TECHNICAL REPORT

ISO/IEC TR 15443-3

First edition
2007-12-15

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

Part 3: Analysis of assurance methods

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Technologies de l'information — Techniques de sécurité — Un canevas pour l'assurance de la sécurité dans les technologies de l'information — Partie 3: Analyses des méthodes d'assurance

ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7382541-c1e9-439d-bac8-86389435acd5/iso-iec-tr-15443-3-2007

Reference number
ISO/IEC TR 15443-3:2007(E)

© ISO/IEC 2007

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7382541-c1e9-439d-bac8-86389435acd5/iso-iec-tr-15443-3-2007

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2007

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 2007 – All rights reserved

Contents

Page

Foreword v

Introduction vi

1 Scope 1
1.1 Purpose 1
1.2 Application 1
1.3 Field of Application 1
1.4 Limitations 1

2 Terms and definitions 1

3 Abbreviated terms 4

4 Understanding Assurance 4
4.1 Setting the assurance goal 4
4.2 Applying assurance methods 7
4.3 Assessing assurance results 12
4.4 Example 14

5 Comparing, selecting and composing assurance 14
5.1 Selecting the assurance approach 14
5.2 Composing assurance methods 16
5.3 Comparing assurance methods 17
5.4 Focus on assurance properties 18

6 Guidance 23
6.1 Developmental Assurance (DA) 24
6.2 Integration Assurance (IA) 25
6.3 Operational Assurance (OA) 29

Annex A — Tabular comparisons 33
A.1 Methods and their target groups 33
A.2 Available Assurance Methods 34

Annex B — Assurance properties of selected methods 35
B.1 ISO/IEC 15408 35
B.2 ISO/IEC 19790 38
B.3 ISO/IEC 21827 40
B.4 ISO/IEC 13335 41
B.5 ISO/IEC 27001 and ISO/IEC 27002 43
B.6 IT Baseline Protection Manual 46
B.7 COBIT 48
B.8 ISO 9000 50

Annex C — Composition of assurance methods 53
C.1 ISO/IEC 15408 + IT Baseline Protection Manual 53
C.2 ISO/IEC 27002 + IT Baseline Protection 53
C.3 ISO/IEC 27001 and ISO/IEC 27002 53
C.4 ISO/IEC 27002 + ISO 9000 54
C.5 COBIT + IT Baseline Protection 54

Annex D — Case Studies 55
D.1 A chip-card manufacturer's assurance composition strategy 55
D.2 A service provider assures the upgrade of business processes 56

Annex E — Determination of the assurance goal 57
E.1 Risk Assessment 57

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7382541-c1e9-439d-bac8-f03389435acd5/iso-iec-tr-15443-3-2007

© ISO 2007 – All rights reserved

E.2 Risk Management 57
E.3 Security Model 58
E.4 Organizational security policy 59
E.5 Applicable Assurance goal 60
E.6 Security Measures 60
E.7 Example: ISO/IEC 15408 61

Bibliography 62

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7382541-c1e9-439d-bac8-86389435acd5/iso-iec-tr-15443-3-2007

© ISO 2007 – All rights reserved

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).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7385f41-c1e9-439d-bac8-86389435acd5/iso-iec-tr-15443-3-2007

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.

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 15443-3, 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*

– *Part 3: Analysis of assurance methods*

© ISO 2007 – All rights reserved

Introduction

The objective of this Technical Report 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, this Technical Report comprises the following:

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

– a collection of assurance methods, their description and reference;

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

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

– identification of assurance schemes currently associated with assurance methods;

– a description of relationships between the different assurance methods; and

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This Technical Report is organised in three parts to address the assurance approach, analysis, and relationships as follows:

ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7382541-c1e9-439d-bac8-86389435acd5/iso-iec-tr-15443-3-2007

Part 1: Overview and framework provides an overview of the fundamental concepts and general description of assurance methods. This material is aimed at understanding Part 2 and Part 3 of this Technical Report. 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, 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.

Part 3: Analysis of assurance methods analyses 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(es) 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 needs to select assurance methods and approaches.

This Technical Report analyses assurance methods that may not be unique to IT security; however, guidance given in this Technical Report 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.

© ISO 2007 – All rights reserved

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

Part 3: Analysis of assurance methods

1 Scope

1.1 Purpose

The purpose of this part of ISO/IEC TR 15443 is to provide general guidance to an assurance authority in the choice of the appropriate type of international communications techology (ICT) assurance methods and to lay the framework for the analysis of specific assurance methods for specific environments.

