TECHNICAL REPORT

ISO/IEC TR 15443-2

First edition
2005-09-01

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

Part 2: 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 2: Méthodes d'assurance

ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed0f-6507-4d42-9ffd-cac260a2fc89/iso-iec-tr-15443-2-2005

Reference number
ISO/IEC TR 15443-2:2005(E)

© ISO/IEC 2005

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 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed0f-6507-4d42-9ffd-cac260a2fc89/iso-iec-tr-15443-2-2005

© ISO/IEC 2005

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 2005 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ad0f-6507-4d42-9ffd-eac269a2f889/iso-iec-tr-15443-2-2005

© ISO/IEC 2005 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed0f-6507-4d42-9ffd-cac260a2fc89/iso-iec-tr-15443-2-2005

© ISO/IEC 2005 – 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 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/40bbcd05-6805-4d42-9ffd-cac260a2fc89/iso-iec-tr-15443-2-2005

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 15443-2, 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*

The following part is under preparation:

— *Part 3: Analysis of assurance methods*

© ISO/IEC 2005 – All rights reserved

Introduction

The objective of this part of ISO/IEC TR 15443 is to describe a variety of assurance methods and approaches that may be applicable to ICT security, as proposed or used by various types of organizations whether they are generally acknowledged, de-facto approved or standardized, and to relate them to the assurance model of ISO/IEC TR 15443-1. The emphasis is to identify qualitative properties of the assurance methods that contribute to assurance, and where possible, to define assurance ratings. This material is catering to an ICT Security professional for the understanding of how to obtain assurance in a given life cycle stage of product or service.

This part of ISO/IEC TR 15443 gives for each item of the collection its aim, description and reference. Each item of collection of assurance methods is then placed within the framework defined in ISO/IEC TR 15443-1.

The assurance methods listed in this part of ISO/IEC TR 15443 are considered to comprise generally known items at the time of its writing. New methods may appear, and enhancements or other modification to the existing ones may occur.

Developers, evaluators, quality managers and acquirers may select assurance methods from this part of ISO/IEC TR 15443 for assurance of the ICT security software and systems; defining assurance requirements, evaluating products, measuring security aspects and other purposes. In complement, they may also use assurance methods which are not included here. This part of ISO/IEC TR 15443 is applicable to the assurance of security aspects, although many of the methods may also be applicable for the assurance of other critical aspects of software and systems.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This part of ISO/IEC TR 15443 is intended to be used together with ISO/IEC TR 15443-1.

ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed0f-6507-4d42-9ffd-ca3260a2f680/iso-iec-tr-15443-2-2005

This part of ISO/IEC TR 15443 will analyze assurance methods that may not be unique to ICT security; however, guidance given in this part of ISO/IEC TR 15443 will be limited to ICT security requirements. Similarly, additional terms and concepts defined in other International standardization 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 ICT security and is not intended for general quality management and assessment, or ICT conformity.

 © ISO/IEC 2005 – All rights reserved

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

Part 2: **Assurance methods**

1 Scope

1.1 Purpose

This part of ISO/IEC TR 15443 provides a collection of assurance methods including those not unique to ICT security as long as they contribute to overall ICT security. It gives an overview as to their aim and describes their features, reference and standardization aspects.

In principle, the resultant ICT security assurance is the assurance of the product, system or service in operation. The resultant assurance is therefore the sum of the assurance increments obtained by each of the assurance methods applied to the product, system or service during its life cycle stages. The large number of available assurance methods makes guidance necessary as to which method to apply to a given ICT field to gain recognized assurance.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/061b0ed0f-6507-4d42-9ffd-eac260a2fe89/iso-iec-tr-15443-2-2005

Each item of the collection presented in this part of ISO/IEC TR 15443 is classified in an overview fashion using the basic assurance concepts and terms developed in ISO/IEC TR 15443-1.

Using this categorization, this part of ISO/IEC TR 15443 guides the ICT professional in the selection, and possible combination, of the assurance method(s) suitable for a given ICT security product, system, or service and its specific environment.

1.2 Field of Application

This part of ISO/IEC TR 15443 gives guidance in a summary and overview fashion. It is suitable to obtain from the presented collection a reduced set of applicable methods to choose from, by way of exclusion of inappropriate methods.

The summaries are informative to provide the basics to facilitate the understanding of the analysis without requiring the source standards.

Intended users of this part of ISO/IEC TR 15443 include the following:

1. acquirer (an individual or organization that acquires or procures a system, software product or software service from a supplier);

2. evaluator (an individual or organization that performs an evaluation; an evaluator may, for example, be a testing laboratory, the quality department of a software development organization, a government organization or a user);

3. developer (an individual or organization that performs development activities, including requirements analysis, design, and testing through acceptance during the software life cycle process);

© ISO/IEC 2005 – All rights reserved

4. maintainer (an individual or organization that performs maintenance activities);

5. supplier (an individual or organization that enters into a contract with the acquirer for the supply of a system, software product or software service under the terms of the contract) when validating software quality at qualification test;

6. user (an individual or organization that uses the software product to perform a specific function) when evaluating quality of software product at acceptance test;

7. security officer or department (an individual or organization that perform a systematic examination of the software product or software services) when evaluating software quality at qualification test.

