INTERNATIONAL STANDARD

ISO/IEC 15408-1

First edition
1999-12-01

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

Part 1: Introduction and general model

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

Partie 1: Introduction et modèle général

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

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Contents

1 Scope . . . 1

2 Definitions . . . 3
2.1 Common abbreviations . . . 3
2.2 Scope of glossary . . . 3
2.3 Glossary . . . 4

3 Overview . . . 9
3.1 Introduction . . . 9
3.2 Target audience of the CC . . . 9
3.2.1 Consumers . . . 9
3.2.2 Developers . . . 10
3.2.3 Evaluators . . . 10
3.2.4 Others . . . 10
3.3 Evaluation context . . . 11
3.4 Organisation of Common Criteria . . . 12

4 General model . . . 13
4.1 Security context . . . 13
4.1.1 General security context . . . 13
4.1.2 Information technology security context . . . 15
4.2 Common Criteria approach . . . 15
4.2.1 Development . . . 16
4.2.2 TOE evaluation . . . 18
4.2.3 Operation . . . 18
4.3 Security concepts . . . 18
4.3.1 Security environment . . . 20
4.3.2 Security objectives . . . 21
4.3.3 IT security requirements . . . 22
4.3.4 TOE summary specification . . . 23
4.3.5 TOE implementation . . . 23
4.4 CC descriptive material . . . 23
4.4.1 Expression of security requirements . . . 23
4.4.2 Use of security requirements . . . 25
4.4.3 Sources of security requirements . . . 27
4.5 Types of evaluation . . . 28
4.5.1 PP evaluation . . . 28
4.5.2 ST evaluation . . . 28

4.5.3 TOE evaluation 28
4.6 Assurance maintenance 28

5 Common Criteria requirements and evaluation results 29
5.1 Introduction 29
5.2 Requirements in PPs and STs 30
5.2.1 PP evaluation results 30
5.3 Requirements in TOE 30
5.3.1 TOE evaluation results 31
5.4 Caveats on evaluation results 31
5.5 Use of TOE evaluation results 32

Annex A The Common Criteria project (informative) 33
A.1 Background to the Common Criteria project 33
A.2 Development of the Common Criteria 33
A.3 Common Criteria project sponsoring organisations 34

Annex B Specification of Protection Profiles 37
B.1 Overview 37
B.2 Content of Protection Profile 37
B.2.1 Content and presentation 37
B.2.2 PP introduction 37
B.2.3 TOE description 38
B.2.4 TOE security environment 38
B.2.5 Security objectives 39
B.2.6 IT security requirements 40
B.2.7 Application notes 41
B.2.8 Rationale 41

Annex C Specification of Security Targets 43
C.1 Overview 43
C.2 Content of Security Target 43
C.2.1 Content and presentation 43
C.2.2 ST introduction 43
C.2.3 TOE description 45
C.2.4 TOE security environment 45
C.2.5 Security objectives 46
C.2.6 IT security requirements 46
C.2.7 TOE summary specification 47
C.2.8 PP claims 48
C.2.9 Rationale 49

Annex D Bibliography (informative) 53

List of Figures

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

List of Tables

Table 3.1 - Roadmap to the Common Criteria 12

Foreword

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

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

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

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

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

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

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

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

INTERNATIONAL STANDARD © ISO/IEC **ISO/IEC 15408-1:1999(E)**

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

Part 1:
Introduction and general model

1 Scope

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

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

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

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

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

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

a) The CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security measures. However, it is recognised that a significant part of the security of a TOE can often be achieved through administrative measures such as organisational, personnel, physical, and procedural controls. Administrative security measures in the operating environment of the TOE are treated as secure usage assumptions where these have an impact on the ability of the IT security measures to counter the identified threats.

b) The evaluation of technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area. In particular, the CC addresses some aspects of physical protection of the TOE.

c) The CC addresses neither the evaluation methodology nor the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that the CC will be used for evaluation purposes in the context of such a framework and such a methodology.

d) The procedures for use of evaluation results in product or system accreditation are outside the scope of the CC. Product or system accreditation is the administrative process whereby authority is granted for the operation of an IT product or system in its full operational environment. Evaluation focuses on the IT security parts of the product or system and those parts of the operational environment that may directly affect the secure use of IT elements. The results of the evaluation process are consequently a valuable input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related product or system security properties and their relationship to the IT security parts, accreditors should make separate provision for those aspects.

e) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. Should independent assessment of mathematical properties of cryptography embedded in a TOE be required, the evaluation scheme under which the CC is applied must make provision for such assessments.

2 Definitions

2.1 Common abbreviations

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

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

2.2 Scope of glossary

This subclause 2.2 contains only those terms which are used in a specialised way throughout the CC. The majority of terms in the CC are used either according to their accepted dictionary definitions or according to commonly accepted definitions that may be found in ISO security glossaries or other well-known collections of security terms. Some combinations of common terms used in the CC, while not meriting glossary definition, are explained for clarity in the context where they are used. Explanations of the use of terms and concepts used in a specialised way in ISO/IEC 15408-2 and ISO/IEC 15408-3 can be found in their respective “paradigm” subclauses.

2.3 Glossary

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

Assignment — The specification of an identified parameter in a component.

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

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

Augmentation — The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package.

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

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

Class — A grouping of families that share a common focus.

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

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

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

Element — An indivisible security requirement.

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

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

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

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

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

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

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

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

Human user — Any person who interacts with the TOE.

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

Informal — Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

Refinement — The addition of details to a component.

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

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

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

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

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

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

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

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

Semiformal — Expressed in a restricted syntax language with defined semantics.

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

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

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

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

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

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

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

TOE resource — Anything useable or consumable in the TOE.

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

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

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

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

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

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

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

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

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

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

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