FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/IEC
FDIS
38503

ISO/IEC JTC **1**/SC **40**

Secretariat: **SA**

Voting begins on:
2021-10-13

Voting terminates on:
2021-12-08

Information technology — Governance of IT — Assessment of the governance of IT

Reference number
ISO/IEC FDIS 38503:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

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 documents 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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 40, *IT Service Management and IT Governance*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

As part of their accountability for an organization, governing bodies are responsible and accountable for the current and future use of IT (information technology) within an organization. To meet this obligation, it is recommended that members of the governing body ensure that there is effective governance of IT within the organization, involving both their own activities in setting the direction for the organizational use of IT, as well as their oversight and evaluation of the management of IT within the organization.

ISO/IEC 38500 provides principles, definitions and a model for governing bodies to use when evaluating, directing and monitoring the use of IT in their organizations. This document provides guidance on how to assess an organization's governance of IT arrangements based on ISO/IEC 38500, ISO/IEC TS 38501 and ISO/IEC TR 38502.

The specific arrangements for the governance of IT vary from organization to organization. The variation depends on various factors including the organization's level of reliance on IT, both strategically and operationally, as well as the size and nature of the organization.

Governing bodies should seek continual improvement of the governance of IT as part of their overall accountability for organization governance and they should assess whether the current arrangements meet the needs of the organization. They should use such an assessment to improve the effectiveness of the governance of IT in a structured way, with a planned approach. The assessment should address not only management's approach to supporting the governance of IT but also the effectiveness of their own approach to evaluating, directing and monitoring management activities.

The purpose of this document is to assist governing bodies, authorized subcommittees and other key stakeholders in assessing the capability and maturity of the arrangements for the governance of IT in the organization.

It provides an objective approach for determining whether the governing body is appropriately governing IT, as well as examples of the practices and outcomes (referred to as 'characteristics' in this document) of the good governance of IT (see Tables A.1 to A.7 in Annex A). The outcomes of the assessment can be used to assist the governing body to determine where and how the governance of IT can be improved in the organization.

The primary audiences for this document are the governing body and its subcommittees, executive managers and assessors, who will also derive benefit from this document when planning and conducting an assessment of the organization's governance of IT.

Information technology — Governance of IT — Assessment of the governance of IT

1 Scope

This document provides guidance on the assessment of governance of information technology (IT) based on the principles, definitions and model for the governance of IT outlined in ISO/IEC 38500 and ISO/IEC TR 38502 and the implementation considerations outlined in ISO/IEC TS 38501.

This document includes approaches to conducting the assessment, the criteria against which the assessment can be made, guidance on the evidence that can be used for the assessment, as well as a method for determining the maturity of the organization's governance of IT.

This document is applicable to organizations of all sizes, regardless of the extent of their use of IT.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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, *Information technology — Governance of IT for the organization*

ISO/IEC/TS 38501, *Information technology — Governance of IT — Implementation guide*

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1
beneficial outcome
achievement of a high-level objective of the organization, related to the successful deployment and use of information technology

3.2
evidence of success
observable and measurable deliverables from information technology functions/processes that support and enable the achievement of beneficial outcomes

4 Benefits of the assessment of the governance of IT

4.1 Context

The governance of IT involves appropriate behaviours from governing bodies and management to create and maintain a framework for the use of IT, that delivers long-term value consistent with the expectations of its stakeholders, including:

- continuous innovation in services, markets and business;
- clarity of responsibility and accountability for both the supply of and demand for IT in achieving the strategic goals of the organization;
- assurance of business continuity and sustainability through IT;
- realization of the expected benefits from each IT investment;
- conformance with relevant obligations (regulatory, legislation, common law, contractual);
- effective oversight of the management of IT risks;
- constructive relationships and effective communications between the business and IT management, and with external partners.

However, organizations can experience a wide variety of challenges, which can prevent them from achieving the desired outcomes from their efforts at governing IT, including:

- the governing body and executive managers delegating the responsibility for the governance of IT to those responsible for implementing technology;
- the lack of policies and frameworks clarifying the relationship between governance of IT and management of IT;
- dependence on organizational processes, rather than effective decision making, appropriate behaviours, proper communication and suitable human interactions;
- difficulty monitoring and measuring behaviours and expected outcomes, including:
  - ensuring that IT objectives are aligned to the organization’s purpose and objectives;
  - ensuring that IT risks are known and mitigated;
  - stewardship of enterprise assets, resources and continuity planning;
  - conformance by the organization with established and expected norms of behaviour;
  - holding IT accountable for the delivery of services and solutions;
  - evolution of business models through the use of information and the adoption of new technologies.

