat developing into an actual attack, the likelihood of such an attack proving successful, and the consequences of any damage that may result.

c) A statement of applicable organisational security policies would identify relevant policies and rules. For an IT system, such policies may be explicitly referenced, whereas for a general purpose IT product or product class, working assumptions about organisational security policy may need to be made.

4.3.2 Security objectives

The results of the analysis of the security environment could then be used to state the security objectives that counter the identified threats and address identified organisational security policies and assumptions. The security objectives should be consistent with the stated operational aim or product purpose of the TOE, and any knowledge about its physical environment.

The intent of determining security objectives is to address all of the security concerns and to declare which security aspects are either addressed directly by the TOE or by its environment. This categorisation is based on a process incorporating engineering judgement, security policy, economic factors and risk acceptance decisions.

The security objectives for the environment would be implemented within the IT domain, and by non-technical or procedural means.

Only the security objectives for the TOE and its IT environment are addressed by IT security requirements.

4.3.3 IT security requirements

The IT security requirements are the refinement of the security objectives into a set of security requirements for the TOE and security requirements for the environment which, if met, will ensure that the TOE can meet its security objectives.

The CC presents security requirements under the distinct categories of functional requirements and assurance requirements.

The functional requirements are levied on those functions of the TOE that are specifically in support of IT security, and define the desired security behaviour. Part 2 defines the CC functional requirements. Examples of functional requirements include requirements for identification, authentication, security audit and non-repudiation of origin.

When the TOE contains security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function), the assurance requirements may specify that a minimum strength level consistent with the security objectives is to be claimed. In this case, the level specified will be one of the following SOF-basic, SOF-medium, SOF-high. Each such function will be required to meet that minimum level or at least an optionally defined specific metric.

The degree of assurance can be varied for a given set of functional requirements; therefore it is typically expressed in terms of increasing levels of rigour built with assurance components. Part 3 defines the CC assurance requirements and a scale of evaluation assurance levels (EALs) constructed using these components. The assurance requirements are levied on actions of the developer, on evidence produced and on the actions of the evaluator. Examples of assurance requirements include constraints on the rigour of the development process and requirements to search for and analyse the impact of potential security vulnerabilities.

Assurance that the security objectives are achieved by the selected security functions is derived from the following two factors:

a) confidence in the correctness of the implementation of the security functions, i.e., the assessment whether they are correctly implemented; and

b) confidence in the effectiveness of the security functions, i.e., the assessment whether they actually satisfy the stated security objectives.

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

is present. The rationale statements provide further support to the claim that such undesired behaviour is absent.

4.3.4 TOE summary specification

The TOE summary specification provided in the ST defines the instantiation of the security requirements for the TOE. It provides a high-level definition of the security functions claimed to meet the functional requirements, and assurance measures taken to meet the assurance requirements.

4.3.5 TOE implementation

The TOE implementation is the realisation of the TOE based on its security functional requirements and the TOE summary specification contained in the ST. TOE implementation is accomplished using a process of applying security and IT engineering skills and knowledge. The TOE will meet the security objectives if it correctly and effectively implements all the security requirements contained in the ST.

4.4 CC descriptive material

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

4.4.1 Expression of security requirements

The CC defines a set of constructs that combine into meaningful assemblies of security requirements of known validity, which can be used in establishing security requirements for prospective products and systems. The relationships among the various constructs for requirements expression are described below and illustrated in figure 4.6.