1.3 Limitations

This part of ISO/IEC TR 15443 gives guidance in an overview fashion only. ISO/IEC TR 15443-3 provides guidance to refine this choice for better resolution of assurance requirements enabling a review of their comparable and synergetic properties.

The regulatory infrastructure to support verification of an assurance approach and the personnel to perform verification is outside the scope of this part of ISO/IEC TR 15443.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 9000, *Quality management systems — Fundamentals and vocabulary*

ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed0f-6507-4d42-9ffd-cac260a2fc89/iso-iec-tr-15443-2-2005

ISO 9001, *Quality management systems — Requirements*

ISO/IEC 9126-1, *Software engineering — Product quality — Part 1: Quality model*

ISO/IEC 12207, *Information technology — Software life cycle processes*

ISO/IEC 13335-1, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

ISO/IEC TR 13335-2, *Information technology — Guidelines for the management of IT Security — Part 2: Managing and planning IT Security*

ISO/IEC TR 13335-3, *Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT Security*

ISO/IEC TR 13335-4, *Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards*

ISO/IEC TR 13335-5, *Information technology — Guidelines for the management of IT Security — Part 5: Management guidance on network security*

ISO/IEC 14598-1, *Information technology — Software product evaluation — Part 1: General overview*

ISO/IEC 15939, *Software engineering — Software measurement process*

ISO/IEC 15288, *Systems engineering — System life cycle processes*

© ISO/IEC 2005 – All rights reserved

ISO/IEC 15408-1, *Information technology —Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*

ISO/IEC 15504-1, *Information technology — Process assessment — Part 1: Concepts and vocabulary*

ISO/IEC 15504-2, *Information technology — Process assessment — Part 2: Performing and assessment*

ISO/IEC 15504-3, *Information technology — Process assessment — Part 3: Guidance on performing an assessment*

ISO/IEC 15504-4, *Information technology — Process assessment — Part 4: Guidance on use for process improvement and process capability determination*

ISO/IEC TR 15504-5, *Information technology — Software Process Assessment — Part 5: An assessment model and indicator guidance*

ISO/IEC 17799, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 21827, *Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 90003, *Software engineering — Guidelines for the application of ISO 9001:2000 to computer software*

ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed0f-6507-4d42-9ffd-cac260a2fc89/iso-iec-tr-15443-2-2005

3 Terms, definitions and abbreviated terms

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

4 Overview and Presentation of Methods

Part 1 of this technical report provides a framework for the categorization of existing assurance methods. This clause lists and presents the available assurance methods that are of interest and directly related to the field of ICT security. It classifies these methods according to the framework:

— according to the different assurance phases - describing its lifecycle aspect: Design, Implementation, Integration, Verification, Deployment, Transition, or Operation;

— according to the different assurance approach: Product, Process or Environment.

As stated in Part 1 of this technical report an assurance method may comprise a combination of assurance approach and assurance phase.

For additional user guidance the overview table in sub-clause 5.4 presents this categorization along with a mention of:

— the ICT security relevance of the individual methods and

— the actuality of the individual methods.

© ISO/IEC 2005 – All rights reserved

5 Assurance Life Cycle Phase and Legend

The overview table in sub-clause 5.4 lists the later presented methods classified according to their Life Cycle Phase. The subclause title of each individual listing repeats this classification.

The different Life Cycle Phases of interest are graphically represented by four columns of the table. For this purpose and approaching the concepts of ISO/IEC 15288 and ISO 9000, the Technical Life Cycle Processes are grouped into four stages, one for each column and abbreviated by one letter as follows:

D **D**esign, including the processes Stakeholder Requirements Definition, Requirements Analysis, Architectural Design and Implementation

I **I**ntegration, including the processes Integration and Verification

T **T**ransition, including the processes Replication, Transition, Deployment and Validation

O **O**peration, including the processes Operation, Maintenance and Disposal

Note 1: A given assurance method may cover one life cycle phase only remotely. In this case, this phase is not flagged in the graphical presentation.

Note 2: The life cycle processes D-I-T-O are those applicable to a specific ICT system and its components, i.e., hardware, software. The development and improvement of the life cycle processes are a second dimension which may be graphically represented but presently is not shown. In ICT security this dimension is particularly important for the security management methods applied to ICT systems in the operations phase, such as ISO/IEC 17799 and BS 7799-2. This second dimension essentially comprises process assessment and documentation, development, measurement, improvement and certification. This second dimension is orthogonal to the D-I-T-O dimension.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5.1 Assurance Approach and Legend

ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed0f-6507-4d42-9ffd-cac260a2fc89/iso-iec-tr-15443-2-2005

The overview table in sub-clause 5.4 lists the later presented methods categorized according to their assurance approach. The subclause title of each individual listing repeats this categorization.

