INTERNATIONAL STANDARD

ISO/IEC 15408-1

Third edition
2009-12-15

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 15408-1:2009(E)

COPYRIGHT PROTECTED DOCUMENT

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 part of ISO/IEC 15408 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. The common XML source for both publications can be found at http://www.oc.ccn.cni.es/xml

This third edition cancels and replaces the second edition (ISO/IEC 15408-1:2005), 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 components*

— *Part 3: Security assurance components*

Introduction

This part of ISO/IEC 15408 permits comparability between the results of independent security evaluations. ISO/IEC 15408 does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

ISO/IEC 15408 is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

ISO/IEC 15408 is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore users of this International Standard are cautioned to exercise care that this flexibility is not misused. For example, using ISO/IEC 15408 in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, may result in meaningless evaluation results.

Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties and methods to determine that an evaluation will provide meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs.

ISO/IEC 15408 addresses protection of assets 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 is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. Apart from IT security, ISO/IEC 15408 may be applied in other areas of IT, but makes no claim of applicability in these areas.

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 functionality. However, it is recognised that significant security can often be achieved through or supported by administrative measures such as organizational, personnel, physical, and procedural controls.

b) The evaluation of some 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.

c) ISO/IEC 15408 does not address the evaluation methodology under which the criteria should be applied. This methodology is given in ISO/IEC 18045.

d) ISO/IEC 15408 does not address 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.

e) The procedures for use of evaluation results in accreditation are outside the scope of ISO/IEC 15408. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the

evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors should make separate provisions for those aspects.

f) 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 be required, the evaluation scheme under which ISO/IEC 15408 is applied must make provision for such assessments.

ISO terminology, such as “can”, “informative”, “may”, “normative”, “shall” and “should” used throughout the document are defined in the ISO/IEC Directives, Part 2. Note that the term “should” has an additional meaning applicable when using this International Standard. See the note below. The following definition is given for the use of “should” in ISO/IEC 15408.

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)

NOTE 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.

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

Part 1:
Introduction and general model

1 Scope

This part of ISO/IEC 15408 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the International Standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of the standard; defines the terms and abbreviations to be used in all parts of the International Standard; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations.

The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. This part of ISO/IEC 15408 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation methodology is given in ISO/IEC 18045 and the scope of evaluation schemes is provided.

2 Normative references

The following referenced documents are indispensable for the application of this part of ISO/IEC 15408. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

3 Terms and definitions

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

NOTE This clause contains only those terms which are used in a specialized way throughout ISO/IEC 15408. Some combinations of common terms used in ISO/IEC 15408, while not meriting inclusion in this clause, are explained for clarity in the context where they are used.

3.1 Terms and definitions common in ISO/IEC 15408

3.1.1
adverse actions
actions performed by a threat agent on an asset

3.1.2
assets
entities that the owner of the TOE presumably places value upon

3.1.3
assignment
specification of an identified parameter in a component (of ISO/IEC 15408) or requirement

3.1.4
assurance
grounds for confidence that a TOE meets the SFRs

3.1.5
attack potential
measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation

3.1.6
augmentation
addition of one or more requirement(s) to a package

3.1.7
authentication data
information used to verify the claimed identity of a user

3.1.8
authorised user
TOE user who may, in accordance with the SFRs, perform an operation

3.1.9
class
set of ISO/IEC 15408 families that share a common focus

3.1.10
coherent
logically ordered and having discernible meaning

NOTE For documentation, this addresses both the actual text and the structure of the document, in terms of whether it is understandable by its target audience.

3.1.11
complete
property where all necessary parts of an entity have been provided

NOTE In terms of documentation, this means that all relevant information is covered in the documentation, at such a level of detail that no further explanation is required at that level of abstraction.

3.1.12
component
smallest selectable set of elements on which requirements may be based

3.1.13
composed assurance package
assurance package consisting of requirements drawn from ISO/IEC 15408-3 (predominately from the ACO class), representing a point on ISO/IEC 15408 predefined composition assurance scale

3.1.14
confirm
declare that something has been reviewed in detail with an independent determination of sufficiency

NOTE The level of rigour required depends on the nature of the subject matter. This term is only applied to evaluator actions.

3.1.15
connectivity
property of the TOE allowing interaction with IT entities external to the TOE

NOTE This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

3.1.16
consistent
relationship between two or more entities such that there are no apparent contradictions between these entities

3.1.17
counter, verb
meet an attack where the impact of a particular threat is mitigated but not necessarily eradicated

3.1.18
demonstrable conformance
relation between an ST and a PP, where the ST provides a solution which solves the generic security problem in the PP

NOTE The PP and the ST may contain entirely different statements that discuss different entities, use different concepts etc. Demonstrable conformance is also suitable for a TOE type where several similar PPs already exist, thus allowing the ST author to claim conformance to these PPs simultaneously, thereby saving work.

3.1.19
demonstrate
provide a conclusion gained by an analysis which is less rigorous than a “proof”

3.1.20
dependency
relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

3.1.21
describe
provide specific details of an entity

3.1.22
determine
affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion

NOTE The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms “confirm” or “verify” which imply that an analysis has already been performed which needs to be reviewed

3.1.23
development environment
environment in which the TOE is developed

3.1.24
element
indivisible statement of a security need

3.1.25
ensure
guarantee a strong causal relationship between an action and its consequences

NOTE When this term is preceded by the word “help” it indicates that the consequence is not fully certain, on the basis of that action alone.

