

AS/NZS ISO/IEC 38506:2020
ISO/IEC 38506:2020



Australian/New Zealand Standard™

Information technology — Governance of IT — Application of ISO/IEC 38500 to the governance of IT enabled investments



AS/NZS ISO/IEC 38506:2020

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 25 November 2020 and by the New Zealand Standards Approval Board on 2 December 2020.

This Standard was published on 11 December 2020.

The following are represented on Committee IT-030:

Australian Information Industry Association
Australian Institute of Company Directors
Consumers' Federation of Australia
Department of Finance (Australian Government)
Governance Institute of Australia
Institute of Internal Auditors — Australia
ISACA
IT Professionals New Zealand
IT Service Management Forum (Australia)
Manukau Institute of Technology
NSW Department of Customer Services
Project Management Institute Australian Chapters
Women on Boards

This Standard was issued in draft form for comment as DR AS/NZS ISO/IEC 38506:2020.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

www.standards.govt.nz

ISBN 978 1 76113 117 2

Australian/New Zealand Standard™

Information technology — Governance of IT — Application of ISO/IEC 38500 to the governance of IT enabled investments

First published as AS/NZS ISO/IEC 38506:2020.

COPYRIGHT

© ISO/IEC 2020 — All rights reserved

© Standards Australia Limited/the Crown in right of New Zealand, administered by the New Zealand Standards Executive 2020

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, unless otherwise permitted under the Copyright Act 1968 (Cth) or the Copyright Act 1994 (New Zealand).

Preface

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

The objective of this document is to provide guidance on governance of IT enabled investments to the governing body of all forms of organizations, whether private, public or government entities, and will equally apply regardless of the size of the organization or its industry or sector. The terms “business” and “business outcome” throughout this document include all forms of organization.

This document provides guidance to other parties interacting with governing bodies such as project personnel, accountants, management consultants, investment portfolio managers and governance support staff.

This document also provides guidance that can be applied in the due diligence process related to business acquisitions. This document may provide guidance on the application of the principles documented in AS ISO/IEC 38500 for ranking IT enabled investments including assessing the value and risks of IT elements in the context of investment banking or as performed by investment companies.

This document does not prescribe or define specific management practices required for IT enabled investments.

This document is identical with, and has been reproduced from, ISO/IEC 38506:2020, *Information technology — Governance of IT — Application of ISO/IEC 38500 to the governance of IT enabled investments*.

As this document has been reproduced from an International Standard, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface	ii
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Good governance of IT enabled investments	2
4.1 Benefits of good governance of IT enabled investments	2
4.2 Focus on value	2
4.3 Accountability of the governing body	3
5 The model for good governance of IT enabled investments	4
5.1 The model for good governance applied to the governance of IT enabled investments	4
5.1.1 Evaluate	4
5.1.2 Direct	5
5.1.3 Monitor	6
6 Principles for governance of IT enabled investments	6
6.1 General	6
6.2 Principle 1 — Responsibility	7
6.2.1 Applying the principle	7
6.2.2 Implications for the governing body	7
6.2.3 Desired outcomes	7
6.2.4 Governance behaviours	7
6.3 Principle 2 — Strategy	8
6.3.1 Applying the principle	8
6.3.2 Implications for the governing body	8
6.3.3 Desired outcomes	8
6.3.4 Governance behaviours	9
6.4 Principle 3 — Acquisition	9
6.4.1 Applying the principle	9
6.4.2 Implications for the governing body	9
6.4.3 Desired outcomes	9
6.4.4 Governance behaviours	10
6.5 Principle 4 — Performance	10
6.5.1 Applying the principle	10
6.5.2 Implications for the governing body	10
6.5.3 Desired outcomes	10
6.5.4 Governance behaviours	11
6.6 Principle 5 — Conformance	11
6.6.1 Applying the principle	11
6.6.2 Implications for the governing body	11
6.6.3 Desired outcomes	11
6.6.4 Governance behaviours	12
6.7 Principle 6 — Human behaviour	12
6.7.1 Applying the principle	12
6.7.2 Implications for the governing body	12
6.7.3 Desired outcomes	12
6.7.4 Governance behaviours	13
Bibliography	14

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see <http://patents.iec.ch>).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 40, *IT Service Management and IT Governance*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

In today's rapidly evolving digital age, the world is experiencing unpredictable changes through shifts in political and economic power combined with disruptive business models, seemingly constant technology breakthroughs and innovative approaches to conducting business.

How can governing bodies prepare their organizations to address constant and new challenges while being ready for an increasing information and technology driven future?

Information Technology (IT) supports the core functions of all organizations, underpins the basis of almost all business activities and interfaces with customers and other stakeholders. Investments in IT enablement and the contribution of IT to the business capability and performance of the organization play a significant role in the achievement of strategic plans and the delivery of business value.

Effective governance of IT enabled investments will provide governing bodies with a better understanding of their obligations and how value is derived to support the organization's business opportunities and to appropriately mitigate the organisation's risk.

Risks comprise such things as the failure to deliver required capabilities, failure of the business to achieve the required benefits, with the impact on the organization leading to e.g. business disruption, breach of obligations, regulatory non-compliance, failures of security, loss of data, down time. Effective governance will proactively prevent or mitigate the IT aspects of the risk of such events occurring, for example, by addressing prolonged underinvestment.

Governance of IT, including investments in IT, is part of sound corporate governance. Governance of IT is not IT management but should be supported by a governance framework and the organization's IT management system.

This document provides guidelines to members of the governing bodies to apply the principles and model documented in ISO/IEC 38500 to IT enabled investments. Throughout this document the word "investments" is synonymous with IT enabled investments.

NOTES