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)

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

difficulties, terms and definitions have been crafted to ensure the neutrality of the assurance framework and applicability to a wide range of assurance methods. Relevant ISO standards are used wherever possible, in particular to maintain compatibility to ISO/IEC TR 15408 Parts 1 - 3 and ISO 9000 series.

The next difficulty was how to address the multiple definitions that existed for the same term and definitions that were not used, as they were not generic enough for the model. Should these terms be ignored or maintained for reference purposes? Ignoring definitions posed the problem of confusing readers when discussing the assurance approach from which they came. Maintaining definitions specific to a unique assurance approach added a level of formatting complexity to ISO/IEC TR 15443; however, the appropriate definition could then be used within the correct context. It was decided to maintain the previous definitions and to present them in a clear manner. Where multiple definitions exist for the same term, the principal definition for the purpose of ISO/IEC TR 15443 is listed first. Alternate definitions, bulleted and denoted in italics, are only applicable when cited in the context of their source.

2.1
accreditation

Procedure by which an authoritative body gives formal recognition, approval, and acceptance of the associated residual risk:

a) *for the operation of an automated system in a particular security mode using a particular set of safeguards [adapted from AGCA];*

b) *that a security body or person is competent to carry out specific tasks [adapted from ISO/IEC Guide 2]; and*

c) *that a security service is suitable for the target environment.*

2.2
approach
The method used or steps taken in setting about a task or problem.

2.3
assessment
Verification of a deliverable against a standard using the corresponding method to establish compliance and determine the assurance.

2.4
assurance
Performance of appropriate activities or processes to instil confidence that a deliverable meets its security objectives.

a) *Grounds for confidence that an entity meets its security objectives [ISO/IEC 15408–1].*

2.5
assurance approach
A grouping of assurance methods according to the aspect examined.

2.6
assurance argument
A set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied.

2.7
assurance assessment
Verification and recording of the overall types and amounts of assurance associated with the deliverable (entered into the assurance argument).

2.8
assurance authority
A person or organisation delegated the authority for decisions (i.e. selection, specification, acceptance, enforcement) related to a deliverable's assurance that ultimately leads to the establishment of confidence in the deliverable.

NOTE In specific schemes or organisations, the term for assurance authority may be different such as evaluation authority.

2.9
assurance evidence
Work products resulting from the assurance analysis of the deliverable (including summary reports or other justification) that supports the assurance claim.

2.10
assurance level
The amount of assurance obtained according to the specific scale used by the assurance method.

NOTE 1 The assurance level may not be measurable in quantitative terms.

NOTE 2 The amount of assurance obtained is generally related to the effort expended on the activities performed.

2.11
assurance method
A recognised specification for obtaining reproducible assurance results.

2.12
assurance property
A characteristic of an assurance method that contributes to the assurance result.

2.13
assurance result
Documented numerical or qualitative assurance statement pertaining to a deliverable.

2.14
assurance scheme
The administrative and regulatory framework under which an assurance method is applied by an assurance authority within a specific community or organisation.

a) *The administrative and regulatory framework under which the Common Criteria is applied by an evaluation authority within a specific community [ISO/IEC 15408–1].*

2.15
assurance stage
The deliverable life cycle stage on which a given assurance method is focused. The overall deliverable assurance takes into account the results of the assurance methods applied throughout the deliverable life cycle.

2.16
assurance evidence
Workproducts or any items generated from the assurance analysis of the deliverable including reports (justification) to support the assurance claim.

2.17
certification
Procedure by which a formal assurance statement is given that a deliverable conforms to specified requirements. Certification may be performed by a third party or self-certified [adapted from ISO/IEC Guide 2:1996].

a) *The issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used where correctly applied [ITSEC].*

b) *The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval [ISO/IEC 15408–1].*

c) *The comprehensive assessment of the technical and non-technical security features of an information technology system, made in support of accreditation that establishes the extent to which a system satisfies a specified security policy [AGCA].*

2.18
confidence
A belief that a deliverable will perform in the way expected or claimed (i.e. properly, trustworthy, enforce security policy, reliably, effectively).

