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.

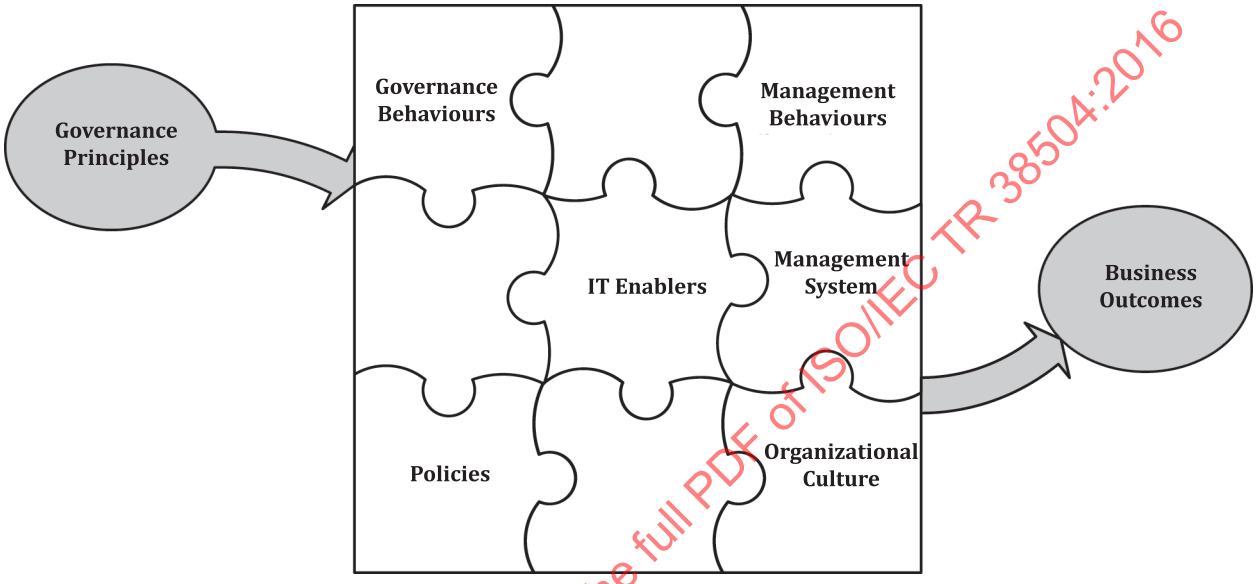

Figure 1 — Relationship between governance principles and business outcomes

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.

6 Information required for each governance principle

6.1 Information elements

The information elements that should be included to support each principle are as shown in Figure 2. The order of the elements does not imply hierarchy; however, the author should consider readability in constructing the standard.

In addition to the informational elements, the standards should include general guidance as described in Clauses 4 and 5.

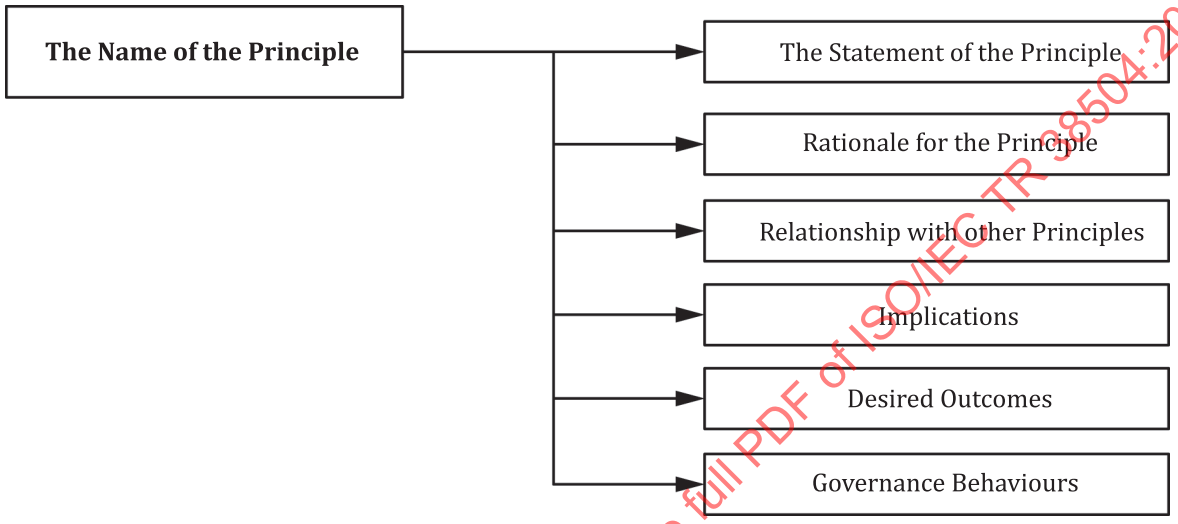

Figure 2 — Information elements for each principle

6.2 Name of the principle

There should be a short form name for each principle. The name should clearly represent the core concepts embodied in the principle and as well as being easy to remember. The name of a principle should be chosen with care so that is not confused with other concepts associated with governance or management of IT.

