TECHNICAL SPECIFICATION

ISO/IEC TS 38501

First edition
2015-04-01

Information technology — Governance of IT — Implementation guide

Technologies de l'information — Gouvernance des technologies de l'information — Guide d'implémentation

Reference number
ISO/IEC TS 38501:2015(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.

This committee responsible for this document is ISO/IEC JTC 1, *Information Technology,* Subcommittee SC 40, *IT Service Maintenance and IT Governance.*

Introduction

Information technology (IT) has become pervasive in supporting and enabling the strategy of organizations and this prevalence mandates the governance of IT as an organizational imperative.

Organizations have made significant investments in IT to automate business processes and to communicate and transact electronically with their customers and suppliers. The benefits from these investments have unfortunately not always materialised and in some instances, organizations have incurred significant financial and reputational damage as a result of IT failures. This has further heightened governing body awareness of the need for the governance of IT and of their responsibilities in this regard.

It might be, however, that some governing bodies are uncertain of what arrangements they need to have in place for the governance of IT.

This Technical Specification has therefore been developed to provide guidance on the implementation of governance of IT within organizations. It considers governance, both from the perspective of gaining assurance that the risks associated with the use of IT are appropriately managed, as well as ensuring that the organization maximizes the value from its investments in IT.

It expands on the model and principles for good governance of IT, as described in ISO/IEC 38500 and ISO/IEC/TR 38502, and provides guidance on a methodology for implementing principles-based governance of IT.

Information technology — Governance of IT — Implementation guide

1 Scope

1.1 Overview

This Technical Specification provides guidance on how to implement arrangements for effective governance of IT within an organization.

1.2 Purpose

This Technical Specification identifies the key activities that an organization has to undertake to implement governance of IT, in accordance with ISO/IEC 38500.

It provides guidance on the design and establishment of the arrangements for the governance of IT, clarifying roles and responsibilities of key stakeholders within the organization, as well as providing examples of matters to consider in the design of the governance of IT.

1.3 Audience

This Technical Specification can be used by individuals responsible for governance of IT within an organization and individuals supporting in the governance of organizations. This Technical Specification is applicable to organizations of all sizes and types.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 38500, *Corporate governance of information technology*

ISO/IEC/TR 38502, *Information technology — Governance of IT — Framework and model*

3 Implementation approach

The implementation of the governance of IT should be based on a cyclic approach considering the model presented in ISO/IEC 38500, Figure 1. The first cycle of activities involves the establishment of the initial "implementation" or baseline, with subsequent cycles of the activities being used to support and enhance the governance of IT implementation by means of continual improvement. The duration of cycles will be different for each organization, depending on a number of factors including the organization's size, its industry, as well as the maturity of the governance of IT in the organization.

The implementation cycle comprises the following main activities which are expanded in the clauses below.

— **Establish and sustain enabling environment:** Commence by establishing an enabling environment which ensures that all stakeholders are appropriately identified and made aware of their roles and responsibilities. Subsequent cycles will ensure that the enabling environment is sustained.

— **Govern IT:** Progress to the evaluate, direct, and monitor activities to perform the governance of IT.

— **Continual review**: Review the governance of IT arrangements to determine whether desired outcomes are being achieved. If not, recommence the implementation cycle to effect the necessary changes, thereby ensuring continual improvement of the governance of IT implementation.

