INTERNATIONAL STANDARD

ISO/IEC 38503

First edition
2022-01

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

Technologies de l'information — Gouvernance des TI — Évaluation de la gouvernance des TI

Reference number
ISO/IEC 38503:2022(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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Benefits of the assessment of the governance of IT **2**
4.1 Context 2
4.2 Benefits of assessing the governance of IT 2
5 Assessment scope and approach **3**
5.1 Establish scope 3
5.2 Assessment approach and involved parties 4
5.3 Roles, responsibilities and competencies 5
5.3.1 Roles associated with the assessment of the governance of IT 5
5.3.2 Governing body 6
5.3.3 Sponsor 6
5.3.4 Executive management 7
5.3.5 Assessment expert (assessor) 7
5.3.6 Business expert 7
5.3.7 Technical expert 8
6 Assessment of the governance of IT **8**
6.1 Assessment overview 8
6.2 Reference model for the governance of IT 9
6.2.1 Governance of IT practice areas 9
6.2.2 Governance of IT characteristics 9
6.2.3 Measurement model for the governance of IT 10
6.2.4 Assessment framework for the governance of IT 11
6.3 Assessment of the governance of IT 12
6.4 Governance of IT maturity model 12
7 Assessment activities **14**
7.1 Plan the assessment 14
7.2 Perform the assessment 15
7.2.1 Collect the data 15
7.2.2 Conduct the assessment 15
7.3 Report the assessment 16
Annex A (Informative) **Assessment framework — Governance of IT practice areas** **17**

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 for 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 terminology 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.

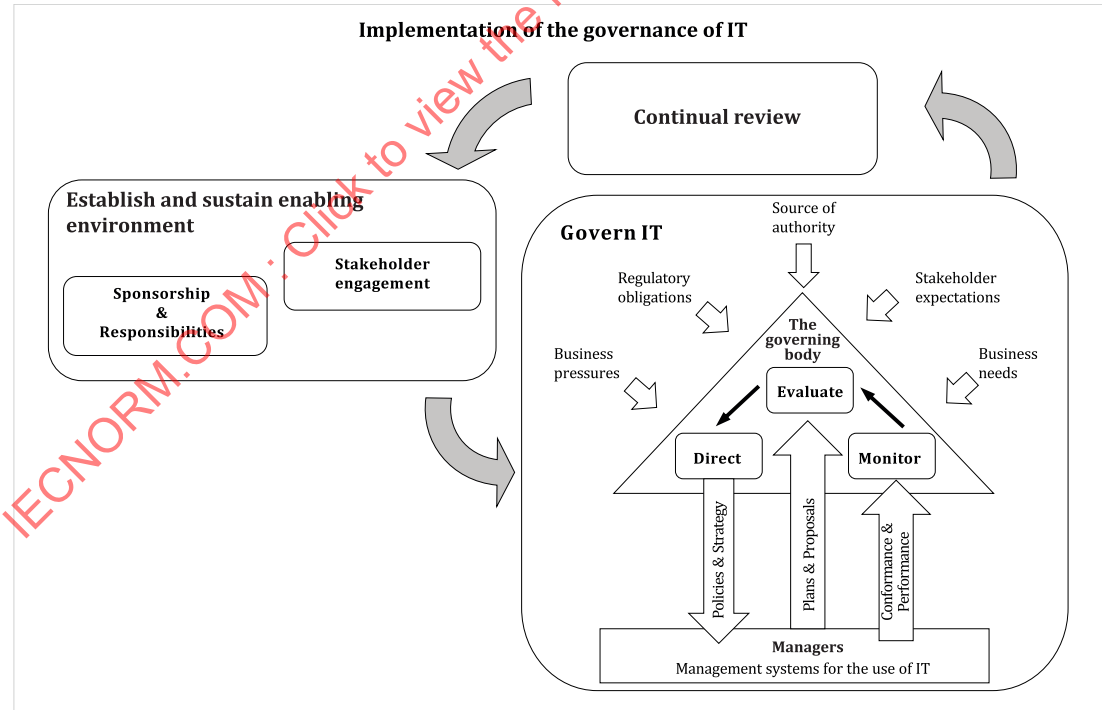


Figure 1 — Areas for consideration in the assessment of the governance of IT [SOURCE: ISO/IEC TS 38501:2015, Figure 1]

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.

