INTERNATIONAL STANDARD

ISO/IEC 15408-1

Second edition
2005-10-01

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 15408-1:2005(E)

© ISO/IEC 2005

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2005

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2005 – All rights reserved

Not for Resale

Contents

Page

Foreword v

Introduction vii

1 Scope 1

2 Terms and definitions 2

3 Symbols and abbreviated terms 7

4 Overview 8
4.1 Introduction 8
4.1.1 Target audience of ISO/IEC 15408 8
4.2 Evaluation context 9
4.3 Organisation of ISO/IEC 15408 10

5 General model 11
5.1 Security context 11
5.1.1 General security context 11
5.1.2 Information technology security context 13
5.2 ISO/IEC 15408 approach 13
5.2.1 Development 13
5.2.2 TOE evaluation 15
5.2.3 Operation 15
5.3 Security concepts 16
5.3.1 Security environment 17
5.3.2 Security objectives 18
5.3.3 IT security requirements 18
5.3.4 TOE summary specification 19
5.3.5 TOE implementation 19
5.4 ISO/IEC 15408 descriptive material 19
5.4.1 Expression of security requirements 19
5.4.2 Types of evaluation 24

6 ISO/IEC 15408 requirements and evaluation results 25
6.1 Introduction 25
6.2 Requirements in PPs and STs 25
6.2.1 PP evaluation results 26
6.3 Requirements in TOE 26
6.3.1 TOE evaluation results 26
6.4 Conformance results 26
6.5 Use of TOE evaluation results 27

Annex A (normative) **Specification of Protection Profiles** 29
A.1 Overview 29
A.2 Content of Protection Profile 29
A.2.1 Content and presentation 29
A.2.2 PP introduction 30
A.2.3 TOE description 30
A.2.4 TOE security environment 31
A.2.5 Security objectives 31
A.2.6 IT security requirements 32
A.2.7 Application notes 33
A.2.8 Rationale 33

Annex B (normative) **Specification of Security Targets** 34
B.1 Overview 34

© ISO/IEC 2005 All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.2 Content of Security Target 34
B.2.1 Content and presentation 34
B.2.2 ST introduction 35
B.2.3 TOE description 36
B.2.4 TOE security environment 36
B.2.5 Security objectives 36
B.2.6 IT security requirements 37
B.2.7 TOE summary specification 38
B.2.8 PP claims 38
B.2.9 Application Notes 39
B.2.10 Rationale 40

Bibliography 41

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15408-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*. The identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organisations as Common Criteria for Information Technology Security Evaluation.

This second edition cancels and replaces the first edition (ISO/IEC 15408-1:1999), which has been technically revised.

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*

Legal notice

The governmental organizations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations, version 2.3 Parts 1 through 3 (called CC 2.3), they hereby grant non-exclusive license to ISO/IEC to use CC 2.3 in the continued development/maintenance of the ISO/IEC 15408 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC 2.3 as they see fit.

Australia/New Zealand:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Canada:	Communications Security Establishment;
France:	Direction Centrale de la Sécurité des Systèmes d'Information;

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Germany:	Bundesamt für Sicherheit in der Informationstechnik;
Japan:	Information Technology Promotion Agency;
Netherlands:	Netherlands National Communications Security Agency;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2005 – All rights reserved
Not for Resale

Introduction

ISO/IEC 15408 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.

ISO/IEC 15408 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.

ISO/IEC 15408 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. ISO/IEC 15408 may also be applicable to aspects of IT security outside of these three. ISO/IEC 15408 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, ISO/IEC 15408 may be applied in other areas of IT, but makes no claim of competence outside the strict domain of IT security.

ISO/IEC 15408 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.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

Part 1: Introduction and general model

1 Scope

ISO/IEC 15408 is meant 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.

Certain topics, because they involve specialized techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of ISO/IEC 15408. Some of these are identified below:

a) ISO/IEC 15408 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, ISO/IEC 15408 addresses some aspects of physical protection of the TOE.

c) ISO/IEC 15408 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 ISO/IEC 15408 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 ISO/IEC 15408. 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 ISO/IEC 15408. Should independent assessment of mathematical properties of cryptography embedded in a TOE be required, the evaluation scheme under which ISO/IEC 15408 is applied must make provision for such assessments.

This part of ISO/IEC 15408 defines two forms for expressing IT security functional and assurance requirements. The protection profile (PP) construct allows creation of generalized reusable sets of these security requirements. The PP can be used by prospective consumers for specification and identification of products with IT security features which will meet their needs. The security target (ST) expresses the security requirements and specifies the security functions for a particular product or system to be evaluated, called the target of evaluation (TOE). The ST is used by evaluators as the basis for evaluations conducted in accordance with ISO/IEC 15408.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE This clause 2 contains only those terms which are used in a specialised way throughout ISO/IEC 15408. The majority of terms in ISO/IEC 15408 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 ISO/IEC 15408, while not meriting inclusion in this clause 2, 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.

2.1
assets
information or resources to be protected by the countermeasures of a TOE.

2.2
assignment
the specification of an identified parameter in a component.

2.3
assurance
grounds for confidence that an entity meets its security objectives.

2.4
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.

2.5
augmentation
the addition of one or more assurance component(s) from ISO/IEC 15408-3 to an EAL or assurance package.

2.6
authentication data
information used to verify the claimed identity of a user.

2.7
authorised user
a user who may, in accordance with the TSP, perform an operation.

2.8
class
a grouping of families that share a common focus.

2.9
component
the smallest selectable set of elements that may be included in a PP, an ST, or a package.

2.10
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.

2.11
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.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.12
element
an indivisible security requirement.

2.13
evaluation
assessment of a PP, an ST or a TOE, against defined criteria.

2.14
evaluation assurance level (EAL)
a package consisting of assurance components from ISO/IEC 15408-3 that represents a point on ISO/IEC 15408 predefined assurance scale.

2.15
evaluation authority
a body that implements ISO/IEC 15408 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.

2.16
evaluation scheme
the administrative and regulatory framework under which ISO/IEC 15408 is applied by an evaluation authority within a specific community.

2.17
extension
the addition to an ST or PP of functional requirements not contained in ISO/IEC 15408-2 and/or assurance requirements not contained in ISO/IEC 15408-3.

2.18
external IT entity
any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

2.19
family
a grouping of components that share security objectives but may differ in emphasis or rigour.

2.20
formal
expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

2.21
guidance documentation
guidance documentation describes the delivery, installation, configuration, operation, management and use of the TOE as these activities apply to the users, administrators, and integrators of the TOE. The requirements on the scope and contents of guidance documents are defined in a PP or ST.

2.22
human user
any person who interacts with the TOE.

2.23
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.

2.24
informal
expressed in natural language.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.25
internal communication channel
a communication channel between separated parts of TOE.

2.26
internal TOE transfer
communicating data between separated parts of the TOE.

2.27
inter-TSF transfers
communicating data between the TOE and the security functions of other trusted IT products.

2.28
iteration
the use of a component more than once with varying operations.

2.29
object
an entity within the TSC that contains or receives information and upon which subjects perform operations.

2.30
organisational security policies
one or more security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

2.31
package
a reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

2.32
product
a package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

2.33
protection profile (PP)
an implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

2.34
reference monitor
the concept of an abstract machine that enforces TOE access control policies.

2.35
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.

2.36
refinement
the addition of details to a component.

2.37
role
a predefined set of rules establishing the allowed interactions between a user and the TOE.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.38
secret
information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

2.39
security attribute
characteristics of subjects, users, objects, information, and/or resources that are used for the enforcement of the TSP.

2.40
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.

2.41
security function policy (SFP)
the security policy enforced by an SF.

2.42
security objective
a statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.

2.43
security target (ST)
a set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

2.44
selection
the specification of one or more items from a list in a component.

2.45
semiformal
expressed in a restricted syntax language with defined semantics.

2.46
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.

2.47
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.

2.48
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.

2.49
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.

2.50
subject
an entity within the TSC that causes operations to be performed.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.51
system
a specific IT installation, with a particular purpose and operational environment.

2.52
target of evaluation (TOE)
an IT product or system and its associated guidance documentation that is the subject of an evaluation.

2.53
TOE resource
anything useable or consumable in the TOE.

2.54
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.

