TECHNICAL REPORT

ISO/IEC TR 15443-1

Second edition
2012-11-15

Information technology — Security techniques — Security assurance framework —

Part 1: Introduction and concepts

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Technologies de l'information — Techniques de sécurité — Assurance de la sécurité cadre —
Partie 1: Introduction et concepts

ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045c755/iso-iec-tr-15443-1-2012

Reference number
ISO/IEC TR 15443-1:2012(E)

© ISO/IEC 2012

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045c755/iso-iec-tr-15443-1-2012

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2012 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84c1-15d32045c755/iso-iec-tr-15443-1-2012

© ISO/IEC 2012 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045c755/iso-iec-tr-15443-1-2012

 © ISO/IEC 2012 – All rights reserved

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.

iTeh STANDARD PREVIEW

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.

(standards.iteh.ai)

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

ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045e755/iso-iec-tr-15443-1-2012

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*

© ISO/IEC 2012 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045e755/iso-iec-tr-15443-1-2012

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.

© ISO/IEC 2012 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045c755/iso-iec-tr-15443-1-2012

© ISO/IEC 2012 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045c755/iso-iec-tr-15443-1-2012

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 15443-1:2012

ISO/IEC TR 15026-1:2010, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

https://standards.iteh.ai/catalog/standards/sist/0d1f6cca-a939-4a22-84c1-f5d32045c755/iso-iec-tr-15443-1-2012

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17000, ISO/IEC TR 15026-1 and the following apply.

NOTE Defining terms for a generic security assurance framework is a difficult task since many security assurance terms have been coined to satisfy the needs of specific security assurance needs. In many cases, similar terms have different definitions making it difficult to construct a generic language for the security assurance framework. Owing to these difficulties, definitions in conflict are reproduced below, and the term's preferred definition in the context of this Technical Report indicated. In particular, definitions from ISO/IEC 17000, ISO/IEC TR 15026, ISO/IEC 15408 part 1 and the ISO/IEC 27000 series may be reproduced below.

3.1
accreditation
third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment results

[SOURCE: ISO/IEC 17000:2004, definition 5.6]

3.2
accreditation
formal declaration by a designated approving authority that a system is approved to operate in a particular security mode using a prescribed set of safeguards

© ISO/IEC 2012 – All rights reserved

NOTE 1 The definition of the term "accreditation" adopted for this standard is from ISO/IEC 17000:2004, definition 5.6.

NOTE 2 Note 1 is not part of the definition from ISO/IEC 21827.

[SOURCE: ISO/IEC 21827:2008, definition 3.2]

3.3
approval authority
SACA approval authority
entity with the authority to decide that the assurance case and the extent of assurance it provides are satisfactory

NOTE 1 The approval authority may include multiple entities, e.g. individuals or organizations. These can include different entitles with different levels of approval and/or different areas of interest.

NOTE 2 Two-party situations; approval authority often rests with the acquirer. In regulatory situations, the approval authority may be a third party such as a governmental organization or its agent. In other situations, e.g. the purchase of off-the-shelf products developed by a single-party, the independence of the approval authority can be a relevant issue to the acquirer.

[SOURCE: Adapted from ISO/IEC 15026-1:2010, definition 2.3]

3.4
approval authority
any national or international organization/authority mandated to approve and/or evaluate security functions

iTeh STANDARD PREVIEW

NOTE 1 An approval authority in the context of this definition evaluates and approves security functions based on their cryptographic or mathematical merits but is not the testing entity which would test for conformance to this International Standard and ISO/IEC 19790:2006.

(standards.iteh.ai)

[SOURCE: ISO/IEC 19790:2006, definition 3.1]

ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045c755/iso-iec-tr-15443-1-2012

3.5
assessment
verification of a product, system or service against a standard using the corresponding assessment method to establish compliance and determine the assurance

[SOURCE: ISO/IEC 21827, definition 3.3]

3.6
assurance
grounds for justified confidence that a claim has been or will be achieved

[SOURCE: ISO/IEC TR 15026-1:2010, definition 2.1]

3.7
assurance
<ISO/IEC 15408> grounds for justified confidence that a TOE meets the SFRs

[SOURCE: ISO/IEC 15408-1:2009, definition 3.1.4]

3.8
assurance authority
individual or organization responsible for specifying security assurance requirements for which assurance is to be obtained

NOTE 1 An assurance authority may be the same individual or organization as the approval authority in definition 3.3.