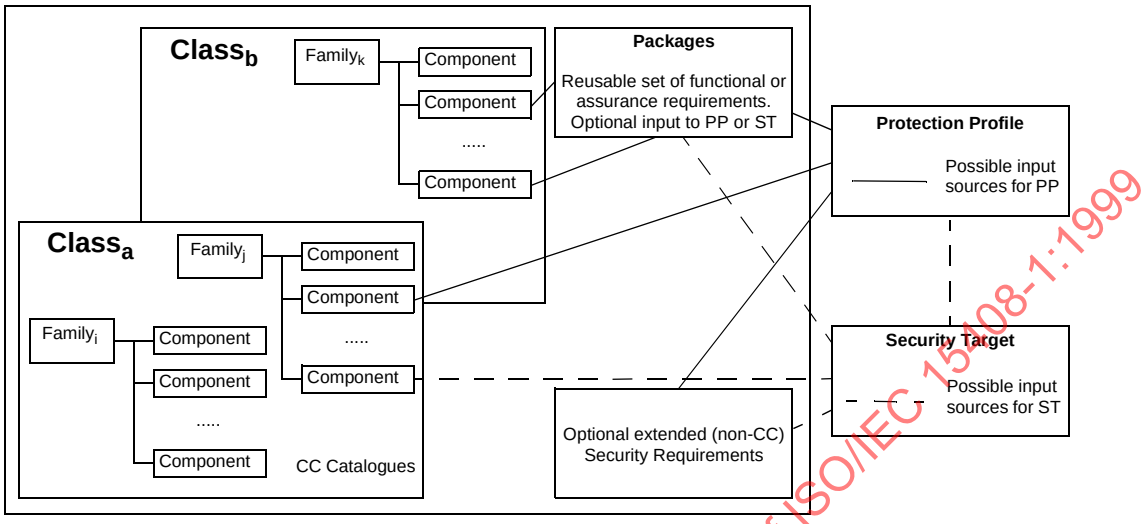

Figure 4.6 - Organisation and construction of requirements

The organisation of the CC security requirements into the hierarchy of class - family - component is provided to help consumers to locate specific security requirements.

The CC presents requirements for functional and assurance aspects in the same general style and uses the same organisation and terminology for each.

4.4.1.1 Class

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

The members of a class are termed families.

4.4.1.2 Family

A family is a grouping of sets of security requirements that share security objectives but may differ in emphasis or rigour.

The members of a family are termed components.

4.4.1.3 Component

A component describes a specific set of security requirements and is the smallest selectable set of security requirements for inclusion in the structures defined in the CC. The set of components within a family may be ordered to represent increasing strength or capability of security requirements that share a common purpose. They may also be partially ordered to represent related non-hierarchical sets. In some instances, there is only one component in a family so ordering is not applicable.

The components are constructed from individual elements. The element is the lowest level expression of security requirements, and is the indivisible security requirement that can be verified by the evaluation.

Dependencies between components

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

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

Permitted operations on components

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 CC component identifies and defines any permitted operations of assignment and selection, the circumstances under which these operations may be applied to the component, and the results of the application of the operation. The operations of iteration and refinement can be performed for any component. These four operations are described as follows:

a) **iteration**, which permits the use of a component more than once with varying operations;

b) **assignment**, which permits the specification of a parameter to be filled in when the component is used;

c) **selection**, which permits the specification of items that are to be selected from a list given in the component;

d) **refinement**, which permits the addition of extra detail when the component is used.

Some required operations may be completed (in whole or part) in the PP or may be left to be completed in the ST. Nevertheless, all operations must be completed in the ST.

4.4.2 Use of security requirements

The CC defines three types of requirement constructs: package, PP and ST. The CC further defines a set of IT security criteria that can address the needs of many communities and thus serve as a major expert input to the production of these constructs. The CC has been developed around the central notion of using wherever possible the security requirements components defined in the CC, which represent a well-known and understood domain. Figure 4.7 shows the relationship between these different constructs.