2.55
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.

2.56
TOE security policy (TSP)
a set of rules that regulate how assets are managed, protected and distributed within a TOE.

2.57
TOE security policy mode
a structured representation of the security policy to be enforced by the TOE.

2.58
transfers outside TSF control
communicating data to entities not under control of the TSF.

2.59
trusted channel
a means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

2.60
trusted path
a means by which a user and a TSF can communicate with necessary confidence to support the TSP.

2.61
TSF data
data created by and for the TOE, that might affect the operation of the TOE.

2.62
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.

2.63
user
any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

2.64
user data
data created by and for the user, that does not affect the operation of the TSF.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.65
normative
normative text is that which “describes the scope of the document, and which set out provisions.” (ISO/IEC Directives, Part 2) Within normative text, the verbs “shall”, “should”, “may”, and “can” have the ISO standard meanings described in this clause and the verb “must” is not used. Unless explicitly labeled “informative”, all ISO/IEC 15408 text is normative. Any text related to meeting requirements is considered normative.

2.66
informative
informative text is that which “provides additional information intended to assist the understanding or use of the document.”(ISO/IEC Directives, Part 2). Informative text is not related to meeting requirements.

2.67
shall
within normative text, “shall” indicates “requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.” (ISO/IEC Directives, Part 2)

2.68
should
within normative text, should indicates “that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.”(ISO/IEC Directives, Part 2) ISO/IEC 15408 interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

2.69
may
within normative text, may indicates “a course of action permissible within the limits of the document”(ISO/IEC Directives, Part 2)

2.70
can
within normative text, can indicates “statements of possibility and capability, whether material, physical or causal”(ISO/IEC Directives, Part 2)

3 Symbols and abbreviated terms

The following abbreviations are common to more than one part of ISO/IEC 15408:

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

© ISO/IEC 2005 All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

TSF TOE Security Functions

TSFI TSF Interface

TSP TOE Security Policy

4 Overview

This clause introduces the main concepts of ISO/IEC 15408. It identifies the target audience, evaluation context, and the approach taken to present the material.

4.1 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).

ISO/IEC 15408 can be used to select the appropriate IT security measures and it contains criteria for evaluation of security requirements.

4.1.1 Target audience of ISO/IEC 15408

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 ISO/IEC 15408. The three groups can benefit from the criteria as explained in the following paragraphs.

4.1.1.1 Consumers

ISO/IEC 15408 plays an important role in supporting techniques for consumer selection of IT security requirements to express their organisational needs. ISO/IEC 15408 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.

ISO/IEC 15408 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.

4.1.1.2 Developers

ISO/IEC 15408 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 ISO/IEC 15408 to support someone, other than the TOE developer, in preparing for and assisting in the evaluation of a developer's TOE.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ISO/IEC 15408 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.

ISO/IEC 15408 describes security functions that a developer could include in the TOE. ISO/IEC 15408 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.

4.1.1.3 Evaluators

ISO/IEC 15408 contains criteria to be used by evaluators when forming judgements about the conformance of TOEs to their security requirements. ISO/IEC 15408 describes the set of general actions the evaluator is to carry out and the security functions on which to perform these actions. Note that ISO/IEC 15408 does not specify procedures to be followed in carrying out those actions.

4.1.1.4 Others

While ISO/IEC 15408 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 ISO/IEC 15408 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.

4.2 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.

ISO/IEC 15408 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 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 ISO/IEC 15408.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

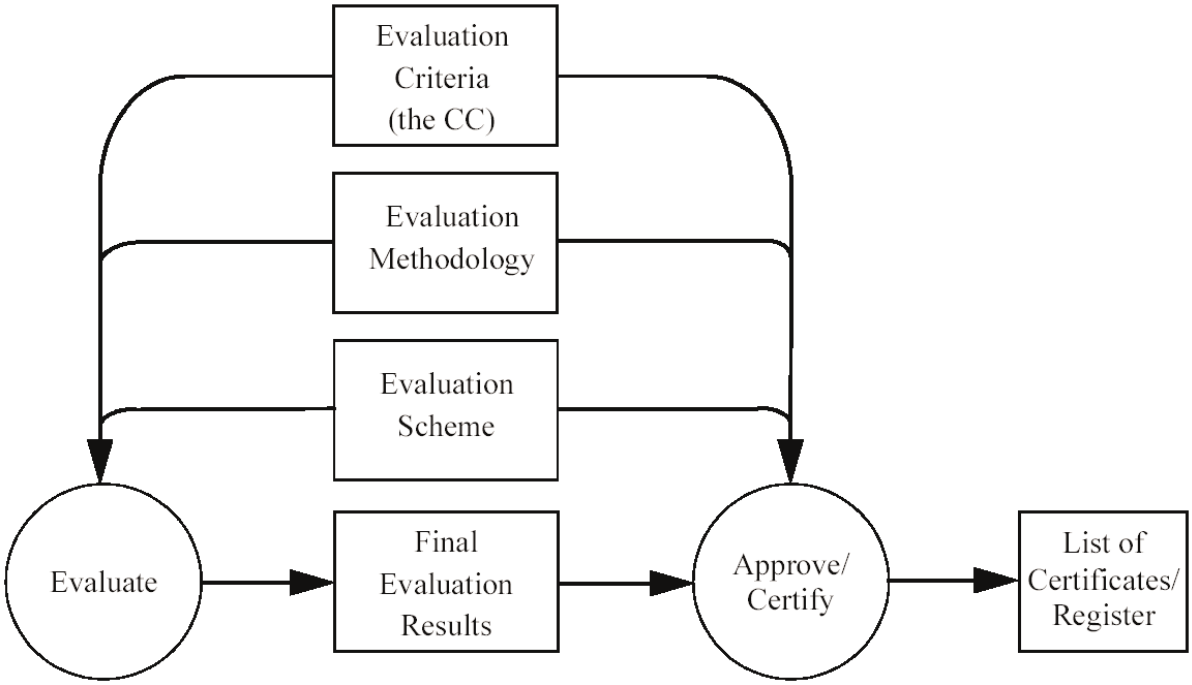


Figure 1 - Evaluation Context

4.3 Organisation of ISO/IEC 15408

ISO/IEC 15408 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 5.

a) **Part 1, Introduction and general model**, is the introduction to ISO/IEC 15408. 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 ISO/IEC 15408 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 ISO/IEC 15408 scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs).

In support of the three parts of ISO/IEC 15408 listed above, it is anticipated that other types of documents will be published, including technical rationale material and guidance documents.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The following table presents, for the three key target audience groupings, how the parts of ISO/IEC 15408 will be of interest.

	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.

Table 1 Roadmap to the "Evaluation criteria for IT security"

5 General model

This clause presents the general concepts used throughout ISO/IEC 15408, including the context in which the concepts are to be used and ISO/IEC 15408 approach for applying the concepts. ISO/IEC 15408-2 and ISO/IEC 15408-3 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.

ISO/IEC 15408 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 ISO/IEC 15408. However, the concepts themselves are quite general and are not intended to restrict the class of IT security problems to which ISO/IEC 15408 is applicable.

5.1 Security context

5.1.1 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 2 illustrates high level concepts and relationships.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

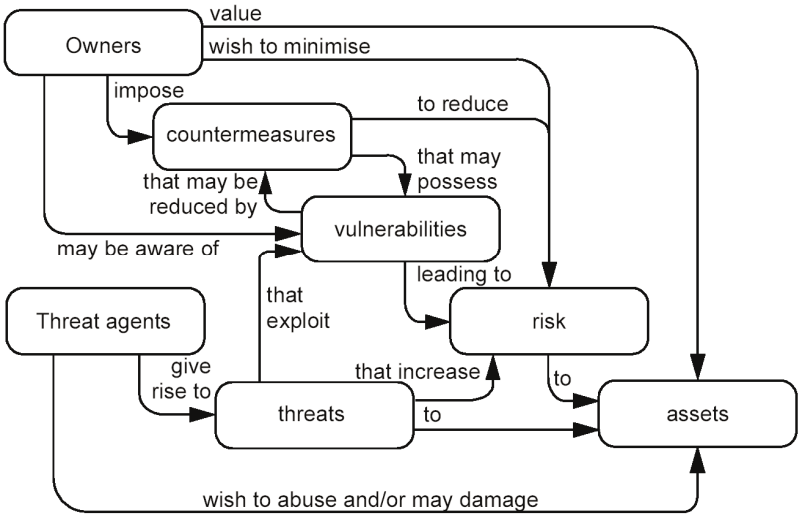


Figure 2 - Security concepts and relationships

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 threats applicable to their assets and their environment, determining the risks associated with them. 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.

