AS ISO/IEC 38500:2016
ISO/IEC 38500:2015

AS ISO/IEC 38500:2016

Australian STANDARD

Information technology—Governance of IT for the organization

STANDARDS Australia

This Australian Standard® was prepared by Committee IT-030, ICT Governance and Management. It was approved on behalf of the Council of Standards Australia on 6 December 2016.
This Standard was published on 23 December 2016.

The following are represented on Committee IT-030:

- Australian Computer Society
- Australian Information Industry Association
- Australian Institute of Company Directors
- Consumers' Federation of Australia
- Department of Finance (Australian Government)
- Governance Institute of Australia
- ISACA
- IT Service Management Forum (Australia)
- Project Management Institute
- Quantitative Enterprise Software Performance
- Women on Boards

This Standard was issued in draft form for comment as DR AS ISO/IEC 38500:2016.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that 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Standards may also be withdrawn.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 that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Information technology—Governance of IT for the organization

First published as AS 8015—2005.
Jointly revised and redesignated as AS/NZS ISO/IEC 38500:2010.
Revised and redesignated as AS ISO/IEC 38500:2016.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 1 76035 647 7

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-030, ICT Governance and Management, to supersede AS/NZS ISO/IEC 38500:2010, *Corporate governance of information technology*.

After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian Standard rather than an Australian/New Zealand Standard.

The objective of this Standard is to provide guiding principles for members of governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use, both current and future, of information technology (IT) within their organizations. This Standard is applicable to all organizations regardless of their size and type.

This Standard is identical with, and has been reproduced from ISO/IEC 38500:2015, *Information technology—Governance of IT for the organization.*

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

(a) In the source text 'this International Standard' should read 'this Australian Standard'.

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

There are no normative references in the source document.

CONTENTS

INTRODUCTION

The objective of this International Standard is to provide principles, definitions, and a model for governing bodies to use when evaluating, directing, and monitoring the use of information technology (IT) in their organizations.

This International Standard is a high level, principles-based advisory standard. In addition to providing broad guidance on the role of a governing body, it encourages organizations to use appropriate standards to underpin their governance of IT.

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 on 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 use of IT.

This International Standard provides principles, definitions, and a model for good 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.

This International 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). Governance is distinct from management, and for the avoidance of confusion, the two concepts are defined in this International Standard and elaborated in ISO/IEC TR 38502.

This International Standard is addressed primarily to the governing body. In some (typically smaller) organizations, the members of the governing body can also be executive managers. This International Standard is applicable for all organizations, from the smallest to the largest, regardless of purpose, design, and ownership structure.

The implementation of governance of IT is covered by ISO/IEC TS 38501.

AUSTRALIAN STANDARD

Information technology—Governance of IT for the organization

1 Scope

This International Standard provides guiding principles for members of governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of information technology (IT) within their organizations.

It also provides guidance to those advising, informing, or assisting governing bodies. They include the following:

— executive managers;

— members of groups monitoring the resources within the organization;

— external business or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies;

— internal and external service providers (including consultants);

— auditors.

This International Standard applies to the governance of the organization's current and future use of IT including management processes and decisions related to the current and future use of IT. These processes can be controlled by IT specialists within the organization, external service providers, or business units within the organization.

This International Standard defines the governance of IT as a subset or domain of organizational governance, or in the case of a corporation, corporate governance.

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

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

— assuring stakeholders that, if the principles and practices proposed by the standard are followed, they can have confidence in the organization's governance of IT,

— informing and guiding governing bodies in governing the use of IT in their organization, and

— establishing a vocabulary for the governance of IT.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
acceptable
meets stakeholder expectations that are capable of being shown as reasonable or merited

2.2
accountable
answerable for actions, decisions, and performance

