TECHNICAL REPORT

ISO/IEC TR 38502

First edition
2014-02-01

Information technology — Governance of IT — Framework and model

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

Reference number
ISO/IEC TR 38502:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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.

ISO/IEC TR 38502 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

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[2] 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 Technical Report 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.

Information technology — Governance of IT — Framework and model

1 Scope

This Technical Report 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 Technical Report 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 Technical Report provides guidance for:

— governing bodies;

— managers who have to 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 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

2.3
accountability
state of being accountable

Note 1 to entry: Accountability relates to an allocated responsibility. The responsibility may be based on regulation or agreement or through assignment as part of delegation.

2.4
corporate governance
system by which corporations are directed and controlled

Note 1 to entry: Corporate governance is organizational governance applied to corporations.

Note 2 to entry: From Cadbury 1992 and OECD 1999.

Note 3 to entry: Definition is included to clarify changes in terminology from previous edition.

2.5
direct
communicate desired purposes and outcomes to

Note 1 to entry: In the context of governance of IT, direct involves setting objectives, strategies and policies to be adopted by the members of the organization to ensure that use of IT meets business objectives.

Note 2 to entry: Objectives, strategies and policies may be set by managers if they have authority from the governing body.

2.6
evaluate
consider and make informed judgements

Note 1 to entry: In the context of governance of IT, evaluate involves judgements about the internal and external, current and future circumstances and opportunities relating to the organization's current and future use of IT.

2.7
executive manager
person who has authority delegated by the governing body for implementation of strategies and policies to fulfil the purpose of the organization

Note 1 to entry: Executive managers can include roles which report to the governing body or the head of the organization or have overall accountability for major reporting function, for example Chief Executive Officers (CEOs), Heads of Government Organizations, Chief Financial Officers (CFOs), Chief Operating Officers (COOs), Chief Information Officers (CIOs), and like roles.

Note 2 to entry: In management standards, executive managers may be referred to as top management.

2.8
governance
system of directing and controlling

2.9
governing body
person or group of people who are accountable for the performance and conformance of the organization

2.10
governance framework
strategies, policies, decision-making structures and accountabilities through which the organization's governance arrangements operate

2.11
governance of IT
system by which the current and future use of IT is directed and controlled

Note 1 to entry: Governance of IT is a component or a subset of organizational governance.

Note 2 to entry: This term is equivalent to the terms "corporate governance of IT", "enterprise governance of IT" and "organizational governance of IT".

2.12
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

2.13
information technology
IT
resources used to acquire, process, store and disseminate information

Note 1 to entry: This term also includes "Communications Technology (CT)" and the composite term "Information and Communications Technology (ICT)".

2.14
investment
allocation of resources to achieve defined objectives and other benefits

2.15
management
exercise of control and supervision within the authority and accountability established by governance

Note 1 to entry: This term is often used as a collective term for those with responsibility for controlling an organization or parts of an organization. The term "managers" is used to avoid confusion with management systems.

2.16
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.

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

[SOURCE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2013, Annex SL, Appendix 2, 3.04, modified – Note 2 has been added.]

2.17
managers
group of people responsible for supervision of an organization or parts of an organization

Note 1 to entry: Executive managers are a category of managers.

2.18
monitor
review as a basis for appropriate decisions and adjustments

Note 1 to entry: Monitor involves routinely obtaining information about progress against plans as well as the periodic examination of overall achievements against agreed strategies and outcomes to provide a basis for decision making and adjustments to plans.

Note 2 to entry: Monitor includes reviewing compliance with relevant legislation, regulations and organizational policies.

2.19
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2013, Annex SL, Appendix 2, 3.01]

2.20
organizational governance
system by which organizations are directed and controlled

2.21
policy
intentions and direction of an organization as formally expressed by its governing body or executive managers acting with appropriate authority

2.22
proposal
compilation of benefits, costs, risks, opportunities, and other factors applicable to decisions to be made

2.23
resources
people, procedures, software, information, equipment, consumables, infrastructure, capital and operating funds, and time

[SOURCE: ISO/IEC 38500:2008, 1.6.13]

2.24
responsibility
obligation to act and take decisions to achieve required outcomes

2.25
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected — positive and/or negative.