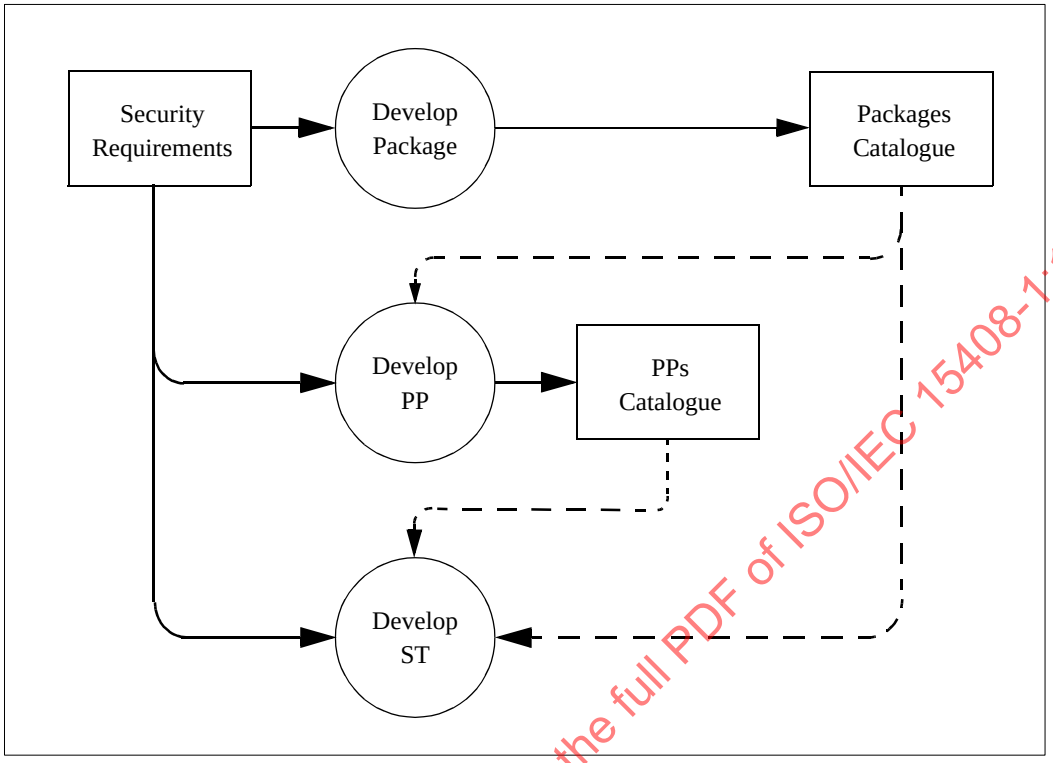

Figure 4.7 - Use of security requirements

4.4.2.1 Package

An intermediate combination of components is termed a package. The package permits the expression of a set of functional or assurance requirements that meet an identifiable subset of security objectives. A package is intended to be reusable and to define requirements that 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.

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

4.4.2.2 Protection Profile

The PP contains a set of security requirements either from the CC, or stated explicitly, which should include an EAL (possibly augmented by additional assurance components). The PP permits the implementation independent expression of security requirements for a set of TOEs that will comply fully with a set of security objectives. A PP is intended to be reusable and to define TOE requirements that are known to be useful and effective in meeting the identified objectives, both for functions and assurance. A PP also contains the rationale for security objectives and security requirements.

A PP could be developed by user communities, IT product developers, or other parties interested in defining such a common set of requirements. A PP gives consumers a means of referring to a specific set of security needs and facilitates future evaluation against those needs.

4.4.2.3 Security Target

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

An ST contains the TOE summary specification, together with the security requirements and objectives, and the rationale for each. An ST is the basis for agreement between all parties as to what security the TOE offers.

4.4.3 Sources of security requirements

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

a) Existing PPs

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

Existing PPs may be used as a basis for a new PP.

b) Existing packages

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

A set of predefined packages is the EALs defined in Part 3. The TOE assurance requirements in a PP or ST should include an EAL from Part 3.

c) Existing functional or assurance requirements components

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

d) Extended requirements

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

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

4.5 Types of evaluation

4.5.1 PP evaluation

The PP evaluation is carried out against the evaluation criteria for PPs contained in Part 3. The goal of such an evaluation is to demonstrate that the PP is complete, consistent, and technically sound and suitable for use as a statement of requirements for an evaluatable TOE.

4.5.2 ST evaluation

The evaluation of the ST for the TOE is carried out against the evaluation criteria for STs contained in Part 3. The goal of such an evaluation is twofold: first to demonstrate that the ST is complete, consistent, and technically sound and hence suitable for use as the basis for the corresponding TOE evaluation; second, in the case where an ST claims conformance to a PP, to demonstrate that the ST properly meets the requirements of the PP.

4.5.3 TOE evaluation

The TOE evaluation is carried out against the evaluation criteria contained in Part 3 using an evaluated ST as the basis. The goal of such an evaluation is to demonstrate that the TOE meets the security requirements contained in the ST.

4.6 Assurance maintenance

TOE assurance maintenance is carried out against the evaluation criteria contained in Part 3 using a previously evaluated TOE as the basis. The goal is to derive confidence that assurance already established in a TOE is maintained and that the TOE will continue to meet its security requirements as changes are made to the TOE or its environment.

5 Common Criteria requirements and evaluation results

5.1 Introduction

This clause presents the expected results from PP and TOE evaluation. PP or TOE evaluations lead respectively to catalogues of evaluated PPs or TOEs. ST evaluation leads to intermediate results that are used in the frame of a TOE evaluation.