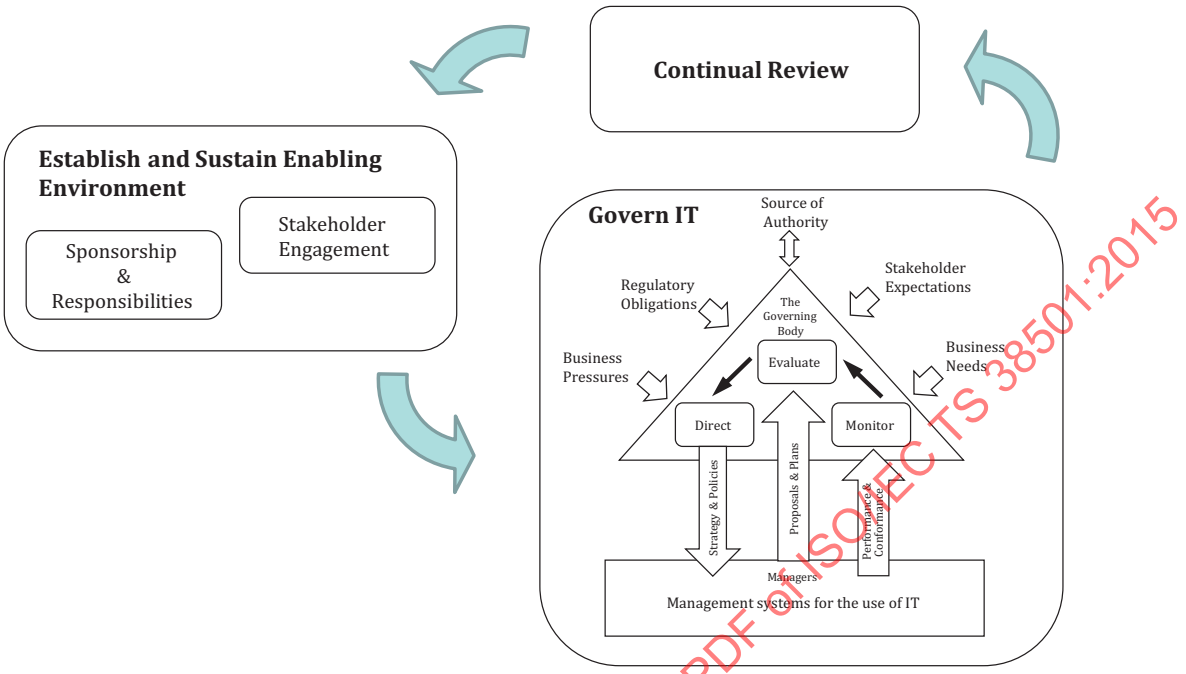


Figure 1 — Implementation approach (incorporates ISO/IEC 38500)

4 Establish and sustain enabling environment

4.1 Overview

The execution and improvement of the governance of IT implementation activities will generally require clear leadership and commitment from the governing body and the executive managers of the organization.

The level of engagement of these stakeholders should be proportionate to the importance of the role of IT to the organization — both currently and in the future, as required by the organization's goals and strategy.

This may lead to changes in terms of organizational culture and behaviours in respect of IT, in addition to requiring new or improved processes in the governance of IT.

This is achieved through the identification and engagement of appropriate stakeholder groups, as well as the clarification of roles and responsibilities for the various stakeholders. This is an on-going activity and therefore needs to be revisited through each pass of the implementation cycle, as individual stakeholders can change and the stakeholder group responsibilities can mature over time. These activities are discussed below.

4.2 Ensure internal stakeholder engagement

Two key stakeholder groups should be considered when commencing with a governance of IT implementation, namely the governing body and executive managers. Awareness should be developed in these stakeholder groups of the purpose and objectives of governing IT and their various roles and responsibilities in this regard (see ISO/IEC/TR 38502 for further detail on the relationships and boundaries between these key stakeholder groups).

Developing and maintaining awareness is an on-going process that is enhanced through the successive iterations of the activities described in this Technical Specification. The awareness should be initiated by holding briefing sessions and or workshops covering, inter alia:

— how business value is realised from the use of IT;

— the risks associated with maintaining current and implementing new IT capability;

— the need for the governance of IT and how it fits with corporate governance;

— the model and principles that are described in ISO/IEC 38500;

— the framework, roles and responsibilities of stakeholders as described in ISO/IEC/TR 38502;

— facilitating stakeholder assessments of the effectiveness of current governance of IT arrangements (see Annex A and Annex B).

