AS/NZS ISO/IEC 38500:2010
ISO/IEC 38500:2008

AS/NZS ISO/IEC 38500:2010

Australian/New Zealand Standard™

Corporate governance of information technology

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-030, ICT Governance and Management. It was approved on behalf of the Council of Standards Australia on 5 February 2010 and on behalf of the Council of Standards New Zealand on 8 February 2010.
This Standard was published on 1 March 2010.

The following are represented on Committee IT-030:

Australian Bankers Association
Australian Chamber of Commerce and Industry
Australian Computer Society
Australian Industry Group
Australian Information Industry Association
Australian Institute of Company Directors
Australian Institute of Project Management
Australian Prudential Regulation Authority
Consumers' Federation of Australia
Council of Small Business Organisations of Australia
Department of Communications, Information Technology and the Arts
Department of Defence (Australia)
Department of Finance and Administration (Federal)
Engineers Australia
Information Systems, Audit and Control Association
IT Service Management Forum (Australia)
Macquarie University
NZ Computer Society
Project Management Institute
RMIT University
Society of Consumer Affairs Professionals
Software Quality Association (ACT)

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 Standards may also be withdrawn.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.saiglobal.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

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 AS/NZS ISO/IEC 38500.

Australian/New Zealand Standard™

Corporate governance of information technology

First published as AS 8015—2005.
Jointly revised and redesignated as AS/NZS ISO/IEC 38500:2010.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6140

ISBN 978 0 7337 9413 1

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-030, ICT Governance and Management.

The objective of this Standard is to promote effective, efficient and acceptable use of IT in all organisations.

It is anticipated that this Standard will generate net benefit to the Australian community, particularly in organizations of all sizes, by saving money associated with IT by avoiding failures and increasing realised benefits.

The realisation of net benefit arising from the implementation of this Standard will be tested through a review of take up by nominating organizations participating on committee IT-030 within three years of publication of this Standard.

This Standard is identical with, and has been reproduced from, ISO/IEC 38500:2008. ISO/IEC 38500:2008 was the result of the 'fast track' adoption of the Australian Standard AS 8015—2005 by ISO/IEC JTC 1. AS 8015—2005 was prepared by Standards Australia Technical Committee IT-030. ISO/IEC 38500:2008 substantially reflects both the content and intent of AS 8015—2005.

ISO/IEC 38500:2008 is a high level, principle based advisory Standard. In addition to providing board guidance on the role of a governing body, it encourages organizations to use appropriate standards to underpin their governance of IT.

At the time of publication of this Standard, IT-030 is continuing efforts to develop further documents relating to the governance of Information Technology.

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 Standard' should read 'this Australian/New Zealand Standard'.

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

None of the normative references in the source document have been adopted as Australian or Australian/New Zealand Standards.

CONTENTS

Page

INTRODUCTION

The objective of this standard is to provide a framework of principles for Directors to use when evaluating, directing and monitoring the use of information technology (IT) in their organizations.

Most organizations use IT as a fundamental business tool and few can function effectively without it. IT is also a significant factor in the future business plans of many organizations.

Expenditure on IT can represent a significant proportion of an organization's expenditure of financial and human resources. However, a return on this investment is often not realized fully and the adverse effects on organizations can be significant.

The main reasons for these negative outcomes are the emphasis on the technical, financial and scheduling aspects of IT activities rather than emphasis on the whole business context of IT use.

This standard provides a framework for effective governance of IT, to assist those at the highest level of organizations to understand and fulfil their legal, regulatory, and ethical obligations in respect of their organizations' use of IT. The framework comprises definitions, principles and a model.

This standard is aligned with the definition of Corporate Governance that was published as a Report of the Committee on the Financial Aspects of Corporate Governance (the Cadbury Report) in 1992. The Cadbury Report also provided the foundation definition of Corporate Governance in the OECD Principles of Corporate Governance in 1999 (revised in 2004). Users of this standard are encouraged to familiarise themselves with the Cadbury Report and the OECD Principles of Corporate Governance.

Governance is distinct from management, and for the avoidance of confusion, the two concepts are clearly defined in the standard.

While this standard is addressed primarily to the governing body, which may in turn direct that certain actions be taken by the management of the organization, it also allows that, in some (typically smaller) organizations, the members of the governing body may also occupy the key roles in management. In this way, it ensures that the standard is applicable for all organizations, from the smallest, to the largest, regardless of purpose, design and ownership structure.

The standard is also intended to inform and guide those involved in designing and implementing the management system of policies, processes, and structures that support governance.

AUSTRALIAN/NEW ZEALAND STANDARD

Corporate governance of information technology

1 SCOPE, APPLICATION AND OBJECTIVES

1.1 Scope

This standard provides guiding principles for directors of organizations (including owners, board members, directors, partners, senior executives, or similar) on the effective, efficient, and acceptable use of Information Technology (IT) within their organizations.

This standard applies to the governance of management processes (and decisions) relating to the information and communication services used by an organization. These processes could be controlled by IT specialists within the organization or external service providers, or by business units within the organization.

It also provides guidance to those advising, informing, or assisting directors. They include:

- senior managers;
- members of groups monitoring the resources within the organization;
- external business or technical specialists, such as legal or accounting; specialists, retail associations, or professional bodies;
- vendors of hardware, software, communications and other IT products;
- internal and external service providers (including consultants);
- IT auditors.

1.2 Application

This standard is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. The standard is applicable to organizations of all sizes from the smallest to the largest, regardless of the extent of their use of IT.

1.3 Objectives

The purpose of this standard is to promote effective, efficient, and acceptable use of IT in all organizations by:

- assuring stakeholders (including consumers, shareholders, and employees) that, if the standard is followed, they can have confidence in the organization's corporate governance of IT;
- informing and guiding directors in governing the use of IT in their organization; and
- providing a basis for objective evaluation of the corporate governance of IT.

1.4 Benefits of Using This Standard

1.4.1 General

This standard establishes principles for the effective, efficient and acceptable use of IT. Ensuring that their organisations follow these principles will assist