Table 2 *(continued)*

	Governing body assessment	Internally facilitated assessment	Externally facilitated 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.

Table 4 — Responsibilities and skills/knowledge of the sponsor

Responsibilities	Skills/Knowledge
— finalize and approve the plan for the assessment; — ensure that the resources required for conducting the assessment are available; — ensure that the assessor has access to business and technical experts required during the assessment; — review of final report and submission to governing body.	— 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.

5.3.4 Executive management

Executive management follows the directives of the governing body as regards the assessment and provides the assessor with the required assessment data and support. The executive management's responsibilities and skills/knowledge requirements are shown in Table 5.

Table 5 — Responsibilities and kills/knowledge of the executive management

Responsibilities	Skill/Knowledge
— work towards achieving the key objectives of the assessment; — review the assessment plan as prepared by the assessor, where required; — provide the assessor with the required assessment data and access to business and technical experts; — review the accuracy and completeness of the assessment report; — manage communication between the governing body and downstream stakeholders.	— should have 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; — should build trust and personal accountability among all participating roles.

5.3.5 Assessment expert (assessor)

The assessment expert (assessor) is the individual or group of individuals who perform the actual assessment. The assessor's responsibilities and skills/knowledge requirements are shown in Table 6.

Table 6 — Responsibilities and skills/knowledge of the assessment expert (assessor)

Responsibilities	Skills/Knowledge
— understand and document the objectives for the assessment; — verify that the assessment approach is approved; — verify that the assessment scope is properly established before the start of assessment; — prepare the assessment plan and conduct the activities as per the assessment plan; — prepare and submit the assessment report.	— shall have a good knowledge of ISO/IEC 38500, ISO/IEC TS 38501 and ISO/IEC TR 38502 and the assessment framework; — shall understand the governance of IT arrangements within the organization and the various roles and their contributions; — shall have good knowledge of assessment standards and best practices and shall have experience enabling them to apply the same towards assessment.

5.3.6 Business expert

The business expert is the individual or group of individuals who constitute the internal resource providing the necessary business data required to perform the actual assessment. The business expert's responsibilities and skills/knowledge requirements are shown in Table 7.

Table 7 — Responsibilities and skills/knowledge of the business expert

Responsibilities	Skills/Knowledge
— understand the scope and objective of the assessment; — provide business domain expertise required during the assessment.	— should have basic knowledge of the business benefits of ISO/IEC 38500, ISO/IEC TS 38501 and ISO/IEC TR 38502; — shall have good knowledge and understanding of organization's business processes and procedures; — should understand how IT can enable business innovation and transformation and value generation.

5.3.7 Technical expert

The technical expert is the individual or group of individuals who constitute the internal resources providing the necessary technical expertise and support required to perform the actual assessment. The technical expert's responsibilities and skills/knowledge requirements are shown in Table 8.

Table 8 — Responsibilities and skills/knowledge of the technical expert

Responsibilities	Skills/Knowledge
— understand the scope and objective of the assessment; — provide the technical expertise required during the assessment.	— should have a good knowledge of ISO/IEC 38500, ISO/IEC TS 38501 and ISO/IEC TR 38502; — shall understand technical risks and mitigations; — should understand how IT can enable business innovation and transformation and value generation; — should understand regulatory aspects of new technology.