4.2 Benefits of assessing the governance of IT

It is important, therefore, for organizations to adopt a structured method to assess whether their governance of IT arrangements are achieving the desired outcomes and the key benefits, including:

- assisting with the development of the framework for the governance of IT;
- determining the strengths and weaknesses of the current governance of IT capability;
- helping to determine improvement actions that need to be taken;

- improving the levels of engagement between executive managers and the governing body as regards expectations and outcomes related to the governance of IT;
- creating an awareness in the governing body of their roles and responsibilities as regards the governance of IT;
- assisting organizations with IT conformance;
- providing feedback to the governance stakeholders and support staff.

5 Assessment scope and approach

5.1 Establish scope

The governing body shall define the scope and the requirements and objectives of the assessment. The governing body shall identify those stakeholders which require, or might benefit from, the results of an assessment of the governance of IT. For these stakeholders, the needs and expectations shall be taken into consideration when designing the assessment.

In establishing the scope, focus and priority of the assessment, consideration shall be given to evaluating issues of highest importance to the organization in order to achieve the greatest benefits and not to waste resources. This can take account of the level of operational reliance on IT, the existence of assurance inputs, as well as any specific strategic initiatives of importance and priority to the organization.

Figure 1 shows areas related to the implementation of governance of IT, as described in ISO/IEC TS 38501, that shall be considered when defining the scope of the assessment.

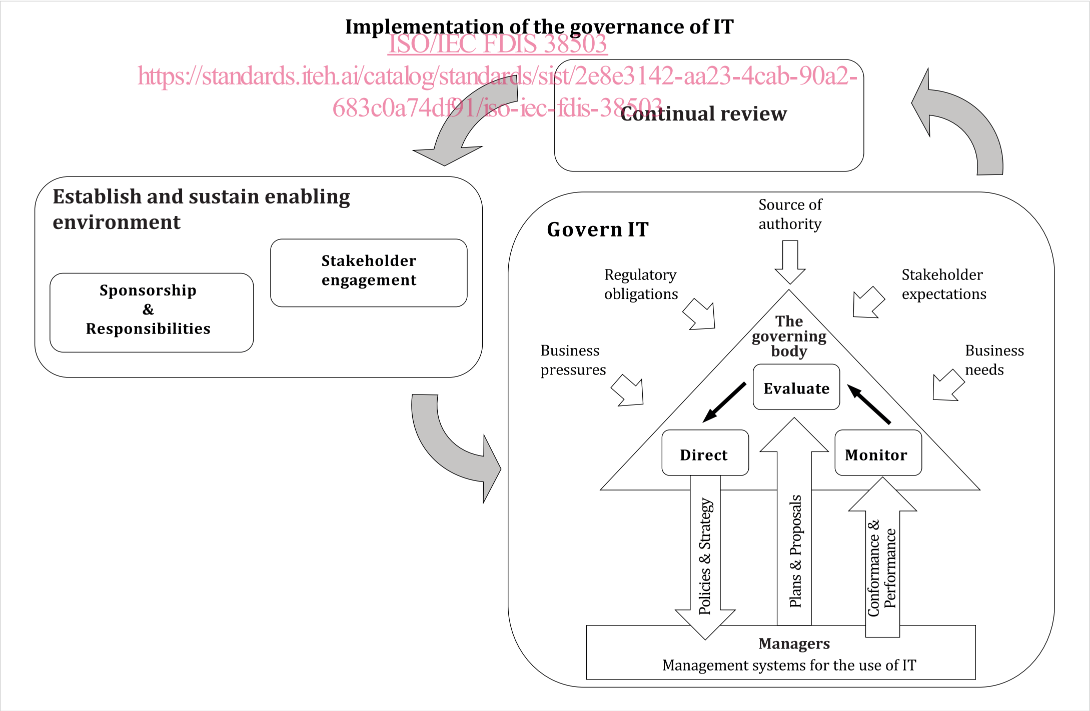

Figure 1 — Areas for consideration in the assessment of the governance of IT [SOURCE: ISO/IEC TS 38501:2015, Figure 1]

Table 1 identifies key aspects related to the implementation of governance of IT, as described in ISO/IEC TS 38501, that shall be considered when defining the scope of the assessment.

