TECHNICAL
REPORT

ISO/IEC
TR
19791

Second edition
2010-04-01

Information technology — Security techniques — Security assessment of operational systems

Technologies de l'information — Techniques de sécurité — Évaluation de la sécurité des systèmes opérationnels

Reference number
ISO/IEC TR 19791:2010(E)

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.

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.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard (“state of the art”, for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

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 TR 19791, which is a Technical Report of type 2, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC TR 19791:2006), which has been technically revised.

Introduction

This Technical Report is a support document that defines extensions to ISO/IEC 15408 to enable the security assessment (evaluation) of operational systems. ISO/IEC 15408, as currently defined, provides support for specifying the IT security functionality that exists in products and systems. However, it does not capture certain critical aspects of an operational system that must be precisely specified in order to effectively evaluate such a system.

This Technical Report provides extended evaluation criteria and guidance for assessing both the information technology and the operational aspects of such systems. It is primarily aimed at those who are involved in the development, integration, deployment and security management of operational systems, as well as evaluators seeking to apply ISO/IEC 15408 to such systems. It will be relevant to evaluation authorities responsible for approving and confirming evaluator actions. Evaluation sponsors, and other parties interested in operational system security, will be a secondary audience, for their background information.

Considering the complexity of this project and the need for additional work, the target has been defined to be a Technical Report Type 2. In the future, once additional experience has been gained in this area, it is hoped that it may be possible to convert this Technical Report into an International Standard to support evaluations of operational systems. Until some formalisation of an approach is performed, it is considered unlikely that many operational system evaluations of this nature will be undertaken due to the lack of specific guidance available, a gap that this Technical Report is designed to fill.

There are fundamental issues in regards to the definition and use of the term *system*. ISO/IEC 15408, with its focus on product evaluation, uses the term system to include only the information technology (IT) aspects of the system. The term *operational system*, as used within this Technical Report, covers the combination of personnel, procedures and processes integrated with technology-based functions and mechanisms, applied together to establish an acceptable level of residual risk in a defined operational environment.

This is a revised edition, updated for compatibility with the third edition of ISO/IEC 15408.

Information technology — Security techniques — Security assessment of operational systems

1 Scope

This Technical Report provides guidance and criteria for the security evaluation of operational systems. It provides an extension to the scope of ISO/IEC 15408, by taking into account a number of critical aspects of operational systems not addressed in ISO/IEC 15408 evaluation. The principal extensions that are required address evaluation of the operational environment surrounding the target of evaluation, and the decomposition of complex operational systems into security domains that can be separately evaluated.

This Technical Report provides

a) a definition and model for operational systems,

b) a description of the extensions to ISO/IEC 15408 evaluation concepts needed to evaluate such operational systems,

c) a methodology and process for performing the security evaluation of operational systems,

d) additional security evaluation criteria to address those aspects of operational systems not covered by the ISO/IEC 15408 evaluation criteria.

This Technical Report permits the incorporation of security products evaluated against ISO/IEC 15408 into operational systems evaluated as a whole using this Technical Report.

This Technical Report is limited to the security evaluation of operational systems and does not consider other forms of system assessment. It does not define techniques for the identification, assessment and acceptance of operational risk.

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 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

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*