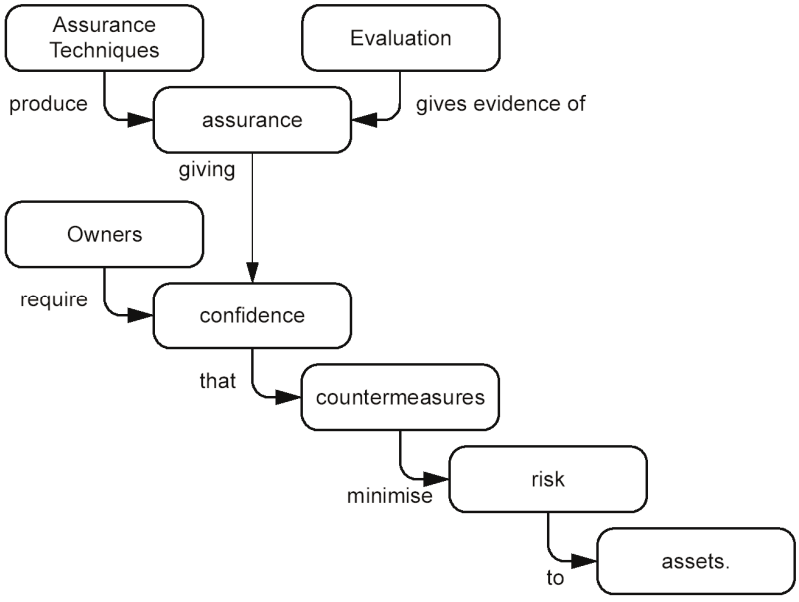


Figure 3 - Evaluation concepts and relationships

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 3 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.

5.1.2 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.

5.2 ISO/IEC 15408 approach

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

5.2.1 Development

ISO/IEC 15408 does not mandate any specific development methodology or life cycle model. Figure 4 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.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2005 All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

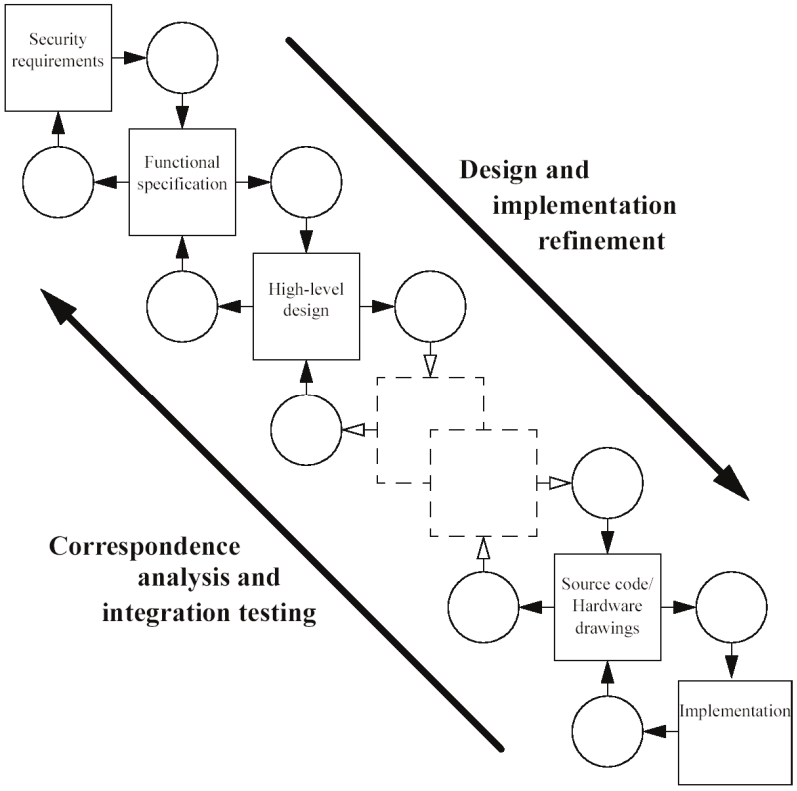


Figure 4 - TOE development model

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.

ISO/IEC 15408 does not mandate a specific set of design representations. ISO/IEC 15408 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).

ISO/IEC 15408 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 ISO/IEC 15408 assurance requirements.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

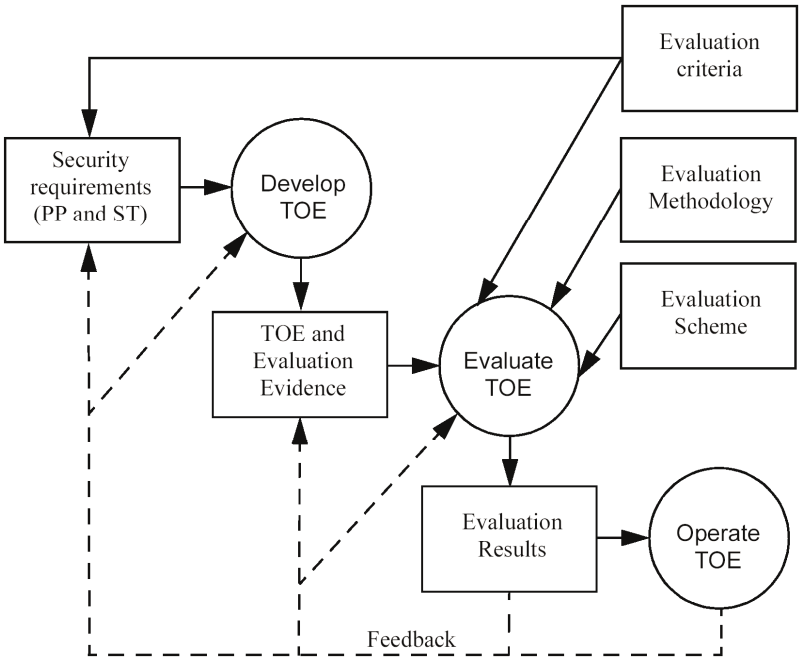


Figure 5 - TOE evaluation process

5.2.2 TOE evaluation

The TOE evaluation process as described in Figure 5 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 an 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 ISO/IEC 15408) 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.

5.2.3 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

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

only require that the needed updates are evaluated in order to regain confidence in the TOE. Detailed procedures for re-evaluation, including reuse of evaluation results, are outside the scope of ISO/IEC 15408.

5.3 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 ISO/IEC 15408 might be employed.

ISO/IEC 15408 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.

ISO/IEC 15408 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.

ISO/IEC 15408 layers the different levels of representation as described in Figure 6, 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.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

