

---

---

**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*

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

[ISO/IEC 38506:2020](https://standards.iteh.ai/catalog/standards/sist/1e524e6e-883f-4c4b-b3a7-11869c5b7197/iso-iec-38506-2020)

<https://standards.iteh.ai/catalog/standards/sist/1e524e6e-883f-4c4b-b3a7-11869c5b7197/iso-iec-38506-2020>



**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO/IEC 38506:2020

<https://standards.iteh.ai/catalog/standards/sist/1e524e6e-883f-4c4b-b3a7-11869c5b7197/iso-iec-38506-2020>



**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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Good governance of IT enabled investments</b> .....	<b>2</b>
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
<b>5 The model for good governance of IT enabled investments</b> .....	<b>4</b>
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
<b>6 Principles for governance of IT enabled investments</b> .....	<b>6</b>
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
<b>Bibliography</b> .....	<b>14</b>

## 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](http://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](http://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](http://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](http://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.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC 38506:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/1e524e6e-883f-4c4b-b3a7-11869c5b7197/iso-iec-38506-2020>

# 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 38506:2020(E)

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]

**STANDARD PREVIEW**  
(standards.iteh.ai)

## 4 Good governance of IT enabled investments

ISO/IEC 38506:2020  
<https://standards.iteh.ai/catalog/standards/sist/1e524e6e-883f-4c4b-b3a7-11869c5b7197/iso-iec-38506-2020>

### 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.



Value from IT enabled investments is not realized by the implementation of IT alone. The achievement of value requires complementary planned business changes, including but not limited to, purpose, organizational values, culture, organization structure, business processes, roles and responsibilities, people skills and reward systems. For successful implementation of IT enabled investment, significant business resources are required and the impact to the business should always be considered foremost. The interdependencies between the business strategy and the underlying technology is inseparable. The achievement of such changes can be difficult to sustain over time, and the governing body should continue to monitor the organization's ability to maintain the required commitment to business changes over time.

Value may relate to increased market share, new opportunities developed, increased customer satisfaction or improved customer access. In addition, direct cost reduction on process outsourcing cost and conformance to rules and regulations can also provide value to an organization. Furthermore, value may be due to societal or environmental objectives. However, the expected value should be clearly defined and be measurable by an accepted mechanism to ensure realization of that value.

The value of business change may be enabled directly by adoption of innovative IT assets and IT capabilities in new business services or products. However, the indirect value of investments in underlying and supportive IT assets, for example infrastructure components or security capabilities, should be carefully evaluated and continued maintenance should be appropriately prioritized within the portfolio of investments.

When considering a business acquisition, value assessment could be obtained by ensuring that a structured due diligence process includes evaluation of performed IT governance principles and practices, IT assets and IT capabilities.

The value forecast from IT enabled investments, as with all investments, should also be evaluated against time and resource diversion from other business activities. Risk based prioritization should be made between current product/services and future product/service development.

Specific guidance relating to focus on value are made in [Clauses 5 and 6](#).

### 4.3 Accountability of the governing body

The governing body is ultimately accountable for the success of all investments an organization undertakes. This accountability derives from the governing body's accountability for governance of the organization and consequently the governance of the IT within the organization.

The governing body should exhibit the same behaviours with all investments whether IT enabled or not.

The governing body should take and retain accountability of business change, to take visible and active leadership and champion the investments rather than delegate all responsibility, as a result, creating an environment for successful strategic innovation. With clear visibility of outcomes, value creation and mitigation of risks will increase the likelihood of successful investment.

The governing body should establish, promote and support an environment to enable the success of the organization's investments, and provide the leadership to support the people involved.

An environment without surprises for the governing body and a supportive response to messages about potential problems builds on two-way trust and transparency and ensures alignment of objectives.

Accountability for the effective, efficient and acceptable use of IT and the success of the organization's investments in IT remain with the governing body and cannot be delegated. Retaining a level of engagement by the governing body significantly increases the organizational focus on successful outcomes and value realization of all investments.

The governing body can delegate the decision-making authority and hold the management accountable for aspects of investments, ensuring that management have the requisite competence to satisfy such responsibilities associated with the delegation, and that the governing body itself retains appropriate

visibility of key decisions. The governing body should clearly communicate the management’s accountability for outcomes.

The governing body should retain visibility of investments that involve:

- a focus on strategic innovation, with potential to provide continued long-term competitive advantage;
- investments evaluated to have high risk to the organization’s sustainability of existence;
- investments evaluated to require a commitment of significant financial magnitude;
- high levels of integration with other investments and/or business activity.

## 5 The model for good governance of IT enabled investments

### 5.1 The model for good governance applied to the governance of IT enabled investments

ISO/IEC 38500 introduces a model for the governance of IT that establishes a cycle of Evaluate – Direct– Monitor. This “EDM” model describes the three main tasks for governing IT and has been applied to the governance of IT enabled investments in the following clauses.

Figure 1 shows the model as it applies to IT enabled investments. This figure is based on the model in ISO/IEC 38500:2015, Figure 1.

