INTERNATIONAL STANDARD

ISO/IEC 18045

Second edition
2008-08-15

Information technology — Security techniques — Methodology for IT security evaluation

Technologies de l'information — Techniques de sécurité — Méthodologie pour l'évaluation de sécurité TI

Reference number
ISO/IEC 18045:2008(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 18045 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*. The identical text of ISO/IEC 18045 is published by the Common Criteria Project Sponsoring Organisations as *Common Methodology for Information Technology Security Evaluation*. The common XML source for both publications can be found at http://www.oc.ccn.cni.es/xml.

This second edition cancels and replaces the first edition (ISO/IEC 18045:2005), which has been technically revised.

Legal Notice

The governmental organizations listed below contributed to the development of this version of the Common Methodology for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Methodology for Information Technology Security Evaluations, version 3.1 (called CEM 3.1), they hereby grant non-exclusive license to ISO/IEC to use CEM 3.1 in the continued development/maintenance of the ISO/IEC 18045 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CEM 3.1 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

The target audience for this International Standard is primarily evaluators applying ISO/IEC 15408 and certifiers confirming evaluator actions; evaluation sponsors, developers, PP/ST authors and other parties interested in IT security are a secondary audience.

This International Standard recognises that not all questions concerning IT security evaluation will be answered herein and that further interpretations will be needed. Individual schemes will determine how to handle such interpretations, although these can be subject to mutual recognition agreements. A list of methodology-related activities that can be handled by individual schemes can be found in Annex A.

Information technology — Security techniques — Methodology for IT security evaluation

1 Scope

This International Standard is a companion document to the evaluation criteria for IT security defined in ISO/IEC 15408. It defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408.

This International Standard does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance.

2 Normative references

The following referenced documents are indispensable for the application of this document. 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 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

3 Terms and definitions

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

NOTE Terms which are presented in bold-faced type are themselves defined in this clause.

3.1
action
evaluator action element of ISO/IEC 15408-3

NOTE These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components.

3.2
activity
application of an assurance class of ISO/IEC 15408-3

3.3
check
generate a **verdict** by a simple comparison

NOTE Evaluator expertise is not required. The statement that uses this verb describes what is mapped.

3.4
evaluation deliverable
any resource required from the sponsor or developer by the evaluator or evaluation authority to perform one or more evaluation or evaluation oversight activities

3.5
evaluation evidence
tangible **evaluation deliverable**