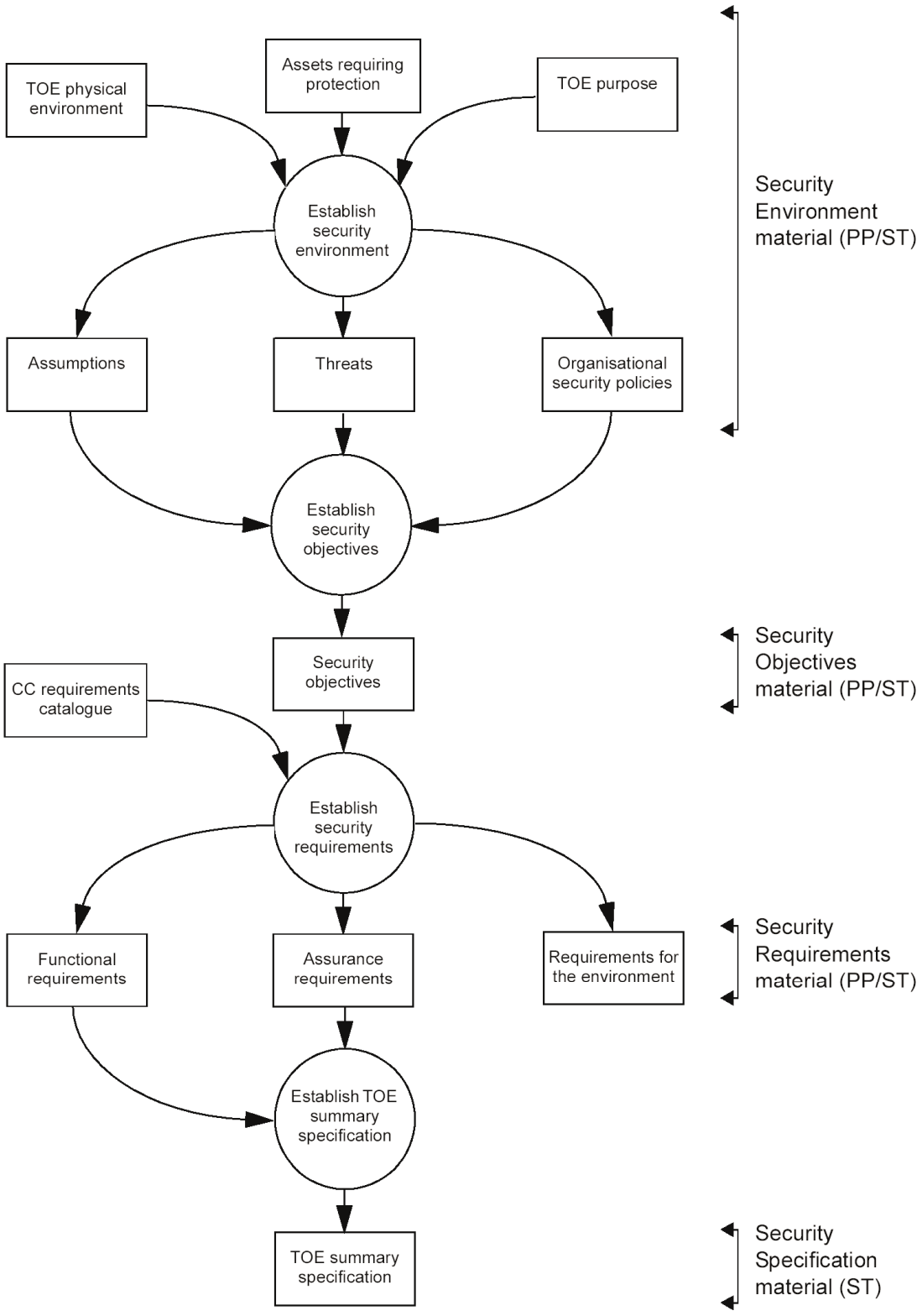


Figure 6 - Derivation of requirements and specifications

5.3.1 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.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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. ISO/IEC 15408 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.

5.3.2 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.

5.3.3 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.

ISO/IEC 15408 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. ISO/IEC 15408-2 defines the functional requirements. Examples of functional requirements include requirements for identification, authentication, security audit and non-repudiation of origin.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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. ISO/IEC 15408-3 defines the 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.

5.3.4 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.

5.3.5 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.

5.4 ISO/IEC 15408 descriptive material

ISO/IEC 15408 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. ISO/IEC 15408 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.

5.4.1 Expression of security requirements

ISO/IEC 15408 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 7.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

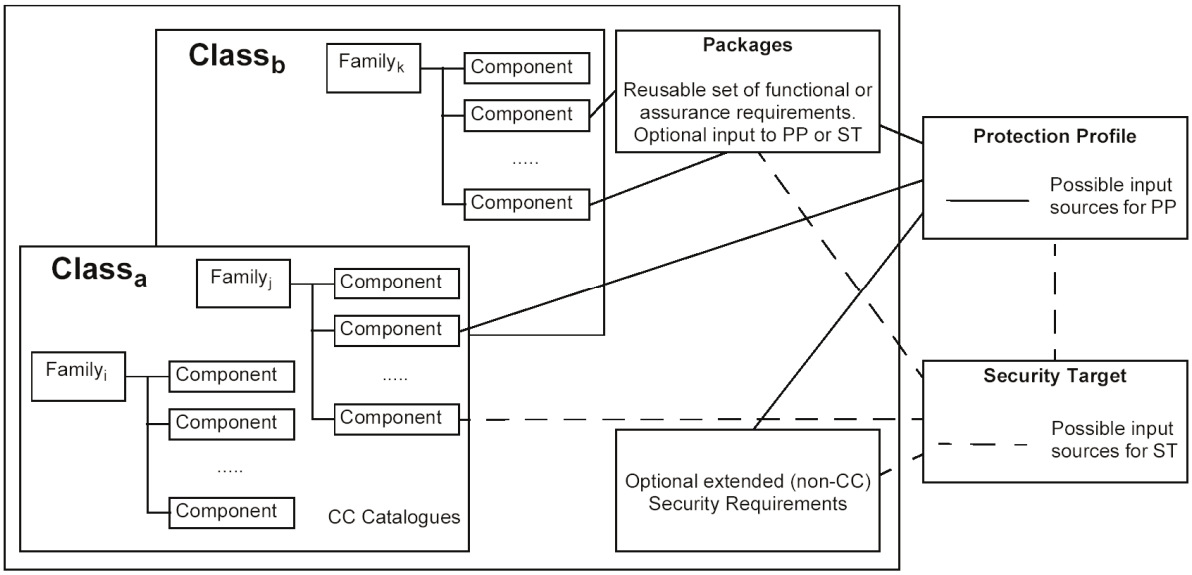


Figure 7 - Organisation and construction of requirements

The organisation of ISO/IEC 15408 security requirements into the hierarchy of class - family - component is provided to help consumers to locate specific security requirements.

ISO/IEC 15408 presents requirements for functional and assurance aspects in the same general style and uses the same organisation and terminology for each.

5.4.1.1 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.

5.4.1.2 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.

5.4.1.3 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 ISO/IEC 15408. 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.

5.4.1.3.1 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.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Component dependency descriptions are part of ISO/IEC 15408 component definitions. In order to ensure completeness of the TOE requirements, dependencies should be satisfied when incorporating components into PPs and STs where appropriate.

5.4.1.3.2 Permitted operations on components

ISO/IEC 15408 functional and assurance components may be used exactly as defined in ISO/IEC 15408, or they may be tailored through the use of permitted operations in order to meet a security objective. When an element within a component undergoes a refinement, the PP/ST author shall clearly identify that such a refinement has been performed. The PP/ST author must also be careful that the dependency needs of other requirements that depend on this requirement are satisfied. The permitted operations are selected from the following set:

a) Iteration: allows a component to be used more than once with varying operations;

b) Assignment: allows the specification of parameters;

c) Selection: allows the specification of one or more items from a list; and

d) Refinement: allows the addition of details.

5.4.1.3.2.1 Iteration

Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use of the same component to cover each aspect is permitted.

While iteration is referred to at the level of a requirement component, it is not always necessary to repeat the full text of each of the iterations of the component, if doing so would result in some elements within the component being repeated multiple times with no changes. It is permissible in the PP or ST to repeat only those requirement elements that are being changed each time, whether by refinement, or by the completion of assignment or selection operations. (See Refinement for further guidance on iterating refined requirements).

5.4.1.3.2.2 Assignment

Some components have elements that contain parameters that enable the PP/ST author to specify a set of values for incorporation into the PP or ST to meet a security objective. These elements clearly identify each parameter and constraint on values that may be assigned to that parameter.

Any aspect of an element whose acceptable values can be unambiguously described or enumerated can be represented by a parameter. The parameter may be an attribute or rule that narrows the requirement to a specific value or range of values. For instance, based on a security objective, an element within a component may state that a given operation should be performed a number of times. In this case, the assignment would provide the number, or range of numbers, to be used in the parameter.

5.4.1.3.2.3 Selection

This is the operation of picking one or more items from a list in order to narrow the scope of an element within a component.

5.4.1.3.2.4 Refinement

For all components, the PP/ST author is permitted to limit the set of acceptable implementations by specifying additional detail in order to meet a security objective. Refinement of an element within a component consists of adding these technical details.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In order for a change to a component to be considered a valid refinement, the change must satisfy all the following conditions:

a) A TOE meeting the refined requirement would also meet the original requirement, as interpreted in the context of the PP/ST;

b) In cases where a refined requirement is iterated, it is permissible that each iteration address only a subset of the scope of the requirement; however, the sum of the iterations must together meet the entire scope of the original requirement;

c) The refined requirement does not extend the scope of the original requirement; and

d) The refined requirement does not alter the list of dependences of the original requirement.