Table 1 — Key aspects for consideration in the assessment of the governance of IT

Establish and sustain enabling environment
— goals and objectives of governance of IT — understanding of stakeholders, roles and responsibilities — stakeholder engagement — delegation of authority
Govern IT
— application of the six principles and EDM Model — governance steering group — internal and external environment — articulation of current and desired states and beneficial outcomes — monitoring capability and identification of evidence of success — change programme
Continual review
— improvement in value derived from IT — management of risks associated with IT — additional governance actions required

5.2 Assessment approach and involved parties

In establishing an assessment approach, consideration shall be given to the objectives/purpose of the assessment, degree of independence required for the assessment, the skills/knowledge of the assessors and participants and other relevant considerations dependent on the specific arrangements for the governance of IT within the organization.

The assessment approach shall be approved by the governing body. It shall be supported with the details of the assessment framework, an assessment plan, roles and responsibilities of assessors, timing of the assessment, resources necessary for the assessment and an understanding of the skills and knowledge of the assessors.

There are different approaches to the assessment of the governance of IT. The assessment approaches and the key considerations are summarized in Table 2.

Table 2 — Assessment approach and key considerations

	Governing body assessment	Internally facilitated assessment	Externally facilitated assessment
Description	Assessment of governance of IT performed by the governing body; this can be considered similar to a self-assessment.	Assessment of governance of IT performed by approved, skilled and knowledgeable internal resources or assessors to support the assessment.	Assessment of governance of IT performed by approved skilled and knowledgeable external resources or assessors to support the assessment.
Objective/ Purpose	— high-level self-assessment — enables the governing body to monitor its own performance in respect to the governance of IT	— detailed internal assessment — provides the governing body with an internal perspective on the extent to which it is meeting its responsibilities in respect of the governance of IT	— detailed independent external assessment — provides the governing body with an external perspective on the extent to which it is meeting its responsibilities in respect of the governance of IT
Benefits	— speed/ease — no dependency on assessors (internal or external)	— broader involvement (executive management) — greater level of information considered	— greater objectivity — ability to support external reporting requirements
Participants	— governing body	— governing body — executive management — business and technical experts	— governing body — executive management — business and technical experts
Assessor	— member of the governing body	— internal assessor/s	— external independent assessor/s
Success factors	— the governing body shall be committed to performing the self-assessment and acting on its conclusions	— the governing body shall be committed to supporting the internal assessment and acting on its conclusions — the internal resource has the necessary authority to assess the governing body	— the governing body shall be committed to supporting the external assessment and acting on its conclusions

5.3 Roles, responsibilities and competencies

5.3.1 Roles associated with the assessment of the governance of IT

The following are the important roles within the context of the assessment of the governance of IT. A full description is provided for each role in the following subclauses:

- governing body (see 5.3.2);
- sponsor (see 5.3.3);
- executive management (see 5.3.4);
- assessment expert (assessor) (see 5.3.5);

- business expert (see 5.3.6);
- technical expert (see 5.3.7).

5.3.2 Governing body

The governing body is a key role in the assessment. It provides the overall direction to the assessment and ensures that the assessment adds value to the overall governance objective. In the event of the governing body performing the assessment itself, there are additional responsibilities and skills/knowledge requirements. These are shown in Table 3.

Table 3 — Responsibilities and skills/knowledge of the governing body

Responsibilities	Skills/Knowledge
— Overall: — establish the key objectives of the assessment; — approve the assessment scope and approach; — enable executive management to achieve the key objectives of the assessment; — evaluate whether the assessment provides the desired deliverables as per the key objectives; — ensure that the assessment adds value to the overall governance objectives; approve/reject the formal assessment report submitted by the sponsor. — Governing body assessment: — the overall responsibilities described above are still applicable; — if there is a gap in competencies for performing the assessment, nominate the relevant members to acquire the competencies for performing the assessment; — manage the operational aspects of the assessment and the production of the report.	— Overall: — should have a basic awareness of ISO/IEC 38500, ISO/IEC TS 38501 and ISO/IEC TR 38502; — shall understand the internal and external context within which the organization operates. — Governing body assessment: — members of the governing body participating as an assessor in the governing body assessment shall have the skills and knowledge required to conduct the governing body assessment, where required.

5.3.3 Sponsor

The sponsor is a member of the governing body. The sponsor ensures that the scope of assessment is finalized and the resources required for conducting the assessment are available. The sponsor's responsibilities and skills/knowledge requirements are shown in Table 4.