© ISO/IEC 2012 – All rights reserved

3.9
assurance case
representation of a claim or claims, and the support for these claims

NOTE 1 An assurance case is a reasoned, auditable artefact created to support the contention its claim or claims are satisfied. It contains the following and their relationships:

— one or more claims about properties;

— arguments that logically link the evidence and any assumptions to the claim(s);

— a body of evidence and possibly assumptions supporting these arguments for the claim(s).

[SOURCE: ISO/IEC TR 15026-1, definition 2.2]

3.10
assurance claim
assertion or supporting assertion that a system meets a stated security need

NOTE 1 Claims address both direct threats (e.g. system data are protected from attacks by outsiders) and indirect threats (e.g. system code has minimal flaws).

NOTE 2 Compare with the definition of "claim" in definition 3.11.

[SOURCE: Adapted from ISO/IEC 21827, definition 3.7]

3.11
certification
iTeh STANDARD PREVIEW
third-party attestation related to products, processes, systems or persons
(standards.iteh.ai)

NOTE 1 Certification of a management system is some-times also called registration.

ISO/IEC TR 15443-1:2012
NOTE 2 Certification is applicable to all objects of conformity assessment except for conformity assessment bodies themselves, to which accreditation is applicable.
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045c755/iso-iec-tr-15443-1-2012

[SOURCE: ISO/IEC 17000:2004, definition 5.5]

3.12
claim
statement of something to be true including associated conditions and limitations

NOTE 1 The statement of a claim does not mean that the only possible intent or desire is to show it is true. Sometimes claims are made for the purpose of evaluating whether they are true or false or undertaking an effort to establish what is true.

NOTE 2 In its entirety, a claim conforming to ISO/IEC 15026-2 is an unambiguous declaration of an assertion with any associated conditionality giving explicit details including limitations on values and uncertainty. It could be about the future, present, or past.

[SOURCE: ISO/IEC 15026-1:2010,definition 2.4]

3.13
conformity assessment scheme
conformity assessment programme
conformity assessment system related to specified objects of conformity assessment, to which the same specified requirements, specific rules and procedures apply

NOTE 1 Conformity assessment schemes may be operated at international, regional, national or sub-national level.

[SOURCE: ISO/IEC 17000:2010, definition 2.8]

© ISO/IEC 2012 – All rights reserved

3.14
deliverable
component, product, system, service, process, organization or personnel that has a security objective

NOTE 1 A deliverable's boundary may include one or many components including the processors, and peripherals, associated communication technologies, peripheral services, the environment in which it operates, associated organizational processes as well as the personnel responsible for developing, operating, maintaining and using it.

3.15
evaluation
systematic determination of the extent to which an entity meets its specified criteria

[SOURCE: ISO/IEC 12207:2007, definition 4.12]

3.16
evaluation
<ISO/IEC 15408> assessment of a PP, an ST or a TOE against defined criteria

[SOURCE: ISO/IEC 15408–1:2009, definition 3.1.26]

3.17
evaluation scheme
the administrative and regulatory framework under which ISO/IEC 15408 is applied by an evaluation authority within a specific community

NOTE 1 Compare with [ISO/IEC 17000, definition 2.8 "conformity assessment scheme"].

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SOURCE: Adapted from ISO/IEC 15408–1:2009, definition 3.1.29]

3.18
mark
assurance argument that substantiates the assurance claim

ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045c755/iso-iec-tr-15443-1-2012

NOTE 1 ISO/IEC 17030:2003 gives general requirements for third party marks of conformity.

3.19
predictive assurance
recognition of the vendor’s consistent repeatability to provide deliverables that satisfy its security policy or to perform as claimed

3.20
secure
not vulnerable to most attacks, are able to tolerate many of the attacks that they are vulnerable to, and that can recover quickly with a minimum of damage from the few attacks that successfully exploit their vulnerabilities

3.21
security
property of a system by which confidentiality, integrity, availability, accountability, authenticity, and reliability are achieved

3.22
security
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

[SOURCE: ISO/IEC 12207:2007, definition 4.39]

© ISO/IEC 2012 – All rights reserved

3.23
security assurance
grounds for justified confidence that a claim about meeting security objectives has been or will be achieved

[SOURCE: Adapted from ISO/IEC 15026-1:2010, definition 2.1]

3.24
security assurance argument
set of structured security assurance claims, supported by evidence and reasoning, that demonstrate clearly how security assurance needs have been satisfied

3.25
security assurance evidence
data on which a judgment or conclusion about an security assurance claim may be based

NOTE 1 The evidence may consist of observation, test results, analysis results, evaluation and appraisals.