1.2 Application

This part of ISO/IEC TR 15443 will allow the user to match specific assurance requirements and/or typical assurance situations with the general characteristics offered by available assurance methods.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

1.3 Field of Application

ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7382541-c1e9-439d-bac8-8e389435acd5/iso-iec-tr-15443-3-2007

The guidance of this part of ISO/IEC TR 15443 is applicable to the development, implementation and operation of ICT products and ICT systems with security requirements.

1.4 Limitations

Security requirements may be complex, assurance methods are of great diversity, and organisational resources and cultures differ considerably.

Therefore the advice given in this part of ISO/IEC TR 15443 will be qualitative and summary, and the user may need to analyse on his own which methods presented in Part 2 of this Technical Report will suit best his specific deliverables and organisational security requirements.

2 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC TR 15443-1, ISO/IEC TR 15443-2 and the following apply.

2.1
assets
anything that has value to the organization

2.2
assessment
systematic examination of the extent to which an entity is capable of fulfilling specified requirements; synonymous to evaluation when applied to a deliverable

[ISO/IEC 14598-1]

© ISO 2007 – All rights reserved

2.3
assessment method
action of applying specific documented assessment criteria to a deliverable for the purpose of determining acceptance or release of that deliverable

2.4
assurance authority
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 could be different such as evaluation authority.

2.5
assurance administrator
responsible (accountable) person for the selection, implementation, or acceptance deliverable

2.6
assurance goal
overall security expectations to be satisfied through application of formal and informal assessment activities

2.7
assurance concern
general type of assurance objective pursued by a major group of assurance authorities

NOTE In this part of ISO/IEC TR 15443, assurance concern is used for the purpose of establishing analyses and conclusions for assurance guidance given to that group of users.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-3:2007
86389435acd5/iso-iec-tr-15443-3-2007

2.8
deliverable
IT security product, system, service, process, or environment factor (i.e. personnel, organisation) in particular as object of an assurance assessment

NOTE 1 An object may be a Protection Profile (PP) or Security Target (ST) as defined by ISO/IEC15408-1.

NOTE 2 ISO 9000 holds that a service is a type of product and "product and/or service" when used in the ISO 9000 family of standards.

NOTE 3 For the purpose of this part of ISO/IEC TR 15443, and similar to the usage in ISO 9000, the term **product** will generally be used in place of deliverable throughout the document.

2.9
environment
environment of life cycle process execution (i.e. people, facilities and other resources) and associated environment assurance characteristics (e.g. reputation, certification)

NOTE In ISO/IEC TR 15443 environment assurance contrasts with product assurance and process assurance.

2.10
information security management system
ISMS
part of the overall management system based on business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

[ISO/IEC 27001:2005, definition 3.7]

2.11
method
a way of performing something according to a plan to obtain reproducible results in a systematic and traceable manner

 © ISO 2007 – All rights reserved

2.12
metric
quantitative scale and method, which can be used for measurement

2.13
process capability
ability of a process to achieve a required goal

2.14
product
IT security product, system, service

NOTE 1 For the purpose of this part of ISO/IEC TR 15443, and similar to its usage in ISO 9000, the term **product** will be used in place of deliverable throughout the document.

NOTE 2 The term **product** is synonymous with **deliverable**.

2.15
residual risk
risk remaining after risk treatment

2.16
risk assessment
overall process of risk analysis and risk evaluation

[ISO/IEC Guide 73:2002, definition 3.3.1]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

NOTE 1 Risk evaluation is the process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

NOTE 2 For the purpose of this part of ISO/IEC TR 15443, risk assessment, risk analysis and threat-risk-analysis are summarily called **risk assessment**.

ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7382541-c1e9-439d-bac8-86389435acd5/iso-iec-tr-15443-3-2007

2.17
risk treatment
process of selection and implementation of measures to modify risk

2.18
security
all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability

[ISO/IEC 13335-1:2004, definition 2.11]

2.19
security objective
statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions

[ISO/IEC 15408-1:2005, definition 2.42]

2.20
security policy
set of rules internal to an organizational unit that regulate how this unit protects the management of its assets conform to specified organizational objectives within its legal and cultural context

2.21
stage
period within the life cycle of a deliverable comprising processes and activities

NOTE Adapted from ISO/IEC 15288.

© ISO 2007 – All rights reserved

3 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC TR 15443-1, ISO/IEC TR 15443-2 and the following apply.