6 Assessment of the governance of IT

6.1 Assessment overview

The assessment of the governance of IT shall be performed using the reference model for the governance of IT, which is derived from the core standards, namely ISO/IEC 38500, ISO/IEC TS 38501 and ISO/IEC TR 38502. The reference model comprises four components, namely:

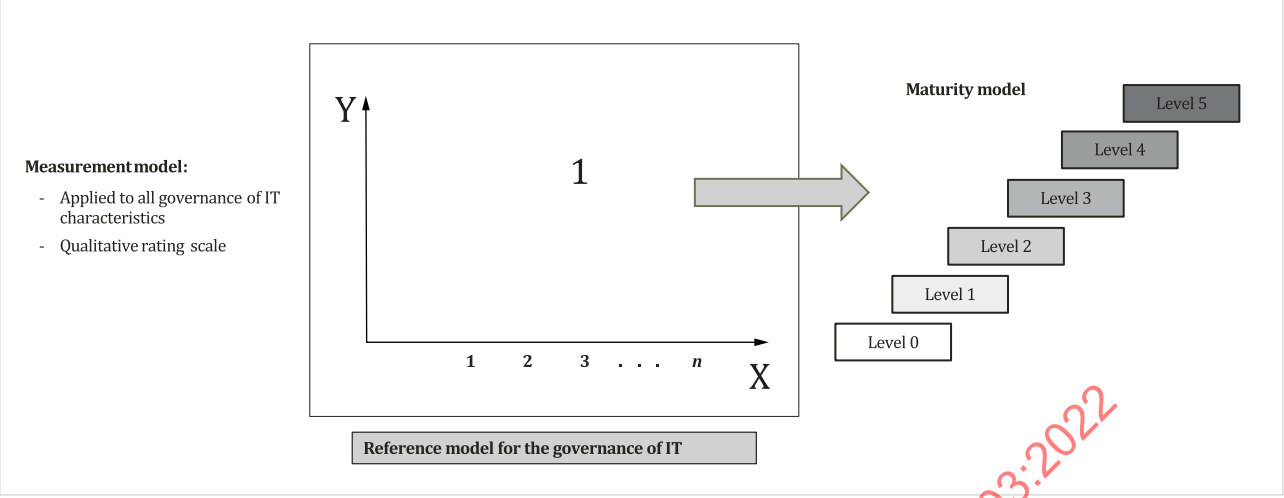
— governance of IT practice areas (see 6.2.1);

— governance of IT characteristics (see 6.2.2);

— measurement model for the governance of IT (see 6.2.3);

— assessment framework for the governance of IT (see 6.2.4).

Figure 2 shows the interrelationship of these concepts.



Key

1 assessment of the governance of IT
X governance of IT practice areas
Y assessment rating

Figure 2 — Overview of the assessment of the governance of IT

6.2 Reference model for the governance of IT

6.2.1 Governance of IT practice areas

The governance of IT practice areas represent the key areas of focus for the organization when effectively governing IT. Seven practice areas have been identified, with the first being derived from ISO/IEC TS 38501 and ISO/IEC TR 38502. The other six practice areas are derived from the six principles in ISO/IEC 38500:

— Enabling mechanisms;

— Responsibility;

— Strategy;

— Acquisition;

— Performance;

— Conformance;

— Human behaviour.

Subclause 6.2.2 and Annex A provide further information on the content that is covered in each practice area.

6.2.2 Governance of IT characteristics

Each practice area contains three categories of characteristics, as defined in the core standards, namely:

— governance tasks and practices (evaluate, direct and monitor);

— evidence of success (deliverables indicating the achievement of beneficial outcomes);

— beneficial outcomes (organizational objectives achieved through IT).

These relationships are shown in Figure 3 below.