Some examples of valid refinements are:

a) Any change that is only editorial, such as changes to enhance the readability of a completed assignment or to address grammatical correctness.

b) A change that does not alter the scope of the requirement due to the context in which it is used in the PP/ST. For example, changing a requirement that stated "TOE users" to "TOE telnet users" would be a valid refinement where the only users of the TOE are telnet users.

c) A change that provides information on allowable approaches to implementation without extending the scope of the requirement. An example of a valid refinement is changing a requirement from "provide the capability to verify" to "provide the capability to verify by implementing cryptographic checksums". The change places restrictions on the nature of the mechanism to be used in implementing an existing requirement, and does not extend the scope of the original.

The ISO/IEC 15408-2 Annexes provide the guidance on the valid completion of selections and assignments. This guidance provides normative instructions on how to complete operations, and those instructions shall be followed unless the PP/ST author justify the deviation:

a) “None” is only available as a choice for the completion of a selection if explicitly provided.

   The lists provided for the completion of selections must be non-empty. If a “None” option is chosen, no additional selection options may be chosen. If “None” is not given as an option in a selection, it is permissible to combine the choices in a selection with “and”s and “or”s, unless the selection explicitly states “choose one of”.

   Selection operations may be combined by iteration where needed. In this case, the applicability of the option chosen for each iteration should not overlap the subject of the other iterated selection, since they are intended to be exclusive.

b) For the completion of assignments, ISO/IEC 15408-2 Annexes indicate when “None” would be a valid completion.

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.

5.4.1.4 Use of security requirements

ISO/IEC 15408 defines three types of requirement constructs: package, PP and ST. ISO/IEC 15408 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. ISO/IEC 15408 has been developed around the central notion of using wherever possible the security requirements components defined in ISO/IEC 15408, which represent a well-known and understood domain. Figure 8 shows the relationship between these different constructs.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

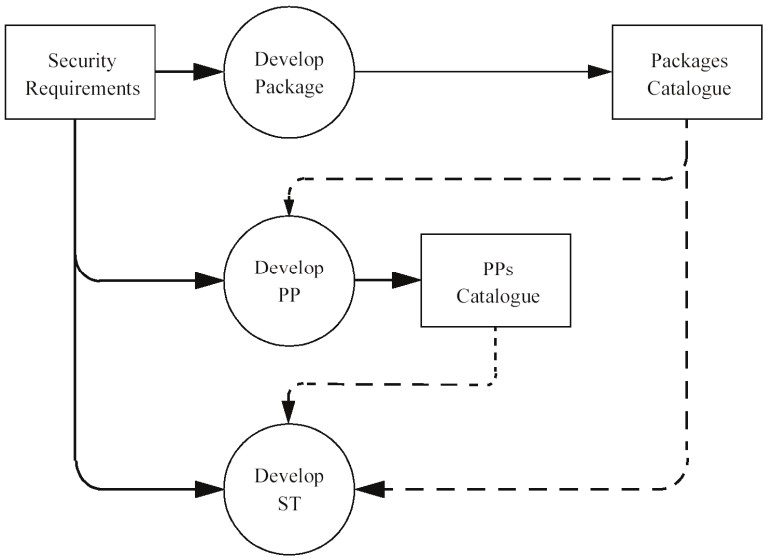


Figure 8 - Use of security requirements

5.4.1.4.1 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 ISO/IEC 15408-3. 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 ISO/IEC 15408.

5.4.1.4.2 Protection Profile

The PP contains a set of security requirements either from ISO/IEC 15408, 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.

5.4.1.4.3 Security Target

An ST contains a set of security requirements that may be made by reference to a PP, directly by reference to ISO/IEC 15408 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.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.4.1.5 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 ISO/IEC 15408-3. The TOE assurance requirements in a PP or ST should include an EAL from ISO/IEC 15408-3.

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 ISO/IEC 15408-2 or ISO/IEC 15408-3.

d) Extended requirements

Additional functional requirements not contained in ISO/IEC 15408-2 and/or additional assurance requirements not contained in ISO/IEC 15408-3 may be used in a PP or ST.

Existing requirements material from ISO/IEC 15408-2 and ISO/IEC 15408-3 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.

5.4.2 Types of evaluation

5.4.2.1 PP evaluation

The PP evaluation is carried out against the evaluation criteria for PPs contained in ISO/IEC 15408-3. 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.

5.4.2.2 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.

5.4.2.3 TOE evaluation

The TOE evaluation is carried out against the evaluation criteria contained in ISO/IEC 15408-3 using a substantially complete ST as the basis. A substantially complete ST reduces the risk of problems later on in the evaluation process and is where all subclauses have been completed to an extent acceptable by the evaluation scheme and for which no significant evaluation hurdles are foreseen. The result of a TOE evaluation is to demonstrate that the TOE meets the security requirements contained in the evaluated ST.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6 ISO/IEC 15408 requirements and evaluation results

6.1 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.

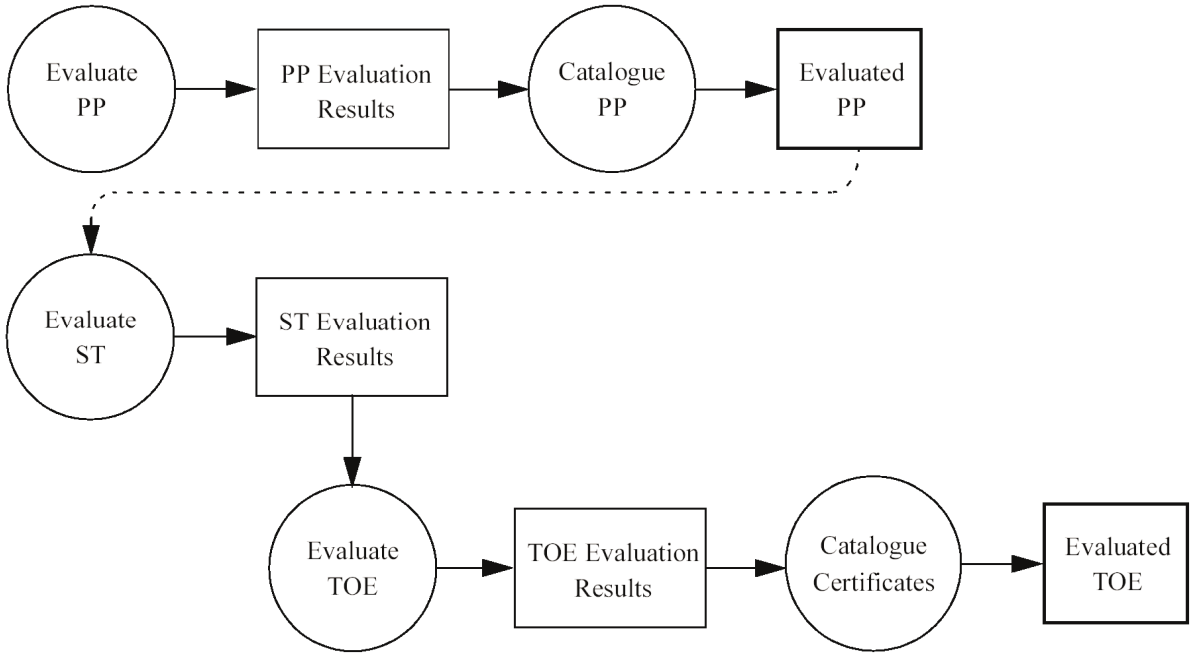


Figure 9 - Evaluation results

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 ISO/IEC 15408 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.

6.2 Requirements in PPs and STs

ISO/IEC 15408 defines a set of IT security criteria that can address the needs of many communities. ISO/IEC 15408 has been developed around the central notion that the use of the security functional components contained in ISO/IEC 15408-2, and the EALs and assurance components contained in ISO/IEC 15408-3, represents the preferred course of action for expression of TOE requirements in PPs and STs, as they represent a well-known and understood domain.