2.19
deliverable
An IT security product, system, service, process, or environmental factor (i.e. personnel, organisation) or the object of an assurance assessment. An object may be a Protection Profile (PP) or Security Target (ST) as defined by ISO/IEC 15408-1.

Note: ISO 9000:2000 holds that a service is a type of product and “product and/or service" when used in the ISO 9000 family of standards.

2.20
evaluation
Assessment of a deliverable against defined criteria (adapted from ISO/IEC 15408–1).

a) *Systematic examination (quality evaluation) of the extent to which an entity is capable of fulfilling specified requirements [ISO/IEC 14598-1].*

2.21
guarantee
Refer to the definition for *Warranty* in clause 2.36.

2.22
IT security product
A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems [ISO/IEC 15408–1].

2.23
life cycle stage
An instance within the deliverable life cycle that relates to the state of the deliverable.

a) *A period within the system life cycle that relates to the state of the system description and/or the system itself [ISO/IEC 15288].*

2.24
pedigree
Informal recognition of the vendor’s consistent repeatability to provide deliverables that satisfy its security policy or to perform as claimed (pedigree is an environmental factor associated with the vendor or deliverable).

2.25
process
An organised set of activities which uses resources to transform inputs to outputs [ISO 9000: 2000]

2.26
process assurance
Assurance derived from an assessment of activities of a process.

2.27
product
Refer to the definition of deliverable.

2.28
scheme
Set of rules defining the environment, including criteria and methodology required to conduct an assessment [adapted from ISO/IEC 18045 (Common Evaluation Methodology)].

2.29
security
All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability [ISO/IEC 13335-1].

NOTE A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way. This is usually considered in the context of an assessment of actual or perceived threats.

a) *The capability of the software product to protect information and data so that unauthorised persons or systems cannot read or modify them and authorised persons or systems are not denied access to them [ISO/IEC 9126-1].*

2.30
security assessment
Verification of a security deliverable against a security standard using the corresponding security method to establish compliance and determine the security assurance.

a) *The last stage of the product evaluation process [ISO/IEC 14598-1].*

2.31
security element
An indivisible security requirement.

2.32
service
A security process or task performed by a deliverable, organisation, or person.

2.33
stakeholder
A party having a right, share, or an asset at risk in a deliverable or in its possession of characteristics that meet the party's needs and expectations.

a) *A party having a right, share, or claim asset in a system or in its possession of characteristics that meet the party's needs and expectations [ISO/IEC 15288].*

2.34
system
A specific IT installation, with a particular purpose and operational environment [ISO/IEC 15408–1].

a) *A combination of interacting elements organized to achieve one or more stated purposes [ISO/IEC 15288].*

NOTE 1 A system may be considered as a product and/or as the services it provides [ISO/IEC 15288].

NOTE 2 In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g. aircraft system. Alternatively the word system may be substituted simply by a context dependent synonym, e.g. aircraft, though this may then obscure a system principles perspective [ISO/IEC 15288].

2.35
system life cycle
The evolution with time of the system from conception through to disposal [ISO/IEC 15288].

2.36
warranty
A security service to correct or mitigate the deliverable's operation (deployment, performance, or delivery) if it does not satisfy its security policy.

2.37
work product
All items (i.e. documents, reports, files, data, etc.) generated in the course of performing any process for developing and supplying the deliverable [SSE-CMM (ISO/IEC 21827)].

a) Result of a system of activities, which use resources to transform inputs into outputs [ISO 9001].

3 Abbreviated terms

AST
Abstract Security Target

BSI
Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency)

CASCO
ISO Committee on conformity assessment

CEM
Common Evaluation Methodology (precursor of, and equivalent to NP N2729r1 Methodology for IT security evaluation)

CMM
Capability Maturity Model

CSE
Communications Security Establishment (Canadian IT Security Agency)

CTCPEC
Canadian Trusted Computer Product Evaluation Criteria (edited by CSE)

HCD
Human Centered Design

IEC
International Electrotechnical Commission

ISO
International Organization for Standardization

IT
Information Technology

ITSEC
Information Technology Security Evaluation Criteria (Office for Official Publications of the European Communities)