The respective assurance approach categories of the methods are represented symbolically (refer to Table 1):

— Product Assurance: showing the life cycle phase letter within arrows, in a blank " field, e.g. ⇒**D**⇒

— Process Assurance: showing the life cycle phase letter white on shaded background, e.g., **D**

— Environmental assurance: showing the life cycle phase cell as with side bars left and right, e.g. ■ **D** ■.

Table 1 — Assurance methods in the framework - Legend

Clause	Assurance --Phase→ --Approach↓	Design/ Implemen-tation	Integration/ Verification	Deployment /Transition	Operation
	Product[/System/Service] [🔒]	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
	Process [🔒]	D	I	T	O
	Environment [/Organization/Personnel] [🔒]	D	I	T	O

Note 1: As methods may feature a combination of approaches, the symbols may be cumulated; e.g., a method offering both process and environmental assurance will be the letter on a dark field with a dark frame.

Note 2: A given assurance method may cover one approach more or less extensively. This visual overview presentation is not suited to represent the extent of coverage of the various assurance approaches by a given method.

© ISO/IEC 2005 – All rights reserved

Note 3: A given assurance method may cover one approach only remotely. In this case, this approach is not flagged in the graphical presentation.

5.2 Actuality and Legend

As of the great number of methods the user of This part of ISO/IEC TR 15443 is given some direction as to their status. The overview table in sub-clause 5.4 reflects this status as follows:

— the methods presently in relatively wide-spread use and active maintenance are represented in the overview table of sub-clause 5.4 in **bold characters**.

— the methods becoming obsolete, superseded, merged or otherwise loosing actuality are represented in the overview table of sub-clause 5.4 in regular slim characters.

Note: This legend is not repeated in the subclause title of the individual listing.

5.3 Security Relevance and Legend

As of the great number of methods the user of This part of ISO/IEC TR 15443 is given some direction as to their ICT security relevance. The overview table in sub-clause 5.4 and the applicable subclause title reflect this status as follows:

— Methods which are specifically oriented towards ICT security have been awarded a "lock" sign (🔒).

5.4 Overview Table

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Table 2 presents an overview of the considered assurance methods, together with their classification according to the framework developed in Part 1 of this Technical Report, as explained above.

ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed0f-6507-4d42-9ffd-cac260a2fc89/iso-iec-tr-15443-2-2005

© ISO/IEC 2005 – All rights reserved

Table 2 — Assurance methods in the framework - Overview

Clause	Assurance --Phase→ --Approach↓	Design/ Implemen-tation	Integration/ Verification	Deployment/ Transition	Operation
6.1	**ISO/IEC 15408 – Evaluation criteria for IT security**	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.2	TCSEC – Trusted Computer System Evaluation Criteria	⇒D⇒	⇒I⇒		⇒O⇒
6.3	ITSEC/ITSEM – Information Technology Security Evaluation Criteria and Methodology	⇒D⇒	⇒I⇒		⇒O⇒
6.4	CTCPEC – Canadian Trusted Product Evaluation Criteria	⇒D⇒	⇒I⇒		
6.5	**KISEC/KISEM – Korea Information Security Evaluation Criteria and Methodology**	⇒D⇒	⇒I⇒		⇒O⇒
6.6	**RAMP – Rating Maintenance Phase**	⇒D⇒	⇒I⇒		⇒O⇒
6.7	**ERM – Evaluation Rating Maintenance (in general)**	⇒D⇒	⇒I⇒		⇒O⇒
6.8	**TTAP – Trust Technology Assessment Program**	⇒D⇒	⇒I⇒		
6.9	**TPEP – Trusted Product Evaluation Program**	⇒D⇒	⇒I⇒		
6.10	**Rational Unified Process® (RUP®)**	⇒D⇒	⇒I⇒	⇒T⇒	
6.11	**ISO/IEC 15288 – System Life Cycle Processes**	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.12	**ISO/IEC 12207 – Software Life Cycle Processes**	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.13	**V–Model**	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.14	**ISO/IEC 14598 – Software product evaluation**	⇒D⇒			⇒O⇒
6.15	**X/Open Baseline Security Services**	⇒D⇒			
6.16	**SCT – Strict Conformance Testing**		⇒I⇒		
6.17	**ISO/IEC 21827 – Systems Security Engineering – Capability Maturity Model (SSE-CMM®)**	D	I	T	O
6.18	**TCMM – Trusted Capability Maturity Model**	D	I		
6.19	**CMMI – Capability Maturity Model ® Integration**	D	I	T	O
6.20	**ISO/IEC 15504 – Software Process Assessment**	D	I	T	O
6.21	**CMM – Capability Maturity Model® (for Software)**	D	I		

