INTERNATIONAL STANDARD

ISO/IEC 38500

Second edition
2015-02-15

Information technology — Governance of IT for the organization

Technologies de l'information — Gouvernance des technologies de l'information pour l'entreprise

Reference number
ISO/IEC 38500:2015(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.

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

ISO/IEC 38500 was prepared by Joint Technical Committee ISO/IEC JTC1, *Information technology*, SC40, *IT Service Management and IT Governance*.

This second edition cancels and replaces the first edition (ISO/IEC 38500:2008), clauses, sub-clauses, and figures of which have been technically revised.

Introduction

The objective of this International Standard is to provide principles, definitions, and a model for governing bodies to use when evaluating, directing, and monitoring the use of information technology (IT) in their organizations.

This International Standard is a high level, principles-based advisory standard. In addition to providing broad guidance on the role of a governing body, it encourages organizations to use appropriate standards to underpin their governance of IT.

Most organizations use IT as a fundamental business tool and few can function effectively without it. IT is also a significant factor in the future business plans of many organizations.

Expenditure on IT can represent a significant proportion of an organization's expenditure of financial and human resources. However, a return on this investment is often not realized fully and the adverse effects on organizations can be significant.

The main reasons for these negative outcomes are the emphasis on the technical, financial, and scheduling aspects of IT activities rather than emphasis on the whole business context of use of IT.

This International Standard provides principles, definitions, and a model for good governance of IT, to assist those at the highest level of organizations to understand and fulfil their legal, regulatory, and ethical obligations in respect of their organizations' use of IT.

This International Standard is aligned with the definition of corporate governance that was published as a Report of the Committee on the Financial Aspects of Corporate Governance (the Cadbury Report) in 1992. The Cadbury Report also provided the foundation definition of corporate governance in the OECD Principles of Corporate Governance in 1999 (revised in 2004). Governance is distinct from management, and for the avoidance of confusion, the two concepts are defined in this International Standard and elaborated in ISO/IEC TR 38502.

This International Standard is addressed primarily to the governing body. In some (typically smaller) organizations, the members of the governing body can also be executive managers. This International Standard is applicable for all organizations, from the smallest to the largest, regardless of purpose, design, and ownership structure.

The implementation of governance of IT is covered by ISO/IEC TS 38501.

Information technology — Governance of IT for the organization

1 Scope

This International Standard provides guiding principles for members of governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of information technology (IT) within their organizations.

It also provides guidance to those advising, informing, or assisting governing bodies. They include the following:

— executive managers;

— members of groups monitoring the resources within the organization;

— external business or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies;

— internal and external service providers (including consultants);

— auditors.

This International Standard applies to the governance of the organization's current and future use of IT including management processes and decisions related to the current and future use of IT. These processes can be controlled by IT specialists within the organization, external service providers, or business units within the organization.

This International Standard defines the governance of IT as a subset or domain of organizational governance, or in the case of a corporation, corporate governance.

This International Standard is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. This International Standard is applicable to organizations of all sizes from the smallest to the largest, regardless of the extent of their use of IT.

The purpose of this International Standard is to promote effective, efficient, and acceptable use of IT in all organizations by

— assuring stakeholders that, if the principles and practices proposed by the standard are followed, they can have confidence in the organization's governance of IT,

— informing and guiding governing bodies in governing the use of IT in their organization, and

— establishing a vocabulary for the governance 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 can 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 evolution 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 can be set by managers if they have authority delegated by 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 from 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 similar roles.

Note 2 to entry: In management standards, executive managers can 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 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: The term governance of IT is equivalent to the terms corporate governance of IT, enterprise governance of IT, and organizational governance of IT.

2.11
human behaviour
interaction among humans and other elements of the system

Note 1 to entry: Human behaviour includes culture, needs, and aspirations of people as individuals and as groups.

Note 2 to entry: In respect of IT, there are numerous groups or communities of humans, each with their own needs, aspirations, and behaviours. For example, people who use information systems might exhibit needs relating to accessibility and ergonomics, as well as availability and performance. People whose job roles are changing because of the use of IT might exhibit needs relating to communication, training, and reassurance. People involved in building and operating IT capabilities might exhibit needs relating to working conditions and development of skills.

2.12
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)".

2.13
investment
allocation of resources to achieve defined objectives and other benefits

2.14
management
exercise of control and supervision within the authority and accountability established by governance

Note 1 to entry: The term management 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.

2.15
managers
group of people responsible for control and supervision of an organization or parts of an organization

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

2.16
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.

