TECHNICAL REPORT

ISO/IEC TR 38504

First edition
2016-09-15

Governance of information technology — Guidance for principles-based standards in the governance of information technology

Gouvernance des technologies de l'information — Lignes directrices pour des normes fondées sur des principes relatives à la gouvernance des technologies de l'information

Reference number
ISO/IEC TR 38504:2016(E)

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

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 World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 40, *IT service management and IT governance*.

Introduction

This document has been developed to give guidance on the information required to support principles-based standards in the area of governance and management of information technology.

A principles-based approach to standardization is aimed at providing non-prescriptive guidance that is applicable to all organizations, including public and private companies, government entities and not-for-profit organizations of all sizes from the smallest to the largest, regardless of the extent of their use of IT.

The benefit of a principles-based standard is that it can identify the outcomes of applying the principles without specifying explicit methodologies, structures, processes and techniques needed to achieve the outcomes.

Within the International Standards arena, the definition of guidance in the area of governance of information technology falls within the scope of ISO/IEC JTC 1/SC 40. The existing International Standards in this area are ISO/IEC 38500, ISO/IEC TS 38501 and ISO/IEC TR 38502.

Experience with principles-based standards in the area of governance of IT has indicated that there is a need to establish a common understanding of proposed principles and the expected outcomes of applying the recommended principles as a basis for consensus. This requires a clear statement of the rationale for the principles, the expected governance behaviours associated with the principle together with the expected outcomes from their adoption.

In order for future standards and revisions of current standards to select the appropriate forms of principle description and apply them in a consistent fashion, it is desired to develop a common characterization of all of these forms of principle description. This document presents guidelines for the general recommendations of principles-based governance standards and the description of principles in terms of their format, content and level of prescription.

The intended audience for this document are the editors, working group members, reviewers and other participants in the development of principles-based standards and technical reports as well as governance of IT practitioners. An additional audience may be experts developing organizational policies and standards. It is intended that they will select the elements suitable for their project from those described in this document. It is further intended that, having selected the appropriate elements, users of this document will apply them in a manner consistent with the guidance provided by this document.

Governance of information technology — Guidance for principles-based standards in the governance of information technology

1 Scope

This document provides guidance on the information required to support principles-based standards in the area of governance and management of information technology.

Guidance includes general recommendations, identification of elements and advice for their formulation. It does not describe the detail of specific principles or how they are aggregated into specific guidance to fulfil business objectives and achieve business outcomes from the use 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 ISO/IEC TR 38502 apply.

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

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

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

3.1
governance behaviour
actions of individuals and groups as part of an organization's governance system

4 Governance standards for information technology

4.1 Purpose and focus of governance standards for information technology

A governance standard provides guidance on the system of directing and controlling for an organization with respect to the business outcomes from the use of information technology.

Governance standards for IT may provide guidance on the role of the governing body within an organization and its interactions with managers or what is required of a governance framework for IT or all of these. Governance standards for information technology can either focus on all or part of the use of information technology within an organization.

Guidance may include consideration of business strategy and IT strategy. It may also explore links between governance behaviour, policy setting, management behaviour and business objectives and outcomes.

The audience for such standards will include members of the governing body of organizations and the executive managers responsible for high level oversight of the organizations.

4.2 General recommendations for governance standards for information technology

Governance standards for information technology

a) should be anchored in accepted fundamental concepts of governance, such as those of the Organisation for Economic Co-operation and Development (OECD), and describe governance of information technology as a subset of organizational governance;

b) should be written in a way that is readable by the target audience including the governing body and executive managers;

c) should clearly describe the domain that they address, particularly when they involve a subset of the domain of information technology;

d) should be principles based;

e) should conform to the model for governance of IT using Evaluate-Direct-Monitor as described in ISO/IEC 38500;

f) should distinguish between the responsibilities and accountabilities of the governing body and those of managers as outlined in ISO/IEC TR 38502;

g) should be able to be applied on a consistent basis without prescribing particular organizational structures or processes;

h) unless otherwise specified, should be applicable to all sizes and types of organization.

5 Principles-based guidance for governance of information technology

5.1 Use of principles-based standards

The benefit of a principles-based standard is that such a standard can identify the value and outcomes of applying the principles without specifying explicit methodologies, structures, processes and techniques. This enables the development of guidance that can be applied on a consistent basis and gives organizations flexibility in how they implement the guidance within their own structures and processes.

5.2 System of governance

A principles-based governance standard should be based on a clear established system of governance involving both the actions of the governing body (or delegates) and the actions of management operating within a governance framework. Good governance both oversees and guides the behaviour of management, and governance principles, to be effective, should become embedded in the organization.

