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)

COPYRIGHT PROTECTED DOCUMENT

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