TECHNICAL REPORT

ISO/IEC TR 15443-2

Second edition
2012-11-15

Information technology — Security techniques — Security assurance framework

Part 2: **Analysis**

Technologies de l'information — Techniques de sécurité — Assurance de la sécurité cadre

Partie 2: Analyses

Reference number
ISO/IEC TR 15443-2:2012(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.

In exceptional circumstances, 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), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

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 15443-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second edition of ISO/IEC TR 15443-2 cancels and replaces the first edition (ISO/IEC TR 15443-2:2005) and ISO/IEC TR 15443-3:2007, which have been technically revised.

ISO/IEC TR 15443 consists of the following parts, under the general title *Information technology — Security techniques — Security assurance framework*:

— *Part 1: Introduction and concepts*

— *Part 2: Analysis*

Introduction

This part of ISO/IEC TR 15443 is intended to be used together with ISO/IEC TR 15443-1. ISO/IEC TR 15443-1 introduced and discussed the concepts of assurance describing a model whereby the security assurance requirements for a deliverable can be satisfied through the presentation of a security case supported by security evidence that was obtained through making security assurance arguments in the development of a security assurance claim, IT security assurance arguments are verified by the application of security assurance conformity assessment methods and a Mark or symbol awarded appropriately.

ISO/IEC TR 15443-1 introduced the notion of methods for obtaining confidence in the security assurance claims made for a deliverable. This includes methods based on national or international agreed standards, specifications and methods as well as de-facto standards, specifications and methodologies which have as a characteristic a specified and systematic repeatable method for obtaining security assurance. These may be supplemented by a governing conformity assessment scheme that has responsibility for the oversight of the conformity of the application of the standard or specification and the testing method and often undertakes other duties such as awarding security assurance Marks.

By defining such a framework, this part of ISO/IEC TR 15443 guides the IT professional in the selection, and possible combination, of the assurance method(s) suitable for a given IT security product, system, or service and its specific environment.

Intended users of this part of ISO/IEC TR 15443 include those specifying security assurance cases including:

— acquirers (an individual or organization that acquires or procures a system, software product or software service from a supplier);

— developer (an individual or organization that performs development activities, including requirements analysis, design, testing and possibly integration during the software life cycle process)

— maintainer (an individual or organization that performs maintenance activities);

— supplier (an individual or organization that enters into a contract with the acquirer for the supply of a system, software product or software service under the terms of the contract);

— user (an individual or organization that uses the deliverable to perform a specific function);

— evaluator, tester or assessor (an individual or organization that performs an evaluation; an evaluator may, for example, be a testing laboratory, the quality department of a software development organization, a government organization or a user);

The objective of this part of ISO/IEC TR 15443 is to describe criteria that may be used in an analysis to support obtaining confidence in a variety of IT security assurance conformity assessment (SACA) paradigms, and to relate the described criteria to the security assurance model of ISO/IEC TR 15443-1. The emphasis is to identify criteria, often qualitative, and where possible quantitative, that can be used to support the degree of confidence that can be placed in the claims, results and Marks obtained from the associated SACA paradigms.

To provide such a framework it is necessary to characterize the criteria that can be used to assess the quality of the subject paradigm. Many of the criteria proposed in this framework rely on subjective analysis, with elements of assessment that may rely upon individual, organizational, and national norms, cultures and beliefs.

Information technology — Security techniques — Security assurance framework

Part 2:
Analysis

1 Scope

This part of ISO/IEC TR 15443 builds on the concepts presented in ISO/IEC TR 15443-1. It provides a discussion of the attributes of security assurance conformity assessment methods that contribute towards making assurance claims and providing assurance evidence to fulfil meeting the assurance requirements for a deliverable.

This part of ISO/IEC TR 15443 proposes criteria for comparing and analysing different SACA methods. The reader is cautioned that the methods used as examples in this part of ISO/IEC TR 15443 are considered to represent popularly used methods at the time of its writing. New methods may appear, and modification or withdrawal of the methods cited may occur. It is intended that the criteria can be used to describe and compare any SACA method whatever its provenance.

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 TR 15443-1:—[1)], *Information technology — Security techniques — Security assurance framework — Part 1: Introduction and concepts*

[1)] To be published.