TECHNICAL REPORT

ISO/IEC TR 38502

Second edition
2017-12

Information technology — Governance of IT — Framework and model

Technologies de l'information — Gouvernance des TI — Cadre général et modèle

Reference number
ISO/IEC TR 38502:2017(E)

© ISO/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Model and framework **2**
4.1 Model for governance of IT 2
4.1.1 Governing body responsibilities and accountabilities 2
4.1.2 Governance tasks 3
4.1.3 Managers' responsibilities and accountabilities 3
4.1.4 Applicability of the model 3
4.2 Relationship between governance and management of IT 3
4.3 Key elements of a governance framework for IT 4
5 Guidance on the application of the model **5**
5.1 Responsibilities of the governing body 5
5.1.1 General 5
5.1.2 Governing body and oversight mechanisms 6
5.2 Strategy formulation and oversight 6
5.2.1 General 6
5.2.2 The governing body's role in strategy formulation 6
5.3 Delegation 7
5.3.1 General 7
5.3.2 Delegation by the governing body 7
5.4 Responsibilities of managers 8
5.4.1 General 8
5.4.2 The role of managers 8
5.5 Governance and internal control 9
5.5.1 General 9
5.5.2 Establishing internal control 9
Annex A (informative) **Principles of good governance of IT** **10**
Bibliography **11**

© ISO/IEC 2017 – 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO/IEC TR 38502:2014) of which it constitutes a minor revision comprising the following changes:

— in Clause 1 “Scope” and the definition 3.3 “Note 2 to entry” the inappropriate words “have to” have been deleted;

— a new Clause 2 “Normative references” has been inserted stating that there are no normative references in this document with the following clauses and sub-clauses appropriately renumbered as a consequence;

— at the beginning of Clause 3 “Terms and definitions” the applicability of “the terms and definitions given in ISO/IEC 38500:2015” is stated in addition and the standard referral to the ISO and IEC terminological databases is also given;

— in Clause 3 “ Terms and definitions” all definitions given in ISO/IEC 38500:2015 have been deleted and the remaining definitions renumbered;

— Figure 1 has been updated to include an ampersand in the Performance/Conformance arrow making it identical with Figure 1 in ISO/IEC 38500:2015 and the caption has been updated to reflect this;

— in the Bibliography reference [1] to ISO/IEC 38500 has been updated to reflect its current title “*Information technology — Governance of IT for the organization*”.

© ISO/IEC 2017 – All rights reserved

Introduction

The measure of success for any investment in the use of information technology (IT), whether for new initiatives or on-going operations, is the benefit that it brings to the organization making the investment.

Benefits from investment in IT are typically not derived directly from the actual IT acquired or supported. Rather, realized benefits are a result of changes in business activities enabled by the use of the technology to meet organizational needs or requirements. Organizations need strategies and support arrangements for IT which maximize the value from such investments while managing the risks associated with the use of IT. Risks comprise such things as the failure to deliver required capabilities, failure of the business to achieve the required benefits, and the impact on the organization from IT failures leading to business disruption, breach of obligations, regulatory non-compliance, failures of security, loss of data, down time, etc.

One of the challenges for organizational investment in IT is ensuring that such investment and acquisition decisions are based on business strategies, priorities and needs. Those responsible for governance of the organization should therefore have appropriate oversight and involvement in decisions related to the use of IT in the business, to ensure that such decisions are based on business strategies, risk appetite, priorities and needs. The effort required to derive the expected benefits should be identified and understood.

ISO/IEC 38500[1] recognizes that the proper balance of demand and supply of IT is a requirement of good governance and management, which must be driven from the top of an organization. The objective of ISO/IEC 38500 is to provide guidance for the governing body of organizations when evaluating, directing and monitoring the use of IT in their organizations.

There is evidence of confusion in the market place regarding the use of the term *governance* when it applies to IT. For instance, there is often inappropriate application of the term *governance* to *management systems*, *control frameworks* and *information systems* that are not, in themselves, governance, but which are both outcomes of, and necessary enablers for, effective governance. As a result, there is often confusion about the respective roles of governance and management, and this has hindered the development of consistent guidance in respect of governance and the effective implementation of governance practices.

This document has been developed to clarify the distinction between the concepts of governance and management in respect of IT. It provides a model that illustrates the relationship between governance and management, and identifies the responsibilities associated with each.