2.17
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: Consolidated ISO Supplement 2013- Procedures specific to ISO, Annex XL, Appendix 2. The note has been added in this International Standard].

2.18
organizational governance
system by which organizations are directed and controlled

2.19
policy
intentions and direction of an organization as formally expressed by its governing body or executive managers acting with appropriate authority

2.20
proposal
compilation of benefits, costs, risks, opportunities, and other factors applicable to decisions to be made

EXAMPLE business cases

2.21
resources
people, procedures, software, information, equipment, consumables, infrastructure, capital and operating funds, and time

2.22
responsibility
obligation to act and take decisions to achieve required outcomes

2.23
risk
effect of uncertainty on objectives

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

Note 2 to entry: Negative effects reflect threats while positive risks reflect opportunities.

[SOURCE: ISO Guide 73:2009]

2.24
stakeholder
any individual, group, or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

[SOURCE: adapted from ISO Guide 73:2009]

2.25
use of IT
planning, design, development, deployment, operation, management, and application of IT to fulfil business objectives and create value for the organization

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 Benefits of Good Governance of IT

Good governance of IT assists governing bodies to ensure that the use of IT contributes positively to the performance of the organization, through:

— innovation in services, markets, and business;

— alignment of IT with business needs;

— appropriate implementation and operation of IT assets;

— clarity of responsibility and accountability for both the supply of and demand for IT in achieving the goals of the organization;

— business continuity and sustainability;

— efficient allocation of resources;

— good practice in relationships with stakeholders; and

— actual realisation of the expected benefits from each IT investment.

This International Standard establishes principles for the effective, efficient and acceptable use of IT. Governing bodies, by ensuring that their organizations follow these principles, will be assisted in managing risks and encouraging the exploitation of opportunities arising from the use of IT.

Good governance of IT also assists governing bodies in assuring conformance with obligations (regulatory, legislation, contractual) concerning the acceptable use of IT.

This International Standard establishes a model for the governance of IT. The risk of governing bodies not fulfilling their obligations is mitigated by giving due attention to the model in appropriately applying the principles.

Inadequate IT systems and improper or inappropriate use of IT can expose an organization to the risk of not complying with legislation. For example, in some jurisdictions, members of governing bodies could be held personally accountable if an inadequate accounting system results in tax not being paid.

Processes dealing with IT incorporate specific risks that should be addressed appropriately. For example governing bodies and members of governing bodies can be held accountable for:

— breaches of privacy, spam, health and safety, record keeping legislation and regulations;

— non-compliance with standards relating to security, social responsibility;

— matters relating to intellectual property rights including licensing agreements.

Governing bodies using the guidance in this standard are more likely to meet their obligations.

4 Principles and Model for Good Governance of IT

4.1 Principles

This clause sets out six principles for good governance of IT. The principles express preferred behaviour to guide decision making. The statement of each principle refers to what should happen, but does not prescribe how, when or by whom the principles would be implemented - as these aspects are dependent on the nature of the organization implementing the principles. Governing bodies should require that these principles are applied.

Principle 1: Responsibility

Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.

Principle 2: Strategy

The organization's business strategy takes into account the current and future capabilities of IT; the plans for the use of IT satisfy the current and on-going needs of the organization's business strategy.

Principle 3: Acquisition

IT acquisitions are made for valid reasons, on the basis of appropriate and on-going analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.

Principle 4: Performance

IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.

Principle 5: Conformance

The use of IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.

Principle 6: Human Behaviour

IT policies, practices and decisions demonstrate respect for Human Behaviour, including the current and evolving needs of all the 'people in the process'.

4.2 Model

Governing bodies should govern IT through three main tasks:

a) Evaluate the current and future use of IT.

b) Direct preparation and implementation of strategies and policies to ensure that use of IT meets business objectives.

c) Monitor conformance to policies, and performance against the strategies.

Authority for specific aspects of IT may be delegated to managers within the organization. However, accountability for the effective, efficient and acceptable use of IT by an organization remains with the governing body and cannot be delegated.

Figure 1 shows the model for governance of IT using Evaluate-Direct- Monitor. The text following Figure 1 explains the elements and relationships depicted.