3.1.26
evaluation
assessment of a PP, an ST or a TOE, against defined criteria

3.1.27
evaluation assurance level
set of assurance requirements drawn from ISO/IEC 15408-3, representing a point on the ISO/IEC 15408 predefined assurance scale, that form an assurance package

3.1.28
evaluation authority
body that sets the standards and monitors the quality of evaluations conducted by bodies within a specific community and implements ISO/IEC 15408 for that community by means of an evaluation scheme

3.1.29
evaluation scheme
administrative and regulatory framework under which ISO/IEC 15408 is applied by an evaluation authority within a specific community

3.1.30
exhaustive
characteristic of a methodical approach taken to perform an analysis or activity according to an unambiguous plan

NOTE This term is used in ISO/IEC 15408 with respect to conducting an analysis or other activity. It is related to “systematic” but is considerably stronger, in that it indicates not only that a methodical approach has been taken to perform the analysis or activity according to an unambiguous plan, but that the plan that was followed is sufficient to ensure that all possible avenues have been exercised.

3.1.31
explain
give argument accounting for the reason for taking a course of action

NOTE This term differs from both “describe” and “demonstrate”. It is intended to answer the question “Why?” without actually attempting to argue that the course of action that was taken was necessarily optimal.

3.1.32
extension
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

3.1.33
external entity
human or IT entity possibly interacting with the TOE from outside of the TOE boundary

NOTE An external entity can also be referred to as a user.

3.1.34
family
set of components that share a similar goal but differ in emphasis or rigour

3.1.35
formal
expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts

3.1.36
guidance documentation
documentation that describes the delivery, preparation, operation, management and/or use of the TOE

3.1.37
identity
representation uniquely identifying entities (e.g. a user, a process or a disk) within the context of the TOE

NOTE An example of such a representation is a string. For a human user, the representation can be the full or abbreviated name or a (still unique) pseudonym.

3.1.38
informal
expressed in natural language

3.1.39
inter TSF transfers
communicating data between the TOE and the security functionality of other trusted IT products

3.1.40
internal communication channel
communication channel between separated parts of the TOE

3.1.41
internal TOE transfer
communicating data between separated parts of the TOE

3.1.42
internally consistent
no apparent contradictions exist between any aspects of an entity

NOTE In terms of documentation, this means that there can be no statements within the documentation that can be taken to contradict each other.

3.1.43
iteration
use of the same component to express two or more distinct requirements

3.1.44
justification
analysis leading to a conclusion

NOTE "Justification" is more rigorous than a demonstration. This term requires significant rigour in terms of very carefully and thoroughly explaining every step of a logical argument.

3.1.45
object
passive entity in the TOE, that contains or receives information, and upon which subjects perform operations

3.1.46
operation
⟨on a component of ISO/IEC 15408⟩ modification or repetition of a component

NOTE Allowed operations on components are assignment, iteration, refinement and selection.

3.1.47
operation
⟨on an object⟩ specific type of action performed by a subject on an object

3.1.48
operational environment
environment in which the TOE is operated

3.1.49
organizational security policy
set of security rules, procedures, or guidelines for an organization

NOTE A policy may pertain to a specific operational environment.

3.1.50
package
named set of either security functional or security assurance requirements

NOTE An example of a package is “EAL 3”.

3.1.51
Protection Profile evaluation
assessment of a PP against defined criteria

3.1.52
Protection Profile
implementation-independent statement of security needs for a TOE type

3.1.53
prove
show correspondence by formal analysis in its mathematical sense

NOTE It is completely rigorous in all ways. Typically, “prove” is used when there is a desire to show correspondence between two TSF representations at a high level of rigour.

3.1.54
refinement
addition of details to a component

3.1.55
role
predefined set of rules establishing the allowed interactions between a user and the TOE

3.1.56
secret
information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP

3.1.57
secure state
state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs

3.1.58
security attribute
property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs

3.1.59
security function policy
set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs

3.1.60
security objective
statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions

3.1.61
security problem
statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address

NOTE This statement consists of a combination of:

— threats to be countered by the TOE,

— the OSPs enforced by the TOE, and

— the assumptions that are upheld for the TOE and its operational environment.

3.1.62
security requirement
requirement, stated in a standardized language, which is meant to contribute to achieving the security objectives for a TOE

3.1.63
Security Target
ST
implementation-dependent statement of security needs for a specific identified TOE

3.1.64
selection
specification of one or more items from a list in a component

3.1.65
semiformal
expressed in a restricted syntax language with defined semantics

3.1.66
specify
provide specific details about an entity in a rigorous and precise manner

3.1.67
strict conformance
hierarchical relationship between a PP and an ST where all the requirements in the PP also exist in the ST

NOTE This relation can be roughly defined as “the ST shall contain all statements that are in the PP, but may contain more”. Strict conformance is expected to be used for stringent requirements that are to be adhered to in a single manner.

3.1.68
ST evaluation
assessment of an ST against defined criteria