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed06507-4d42-9ff1-cac260a2fc89/iso-iec-tr-15443-2-2005

© ISO/IEC 2005 – All rights reserved

Table 2 *(continued)*

Clause	Assurance --Phase→ --Approach↓	Design/ Implemen-tation	Integration/ Verification	Deployment/ Transition	Operation
6.22	SE-CMM® – Systems Engineering Capability Maturity Model ®	D	I		
6.23	TSDM – Trusted Software Development Methodology	D	I		
6.24	SdoC – Supplier's declaration of Conformity	D			
6.25	SA-CMM® – Software Acquisition Capability Maturity Model®			T	
6.26	ISO 9000 Series – Quality Management	D	I	T	O
6.27	ISO 13407 – Human Centered Design (HCD)	D			
6.28	Developer's Pedigree (in general)	D			
6.29	ISO/IEC 17025 – Accreditation Assurance	D	I		
6.30	ISO/IEC TR 13335 – Guidelines for the management of IT Security (GMITS) 🔒		I	T	O
6.31	BS 7799-2 – Information security management systems – Specification with guidance for use 🔒				O
6.32	ISO/IEC 17799 – Code of practice for information security management 🔒				O
6.33	FR – Flaw Remediation (in general)				O
6.34	IT Baseline Protection Manual 🔒				⇒O⇒
6.35	Penetration Testing 🔒				⇒O⇒
6.36	Personnel Certification (non security related)				O
6.37	Personnel Certification (security related) 🔒	D	I	T	O

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed0f-6507-4d42-9ffd-cae200a2f689/iso-iec-tr-15443-2-2005

5.5 Presentation Methodology

Clause 6 is intended to provide a review of identified assurance methods. Because many assurance methods contribute to different assurance approaches and assurance, each assurance method shall be presented here with its own way of description and views. No comparing is provided at this stage.

In the subclauses Clause 6 there will be a structured synopsis for each assurance method identified in this technical framework.

© ISO/IEC 2005 – All rights reserved

The **title** of the method is the a self explanatory name, if possible the full and official name of the assurance method for proper reference, as well as a Mnemonic for its reference when appropriate.

Each synopsis is broken down into:

- **Aim:** Brief characteristic purpose of the method.
- **Description:** Short description of the method.
- **Sources:** Address/Reference to committees and/or organizations involved, documents the describing method and/or standardisation thereof.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed0f-6507-4d42-9ffd-cac260a2fc89/iso-iec-tr-15443-2-2005

© ISO/IEC 2005 – All rights reserved

6 Assurance Methods

6.1 ISO/IEC 15408 – Evaluation criteria for IT security

⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒

6.1.1 Aim

To provide a harmonized framework and detailed evaluation criteria for ICT security evaluation, suitable for both government and general use.

6.1.2 Description

The Common Criteria were developed on behalf of a number of governmental information security agencies as a way of independently assessing the security characteristics of ICT products and systems. The criteria were developed in conjunction with JTC 1 Subcommittee 27, Security Techniques, and published as International Standard ISO/IEC 15408.

The Common Criteria separate consideration of security functionality from security assurance and specify detailed techniques and functions that can aid in the development of confidence that a security product or system meets its security objectives. The specific assurance techniques and functions are defined in ISO/IEC 15408-3, and are primarily, but not exclusively, aimed towards assurance obtained through independent assessment or verification. It is intended that consistent application of the evaluation criteria can be verified through national certification schemes.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Within ISO/IEC 15408-3, assurance techniques are divided into different areas of applicability, called classes. Within each class, different techniques are identified, called families. Each family then identifies one or more levels of rigor by which the technique can be applied; these are called components. Each component specifies the precise actions and evidence elements required.

ISO/IEC TR 15443-2:2005
https://standards.iteh.ai/catalog/standards/sist/06b9ed0f-6507-4d42-9ffd-cac260a2fc89/iso-iec-tr-15443-2-2005

A number of packages of assurance components that work together in a complementary manner are defined within ISO/IEC 15408-3. These are called Evaluation Assurance Levels (Earls).

A supporting methodology for application of these criteria, the Common Evaluation Methodology, is being developed by the Common Evaluation Methodology Working Group, part of the Common Criteria project.

6.1.3 Sources

Refer to Clause 2: ISO/IEC 15408-1, ; ISO/IEC 15408-2, ; ISO/IEC 15408-3,

Note: ISO/IEC 15408 is a product of the committee:
ISO/IEC JTC 1/SC 27/WG 3 Information technology - Security techniques - Security evaluation criteria

© ISO/IEC 2005 – All rights reserved