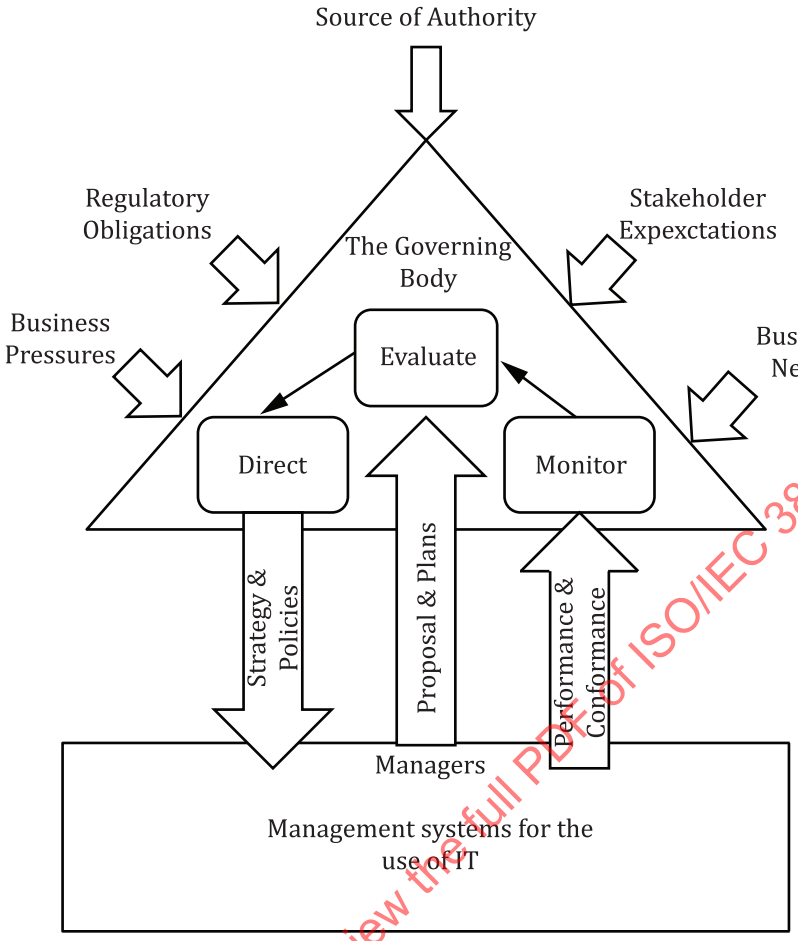

Figure 1 — Model for Governance of IT

Evaluate

Governing bodies should examine and make judgement on the current and future use of IT, including plans, proposals and supply arrangements (whether internal, external, or both).

In evaluating the use of IT, governing bodies should consider the external or internal pressures acting upon the organization, such as technological change, economic and social trends, regulatory obligations, legitimate stakeholder expectations and political influences. Governing bodies should undertake evaluation continually as circumstances change. Governing bodies should also take account of both current and future business needs— the current and future organizational objectives that they must achieve, such as maintaining competitive advantage, as well as the specific objectives of the plans and proposals they are evaluating.

Direct

Governing bodies should assign responsibility for, and direct preparation and implementation of strategies and policies. Strategies should set the direction for investments in IT and what IT should achieve. Policies should establish sound behaviour in the use of IT.

Governing bodies should encourage a culture of good governance of IT in their organization by requiring managers to provide timely information, to comply with direction and to conform with the six principles of good governance.

If necessary, governing bodies should direct the submission of proposals for approval to address identified needs.

Monitor

Governing bodies should monitor, through appropriate measurement systems, the performance of IT. They should reassure themselves that performance is in accordance with strategies, particularly with regard to business objectives.

Governing bodies should also make sure that IT conforms with external obligations (regulatory, legislation, contractual) and internal work practices.

5 Guidance for the Governance of IT

5.1 General

The following sub-clauses provide guidance for the general principles of good governance of IT and the practices required to implement the principles.

The practices described are not exhaustive but provide a starting point for discussion of the responsibilities of the governing body for the governance of IT. That is, the practices described are suggested guidance for the Governance of IT.

It is the responsibility of each organization, individually, to identify the specific actions required to implement the principles, giving due consideration to the nature of the organization, and appropriate analysis of the risks and opportunities of the use of IT.

5.2 Principle 1: Responsibility

Evaluate

Governing bodies should evaluate the options for assigning responsibilities in respect of the organization's current and future use of IT. In evaluating options, governing bodies should seek to ensure effective, efficient, and acceptable use of IT in support of current and future business objectives.

Governing bodies should evaluate the competence of those given responsibility to make decisions regarding IT. Generally, these people should be business managers who are also responsible for the organization's business objectives and performance, assisted by IT specialists who understand business values and processes.