The first cycle of the implementation provides the opportunity to explain and bed down these concepts in the context of the organization. This will lead to greater stakeholder understanding and ownership of their respective roles and responsibilities, as well as the identification of areas for improvement. Subsequent cycles will provide for the on-boarding of new stakeholders, as well as the refinement and updating of knowledge and responsibilities for existing stakeholders.

4.3 Clarify sponsorship and responsibilities

There are many activities associated with improving and maintaining effective governance of IT that need to be actively managed within the organization. These include awareness and education about the governance of IT, as well as on-going coordination and administration activities. It is therefore important to determine and appoint a sponsor and a small group of individuals on the first cycle of the implementation. This group is referred to as the Governance Steering Group in this Technical Specification but in smaller organizations it may simply be an individual. The Governance Steering Group has the responsibility to drive the adoption and or transformation of the governance of IT in the organization. These activities are discussed in further detail in 5.3.4.

The sponsor should be a key influential business/marketing/operations executive manager and should not be a risk or governance expert or department.

5 Govern IT

5.1 Overview

The three activities of the governance model in ISO/IEC 38500, namely evaluate, direct and monitor, take place in the Govern IT phase. These are framed and guided by the six principles of the standard (responsibility, strategy, acquisition, performance, conformance, human behaviour) within the context of the internal and external environments, as well as organization's culture for the governance of IT.

It is important to focus and describe what the result of the governance of IT should be when applying the ISO/IEC 38500 framework, rather than being process or control oriented. This will ensure that the governing body determines what needs to be achieved, rather than prescribing how it should be done, thereby appropriately guiding or steering the organization in its use of IT.

In addition, an appropriate mechanism of assessment is required, which must take into account the principles-based nature of ISO/IEC 38500.

5.2 Evaluate

5.2.1 Overview

The evaluate activity is used to establish the internal and external environment and to determine how the organization is currently supported and enabled through the use of IT (the current state).

The first cycle of the implementation approach also provides an opportunity to introduce, explain and reinforce the concepts of ISO/IEC 38500 and to highlight the value of the standard to key stakeholders. Subsequent cycles should also form a key part of the on-going awareness and education program for the governing body and executive managers.

5.2.2 Understand internal environment

The governing body should maintain an understanding of key aspects of the organization so that IT related assessments and decisions can be made that are relevant to the organization. Key considerations include:

— business goals;

— business strategy;

— risk appetite and performance;

— culture of the organization and tone at the top;

— organizational maturity and levels of skill, training and competence in the use of IT;

— strategic change initiatives;

— the need for innovative use of IT to obtain competitive advantage;

— assurance reporting including audit and risk;

— how key business processes use and are supported by IT;

— key IT services and how they are provided;

— how the organization engages with partner organizations.

Much of this information will be provided to the governing body for validation or review (e.g. business strategy, organizational performance, strategic change initiatives, risk appetite, etc.), however, some of the "softer", more human aspects might not be formally quantified. In these instances, the governing body should request executive managers to perform organizational assessments so that this feedback can be presented to the governing body and taken into consideration.

5.2.3 Understand external environment

The governing body should ensure that they are kept appraised of external factors that might drive business opportunities and risks, thereby mandating IT related business change responses. These factors should form part of the environmental reviews that are presented by executive managers when preparing strategic plans for approval by the governing body. Key considerations include:

Regulatory environment	The impacts that local and global regulations might have on how the organization treats its IT
Technological advances	How advances in IT can be used to redefine business models and change the ways in which individuals engage
Generational trends	The social and cultural expectations of younger generations and the risks and opportunities that these present for IT – both for members of the organization, as well as for consumers of the organization's products and services

Skills availability	How the sourcing of skills or capabilities from other organizations and or geographies will impact the organization and can be enabled by IT
Competitive forces	How competitors are using IT to gain strategic advantage
Market developments	How new products and consumer demands are driving the use of IT
Stakeholder requirements	The impacts that external stakeholder groups (e.g. environmental, social responsibility) might have on the organization's IT
External threats	The overall risk to the organization's reputation from unauthorized access to the IT environment.

