TECHNICAL REPORT

ISO/IEC TR 15443-1

Second edition
2012-11-15

Information technology — Security techniques — Security assurance framework —

Part 1: Introduction and concepts

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

Partie 1: Introduction et concepts

Reference number
ISO/IEC TR 15443-1:2012(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) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a 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 by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.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 shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 15443-1 was prepared by Joint Technical Committee ISO/IEC JTC1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC TR 15443-1:2005), which has been technically revised. It also replaces ISO/IEC TR 15443-3.

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

At the plenary meeting of ISO/IEC JTC 1/SC 27 in November 1994, a study group was set up to consider the question of testing and assessment methods which contribute to assurance that IT products and systems conform to security standards from SC 27 and elsewhere (e.g. SC 21 and ETSI; and some Internet standards contain security aspects). In parallel, the Common Criteria project created a working group on assurances approaches in early 1996. ISO/IEC TR 15443 resulted from these two activities. Since then the subject of security assurance has advanced and matured. This second edition of ISO/IEC TR 15443 reflects the current state of the art in this topic.

Assurance in general may extend to include many properties of IT systems such as usability, interoperability, quality, reliability and so on and are discussed in other complementary documents such as ISO/IEC 15026 "Systems and software engineering — Systems and software assurance". Hence a detailed discussion of these properties is outside the scope of this Technical Report which focuses on IT security assurance.

The objective of ISO/IEC TR 15443 is to describe the topic of security assurance, providing the fundamental concepts of the topic and present the various security assurance techniques. Provision of a framework in which an appropriate security assurance case can be made is given. The framework provides guidance to the IT Security Professional in the use of security assurance to achieve confidence that a given deliverable satisfies its stated IT security assurance requirements. This report examines security assurance techniques, and security assurance methods proposed by various types of organisations whether they are de-jure or de-facto in nature.

In pursuit of this objective, ISO/IEC TR 15443 comprises the following:

a) the terms and definitions relating to the topic of security assurance

b) the fundamental concepts relating to security assurance

c) guidance to the selection, application, composition and recognition of assurance methods.

d) a presentation of common and unique properties specific to assurance methods;

e) a framework model to position existing assurance methods and to show their relationships;

ISO/IEC TR 15443 is organised in two parts to address the analysis of security assurance techniques as follows:

In this part, the introduction and concepts provides an overview of the definitions, fundamental concepts and a general description of security assurance. This material is aimed at providing the fundamental knowledge necessary to use the framework for analysis presented in ISO/IEC TR 15443-2 appropriately.

This part of ISO/IEC TR 15443 targets:

a) security assurance authorities, i.e. those responsible for decisions related to a deliverable's security assurance,

b) those responsible for developing deliverables with security functionality, such as security officers, IT security architects, developers and integrators,

c) those who are responsible for determining the security assurance of a deliverable, for example through the use of SACA methods such as those offered by ISO/IEC 27001, ISO/IEC 15408 and ISO/IEC 19790, This audience may include government agencies, suppliers and integrators.

d) consumers of IT security assurance such as those acquirers and end-users who are responsible for procuring or using deliverables that make claims about their security properties.

ISO/IEC TR 15443 -2, Analysis, describes a security assurance framework model that can be used to assess a variety of assurance methods and approaches and relates them to ISO/IEC TR 15443-1. The emphasis is to identify qualitative properties of the security assurance methods that contribute to security assurance. This material is catering to an IT security professional to provide understanding of how to obtain security assurance in a given life cycle stage of a deliverable.

ISO/IEC TR 15443 is relevant to security assurance methods that may not be unique to IT security; however, guidance given in ISO/IEC TR 15443 will be limited to IT security requirements. A Technical Report, ISO/IEC TR 15026, covers the related topic of systems and software assurance.

Similarly, additional terms and concepts defined in other International standardisation initiatives (i.e. CASCO) and International guides (e.g., ISO/IEC 17000) will be incorporated; however, guidance will be provided specific to the field of IT security and is not intended for general quality management and assessment, or IT conformity.

Information technology — Security techniques — Security assurance framework —

Part 1:
Introduction and concepts

1 Scope

This part of ISO/IEC TR 15443 defines terms and establishes an extensive and organised set of concepts and their relationships for understanding IT security assurance, thereby establishing a basis for shared understanding of the concepts and principles central to ISO/IEC TR 15443 across its user communities. It provides information fundamental to users of ISO/IEC TR 15443-2.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 15026-1:2010, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

ISO/IEC 17000:2004, *Conformity assessment — Vocabulary and general principles*