TECHNICAL REPORT

ISO/IEC TR 15443-1

First edition
2005-02-01

Information technology — Security techniques — A framework for IT security assurance —

Part 1: Overview and framework

Technologies de l'information — Techniques de sécurité — Un canevas pour l'assurance de la sécurité dans les technologies de l'information —

Partie 1: Vue d'ensemble et canevas

Reference number
ISO/IEC TR 15443-1:2005(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.

ISO/IEC TR 15443-1, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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

- *Part 1: Overview and framework*
- *Part 2: Assurance methods*

Analysis of assurance methods will form the subject of a future Part 3.

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.

The objective of ISO/IEC TR 15443 is to present a variety of assurance methods, and to guide the IT Security Professional in the selection of an appropriate assurance method (or combination of methods) to achieve confidence that a given deliverable satisfies its stated IT security assurance requirements. This report examines assurance methods and approaches proposed by various types of organisations whether they are approved or de-facto standards.

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

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

b) a collection of assurance methods, their description and reference;

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

d) qualitative, and where possible, quantitative comparison of existing assurance methods;

e) identification of assurance schemes currently associated with assurance methods;

f) a description of relationships between the different assurance methods; and

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

ISO/IEC TR 15443 is organised in three parts to address the assurance approach, analysis, and relationships as follows:

Part 1 Overview and Framework provides an overview of the fundamental concepts and a general description of assurance methods. This material is aimed at understanding Part 2 and the future Part 3 of ISO/IEC TR 15443. Part 1 targets IT security managers and others responsible for developing a security assurance program, determining the security assurance of their deliverable, entering an assurance assessment audit (e.g. ISO 9000, SSE-CMM (ISO/IEC 21827), ISO/IEC 15408-3), or other assurance activities.

Part 2 Assurance Methods describes a variety of assurance methods and approaches and relates them to the security assurance framework model of Part 1. The emphasis is to identify qualitative properties of the assurance methods that contribute to assurance. This material is catering to an IT security professional for the understanding of how to obtain assurance in a given life cycle stage of deliverable.

The future *Part 3 Analysis of Assurance Methods* will analyse the various assurance methods with respect to their assurance properties. The analysis will aid the Assurance Authority in deciding the relative value of each Assurance Approach and determining the assurance approach(s) that will provide the assurance results most appropriate to their needs within the specific context of their operating environment. Furthermore, the analysis will also aid the Assurance Authority to use the assurance results to achieve the desired confidence of the deliverable. The material in this part targets the IT security professional who must select assurance methods and approaches.

ISO/IEC TR 15443 analyses 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. Similarly, additional terms and concepts defined in other International standardisation initiatives (i.e. CASCO) and International guides (e.g., ISO/IEC Guide 2) 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 — A framework for IT security assurance —

Part 1: **Overview and framework**

1 Scope

1.1 Purpose

The purpose of this part of ISO/IEC TR 15443 is to introduce, relate and categorise security assurance methods to a generic life cycle model in a manner enabling an increased level of confidence to be obtained in the security functionality of a deliverable.

1.2 Approach

The approach adopted throughout this part of ISO/IEC TR 15443 presents an overview of the basic assurance concepts and terms required for understanding and applying assurance methods through a framework of identifying various assurance approaches and assurance stages.

1.3 Application

Using the categorisation obtained through this part of ISO/IEC TR 15443, Part 2 and the future Part 3 will guide the reader in the selection, and possible combination, of the assurance method(s) suitable for application to a given deliverable.

1.4 Field of Application

This part of ISO/IEC TR 15443 provides guidance for the categorisation of assurance methods including those not unique to IT security. It may be used in areas outside of IT security where criticality warrants assurance.

1.5 Limitations

This part of ISO/IEC TR 15443 applies to deliverables (refer to Clause 4.3) and their related organisational security issues only.

2 Terms and definitions

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

NOTE The terms and definitions have been developed to be as generic as possible to support the assurance model developed in this part of ISO/IEC TR 15443. The assurance model, being applicable to a broad spectrum of assurance approaches, requires non-specific terminology to be applicable to a broad spectrum of assurance approaches.

Defining terms for a generic assurance model is a difficult task owing to the myriad of assurance terms that exist to satisfy the available assurance approaches. Furthermore, similar terms have different definitions and many are unique to a particular assurance approach making it difficult to construct a generic language for the assurance model. Owing to these