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 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

Contents

Page

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;

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.

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.

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.

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.

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.

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.

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.

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.

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