Australian/New Zealand Standard™

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

Part 1: Overview and framework

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 Standards may also be withdrawn.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.

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.

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

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.

CONTENTS

Page

NOTES

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