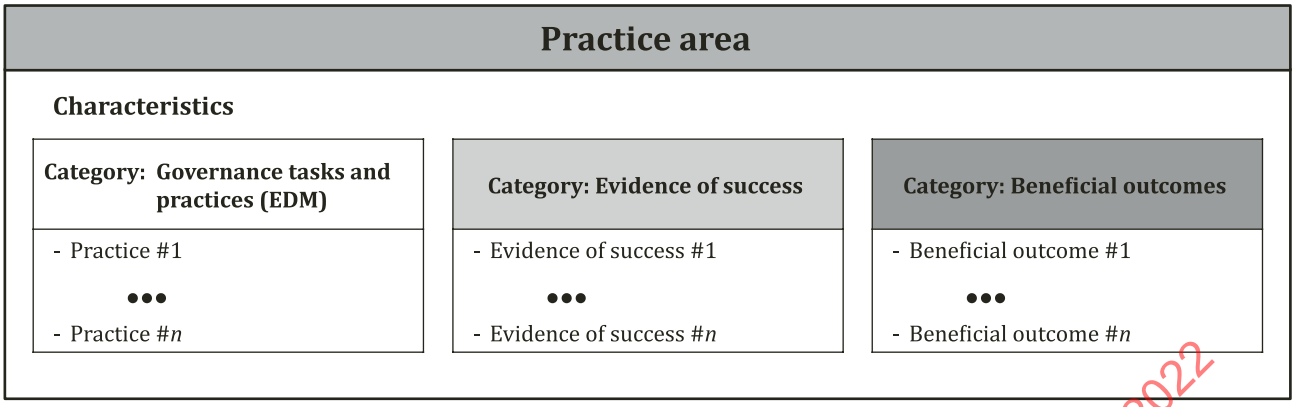


Figure 3 — Practice area with the 3 categories of governance of IT characteristics

Example characteristics, by practice area and category, are provided in Tables A.1 to A.7 of Annex A as part of the sample assessment framework for the governance of IT.

It is anticipated that organizations will customize the characteristics to suit their particular organizational circumstances.

6.2.3 Measurement model for the governance of IT

ISO/IEC TS 38501 defines a measurement model that is more qualitative than quantitative in nature, since principles-based standards focus on the achievement of outcomes, rather than the means of achieving outcomes.

The measurement model from ISO/IEC TS 38501 has been adopted with minor amendments to include the evaluate, direct and monitor (EDM) tasks and practices. The standardized rating scale is maintained (left hand column), with specific measures being defined for each of the three categories of governance of IT characteristics. This is shown in Table 9.

Table 9 — Measurement rating scale

Rating	EDM tasks and practices	Evidence of success	Beneficial outcomes
Unknown	EDM tasks and practices not being performed	No evidence of success	No knowledge of the level of achievement of outcomes
Not applied	Limited performance of EDM tasks and practices	Little evidence of success	The majority of beneficial outcomes are not being achieved
Somewhat applied	Some evaluate and direct tasks and practices being performed but limited monitoring practices	Some evidence of success visible with one or more aspects not in place at all	Some beneficial outcomes being achieved to a certain degree with one or more beneficial outcomes not being achieved at all
Largely applied	The majority of evaluate and direct tasks and practices being performed with a fair degree of monitoring practices	All evidence of success visible to a large extent with certain aspects being fully in place	All beneficial outcomes being achieved to a large degree with certain beneficial outcomes being fully achieved
Fully applied	All EDM tasks and practices being fully performed	All evidence of success fully implemented and working effectively	All beneficial outcomes being fully achieved

6.2.4 Assessment framework for the governance of IT

The assessment framework for the governance of IT is then defined by applying the measurement model to each category of governance of IT characteristics for each practice area. This is illustrated in Figure 4.