© ISO/IEC 2017 – All rights reserved

Information technology — Governance of IT — Framework and model

1 Scope

This document provides guidance on the nature and mechanisms of governance and management together with the relationships between them, in the context of IT within an organization.

The purpose of this document is to provide information on a framework and model that can be used to establish the boundaries and relationships between governance and management of an organization's current and future use of IT.

This document provides guidance for:

— governing bodies;

— managers who work within the authority and accountability established by governance;

— advisors or those assisting in the governance of organizations of all sizes and types; and

— developers of standards in the areas of governance of IT and management of IT.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

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

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

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

3.1
governance framework
strategies, policies, decision-making structures and accountabilities through which the organization's governance arrangements operate

3.2
internal control
policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected

3.3
management system
set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

© ISO/IEC 2017 – All rights reserved

Note 2 to entry: Management systems operate within the strategies, structures, responsibilities and accountabilities specified within the organization's governance framework.

[SOURCE: ISO 9000:2015, 3.5.3, modified - The notes to entry have been modified.]

3.4
risk appetite
amount and type of risk that an organization is willing to pursue or retain

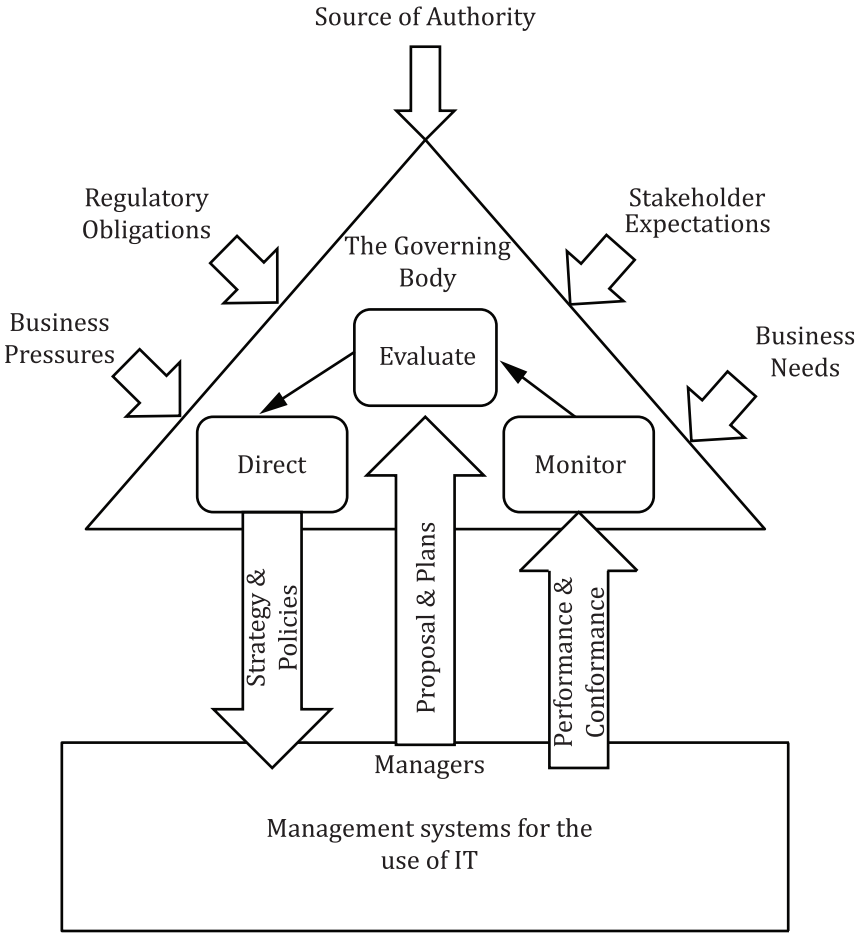
[SOURCE: ISO Guide 73:2009, 3.7.1.2]

4 Model and framework

4.1 Model for governance of IT

4.1.1 Governing body responsibilities and accountabilities

The governing body is responsible and accountable for the current and future use of IT within an organization as part of their overall responsibility for organizational governance.



NOTE SOURCE: ISO/IEC 38500.

Figure 1 — Model for governance of IT

The governing body's authority, responsibility and accountability will depend on its source of authority such as the legislative arrangement under which it operates. The agreed level of authority and boundaries on the scope of the organization will generally be documented. Depending on the size, type

 © ISO/IEC 2017 – All rights reserved