ISO/IEC 15408 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

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

detail and manner of expression of existing ISO/IEC 15408 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 ISO/IEC 15408-3, as appropriate.

6.2.1 PP evaluation results

ISO/IEC 15408 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.

6.3 Requirements in TOE

ISO/IEC 15408 contains the evaluation criteria that permit an evaluator to determine whether the TOE satisfies the security requirements expressed in the ST. By using ISO/IEC 15408 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 ISO/IEC 15408 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 ISO/IEC 15408 will be evaluatable against ISO/IEC 15408. 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 ISO/IEC 15408. ISO/IEC 15408 recognises the necessity to evaluate such a TOE but, as the additional requirements lie outside the known domain of applicability of ISO/IEC 15408, 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 ISO/IEC 15408. The use of ISO/IEC 15408 terms to describe the security of a TOE permits comparison of the security characteristics of TOEs in general.

6.3.1 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. The results of evaluation shall also include a “Conformance Result”.

6.4 Conformance results

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to ISO/IEC 15408-2 (functional requirements), ISO/IEC 15408-3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The conformance result consists of one of the following:

a) **ISO/IEC 15408-2 conformant** - A PP or TOE is ISO/IEC 15408-2 conformant if the functional requirements are based only upon functional components in ISO/IEC 15408-2.

b) **ISO/IEC 15408-2 extended** - A PP or TOE is ISO/IEC 15408-2 extended if the functional requirements include functional components not in ISO/IEC 15408-2.

plus one of the following:

a) **ISO/IEC 15408-3 conformant** - A PP or TOE is ISO/IEC 15408-3 conformant if the assurance requirements are based only upon assurance components in ISO/IEC 15408-3.

b) **ISO/IEC 15408-3 extended** - A PP or TOE is ISO/IEC 15408-3 extended if the assurance requirements include assurance requirements not in ISO/IEC 15408-3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

a) **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

b) **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

a) **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

6.5 Use of TOE evaluation results

IT products and systems differ in respect to the use of the results of the evaluation. Figure 10 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.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

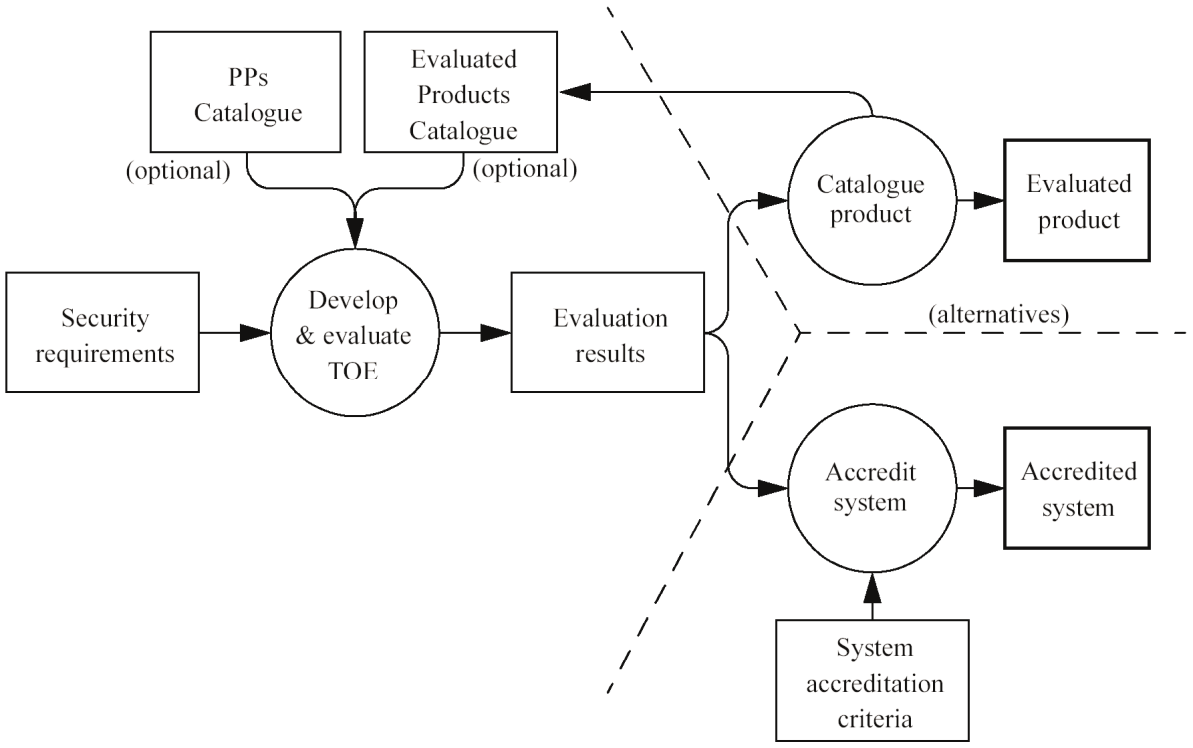


Figure 10 - Use of TOE evaluation results

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. ISO/IEC 15408 evaluation results may then be considered by the accreditor when applying organisation specific accreditation criteria that call for ISO/IEC 15408 evaluation. ISO/IEC 15408 evaluation results are one of the inputs to an accreditation process that leads to a decision on accepting the risk of system operation.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(normative)

Specification of Protection Profiles

A.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 8 of ISO/IEC 15408-3, contains these requirements in the form of assurance components to be used for evaluation of the PP.

A.2 Content of Protection Profile

A.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 A.1, which should be used when constructing the structural outline of the PP document.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

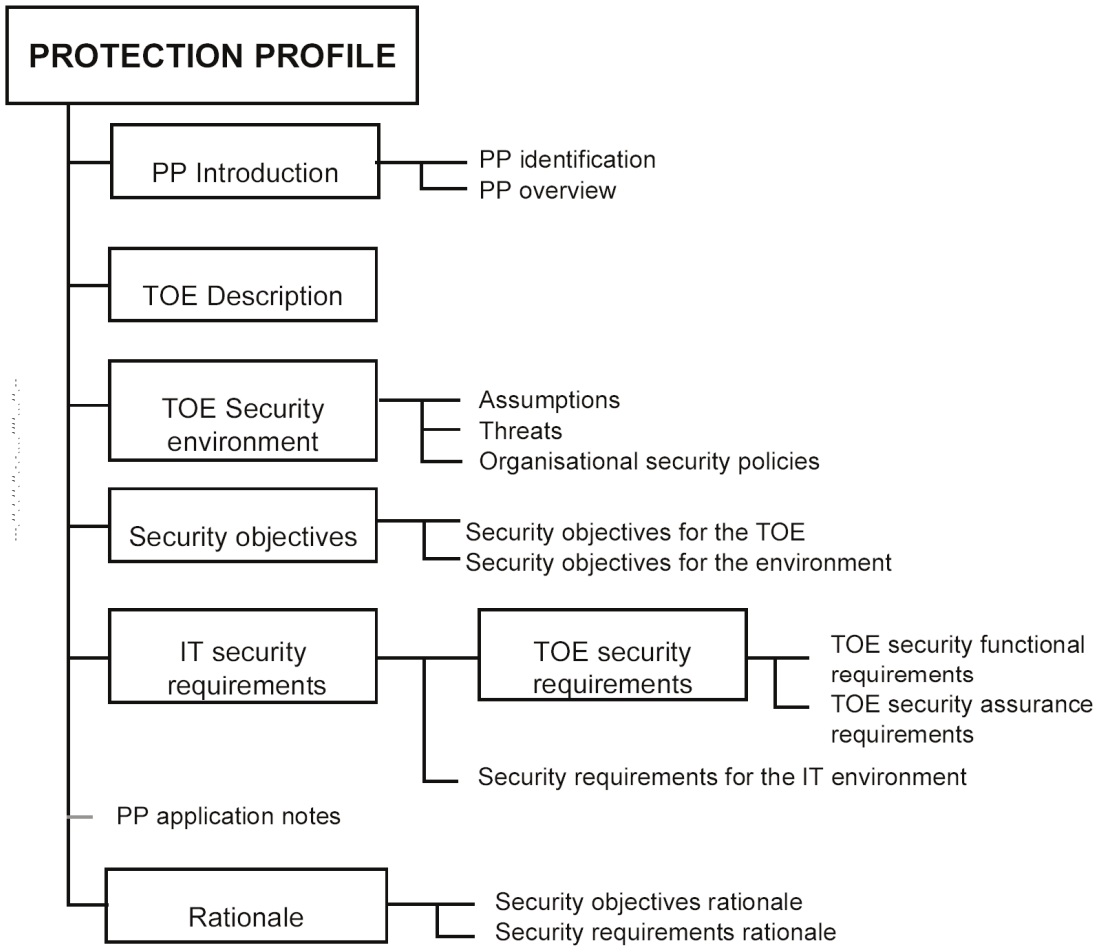


Figure A.1 - Protection Profile content

A.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.