5.3 Set of principles

A principles-based standard for a governance domain should include the set of principles that describe the fundamental concepts or propositions that underpin the system of governance for the domain being addressed and include other guidance on the adoption and implementation of the principles.

Each principle should be stated with sufficient detail to ensure that there is clarity about the concepts and its implication for organization's system of governance.

Any relationship between the principles and the avoidance of overlap should be stated.

5.4 Relationship between the adoption of principles and business outcomes

Underpinning the guidance in a principles-based standard for governance of IT is the expectation that there is a relationship between the adoption of the governance principles and the achievement

of business outcomes. The actual relationship between governance principles and business outcomes will differ between organizations and will be influenced by the governance framework, organizational capability and external factors.

Figure 1 shows some example factors that are represented by puzzle pieces, such as governance behaviours, management behaviours, IT enablers, policies and culture, that could assist in understanding and establishing a causal link. The figure is not intended to infer any specific relationship between the factors or puzzle pieces and leaves gaps for other factors that may be important for a specific organization.

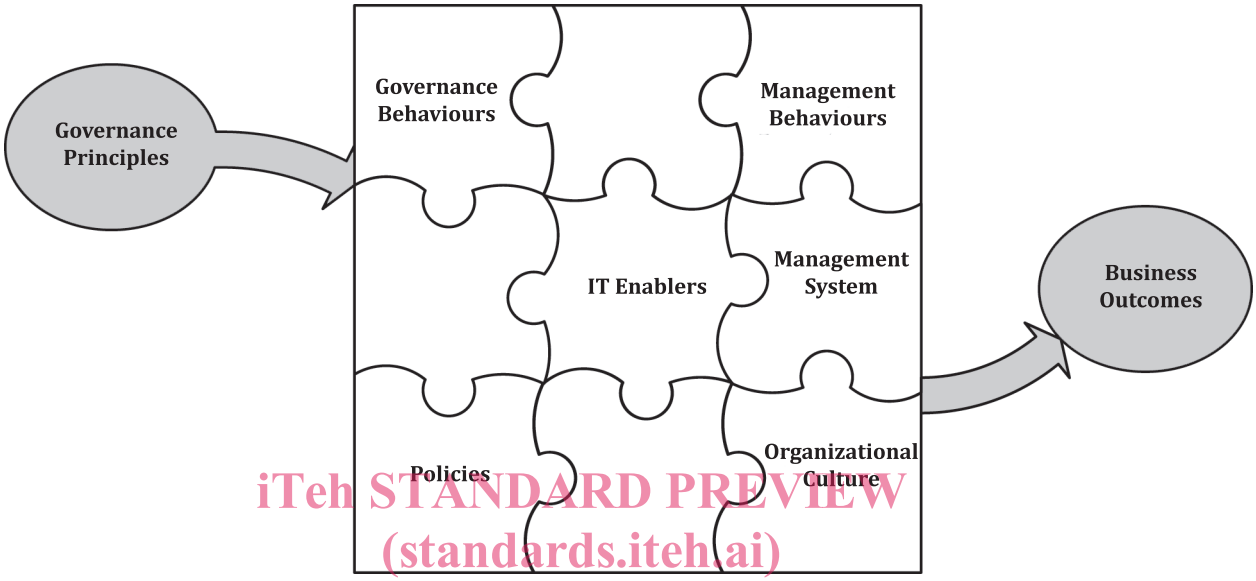

Figure 1 — Relationship between governance principles and business outcomes

The end objective of the adoption of governance to IT is the fulfilment of strategic business objectives and the achievement of positive business outcomes, enabled by IT. However, adopting governance principles for IT should result in the establishment of a system of governance, involving both the action of the governing body and of managers operating within a governance framework and will lead to the achievement of beneficial business outcomes as depicted in Figure 1.

This document proposes that principles-based guidance clearly identifies appropriate governance behaviours and the outcomes that are the direct results of the adoption of the specified principles as a basis for assessing and improving governance of IT and the system of governance in place.

A principles-based guidance document should contain all of the principles that are relevant and advice on the consistent and complete application of these. Failure to comprehensively apply any of the principles may lead to sub-optimal outcomes. Advice should encourage the organization's leaders to deeply consider each of the principles and how they will become part of the core culture of the organization.

It may be difficult to develop guidance that attributes business outcomes directly to a specific principle of governance of IT. Business outcomes are generally relatively specific to individual businesses or industries and there are other factors that influence successful achievement, including organizational capability and external factors such as competition.

One option that can be taken is to express the relationship in generic terms as a basis for guidance. However, when establishing the principles for governance of IT and in communicating principles-based guidance, the potential relationship between the desired governance behaviours, the desired IT-related enablers, other important organizational factors and possible business outcomes should be understood and articulated to the fullest extent possible as a basis for developing guidance for the implementation of governance of IT.