External changes can have material impacts on the organization's IT and the governing body should carefully consider these factors in its governance of IT.

5.2.4 Identify current state of the use of IT

Once the internal and external context has been identified, the governing body can appropriately determine how the organization is currently being supported and enabled through the use of IT.

The principles-based evaluation method requires an assessment of the extent to which appropriate outcomes are being achieved for each of the principles of the ISO/IEC 38500 standard. Annex A provides an example assessment scheme and a suggested graphical representation for displaying the outcome of the assessment.

Careful judgement is required when performing these ratings, as the basis of assessment is qualitative in nature and variances may arise owing to differences in interpretation. Governing bodies should ensure that there is a broad base of participants in this process to achieve the best result.

One of the difficulties of evaluating at the principle level is that it is easy to exclude or neglect key aspects that might not be explicitly referenced. To this end, sample assessment criteria have been identified for each of the six ISO/IEC 38500 principles (see Annex B). These take the form of ***beneficial outcomes*** which are more granular in nature and thus more readily assessed. The ***evidence of success*** that is associated with these beneficial outcomes is primarily used for the monitor activity (described later), but may also be used to assist with the identification and assessment of the current state of achievement of the beneficial outcomes.

These assessment criteria may be used as a baseline for determining the current state during the initial 'implementation' cycle, but should then be revisited during subsequent iterations through the cycle to reflect the governing body's evolving vision of how the organization is supported and enabled through appropriate use of IT.

5.3 Direct

5.3.1 Overview

The governing body should define how it believes the organization should be supported and enabled through the appropriate use of IT (the desired state). In addition, it should initiate an appropriate program of change activities and establish governance enabling mechanisms.

5.3.2 Define desired state for the use of IT

In order to assist the governing body in defining the desired state for the use of IT within the organization, the organizational culture or foundation upon which this vision will be based, should be determined.

The culture for the governance of IT should align with the broader governance criteria for the organization and represents the distillation of the governing body's perspective on how the internal and external

environmental factors should shape the use of IT in the organization. These distillations may take the form of statements or short paragraphs and might cover:

— the organization's business strategy and reliance on IT;

— risk;

— compliance;

— decision making model (rights/delegations of authority).

Having established this culture, the governing body is now able to revisit the six principles of ISO/IEC 38500 (per Annex B) and define the desired state for the use of IT in the organization. The desired state represents the optimal outcomes for the organization and can also be guided by other factors, including costs vs. benefits, resource availability, organizational change readiness, etc.

As indicated in 5.2.4 above, the existing assessment criteria may be used for the first cycle of this activity to establish a baseline, however, subsequent iterations might result in different and/or additional assessment criteria being defined that are relevant and appropriate to the organization.

The desired states should be positioned on the same graphical representations that were used for assessing the current state for each principle.

5.3.3 Initiate change program

Once the organization's current and desired states for each of the ISO/IEC 38500 principles have been identified, it is possible to perform a gap analysis between the two states.

Each identified gap area might require change activities or projects to be initiated to achieve the desired outcomes for the organization. The evidence of success statements, listed in the assessment criteria, provide useful guidance in this regard.

Once all of the change activities have been identified, these should be compiled into a change program that considers the following aspects:

— resources and skills required to implement the program;

— stakeholder involvement and responsibilities;

— budget and schedule;

— dependencies with business-as-usual and other special projects;

— prioritisation of initiatives based on the organization's needs;

— quick-win opportunities that require little implementation effort, but deliver visible results.

The governing body should review the change program and, if satisfied, approve the program and ensure that that there is executive sponsorship for its implementation. The program may simply require an individual to perform a task, or the change might need to be coordinated across multiple organizational structures. The administration of these activities, as well as the appropriate delegation of authority, is required to successfully implement the changes and this is discussed in clause 5.3.4 below.