[SOURCE: ISO Guide 73:2009, 1.1, modified — NOTES 2 to 5 have been deleted.]

2.26
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]

2.27
stakeholder
any individual, group or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

[SOURCE: ISO Guide 73:2009, 3.2.1.1, modified — The NOTE has been deleted.]

2.28
use of IT
planning, design, development, deployment, operation, management, and application of IT to fulfil business objectives and create value for the business

Note 1 to entry: The use of IT includes both the demand for, and the supply of, IT.

Note 2 to entry: The use of IT includes both current and future use.

3 The Model and Framework

3.1 The Model for governance of IT

3.1.1 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.

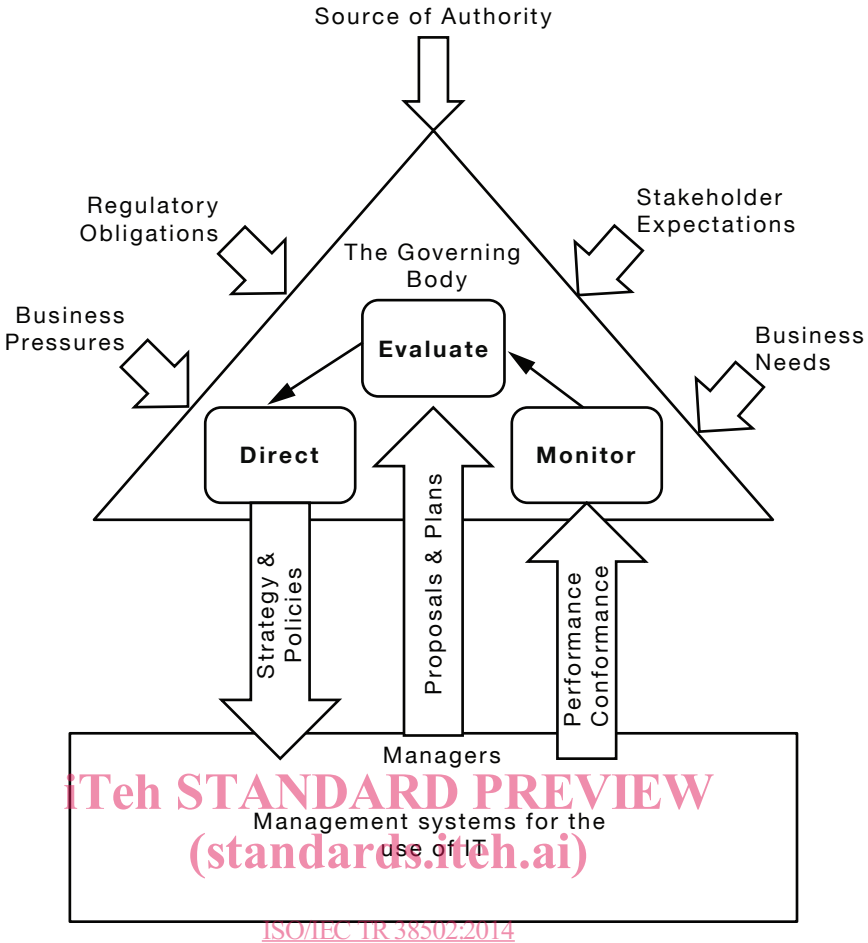

Figure 1 — Model for governance of IT (adapted from ISO/IEC 38500:2008)

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 of the organization, and legislative framework applicable to the organization, this will be in the form of a constitution or charter for the organization or a simple agreement between the parties.

In many public companies, the governing body is a board e.g. board of directors. There are jurisdictions in which a two-tier board structure is utilized, with both a supervisory and executive board.

3.1.2 Governance Tasks

ISO/IEC 38500[2] recommends that the governing body govern the use of IT through the tasks of:

— Evaluate

— Direct

— Monitor

The tasks evaluate, direct and monitor are carried out in close cooperation between the governing body and managers to enable the governing body to direct and control the use of IT to fulfil the business objectives.

While undertaking governance activities, the governing body should take into account regulatory obligations and the legitimate expectations of stakeholders in its decisions as well as the impact of the business environment including business pressures and business needs.