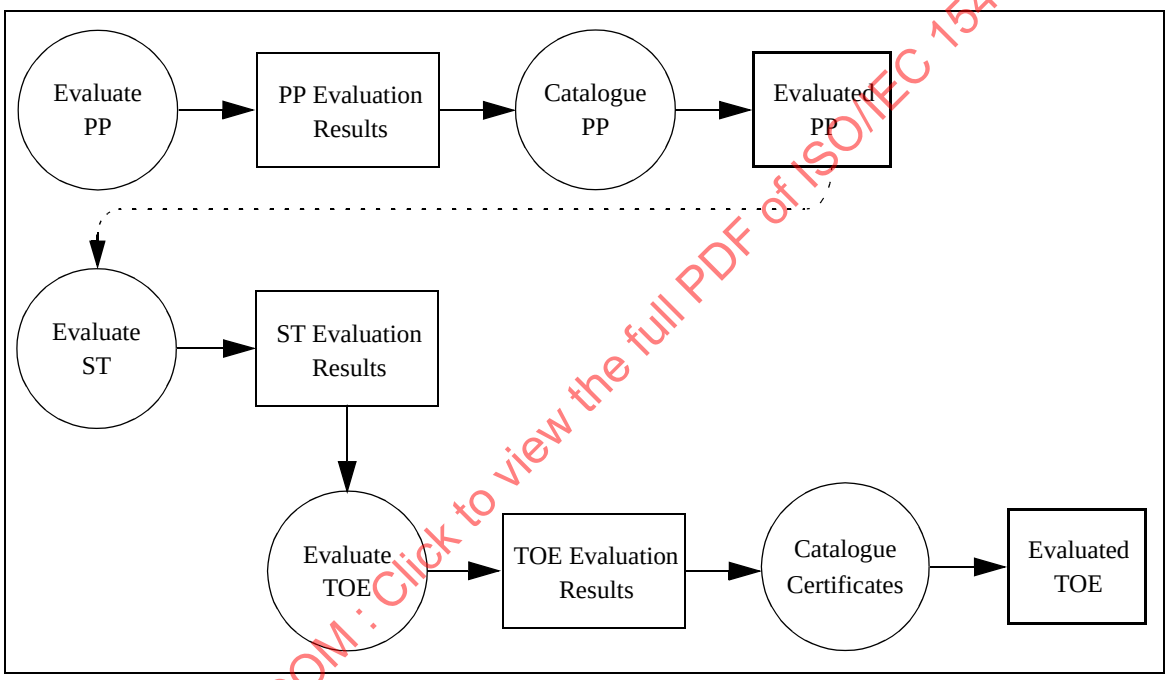

Figure 5.1 - Evaluation results

Evaluation should lead to objective and repeatable results that can be cited as evidence, even if there is no totally objective scale for representing the results of an IT security evaluation. The existence of a set of evaluation criteria is a necessary pre-condition for evaluation to lead to a meaningful result and provides a technical basis for mutual recognition of evaluation results between evaluation authorities. But the application of criteria contains both objective and subjective elements, that's why precise and universal ratings for IT security are not, therefore, feasible.

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

5.2 Requirements in PPs and STs

The CC defines a set of IT security criteria that can address the needs of many communities. The CC has been developed around the central notion that the use of the security functional components contained in Part 2, and the EALs and assurance components contained in Part 3, represents the preferred course of action for expression of TOE requirements in PPs and STs, as they represent a well-known and understood domain.

The CC recognises the possibility that functional and assurance requirements not included in the provided catalogues may be required in order to represent the complete set of IT security requirements. The following shall apply to the inclusion of these extended functional or assurance requirements:

a) Any extended functional or assurance requirements included in a PP or ST shall be clearly and unambiguously expressed such that evaluation and demonstration of compliance is feasible. The level of detail and manner of expression of existing CC functional or assurance components shall be used as a model.

b) Evaluation results obtained using extended functional or assurance requirements shall be caveated as such.

c) The incorporation of extended functional or assurance requirements into a PP or ST shall conform to the APE or ASE classes of the Part 3, as appropriate.

5.2.1 PP evaluation results

The CC contains the evaluation criteria that permit an evaluator to state whether a PP is complete, consistent, and technically sound and hence suitable for use as a statement of requirements for an evaluatable TOE.

Evaluation of the PP shall result in a pass/fail statement. A PP for which the evaluation results in a pass statement shall be eligible for inclusion within a registry.

5.3 Requirements in TOE

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

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

b) whether the specified security functions of the TOE are correctly implemented.

The security requirements expressed in the CC define the known working domain of applicability of IT security evaluation criteria. A TOE for which the security requirements are expressed only in terms of the functional and assurance requirements drawn from the CC will be evaluatable against the CC. Use of assurance packages that do not contain an EAL shall be justified.

However, there may be a need for a TOE to meet security requirements not directly expressed in the CC. The CC recognises the necessity to evaluate such a TOE but, as the additional requirements lie outside the known domain of applicability of the CC, the results of such an evaluation must be caveated accordingly. Such a caveat may place at risk universal acceptance of the evaluation results by the involved evaluation authorities.