5.3.4 Identify governance enabling mechanisms

Governance of IT is enabled through the establishment of a governance framework which specifies the applicable strategies, policies, decision-making structures and accountabilities through which the organization's governance arrangements operate.

A key aspect of the governance framework is the allocation of responsibility, delegation of authority and accountability for IT related decisions. These may be documented in a Charter, or in appropriate

policy statements, which specify the types of decisions that may be made by specific structures and or individuals in the organization. Key issues might include:

— governing body's reserve powers;

— the responsibility and authority for policies (this might include indicating what policies are required);

— business strategy for IT;

— IT-related architecture decision making;

— sourcing strategies and decisions;

— investment decision making.

Consideration should also be given to specific roles within the governance structure where they exist within the organizations, including:

— Governance Steering Group;

— Risk Committee;

— Audit Committee.

It is important that delegated decisions are performed in a transparent manner. This ensures that the delegation process remains effective, whilst ensuring that the governing body is able to take final accountability.

The Governance Steering Group, described in 4.3, plays a critical role in facilitating the transparent delegation of authority. It is also responsible for tracking progress on the change program activities, as well as performing the necessary administration activities to effectively orchestrate the governance of IT. These include:

— administering procedures and documenting activities;

— compiling the terms of reference for the Governance Steering Group;

— compiling a Charter that records the IT-related delegations of authority;

— presenting all necessary information to the governing body for review and direction;

— following up with executive managers and other relevant parties;

— gathering and coordinating all relevant information required for monitoring.

5.4 Monitor

5.4.1 Overview

Once the governing body has identified the desired state for the use of IT within the organization, it should be able to answer the following key questions, namely:

— Are we doing the right things?

— Are we making progress?

— Have we reached the desired state?

This requires the identification of likely evidence of success to measure the achievement of outcomes, as well as the establishment of an effective monitoring system that collects and analyses data and appropriately reports on the evidence of success to the governing body.

As in the evaluate and direct activities above, the initial monitor cycle is used to establish a baseline for the evidence of success and the monitoring system, with subsequent iterations resulting in refinements as required.

5.4.2 Define evidence of success

When defining the desired state for the use of IT within the organization (part of direct), it might be appropriate to also identify the evidence of success that will be used to monitor the progress towards the achievement of these outcomes.

This evidence may be qualitative or quantitative in nature, but should aim to be: specific, relevant, realistically achievable and measurable.

To assist with this process, statements indicating likely evidence of success have been identified in the assessment criteria for each of the six ISO/IEC 38500 principles (see Annex B). These statements describe desired end-states which, when attained, would indicate the achievement of the beneficial outcomes. They encompass key aspects of IT deployment and use, and may include:

— business engagement;

— strategic alignment;

— business case and benefits realisation;

— functional and technical fit;

— IT service delivery, service levels and support;

— information security and integrity;

— risk and control;

— education and training.

The initial monitor cycle may use these statements as a baseline for defining the evidence of success. As subsequent iterations are made through the cycle, these evidence of success statements may be refined to appropriately to reflect the governing body's evolving vision of how the organization is supported and enabled through appropriate use of IT.

5.4.3 Establish monitoring system

The Governance Steering Group is responsible for ensuring that the governing body is provided with appropriate and timely reporting on the evidence of success as well as any change projects that were initiated.

The Governance Steering Group should not be compiling this information itself, but should rather be obtaining this information through the organization's management systems to ensure that relevant information is properly sourced, collected, analysed and presented. Typical challenges that may be encountered include:

— spanning organizational boundaries;

— trade-offs between cost, accuracy, and timeliness.

6 Continual Review

Once the first cycle through the 'Establish and Sustain Enabling Environment' and 'Govern IT' activities has been completed, the baseline for the governance of IT will have been established.

