

---

---

**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*

**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.

This document is a preview generated by EVS

© 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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# 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

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

This document is a preview generated by EVS

## 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.

This document is a preview generated by EVS

## 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.

This document is a preview generated by EVS



# 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.