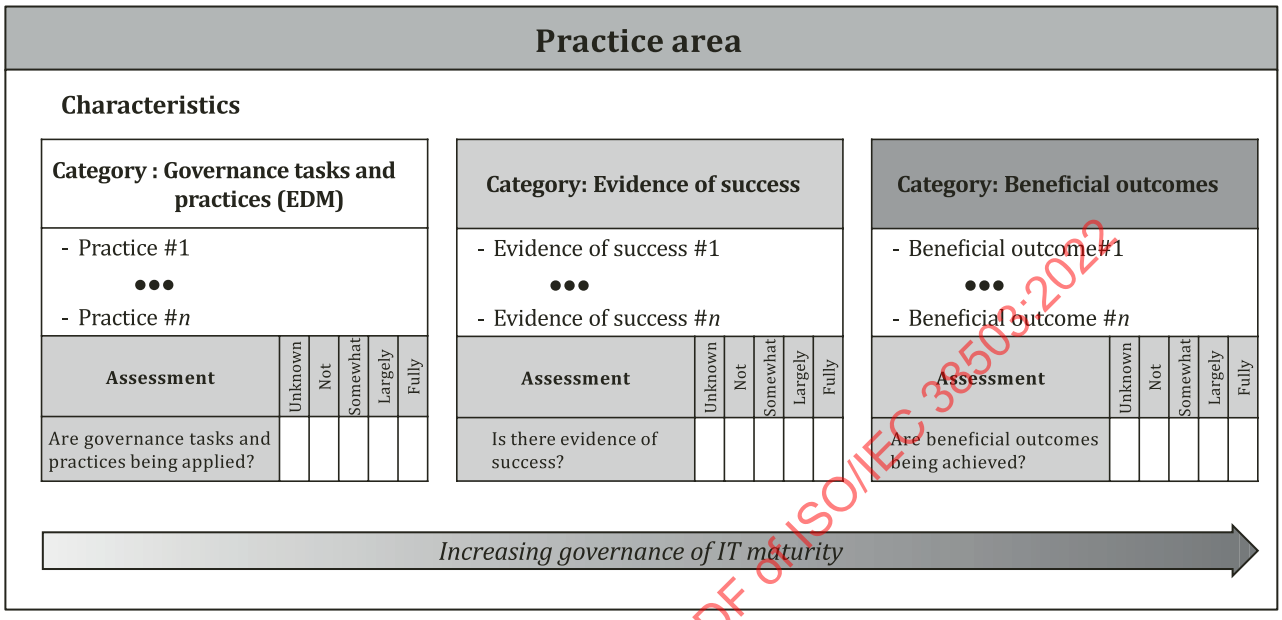


Figure 4 — Assessment framework for the governance of IT

The measurement model is applied to the overall category of governance of IT characteristics, rather than to individual characteristics within each category, for the following reasons:

— assessing individual characteristics within a category creates additional complexity, requiring an aggregation formula per category;

— different characteristics can be perceived to be more important than others, necessitating a weighting scheme that would add further complexity;

— assessing at the governance of IT characteristics level will not bring further accuracy to the inherently qualitative assessment approach and will require additional work. This can lead to the perception of "overkill".

Figure 4 also illustrates the relationship between the categories of governance of IT characteristics and increasing governance of IT maturity, as indicated by the arrow at the bottom of the diagram. This can be briefly summarized as follows:

— in the absence of formalized governance of IT, it is likely that the organization will have a low level of governance of IT maturity;

— to improve the level of maturity, the governing body can undertake appropriate governance of IT tasks and practices;

— this can lead to improved deployment and use of IT in the organization, as demonstrated by evidence of success;

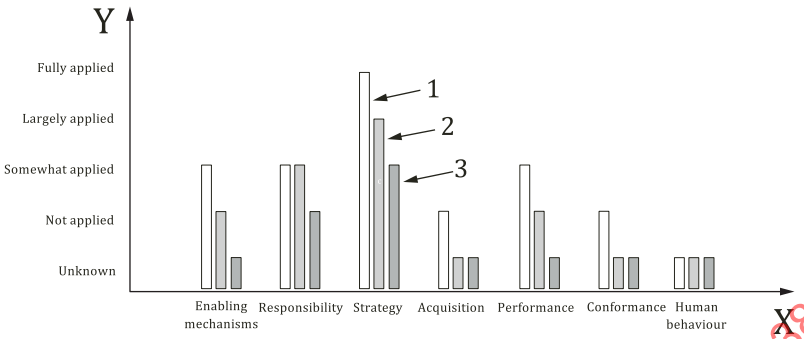
— this, in turn, can support and enable the achievement of beneficial outcomes for the organization.