COBIT Control Objectives for Information and related Technology, a method of **ISACA**

DA Developmental Assurance

IA Integration Assurance

ISACA Information Systems Audit and Control Association

ISSEA International Systems Security Engineering Association

OA Operation Assurance

ST Security Target

4 Understanding Assurance

Objective of assurance is to provide confidence that the product will operate securely in a given context. This clause gives consideration to some basic issues while detail analysis and guidance is presented in the remainder of this part of ISO/IEC TR 15443.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

In terms of the concepts developed in Parts 1 and 2 of ISO/IEC TR 15443, this means that the product satisfies a given assurance goal. This goal has to be set in a more or less formal manner. The user of assurance has to be aware of the residual risk.

ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f5382541-ca59-4301-bac8-86389435acd5/iso-iec-tr-15443-3-2007

Confidence will be gained by use and interpretation of assurance results which may be already available or which may be gained by the application of assurance methods. These methods need to be properly selected and applied.

Numerous methods are available, and many are presented in Part 2 of ISO/IEC TR 15443. Some basic aspects of their application is explained in 4.2.

The user of the assurance result may present a varying level of sophistication. This sophistication may guide the associated level of rigor (refer to Subclause 4.2.1) of assurance methods, the extent application (refer to Subclause 4.2.2), and the Life Cycle stages to be covered (refer to Subclause 4.2.3).

Particular attention is to be given to the assessment of an assurance result. To gain higher levels of confidence formal assessment or certification may be required (refer to Subclause 4.3).

4.1 Setting the assurance goal

The assurance goals will depend on the assurance requirements to be satisfied:

– A product provider may have generic assurance requirements intended to satisfy the specific requirements of more than one user, i.e. those of a user community of its product, system or service.

– A product user typically has very specific assurance requirements, usually depending on a specific security policy of the user's organization.

The following explains this aspect and relates it to appropriate assurance offerings and use.

NOTE 1 The example comparison of Annex A.1 distinguishes between Hardware vendor, Software vendor, Network provider, Server operator, Content provider and Enterprise as user. In this example, the vendors clearly belong to the first group of assurance providers, and the user organization clearly belongs to the assurance user group. However, the others are both providers and users of assurance.

 © ISO 2007 – All rights reserved

NOTE 2 An organization may need to combine assurance results arising from two or more sources of assurance into a consistent compound assurance result. This is an important aspect and will be covered in subclause 5.2 and 6.2.3.1 of this Part of ISO/IEC 15443. This situation arises i.e. when multiple results of assurance are available to a user of assurance, or when a provider of assurance is projecting the use of two or more assurance methods.

Subclauses 4.1.1 and 4.1.2 typically relate to the assurance of product during development and integration. This difference of assurance concern is discussed in subclause 6.

NOTE 3 It is important to understand that the operation of a product typically is under the sole responsibility and supervision of the user organization even if security services are subcontracted to a service provider. Therefore subclauses 4.1.1 and 4.1.2 are not directly applicable to Operational Assurance.

4.1.1 Offering assurance

From the perspective of an organisation offering products, systems or services commercially (or to internal customers) the appropriate assurance method(s) will differ based on the prospective user or user community, their organizational size and expertise. Assurance will have to be customized according to these differences. In particular, assurance has to be sufficiently generic if a community of users is the recipient.

Providing assurances usually is an important factor in terms of additional time-to-market and/or cost involved. Organization providing assurance will have to weigh the benefit against its cost.

Given the above, the first two steps in the decision process are to identify:

– why the user might be willing to pay for assurance;

– to what purpose the user intends to put the assurance.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Taking these steps further we can derive customer assurance requirements and eventually derive the applicable assurance methods.

ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7382541-c1e9-439d-bac8-86389435acd5/iso-iec-tr-15443-3-2007

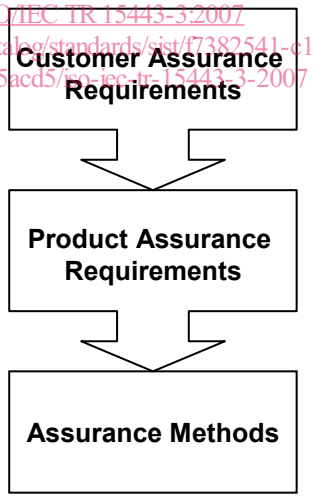

Figure 1 — Assurance Offering

In conclusion assurance may typically be offered as presented in Table 1.