The results of a TOE evaluation shall include a statement of conformance to the CC. The use of CC terms to describe the security of a TOE permits comparison of the security characteristics of TOEs in general.

5.3.1 TOE evaluation results

The result of the TOE evaluation shall be a statement that describes the extent to which the TOE can be trusted to conform to the requirements.

Evaluation of the TOE shall result in a pass/fail statement. A TOE for which the evaluation results in a pass statement shall be eligible for inclusion within a registry.

5.4 Caveats on evaluation results

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

a) **Part 2 conformant** - A PP or TOE is Part 2 conformant if the functional requirements are only based upon functional components in Part 2.

b) **Part 2 extended** - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2.

c) **Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are in the form of an **EAL** or **assurance package** that is based only upon assurance components in Part 3.

d) **Part 3 augmented** - A PP or TOE is Part 3 augmented if the assurance requirements are in the form of an **EAL** or **assurance package,** plus other assurance components in Part 3.

e) **Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements are in the form of an **EAL** associated with additional assurance requirements not in Part 3 or an **assurance package** that includes (or is entirely made up from) assurance requirements not in Part 3.

f) **Conformant to PP** - A TOE is conformant to a PP only if it is compliant with all parts of the PP.

5.5 Use of TOE evaluation results

IT products and systems differ in respect to the use of the results of the evaluation. Figure 5.2 shows options for processing the results of evaluation. Products can be evaluated and catalogued at successively higher levels of aggregation until operational systems are achieved, at which time they may be subject to evaluation in connection with system accreditation.

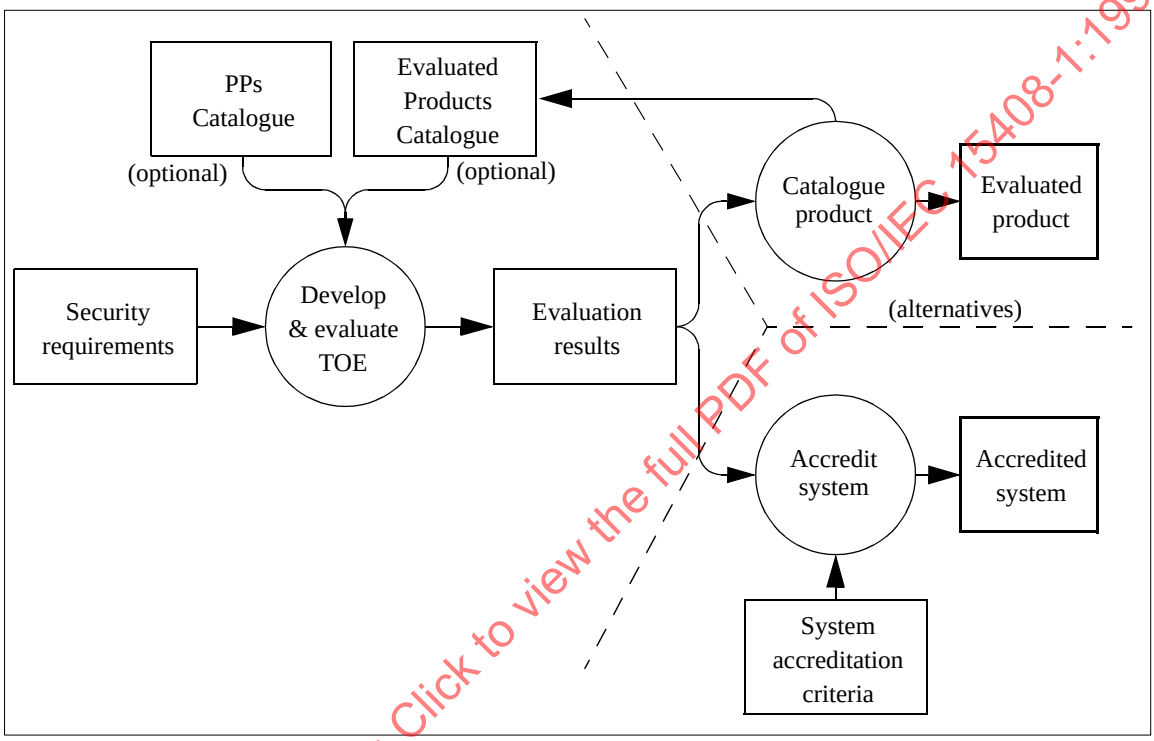

Figure 5.2 - Use of TOE evaluation results

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

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

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

Annex A
(informative)

The Common Criteria project

A.1 Background to the Common Criteria project

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 Organization for Standardization (ISO) to develop an international standard evaluation criteria for general use. The new criteria was to be responsive to the need for mutual recognition of standardised security evaluation results in a global IT market. This task was assigned to Working Group 3 (WG 3) of subcommittee 27 (SC 27) of the Joint Technical Committee 1 (JTC 1). Initially, progress was slow within WG3 because of the extensive amount of work and intensive multilateral negotiations required.