These concepts are expanded further in the governance of IT maturity model in 6.4.

6.3 Assessment of the governance of IT

The assessment of the governance of IT is performed by rating each category of characteristics, for all of the in-scope practice areas in the governance of IT reference model.

Figure 5 shows an example graphical representation of an assessment of all governance of IT practice areas. This would need to be supported with appropriate detail in a report as further discussed in 7.3.



Key

1	governance tasks and practices (EDM)	X	practice areas
2	evidence of success	Y	assessment rating
3	beneficial outcomes		

Figure 5 — Example graphical representation of an assessment of the governance of IT

6.4 Governance of IT maturity model

The governance of IT maturity model relates to the growing ability of an organization to achieve higher levels of capability across its key governance of IT characteristics. The overarching theme evolves from initially performing governance tasks, through seeing evidence of success and eventually to achieving beneficial outcomes for the organization. This growing capability needs to be demonstrated across all governance of IT practice areas.

The organization's governance of IT maturity level is based on the rating of each category of characteristics, for all practice areas in the governance of IT reference model and is obtained according to the measurement model described in 6.2.3.

Each maturity level describes the minimum rating that the organization needs to achieve in each category of governance of IT characteristics, for all practice areas. For example, to achieve a level 2 rating, for all practice areas, the governance tasks (EDM) need to be 'largely applied' while evidence of success and beneficial outcomes need to be 'somewhat applied'.

The governance of IT maturity level shall be determined according to Table 10.

Table 10 — Governance of IT maturity model

Characteristics				
Governance tasks (EDM)	**Evidence of success**	**Beneficial outcomes**		
Unknown or not applied	**Unknown or not applied**	**Unknown or not applied**	— No leadership commitment to the governance of IT — Governing body and executive managers not aware of the mechanisms that could be applied to govern IT — Lack of internal controls for IT — The organization is largely unaware of the risks associated with the use of IT	**No governance (Level 0)**
Somewhat applied	**Unknown or not applied**	**Unknown or not applied**	— Governing body and executive managers aware of the purpose and objectives of governing IT — Implementation of basic governance of IT mechanisms initiated — Some internal controls for IT in place — The organization is aware of the risks associated with the use of IT	**Initial governance (Level 1)**
Largely applied	**Somewhat applied**	**Somewhat applied**	— Governing body and executive managers start demonstrating commitment to the governance of IT — Key stakeholders identified and engaged — Broader implementation of governance of IT mechanisms across the organization — Broader implementation of internal controls for IT across the organization — Organization starting to manage IT risk — Benefits starting to be achieved from investments in IT	**Applied governance (Level 2)**

Table 10 *(continued)*

Fully applied	**Largely applied**	**Somewhat applied**	— Enabling environment for governance of IT established by governing body, including leadership commitment, awareness and education, stakeholder engagement — Governance of IT framework established, including policies, structures and processes — System of internal control for IT established as part of the organization's management systems — Organization identifies opportunities to improve the governance of IT — Organization ensures that IT risks are managed — Benefits regularly achieved from investments in IT	**Established governance (Level 3)**
Fully applied	**Fully applied**	**Largely applied**	— Enabling environment for governance of IT sustained resulting in behavioural change from governing body and executive managers — Governance of IT framework enhanced, including charter, roles and responsibilities, governance steering group, governing body's reserve powers — System of internal control for IT enhanced to support the governance of IT, including Responsibility, Strategy, Acquisition, Performance, Conformance, Human behaviour — Continual review implemented to ensure improvement of the governance of IT in the organization — Organization ensures that IT risks are managed and IT investments drive the achievement of business value	**Achieved governance (Level 4)**
Fully applied	**Fully applied**	**Fully applied**	— Enabling environment for governance of IT optimized resulting in behavioural and cultural change across the organization — Governance of IT framework optimized to suit organizational and external requirements — System of internal control for IT optimized to suit organizational and external requirements — organization consistently leverages IT improvement opportunities from continual review and from feedback obtained from all interested parties — Continual review optimized. with feedback loops to all stakeholders, to ensure the improvement of the governance of IT in the organization — Organization ensures that IT risks are managed and IT innovation drives business transformation	**Optimized governance (Level 5)**