The customer assurance requirements are identified in the form of assurance statement provided by the assurance method.

The supporting assurance arguments and in particular their assurance rigor (refer to Table 3) must be taken into consideration. The majority of assurance methods produce more than one type of assurance requirement and the assurance rigor varies depending upon the method. Thus the combination of assurance methods selected must be done carefully in order to ensure that the users' assurance requirements and ultimately their assurance goals are ultimately satisfied.

© ISO 2007 – All rights reserved

Table 1 — Assurance types offered

Assurance offered	Target customer	Customer assurance requirements	Required assessment rigor
Pass Through Assurance	End user	Content labelling; meaningful and recognisable to the end user	Low
Marketing Assurance	Generic user community	Mark, label, seal; labelling referring to generic assurance needs; presented in a very brief or encapsulated manner; meaningful and recognisable to end user, i.e. recognized "Quality Mark".	Low
Internal Assurance	Internal customer	Proprietary form of assurance statement; provided internal to the organization and based on trust	Any
External Assurance	Specific user community	Labelling including extensive supporting arguments and materials: may have restricted circulation	High
Small Organisation Assurance	Small organisations	Mark or Seal; intended to create trust through belief; meaningful and recognisable to end user, i.e. recognized "Quality Mark". Note: Usually, due to their small organizational size less expertise is available to verify presented assurance claims	Medium
Large Organisation Assurance	Large organisations	Detailed assurance statement Note: Expertise is available to verify assurance claims	High
Mandated Assurance	Specific sophisticated organization	Certificate or Fit-for-purpose statement Assurance form or even the method used is mandated by the organization, e.g. through contractual or registration requirements	High

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-3:2007

4.1.2 Using assurance

The user of an assurance offering has a different perspective. Being the ultimate assurance authority this user's objective is to gain confidence that the specific product satisfies his specific assurance goal, which is the overall security expectation in the product, in the context of the organization in which the product is to be realized, deployed and/or operated.

The assurance goal ideally is established through a risk assessment or may be imposed by organizational policy (refer to Annex E).

Confidence may be gained through selection and application of formal and informal assessment activities which may be offered by vendors, system integrators, or executed by the user or under his mandate for the specific audience requiring proof.

Assurances may be used as presented in Table 2. The table also provides activities by which the user may establish ultimate confidence.

 © ISO 2007 – All rights reserved

Table 2 — Assurance offerings used

User profile	Assurance to look for	User assurance appreciation activities	Related assessment rigor
Specific user	Content labelling	Check if content labelling is meaningful, recognisable and applicable to perceived assurance goal	Low
General user	Mark, label, seal	Check if content labelling is meaningful, recognisable and applicable to perceived assurance goal. A recognized "Quality Mark" is preferable.	Low
Internal customer	Proprietary form of assurance statement	Validate internal trust, e.g. through appropriate questioning.	Any
Member of specific user community	Labelling	Validate trust in the label, e.g. through questioning of other members of community or community organizations.	High
Small organisation	Mark or Seal	Check if content labelling is meaningful, recognisable and applicable to perceived assurance goal. A recognized "Quality Mark" is preferable.	Medium
Large organisation	Detailed assurance statement	Have assurance statements verified and validated by organization's experts.	High
Specific sophisticated organization	Certificate or Fit-for-purpose statement	Trust may be provided by third-party evaluation and/or certification, at least through reputation of assurance provider.	High

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7382541-c1e9-439d-bac8-86389435acd5/iso-iec-tr-15443-3-2007

4.1.3 Residual risk

At its most basic level, assurance provides confidence to the user that a product will function as claimed by the provider, and will not show unintended behaviour. However, unlike other security safeguards, assurance does not provide any additional functionality (security mechanisms) in and of itself, and thus does not counter any additional vulnerability or threat.

All elements of security, in particular risk management, independent of the method used, include uncertainty. This uncertainty arises from many sources such as incomplete knowledge of all factors, tolerances in measurements, extrapolation of factors, etc. This uncertainty can, in some cases, become so large that it represents the major factor of the residual risk. Other factors are the vulnerabilities of the target operating environment and the imperfection of security mechanisms. If the rigor of assurance the security properties and mechanisms is raised, then the uncertainty related to those factors is reduced, thus reducing overall risk.