A.2 Development of the Common Criteria

In June 1993, the sponsoring organisations of the CTCPEC, FC, TCSEC and ITSEC (which are identified in the next subclause) pooled their efforts and began a joint activity to align their separate criteria into a single set of IT security criteria that could be widely used. This activity was named the CC Project. Its purpose was to resolve the conceptual and technical differences found in the source criteria and to deliver the results to ISO as a contribution to the international standard under development. Representatives of the sponsoring organisations formed CC Editorial Board (CCEB) to develop the CC. A liaison was then established between the CCEB and WG 3, and the CCEB contributed several early versions of the CC to WG 3 via the liaison channel. As a result of the interaction between WG 3 and the CCEB, these versions were adopted as successive working drafts of various Parts of the ISO criteria beginning in 1994.

Version 1.0 of the CC was completed by the CCEB in January 1996 and was approved by ISO in April 1996 for distribution as a Committee Draft (CD). The CC Project then performed a number of trial evaluations using CC Version 1.0, and an extensive public review of the document was

conducted. The CC Project subsequently undertook an extensive revision of the CC based on the comments received from trial use, public review and interaction with ISO. The revision work has been carried out by the successor to the CCEB, now called the CC Implementation Board (CCIB).

The CCIB completed CC version 2.0 “Beta” in October 1997 and presented it to WG 3, which approved it as a Second Committee Draft. Subsequent intermediate draft versions were provided informally to WG 3 experts for feedback as they were produced by the CCIB. The CCIB received and responded to a series of comments that came both directly from WG 3 experts and from ISO National Bodies via the CD balloting. The culmination of this process is CC Version 2.0.

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

A.3 Common Criteria project sponsoring organisations

The seven European and North American governmental organisations listed below 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 2.0 now that its technical development has been completed and it is in the final stages of acceptance as an International Standard.

CANADA:
Communications Security Establishment
Criteria Coordinator
I2A 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

FRANCE:
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

GERMANY:
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

NETHERLANDS:
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

UNITED KINGDOM:
Communications-Electronics Security Group
Compusec Evaluation Methodology
P.O. Box 144
Cheltenham GL52 5UE
United Kingdom
Tel: +44.1242.221.491 ext. 5257, Fax: +44.1242.252.291
E-mail: criteria@cesg.gov.uk
WWW: http://www.cesg.gov.uk/cchtml
FTP: ftp://ftp.cesg.gov.uk/pub

UNITED STATES - NSA:
National Security Agency
Attn: V2, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 20755-6740
U.S.A.
Tel: +1.410.859.4458, Fax: +1.410.684.7512
E-mail: common_criteria@radium.ncsc.mil
WWW: http://www.radium.ncsc.mil/tpep/

UNITED STATES - NIST:
National Institute of Standards and Technology
Computer Security Division
820 Diamond, MS: NN426
Gaithersburg, Maryland 20899
U.S.A.
Tel: +1.301.975.2934, Fax: +1.301.948.0279
E-mail: criteria@nist.gov
WWW: http://csrc.nist.gov/cc

Annex B
(normative)

Specification of Protection Profiles

B.1 Overview

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

This annex contains the requirements for the PP in descriptive form. The assurance class APE, contained in clause 4 of ISO/IEC 15408-3, contains these requirements in the form of assurance components to be used for evaluation of the PP.

B.2 Content of Protection Profile

B.2.1 Content and presentation

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

The contents of the PP are portrayed in Figure B.1, which should be used when constructing the structural outline of the PP document.

B.2.2 PP introduction

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

a) The **PP identification** shall provide the labelling and descriptive information necessary to identify, catalogue, register, and cross reference a PP.

b) The **PP overview** shall summarise the PP in narrative form. The overview should be sufficiently detailed for a potential user of the PP to determine whether the PP is of interest. The overview should also be usable as a stand alone abstract for use in PP catalogues and registers.