A.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.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.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.

A.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. A threat may be countered by one or more objectives for the TOE, one or more objectives for the environment, or a combination of these. 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.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.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) 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 ISO/IEC 15408-2 component to cover each aspect is possible. 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 ISO/IEC 15408-2 where applicable.

      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 ISO/IEC 15408-3 assurance components. The PP may also extend the EAL by explicitly stating additional assurance requirements not taken from ISO/IEC 15408-3.

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. The requirements in this part of the PP may be drawn from ISO/IEC 15408-2 and ISO/IEC 15408-3 and, if so, should be rephrased to clearly indicate that the IT environment, not the TOE, must meet the requirement. Such rephrasing is a special case of refinement and not subject to the assessment requirements associated with modified ISO/IEC 15408 components. If the TOE has no asserted dependencies on the IT environment, this part of the PP may be omitted.

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 ISO/IEC 15408-2 or ISO/IEC 15408-3 where applicable. Should none of ISO/IEC 15408-2 or ISO/IEC 15408-3 requirements components be readily applicable to all or part of the security requirements, the PP may state those requirements explicitly without reference to ISO/IEC 15408.

   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 ISO/IEC 15408 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.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

A.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.

A.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.

b) The **security requirements rationale** shall demonstrate that the set of security requirements (TOE and environment) is suitable to meet and traceable to the security objectives. The following shall be demonstrated:

   1) that the combination of the individual functional and assurance requirements components for the TOE and its IT environment together meet the stated security objectives;

   2) that the set of security requirements together forms a mutually supportive and internally consistent whole;

   3) that the choice of security requirements is justified. Any of the following conditions shall be specifically justified:

      i) choice of requirements not contained in ISO/IEC 15408-2 or ISO/IEC 15408-3;

      ii) choice of assurance requirements not including an EAL; and

      iii) non-satisfaction of dependencies;

   4) that the selected strength of function level for the PP, together with any explicit strength of function claim, is consistent with the security objectives for the TOE.

This potentially bulky material may be distributed separately as it may not be appropriate or useful to all PP users.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(normative)

Specification of Security Targets

B.1 Overview

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

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

The ST may incorporate the requirements of, or claim conformance to, one or more PPs. The impact of such a PP conformance claim is not considered when initially defining the required ST content in subclause B.2. Subclause B.2.8 addresses the impact of a PP conformance claim on the required ST content.

This annex contains the requirements for the ST in descriptive form. The assurance class ASE, contained in clause 9 of ISO/IEC 15408-3, contains these requirements in the form of assurance components to be used for evaluation of the ST.

B.2 Content of Security Target

B.2.1 Content and presentation

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

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

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

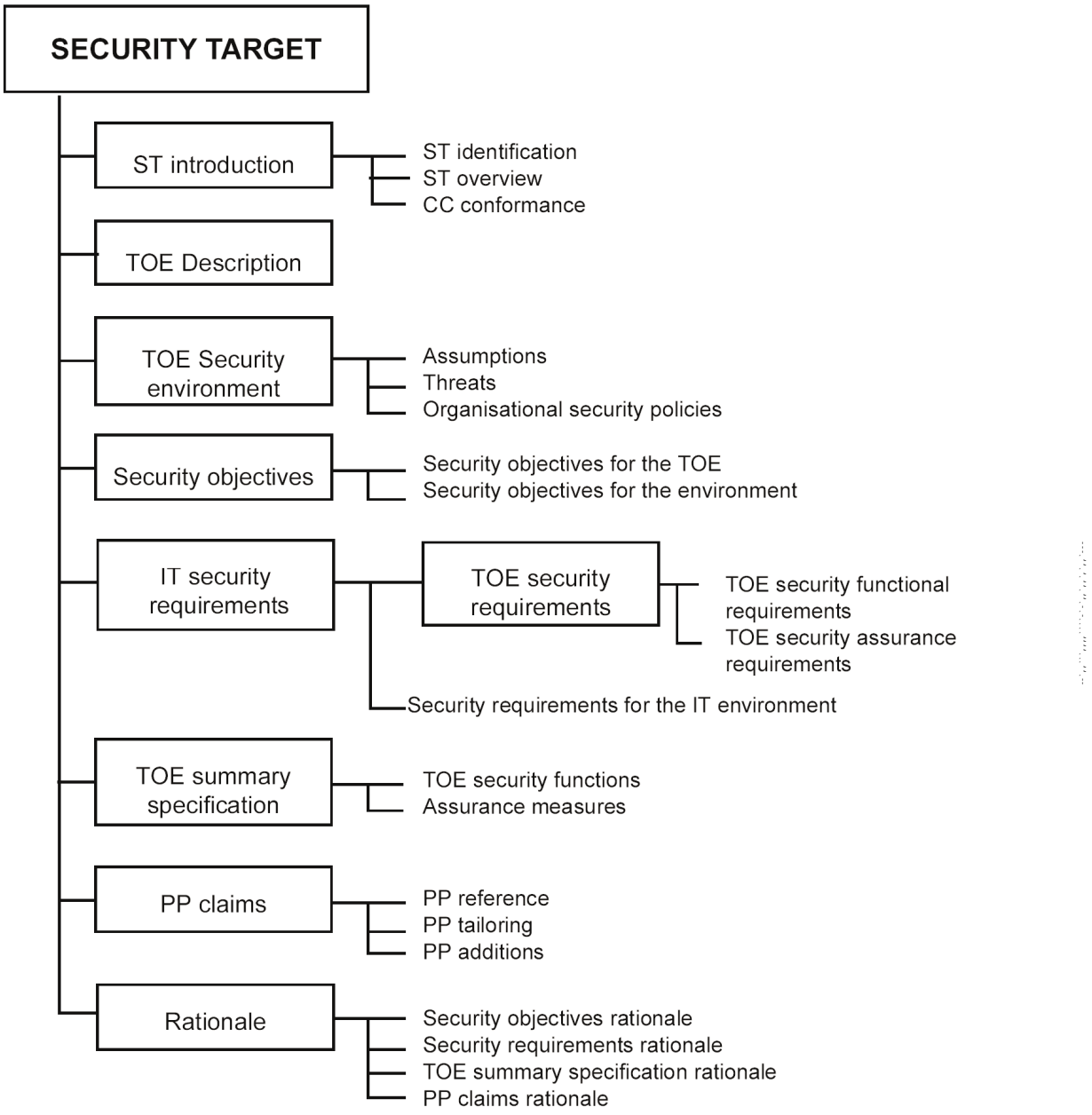


Figure B.1 - Security Target content

B.2.2 ST introduction

The ST introduction shall contain the following document management and overview information:

a) The **ST identification** shall provide the labelling and descriptive information necessary to control and identify the ST and the TOE to which it refers.

b) The **ST overview** shall summarise the ST in narrative form. The overview should be sufficiently detailed for a potential consumer of the TOE to determine whether the TOE is of interest. The overview should also be usable as a stand alone abstract for incorporation in evaluated products lists.

c) A **ISO/IEC 15408 conformance claim** shall state any evaluatable claim of ISO/IEC 15408 conformance for the TOE, as identified in subclause 6.4 of this part of ISO/IEC 15408.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.2.3 TOE description

This part of the ST shall describe the TOE as an aid to the understanding of its security requirements, and shall address the product or system type. The scope and boundaries of the TOE shall be described in general terms both in a physical way (hardware and/or software components/modules) and a logical way (IT and security features offered by 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. If the TOE is a product or system whose primary function is security, this part of the ST 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. A threat may be countered by one or more objectives for the TOE, one or more objectives for the environment, or a combination of these. 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.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 ST 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) 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 ISO/IEC 15408-2 component to cover each aspect is possible. 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 ISO/IEC 15408-2 where applicable.

