AS/NZS ISO/IEC 15443.1:2006
ISO/IEC TR 15443-1:2005

AS/NZS ISO/IEC 15443.1:2006

Australian/New Zealand Standard™

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

Part 1: Overview and framework

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Full document details: AS NZS ISO IEC 15443.1-2006

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification. It was approved on behalf of the Council of Standards Australia on 23 June 2006 and on behalf of the Council of Standards New Zealand on 30 June 2006.
This Standard was published on 2 August 2006.

The following are represented on Committee IT-012:

Attorney General's Department
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Certification Forum of Australia
Department of Defence
Department of Social Welfare, NZ
Government Communications Security Bureau, NZ
Internet Industry Association
NSW Police Service
New Zealand Defence Force
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 06257.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15443.1-2006

Australian/New Zealand Standard™

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

Part 1: Overview and framework

First published as AS/NZS ISO/IEC 15443.1:2006.

COPYRIGHT

© Standards Australia/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 7659 0

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

AVA Documents Document Sharing Hub

Full document details: AS NZS ISO IEC 15443.1-2006

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification.

The objective of this Standard 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 organisms whether they are approved or de-facto standards.

This Standard provides an overview of the fundamental concepts and a general description of assurance methods. It targets IT security manages and others responsible for developing a security assurance program, determining the security assurance of their deliverable, entering an assurance assessment audit or other assurance.

This Standard is identical with, and has been reproduced from ISO/IEC TR 15443-1:2005, *Information technology—Security techniques—A framework for IT security assurance*—Part 1: *Overview and framework*.

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover

(b) In the source text ‘this part of ISO/IEC TR 15443’ should read ‘this Australian/New Zealand Standard’.

(c) A full point substitutes for a comma when referring to a decimal marker.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15443.1-2006

CONTENTS

Page

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

2 Terms and definitions 1

3 Abbreviated terms 6

4 Concepts 7
4.1 Why do we need assurance? 8
4.2 Assurance is distinguishable from confidence 8
4.3 What is a deliverable? 8
4.4 Stakeholders 9
4.5 Assurance requirements 9
4.6 Assurance methods applicability to IT security 10
4.7 Assurance schemes 10
4.8 Quantifying assurance risk and mechanism strength 11
4.9 Assurance reduces security risk 11
4.10 Quantifying assurance 11
4.11 Assurance authority 11

5 Selecting security assurance 12
5.1 Assurance requirements specification 13
5.2 Economical aspects 13
5.3 Organisational aspects 14
5.4 Type of assurance 14
5.5 Technical aspects 15
5.6 Optimisation considerations 15

6 Framework 16
6.1 Assurance approach 16
6.2 Assurance methods 16
6.3 Life cycle aspects 17
6.4 Correctness versus effectiveness assurance 18
6.5 Categorisation of assurance methods 19
6.6 Composite assurance 20
6.7 Assurance rating 20

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15443.1-2006

NOTES

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15443.1-2006

AUSTRALIAN/NEW ZEALAND STANDARD

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

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15443.1-2006

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).

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15443.1-2006

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].

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15443.1-2006

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.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 15443.1-2006