Direct

Governing bodies should direct that strategies be followed according to the assigned IT responsibilities.

Governing bodies should direct that they receive the information that they need to meet their responsibilities and accountability.

Monitor

Governing bodies should monitor that appropriate mechanisms for governance of IT are established.

Governing bodies should monitor that those given responsibility acknowledge and understand their responsibilities.

Governing bodies should monitor the performance of those given responsibility in the governance of IT (for example, those people serving on steering committees or presenting proposals to governing bodies).

5.3 Principle 2: Strategy

Evaluate

Governing bodies should evaluate developments in IT and business processes to ensure that IT will provide support for future business needs.

When considering plans and policies, the governing body should evaluate the use of IT and IT activities to ensure they align with the organization's objectives and satisfy key legitimate stakeholder requirements. The governing body should also take into consideration good practices.

Governing bodies should ensure that the use of IT is subject to appropriate risk management.

Direct

Governing bodies should direct the preparation and use of strategies and policies that ensure the organization does benefit from developments in IT.

Governing bodies should also encourage the submission of proposals for innovative uses of IT that enable the organization to respond to new opportunities or challenges, undertake new businesses or improve processes.

Monitor

Governing bodies should monitor the progress of approved IT proposals to ensure that they are achieving objectives in required timeframes using allocated resources.

Governing bodies should monitor the use of IT to ensure that it is achieving its intended benefits.

5.4 Principle 3: Acquisition

Evaluate

Governing bodies should evaluate options for providing IT to realize approved proposals, balancing risks and value for money of proposed investments.

Direct

Governing bodies should direct that IT assets (systems and infrastructure) be acquired in an appropriate manner, including the preparation of suitable documentation, while ensuring that required capabilities are provided.

Governing bodies should direct that supply arrangements (including both internal and external supply arrangements) support the business needs of the organization.

Governing bodies should direct that their organization and suppliers develop a shared understanding of the organization's intent in making any IT acquisition.

Monitor

Governing bodies should monitor IT investments to ensure that they provide the required capabilities.

Governing bodies should monitor the extent to which their organization and suppliers maintain the shared understanding of the organization's intent in making any IT acquisition.

5.5 Principle 4: Performance

Evaluate

Governing bodies should evaluate the plans proposed by the managers to ensure that IT will support business processes with the required capability and capacity. These proposals should address the continuing normal operation of the organization and the treatment of risk associated with the use of IT.

Governing bodies should evaluate the risks to continued operation of the business arising from IT activities.

Governing bodies should evaluate the risks to the integrity of information and the protection of IT assets, including associated intellectual property and organizational memory.

Governing bodies should evaluate options for assuring effective, timely decisions about use of IT in support of business goals.

Governing bodies should regularly evaluate the effectiveness and performance of the organization's governance of IT.

Direct

Governing bodies should ensure allocation of sufficient resources so that IT meets the needs of the organization, according to the agreed priorities and budgetary constraints.

Governing bodies should direct those responsible to ensure that IT supports the organization, when required for business reasons, with correct and up-to-date data that is protected from loss or misuse.

Monitor

Governing bodies should monitor the extent to which IT supports the business. Governing bodies should monitor the extent to which allocated resources and budgets are prioritised according to business objectives.

Governing bodies should monitor the extent to which the policies, such as for data accuracy and the efficient use of IT, are followed properly.

5.6 Principle 5: Conformance

Evaluate

Governing bodies should regularly evaluate the extent to which IT satisfies obligations (regulatory, legislation, contractual), internal policies, standards and professional guidelines.

Governing bodies should regularly evaluate the organization's internal conformance to its framework for governance of IT.

Direct

Governing bodies should direct those responsible to establish regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations, internal policies, standards and guidelines.

Governing bodies should direct that policies are established and enforced to enable the organization to meet its internal obligations in its use of IT.

Governing bodies should direct that IT staff follow relevant guidelines for professional behaviour and development.

Governing bodies should direct that all actions relating to IT be ethical.

Monitor

Governing bodies should monitor IT compliance and conformance through appropriate reporting and audit practices, ensuring that reviews are timely, comprehensive, and suitable for the evaluation of the extent of satisfaction of the organization.

Governing bodies should monitor IT activities, including disposal of assets and data, to ensure that environmental, privacy, strategic knowledge management, preservation of organizational memory and other relevant obligations are met.

5.7 Principle 6: Human Behaviour

Evaluate

Governing bodies should evaluate IT activities to ensure that human behaviours are identified and appropriately considered.