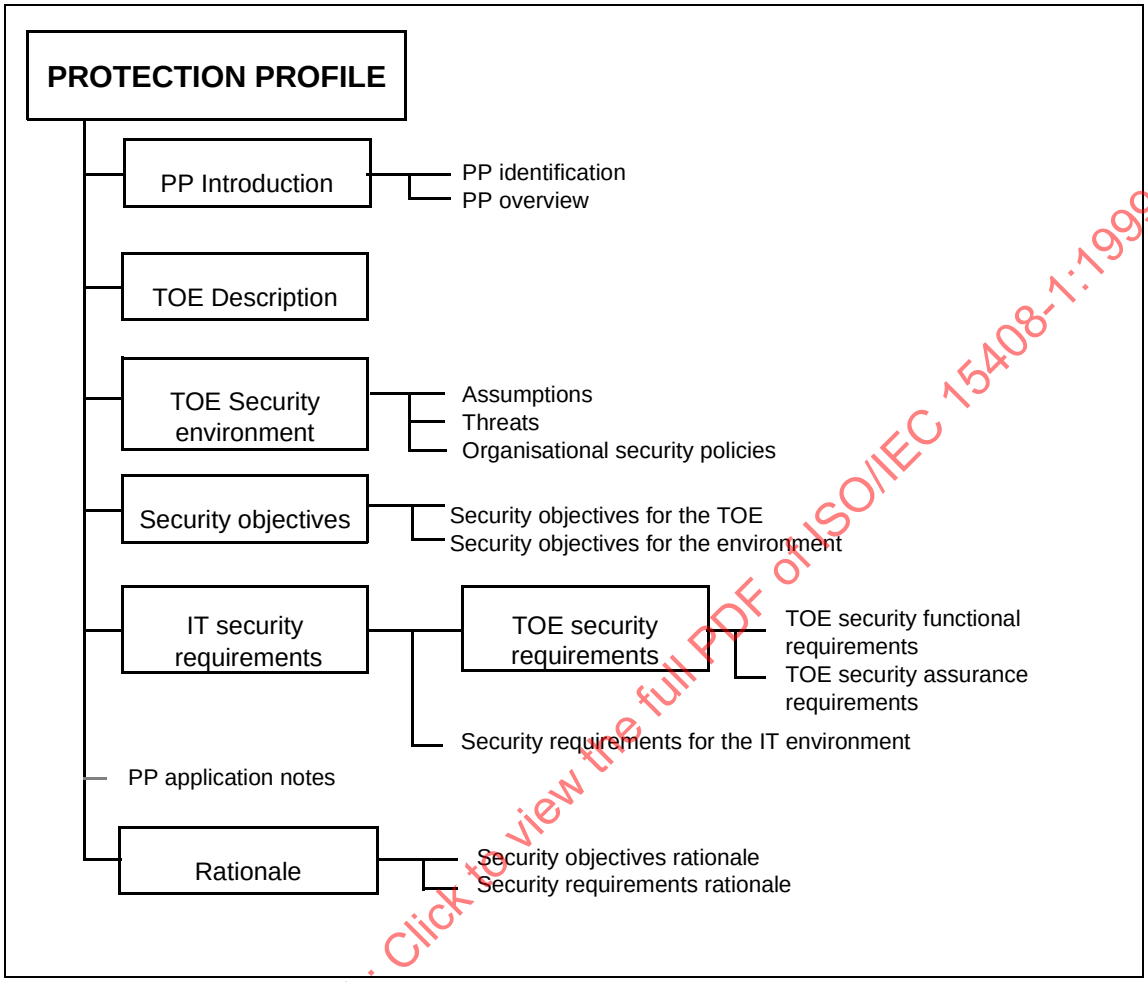

Figure B.1 - Protection Profile content

B.2.3 TOE description

This part of the PP shall describe the TOE as an aid to the understanding of its security requirements, and shall address the product type and the general IT features of the TOE.

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

B.2.4 TOE security environment

The statement of **TOE security environment** shall describe the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed. This statement shall include the following:

a) A description of **assumptions** shall describe the security aspects of the environment in which the TOE will be used or is intended to be used. This shall include the following:

information about the intended usage of the TOE, including such aspects as the intended application, potential asset value, and possible limitations of use; and

information about the environment of use of the TOE, including physical, personnel, and connectivity aspects.

b) A description of **threats** shall include all threats to the assets against which specific protection within the TOE or its environment is required. Note that not all possible threats that might be encountered in the environment need to be listed, only those which are relevant for secure TOE operation.

