INTERNATIONAL STANDARD

ISO/IEC 38506

First edition
2020-02

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

Technologies de l'information — Gouvernance des technologies de l'information — Application de l'ISO/IEC 38500 à la gouvernance des investissements reposant sur les technologies de l'information

Reference number
ISO/IEC 38506:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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 ... 5
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 ... 10
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 ... 11
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 ... 12
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 ... 13
6.7.4 Governance behaviours ... 13

Bibliography ... **14**

© ISO/IEC 2020 – All rights reserved

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.

© ISO/IEC 2020 – All rights reserved

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.

© ISO/IEC 2020 – All rights reserved

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

1 Scope

This document provides 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 covered by this document.

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

IT enabled investments within the scope of this document could be investments of any scale from acquiring businesses to any business change incorporating IT, building new business services or addressing effectiveness and efficiency gains in IT operational services to gain competitive edge, whether those services are internal or provided by external parties.

Resource allocation for strategic innovation is addressed by providing guidance to the governing body's decision for investment resource allocation between short-, medium- and long-term innovation projects.

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 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.

ISO/IEC TS 38501 contains guidance on the implementation arrangement for the effective governance of IT in general. The constructs in ISO/IEC TS 38501 can help to identify internal and external factors relating to the governance of IT and to define beneficial outcomes and identify evidence of success. ISO/IEC TR 38502 contains guidance on the integration between the governing body and management of an organization in general.

This document is written in accordance with the principles of ISO/IEC TR 38504:2016.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 38500:2015, *Information technology — Governance of IT for the organization*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 38500 and the following apply.

© ISO/IEC 2020 – All rights reserved

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
benefit
created advantage, value or other positive effect

[SOURCE: ISO 21505:2017, 3.4]

3.2
governance framework
strategies, policies, decision-making structures and accountabilities through which the organization's governance arrangements operate

[SOURCE: ISO/IEC TR 38502:2017, 3.1]

3.3
IT enabled investments
investments that are dependent on the use of information technology for the achievement of business outcomes

3.4
value
quantifiable financial or non-financial gain

[SOURCE: ISO 37500:2014, 3.25]

4 Good governance of IT enabled investments

4.1 Benefits of good governance of IT enabled investments

When technology investment outcomes are established as assets rather than cost elements, they become a strategic enabler of growth and sustainability of organizations in an increasingly competitive environment.

Good governance of IT enabled investments helps the organization to ensure that those investments contribute positively to the performance and conformance of the organization through:

— giving priority to investments that align with the organization's strategy and business objectives and have the potential to return the greatest value to the organization;

— optimising the value from investments;

— providing a mechanism for appropriate risk mitigation of the investments;

— balancing investments between short and longer term outcomes to ensure continued business sustainability;

— ensuring conformance with obligations (regulatory, legislation, common law and contractual).

Inadequate governance of IT enabled investments can expose an organization to loss of confidence by clients and consumers in the brand or product/services being provided, unsuccessful or delayed innovation and penalties of not being conformant with obligations.

4.2 Focus on value

The value to the organization of any and all investments should be the first and main focus when evaluating and prioritizing investments.

© ISO/IEC 2020 – All rights reserved