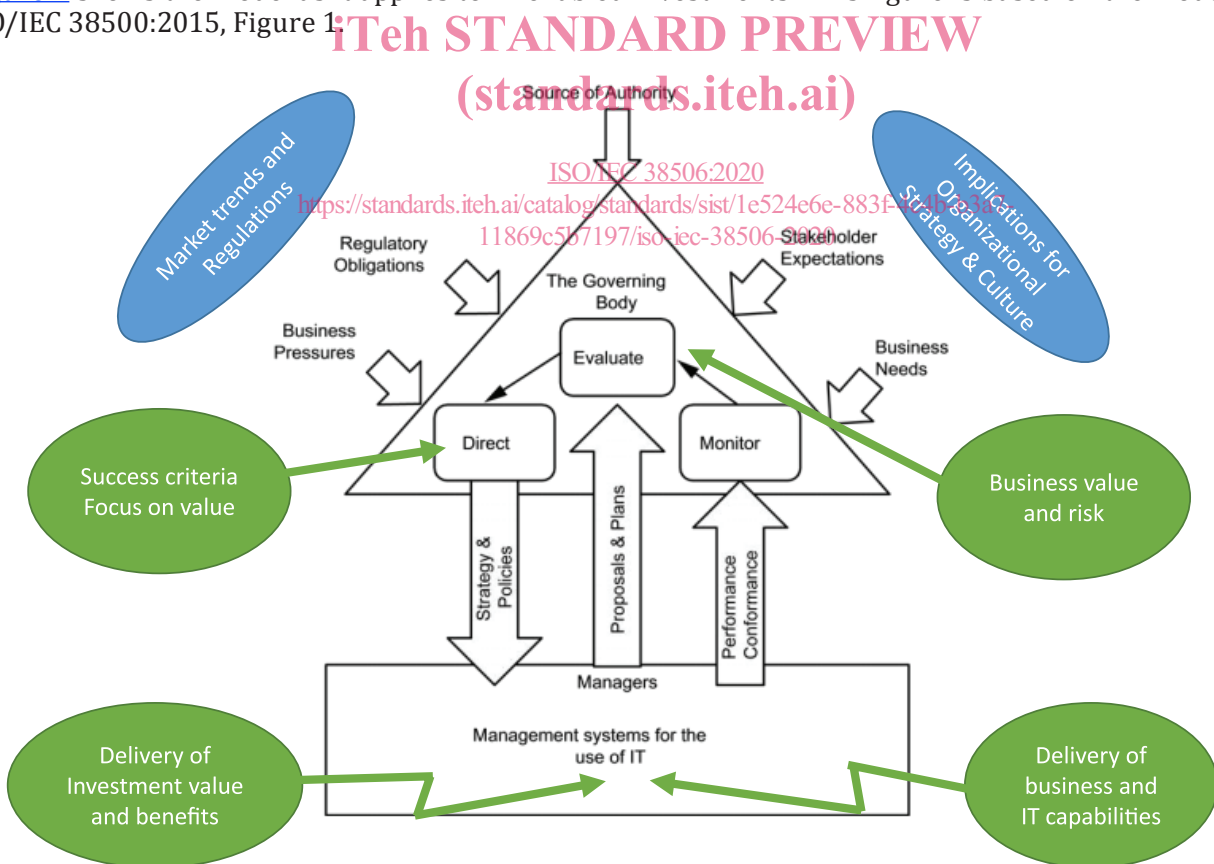


Figure 1 — Model for governance of IT

### 5.1.1 Evaluate

In applying the ISO/IEC 38500 model the key questions asked by the governing body, when evaluating IT enabled investments, should include the following:

- To what extent is value being created or eroded by the investments over the full lifecycle of the investment decision?
- In what way does the portfolio of investments deliver to the business strategy plan, the development of existing and new (business and IT) capabilities and is the timing right for the business?
- Is the resource allocation between short- and long-term investments right for ensuring relevant business capabilities?
- What steps are being taken to enhance and protect the reputation and brand of the business, is the trustworthiness of the organization being considered?
- How are security, privacy, data governance, legal, societal and business requirements being enforced?
- Does the risk profile of the overall portfolio of IT enabled investment sufficiently business sustainability and match the organization's risk appetite?
- Is the balance between growth, innovation and cost reduction consistent with the organization's strategic objectives for IT effectiveness and efficiency?
- What use is being made of evolving technologies to optimise the future growth of the organization?
- Is the overall level of business change right for the capability of the organization, customers and external stakeholders?
- What are the organizational barriers where the governing body's assistance is required to ensure an environment for success?
- Is the proposed approach to deliver the investment appropriate and consistent with future strategic direction on development versus acquisition, internal versus outsourcing, service versus product?

### 5.1.2 Direct

The governing body should direct the establishment of a framework for control and visibility of investments that is appropriate to the size, number and type being undertaken. The governance framework and management system may:

- direct that the focus of all investments is to create and sustain short- and long-term business value where value is a function of strategic alignment, benefits, costs and risks over the full life cycle of an investment;
- direct that the investments include all the necessary business changes for the expected value to be realized;
- direct that the investments must have an accountable business owner/sponsor and that relevant metrics and feedback mechanisms are in place to ensure and assure the value is delivered;
- direct that business strategic plans include identified success criteria to drive the investments;
- direct clearly defined policies, processes, responsibilities and accountabilities for transparency in delegated decision-making authority;
- direct the required speed, timeliness and resource allocation with respect to the innovation investment or application of current and future technologies;
- direct the application of appropriate due diligence for all types of investments;