In certain situations assurance may be the only way to reduce uncertainty. Without adding any new security mechanism, assurance may reduce risk to an acceptable level. In this case the cost of assurance can be directly attributed to the benefit of security. It can be seen from the above that assurance is targeted at risk reduction.

4.2 Applying assurance methods

Assurance methods possess distinguishable properties as components or aspects. To provide guidance in the choice of one or several methods it is necessary to characterize those components and aspects which can be found in different assurance methods in similar form. A given assurance method may include general assurance properties or might focus on specific ones.

© ISO 2007 – All rights reserved

As described in Parts 1 and 2 of ISO/IEC 15443, methods may approach the assurance of a product by assessing:

– the product, either after of during creation of the product;

– the processes used during the creation of the product;

– the environment in which the product is realized, i.e. in terms of the personnel or organization involved.

4.2.1 Assurance rigor

The rigor provided by the assurance method generally prescribes its use as explicated in Table 3.

Table 3 — Assurance rigor and use

Rigor Level	Use
1	simple “Assurance Seal of Approval”,
2	comfort level statements about assurance,
3	detailed facts supporting the claimed assurance,
4	detailed facts supporting the claimed assurance that can be verified,
5	presentation to a general audience, e.g. a board of directors, and recognisable by that audience.
6	presentation to a security professional audience, and recognisable by that qualified audience.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

NOTE 1 In addition the strength of that representation must be taken into consideration and the strength of the supporting arguments for the representation. Limitations and constraints may apply in particular situations.

ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7382541-c1e9-439d-bac8-86389435acd5/iso-iec-tr-15443-3-2007

NOTE 2 When combining assurance evaluated components into a deployable system, metrics may be overlap and/or gaps may be questioned.

NOTE 3 Part 2 of 15443 does not provide a rating of the rigor of assessment provided.

4.2.2 Extent of application

Assurance obtained also may vary by the extent to which the focus of the assurance approach is applied, refer to Table 4.

© ISO 2007 – All rights reserved

Table 4 — Extent of Assurance Approach application

Assurance Approach	Focus of the assurance method	Extent of application
Product	**Properties** of the (completed specific) product, system or service to determine the assurance that can be derived for that product or system	**some** aspects of the product or system
		all aspects of the product or system
Process	Development **process** used by the organization **for a specific** product or system to determine the assurance that can be derived for that product or system	**some** aspects of the development
		all aspects of the development
	Development **process** used by the organization **for all** products and systems	**some** aspects of the development
		all aspects of the development
Environment	Individual(s) employed to perform the tasks	qualification of the individuals(s)
		reputation
	organization	actions the organization will demonstrably take to address any problems found later and the speed of those actions
		reputation

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4.2.3 Application and Life Cycle

ISO/IEC TR 15443-3:2007
https://standards.iteh.ai/catalog/standards/sist/f7382541-c1e9-439d-bac8-80b0f455acd5/iso-iec-tr-15443-3-2007

Part 1 of ISO/IEC TR 15443 has adopted a stage model based on ISO/IEC 15288. Each life cycle stage corresponds to processes applied to a product in an environment. Each of the processes comprises a set of activities and uses resources of its environment.

Applying the processes of each stage, and their activities, a product, system or service deliverable is processed through its life cycle.

Part 1 of ISO/IEC TR 15443 introduced a framework allowing to characterize the type of product, assurance approach, and assurance stage to be assessed.

There are still many issues to be addressed. This clause of this part of ISO/IEC TR 15443 will extend the conceptual framework set up in Part 1 of ISO/IEC TR 15443 to allow further analysis.

In this part of ISO/IEC TR 15443 the Life Cycle stage model will be enhanced by adding the Conception/Specification stage (refer to Table 5).

Presence of processes corresponding to a Conception and/or Specification Stage is postulated by many standards. However, a separate life cycle stage is usually not postulated for these processes. Few assurance methods offer well defined associated processes and activities for this life cycle stage, i.e. a discipline also known as requirements engineering.

The reason for this enhancement in this part of ISO/IEC TR 15443 is the fact that ICT security requires particular attention and an increased effort to produce a coherent and non-contradicting specification for the security features of a product. Few assurance methods offer well defined processes and activities for this life cycle stage suitable to the ICT security domain.

In the enhanced model the different Life Cycle Stages of interest are represented by five columns of the table. For this and approaching the concepts of ISO/IEC 15288 and ISO 9000, the Technical Life Cycle Processes are grouped into five stages, one for each column and abbreviated by one (1) letter:

© ISO 2007 – All rights reserved