The following apply:

a) The name should be short (one to three words).

b) Specific outcomes methodologies or techniques should not be mentioned in the name or statement of a principle.

6.3 The statement of the principle

There should be a statement of the principle that clearly articulates the fundamental rule or proposition embodied in the principle.

The following apply:

a) The statement of the principle should be applicable to all sizes and types of organization.

b) Each principle statement should be unambiguous.

6.4 Rationale for the principle

There should be a high level statement as to why the principle is important to the achievement of business outcomes. This should describe how the adoption of the principle will enable a governing body and executive management to achieve business outcomes through the use of IT. In particular, it should articulate the relationship between the desired governance behaviours, management behaviours and how the IT enablers will support the achievement of expected or desired business outcomes.

6.5 Relationship with other principles

There should be an explanation for each principle about any interrelationships between principles. If the effective adoption of one principle is dependent on others then this should be stated.

If there are situations where one principle would be given precedence or carry more weight than another in the achievement of outcomes then this should be highlighted.

6.6 Implications

There should be a statement of the implications for each principle. Each statement should highlight the recommendations for the governing body in applying the principle to the governance of IT in terms of activities/tasks that they would undertake.

The impact to the business and consequences of adopting a principle should be clearly stated. The reader should be able to readily discern the answer to the question "How does this affect the governing body?" It is important not to oversimplify, trivialize or judge the merit of the impact. Some of the implications will be identified as potential impacts only and may be speculative rather than fully analysed.

An example (not validated) of how this might be structured is as follows:

The implications of the adoption of the strategy principle are as follows:

- *The governing body working with and advised by executive managers should provide leadership in developing strategies for obtaining value from the use of IT.*
- *The governing body should approve the organization's business strategy for IT taking into account the implications of the strategy for achieving business objectives and any associated risks that might arise.*
- *The governing body should ensure that the organization's external and internal environment are regularly monitored and analysed to determine if there is a need to review and, when appropriate, revise the strategy for IT and any associated policies.*
- *The governing body should ensure that policies are developed to guide organizational behaviour.*
- *The governing body should ensure that there are mechanisms to clarify and interpret objectives, strategies and policies as emergent issues arise.*
- *The governing body should understand the business readiness for any major changes proposed as part of the business strategy for IT and ensure that there is a commitment and capability within the organization to undertake required changes.*

6.7 Desired outcomes

There should be a statement of desired outcomes for each principle. Each statement should articulate one or more expected outcome from applying soundly based governance. An example (not validated) of how this might be structured is as follows:

The expected and desired outcomes from the adoption of the strategy principle are:

- *The business strategy makes the most effective use of technology to achieve business objectives.*
- *The organization has the IT related capabilities required to support and sustain the business.*

The totality of the outcomes for all principles should provide guidance on the characteristics of a system of governance based on the adoption of the principles.

The following apply to the structure of outcome statements:

a) Each outcome should be stated clearly and concisely, since the outcome statement will guide the implementation of governance of IT by articulating what is to be achieved.

b) Each outcome should be expressed in terms of a positive, observable (or confirmable) objective result.

c) Each statement of outcome should express a single result. Hence, the use of the word "and" or "and/or" to conjoin clauses should be avoided; such constructions are better expressed as multiple outcomes.

6.8 Governance behaviours

There should be a statement of the governance behaviours desired from the adoption of each principle.

The statement of governance behaviours should describe the desired characteristics of the system of governance for IT. The statement may be used to guide the design, implementation and assessment of an organization's governance framework.

There should be clarity about how the governance behaviours cascade through the organization and its management structure. The guidance should explain how managers adopt and exhibit the behaviours arising from adoption of the principles by the governing body.

An example (not validated) of how this might be structured is as follows:

The desired behaviours from the adoption of the strategy principle are as follows:

— ***Strategic decision making.*** *Decisions about business strategies for IT are made at an appropriate level within the organization based on careful analysis and advice.*

— ***Information strategy****. The strategic advantage of information is recognized and planned for.*

— ***Strategic risk.*** *The risk to the organization through its reliance on technology is identified and managed.*

— ***Alignment.*** *IT strategies, architecture and policies support the ongoing requirements of businesses for delivering new or changed IT capability.*

— ***Capabilities.*** *Required capabilities are understood and planned for.*

— ***Customer interactions.*** *There is a clear strategic approach to supporting customers in their use of IT.*

The following apply:

a) Each statement of governance behaviour should comprise a short form name together with an explanatory statement.

b) There should be a clear relationship between the desired governance behaviours and the outcome of applying sound governance of IT.

c) The desired governance behaviours associated with a principle should be necessary and sufficient to meet the expected and desired outcomes of the principle as outlined in the outcome statement.

d) A statement of desired governance behaviours should be written in a manner that is meaningful for any scope of applicability, e.g., for organizations of any relevant domain or size. Thus, it should not require a specific technique or methodology. For example, a statement that "There should be clearly defined mechanisms for oversight of the supply and use of IT within the organization" is a more appropriate desired governance behaviour than "There should be an IT steering committee", although examples of how the desired governance behaviour can be implemented, e.g., "IT steering committee" could be given.