In time, as the governance of IT matures in the organization, or the organizational context changes, opportunities for improvement may become apparent. The Governance Steering Group should identify

and track these opportunities and, on an on-going basis, review the governance of IT implementation to determine whether the desired outcomes are being achieved. Key review considerations may include:

— Is there a better understanding in the governing body of what value IT can bring to the organization?

— Is there a better understanding in management for the business need regarding the use of IT?

— Is the use of IT bringing more value to the organization due to the governing activities?

— Are the risks of using IT fully understood and appropriately managed in the organization due to the governing activities?

Where appropriate, the Governance Steering Group should initiate the re-application of a cycle of the activities, thereby ensuring continual improvement of the implementation of the governance of IT in the organization.

Annex A
(informative)

Assessment Scheme

The assessment scheme for implementing principles-based governance of IT focuses on the achievement of beneficial outcomes, rather than the means of achieving outcomes. It needs to be sufficiently broad to cater for different jurisdictions, regulations & organizations and is therefore inherently more qualitative than quantitative in nature.

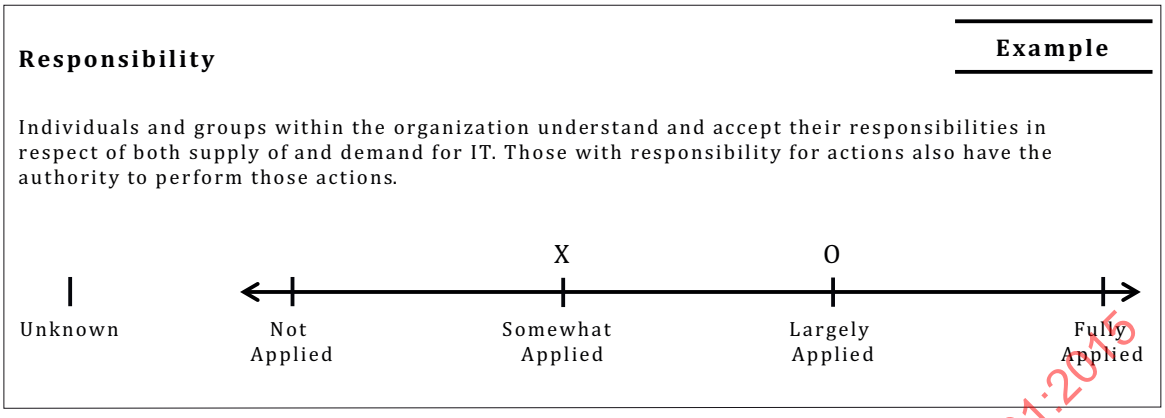
A five-level evaluation scheme may be used by the governing body to assess the current state and to determine desired levels of achievement of beneficial outcomes for the organization, across the six principles in the ISO/IEC 38500 standard. (Annex B provides example evidence of success for each ISO/IEC 3800 principle that could be used in the assessment process)

Table A.1 provides high level guidance for evaluating the current and desired states of the beneficial outcomes. Organizations should consider both the achievement of beneficial outcomes and evidence of success when performing assessments, as there may be situations where there is little evidence of success, but the beneficial outcomes are perceived to being achieved.

Table A.1 — Rating scale and description

Rating	Description
Unknown	— No knowledge of the level of achievement of outcomes and no evidence of success
Not Applied	— The majority of beneficial outcomes are not being achieved — Little evidence of success
Somewhat applied	— Some beneficial outcomes being achieved to a certain degree with one or more beneficial outcomes not being achieved at all — Some evidence of success visible with one or more aspects not in place at all
Largely Applied	— All beneficial outcomes being achieved to a large degree with certain beneficial outcomes being fully achieved — All evidence of success visible to a large extent with certain aspects being fully in place
Fully Applied	— All beneficial outcomes are being fully achieved — All evidence of success fully implemented and working effectively

Figure A.1 provides a suggested graphical representation of the output of this activity.



Key

X current state

O desired state

Figure A.1 — Suggested method of displaying output