[SOURCE: Adapted from ISO/IEC 21827, definition 3.8]

3.26
Security assurance conformance assessment method
SACA method
systematic process, procedure or technique for obtaining security assurance evidence and consistently verifying security assurance claims

NOTE 1 Compare with conformity assessment scheme, definition 2.8 in ISO/IEC 17000.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.27
Security assurance conformance assessment paradigm
SACA paradigm
complete system for the provision and recognition of a single or several related SACA Marks including the specification of SACA methods, SACA schemes and a set of stakeholders

ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d76fcca-a939-4a22-84e1-f5d32045c755/iso-iec-tr-15443-1-2012

3.28
Security assurance conformance assessment scheme
SACA scheme
system of common rules, procedures and management for demonstrating that specified security assurance requirements relating to a product, process, system, person or body are applied to specific objects of conformity assessment

NOTE 1 Conformity assessment schemes may be operated at international, national or sub-national level.

NOTE 2 Adapted from ISO/IEC 17000:2004 definition 2.8.

NOTE 3 Compare with "evaluation scheme" definition 3.17.

3.29
security assurance rating
indication of assessment rigour and coverage of security assurance requirements according to a specific scale used by the security assurance method

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

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

3.30
security assurance result
documented quantitative or qualitative security assurance statement pertaining to a deliverable

© ISO/IEC 2012 – All rights reserved

3.31
security objective
statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions

[SOURCE: ISO/IEC 15408-1:2009, definition 3.1.60]

3.32
security problem
statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address

NOTE 1 This statement consists of a combination of:

— threats to be countered by the deliverable,

— the OSPs enforced by the deliverable, and

— the assumptions that are upheld for the deliverable and its operational environment.

[SOURCE: ISO/IEC 15408-1:2009, definition 3.1.61]

3.33
system
combination of interacting elements organized to achieve one or more stated purposes

NOTE 1 A system may be considered as a product and/or as the services it provides.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045c755/iso-iec-tr-15443-1-2012

[SOURCE: ISO/IEC 15288:2008, definition 4.31]

4 Abbreviated Terms

CASCO
ISO Committee on conformity assessment

CC
Common Criteria

CCMC
Common Criteria Management Committee

CCRA
Common Criteria Recognition Arrangement

CEM
Common Evaluation Methodology

CMM
Capability Maturity Model

COTS
Commercial off the shef

CSEC
Communications Security Establishment of Canada (Canadian IT Security Agency)

© ISO/IEC 2012 – All rights reserved

EAL
Evaluation Assurance Level

IEC
International Electrotechnical Commission

ISMS
Information Security Management System

ISO
International Organization for Standardization

IT
Information Technology

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

ITSEF
Information Technology Security Evaluation Facility

ITSEM
Information Technology Security Evaluation Methodology (Office for Official Publications of the European Communities)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

NIST
National Institute of Standards and Technology (Government Agency of the USA)

ISO/IEC TR 15443-1:2012
https://standards.iteh.ai/catalog/standards/sist/0d16fcca-a939-4a22-84e1-f5d32045c755/iso-iec-tr-15443-1-2012

NSA
National Security Agency (Government Agency of the USA)

PCI DSS
Payment Card Industry Data Security Standard

PCI SSC
Payment Card Industry Security Standards Council

PP
Protection Profile (defined in ISO/IEC 15408-1)

SACA
Security assurance conformance assessment

SCT
Strict (Security) Conformance Testing

SDO
Standards Development Organization

SOG-IS
Senior Officials Group, Information System Security

SSE-CMM
System Security Engineering - Capability Maturity Model ISO/IEC 21827 (submitted to ISO as a publicly available standard by the Support Organization of the International Systems Security Engineering Association (ISSEA)

© ISO/IEC 2012 – All rights reserved