A threat shall be described in terms of an identified threat agent, the attack, and the asset that is the subject of the attack. Threat agents should be described by addressing aspects such as expertise, available resources, and motivation. Attacks should be described by addressing aspects such as attack methods, any vulnerabilities exploited, and opportunity.
If security objectives are derived from only organisational security policies and assumptions, then the description of threats may be omitted.

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

If security objectives are derived from only threats and assumptions, then the description of organisational security policies may be omitted.

Where the TOE is physically distributed, it may be necessary to discuss the security environmental aspects (assumptions, threats, organisational security policies) separately for distinct domains of the TOE environment.

B.2.5 Security objectives

The statement of **security objectives** shall define the security objectives for the TOE and its environment. The security objectives shall address all of the security environment aspects identified. The security objectives shall reflect the stated intent and shall be suitable to counter all identified threats and cover all identified organisational security policies and assumptions. The following categories of objectives shall be identified. Note: when a threat or organisational security policy is to be covered partly by the TOE and partly by its environment, then the related objective shall be repeated in each category.

a) The **security objectives for the TOE** shall be clearly stated and traced back to aspects of identified threats to be countered by the TOE and/or organisational security policies to be met by the TOE.

b) The **security objectives for the environment** shall be clearly stated and traced back to aspects of identified threats not completely countered by the TOE and/or organisational security policies or assumptions not completely met by the TOE.

Note that security objectives for the environment may be a re-statement, in whole or part, of the assumptions portion of the statement of the TOE security environment.

B.2.6 IT security requirements

This part of the PP defines the detailed IT security requirements that shall be satisfied by the TOE or its environment. The IT security requirements shall be stated as follows:

a) The statement of **TOE security requirements** shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. The TOE security requirements shall be stated as follows:

1) The statement of **TOE security functional requirements** should define the functional requirements for the TOE as functional components drawn from Part 2 where applicable.

Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 component to cover each aspect is possible.

Where AVA_SOF.1 is included in the TOE security assurance requirements (e.g. EAL2 and higher), the statement of TOE security functional requirements shall include a minimum strength level for the TOE security functions realised by a probabilistic or permutational mechanism (e.g. a password or hash function). All such functions shall meet this minimum level. The level shall be one of the following: SOF-basic, SOF-medium, SOF-high. The selection of the level shall be consistent with the identified security objectives for the TOE. Optionally, specific strength of function metrics may be defined for selected functional requirements, in order to meet certain security objectives for the TOE.

As part of the strength of TOE security functions evaluation (AVA_SOF.1), it will be assessed whether the strength claims made for individual TOE security functions and the overall minimum strength level are met by the TOE.

2) The statement of **TOE security assurance requirements** should state the assurance requirements as one of the EALs optionally augmented by Part 3 assurance components. The PP may also extend the EAL by explicitly stating additional assurance requirements not taken from Part 3.

b) The optional statement of **Security requirements for the IT environment** shall identify the IT security requirements that are to be met by the IT environment of the TOE. If the TOE has no asserted dependencies on the IT environment, this part of the PP may be omitted.

Note that **security requirements for the non-IT environment**, while often useful in practice, are not required to be a formal part of the PP as they do not relate directly to the implementation of the TOE.

c) The following **common conditions** shall apply equally to the expression of security functional and assurance requirements for the TOE and its IT environment:

1) All IT security requirements should be stated by reference to security requirements components drawn from Part 2 or Part 3 where applicable. Should none of the Part 2 or Part 3 requirements components be readily applicable to all or part of the security requirements, the PP may state those requirements explicitly without reference to the CC.

2) Any explicit statement of TOE security functional or assurance requirements shall be clearly and unambiguously expressed such that evaluation and demonstration of compliance is feasible. The level of detail and manner of expression of existing CC functional or assurance requirements shall be used as a model.

3) When requirements components that specify required operations (assignment or selection) are selected, the PP shall use those operations to amplify the requirements to the level of detail necessary to demonstrate that the security objectives are met. Any required operations that are not performed within the PP shall be identified as such.

4) By using operations on the requirements components, the TOE security requirements statements may optionally prescribe or forbid the use of particular security mechanisms where necessary.

5) All dependencies among the IT security requirements should be satisfied. Dependencies may be satisfied by the inclusion of the relevant requirement within the TOE security requirements, or as a requirement on the environment.

B.2.7 Application notes

This optional part of the PP may contain additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

B.2.8 Rationale

This part of the PP presents the evidence used in the PP evaluation. This evidence supports the claims that the PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The rationale shall include the following:

a) The **security objectives rationale** shall demonstrate that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them.