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 ISO/IEC 15408-3 assurance components. The ST may also extend the EAL by explicitly stating additional assurance requirements not taken from ISO/IEC 15408-3.

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. The requirements in this part of the ST may be drawn from ISO/IEC 15408-2 and ISO/IEC 15408-3 and if so should be rephrased to clearly indicate that the IT environment, not the TOE, must meet the requirement. Such rephrasing is a special case of refinement and not subject to the assessment requirements associated with modified ISO/IEC 15408 components. If the TOE has no asserted dependencies on the IT environment, this part of the ST may be omitted.

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 ISO/IEC 15408-2 or ISO/IEC 15408-3 where applicable. Should none of ISO/IEC 15408-2 or ISO/IEC 15408-3 requirements components be readily applicable to all or part of the security requirements, the ST may state those requirements explicitly without reference to ISO/IEC 15408.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 ISO/IEC 15408 functional or assurance requirements shall be used as a model.

3) Any required operations shall be used to amplify the requirements to the level of detail necessary to demonstrate that the security objectives are met. All specified operations on the requirements components shall be performed.

4) 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 TOE summary specification

The TOE summary specification shall define the instantiation of the security requirements for the TOE. This specification shall provide a description of the security functions and assurance measures of the TOE that meet the TOE security requirements. Note that the functional information provided as part of the TOE summary specification could be identical in some cases to the information to be provided for the TOE as part of the ADV_FSP requirements.

The TOE summary specification contains the following:

a) The **statement of TOE security functions** shall cover the IT security functions and shall specify how these functions satisfy the TOE security functional requirements. This statement shall include a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met. Each security function shall contribute to the satisfaction of at least one TOE security functional requirement.

   1) The IT security functions shall be defined in an informal style to a level of detail necessary for understanding their intent.

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

   3) When AVA_SOF.1 is included in the TOE assurance requirements, all IT security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function), shall be identified. The likelihood to breach the mechanisms of such functions by deliberate or accidental attack is of relevance to the security of the TOE. A strength of TOE security function claim shall be provided for each of these functions. The strength of each identified function shall be determined and claimed as either SOF-basic, SOF-medium or SOF-high, or as the optionally defined specific metric.

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

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

B.2.8 PP claims

The ST may optionally make a claim that the TOE conforms with the requirements of one (or possibly more than one) PP. For any PP conformance claims made, the ST shall include a **PP claims** statement that contains the explanation, justification, and any other supporting material necessary to substantiate the claims.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The content and presentation of the ST statements of TOE objectives and requirements could be affected by PP claims made for the TOE. The impact on the ST can be summarised by considering the following cases for each PP claimed:

a) If there is no claim of PP compliance made, then the full presentation of the TOE objectives and requirements should be made as described in this annex. No PP claims are included.

b) If the ST claims only compliance with the requirements of a PP without need for further qualification, then reference to the PP is sufficient to define and justify the TOE objectives and requirements. Restatement of the PP contents is unnecessary.

c) If the ST claims compliance with the requirements of a PP, and that PP requires further qualification, then the ST shall show that the PP requirements for qualification have been met. Such a situation would typically arise where the PP contains uncompleted operations. In such a situation, the ST may refer to the specific requirements but complete the operations within the ST. In some circumstances, where the requirements to complete operations are substantial, it may be preferable to restate the PP contents within the ST as an aid to clarity.

d) If the ST claims compliance with the requirements of a PP but extends that PP by the addition of further objectives and requirements, then the ST shall define the additions, whereas a PP reference may be sufficient to define the PP objectives and requirements. In some circumstances, where the additions are substantial, it may be preferable to restate the PP contents within the ST as an aid to clarity.

e) The case where an ST claims to be partially conformant to a PP is not admissible for ISO/IEC 15408 evaluation.

ISO/IEC 15408 is not prescriptive with respect to the choice of restating or referencing PP objectives and requirements. The fundamental requirement is that the ST content be complete, clear, and unambiguous such that evaluation of the ST is possible, the ST is an acceptable basis for the TOE evaluation, and the traceability to any claimed PP is clear.

If any PP conformance claim is made, the PP claims statement shall contain the following material for each PP claimed:

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

b) The **PP tailoring** statement shall identify the IT security requirements statements that satisfy the permitted operations of the PP or otherwise further qualify the PP requirements.

c) The **PP additions** statement shall identify the TOE objectives and requirements statements that are additional to the PP objectives and requirements.

B.2.9 Application Notes

This optional part of an ST may contain additional information considered relevant or useful for the understanding of the ST. Note that if the ST claims compliance with the requirements of a PP, it may be appropriate that certain information contained in a potential application notes subclause of the PP is incorporated into other subclauses of the ST. For example, information concerning the construction of the TOE is probably more appropriately presented in the TOE summary specification or the ST rationale than in a separate application notes subclause. To ease evaluation of the ST, and given that the structure for the presentation of an ST outlined in this annex is not normative, an application note containing evaluation relevant material should be a part of the subclause of the ST that provides the evidence for that evaluation aspect.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.2.10 Rationale

This part of the ST presents the evidence used in the ST evaluation. This evidence supports the claims that the ST is a complete and cohesive set of requirements, that a conformant TOE would provide an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements. The rationale also demonstrates that any PP conformance claims are valid. 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.

b) The **security requirements rationale** shall demonstrate that the set of security requirements (TOE and environment) is suitable to meet and traceable to the security objectives. The following shall be demonstrated:

   1) that the combination of the individual functional and assurance requirements components for the TOE and its IT environment together meet the stated security objectives;

   2) that the set of security requirements together forms a mutually supportive and internally consistent whole;

   3) that the choice of security requirements is justified. Any of the following conditions shall be specifically justified:

      i) choice of requirements not contained in ISO/IEC 15408-2 or ISO/IEC 15408-3;

      ii) choice of assurance requirements not including an EAL; and

      iii) non-satisfaction of dependencies;

   4) that the selected strength of function level for the ST, together with any explicit strength of function claim, is consistent with the security objectives for the TOE.

c) The **TOE summary specification rationale** shall show that the TOE security functions and assurance measures are suitable to meet the TOE security requirements. The following shall be demonstrated:

   1) that the combination of specified TOE IT security functions work together so as to satisfy the TOE security functional requirements;

   2) that the strength of TOE function claims made are valid, or that assertions that such claims are unnecessary are valid.

   3) that the claim is justified that the stated assurance measures are compliant with the assurance requirements.

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

d) The **PP claims rationale** statement shall explain any difference between the ST security objectives and requirements and those of any PP to which conformance is claimed. This part of the ST may be omitted if no claims of PP conformance are made or if ST security objectives and requirements are identical to those of any claimed PP.

This potentially bulky material may be distributed separately as it may not be appropriate or useful to all ST users.

© ISO/IEC 2005 - All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] Bell, D. E. and LaPadula, L. J., Secure Computer Systems: Unified Exposition and MULTICS Interpretation, Revision 1, US Air Force ESD-TR-75-306, MITRE Corporation MTR-2997, Bedford MA, March 1976.

[2] Biba, K. J., Integrity Considerations for Secure Computer Systems, ESD-TR-372, ESD/AFSC, Hanscom AFB, Bedford MA., April 1977.

[3] Canadian Trusted Computer Product Evaluation Criteria, Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993.

[4] Federal Criteria for Information Technology Security, Draft Version 1.0, (Volumes I and II), jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993.

[5] Goguen, J. A. and Meseguer, J., "Security Policies and Security Models," 1982 Symposium on Security and Privacy, pp.11-20, IEEE, April 1982.

[6] Goguen, J. A. and Meseguer, J., "Unwinding and Inference Control," 1984 Symposium on Security and Privacy, pp.75-85, IEEE, May 1984.

[7] Information Technology Security Evaluation Criteria, Version 1.2, Office for Official Publications of the European Communities, June 1991.

[8] ISO/IEC 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture.*

[9] ISO/IEC 15292:2001, *Information technology — Security techniques — Protection Profile registration procedures.*

[10] Trusted Computer Systems Evaluation Criteria, US DoD 5200.28-STD, December 1985.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 41 pages

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale