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;