7 Assessment activities

7.1 Plan the assessment

A plan for the assessment shall be developed and documented by the assessor, which shall be reviewed and approved by the sponsor. The plan shall include at a minimum:

— the sponsor and the sponsor's relationship to the organization (see 5.1, 5.3.3);

— objectives of the assessment (see 5.1, 5.2);

— the scope of the assessment (see 5.1);

— the type of the assessment (see 5.2);

— the practice areas and characteristic groups for assessment (see 6.2.1, 6.2.3);

— the timeframe of the assessment (see 5.2);

— activities to be performed during the assessment (see 5.2, 7.2);

— roles and responsibilities of the participants in the assessment (see 5.3);

— resources necessary to perform the assessment (see 5.3);

— budget of the assessment (see 5.2);

— description of the planned assessment report (see 7.3).

Annex A provides a sample assessment framework to assist organizations conduct the assessment of the governance of IT. Each organization shall customize the practice areas through the revision, addition and removal of characteristics in each category, as appropriate, based on the extent to which the organization has determined its future governance state.

Roles and responsibilities for the assessment shall be assigned and communicated to personnel impacted by the assessment.

7.2 Perform the assessment

7.2.1 Collect the data

The data required for assessing the governance of IT shall be sufficient to cover the scope of the assessment, as detailed in the assessment plan.

Data determined as above shall be collected in a systematic manner, including the following requirements:

— objective evidence shall be identified and gathered to provide the basis for verification of the ratings;

— methods to gather subjective evidence shall be developed, including the list of questions to the governing body, executive managers and IT professionals within the organization;

— objective and subjective evidence shall be evaluated to ensure that it is sufficient to meet the purpose, scope and type of the assessment.

7.2.2 Conduct the assessment

The assessment process can vary depending on the governance of IT practice areas and characteristics being assessed, as described in the assessment plan. However, the following common activities shall be followed:

— rate the characteristics in the governance of IT practice area according to the measurement model (see 6.2.3);

— record the relationship between the governance practice area and characteristics being rated and the data collected (see 7.2.1);

— determine the maturity level (see 6.4);

— review the assessed maturity levels and determine the root cause of lower maturity as a basis for improvement (see 6.4);

— identify and document the list of improvements (see 7.3).

7.3 Report the assessment

A formal assessment report shall be created by the assessor capturing the key findings of the assessment. In addition, the relevant supporting documentation shall be compiled and made available should this be required. The report shall also include an improvement plan that addresses any key weaknesses or risks that have been identified. The formal assessment report shall be documented and issued to the assessment sponsor in a way that enables effective communication to the sponsor and affected parties and shall be approved by the governing body.

Key aspects of the report's content shall include:

— date and duration of the assessment;

— the names and roles of the assessors;

— the assessment participants (by name, role or functional area);

— scope of the assessment;

— type of assessment adopted;

— rating and maturity model;

— assessment result of the governance of IT in the organization;

— improvement and risk mitigation indicators.

Annex A
(Informative)

Assessment framework — Governance of IT practice areas

This annex provides an example assessment framework for the seven practice areas of the governance of IT reference model. It contains sample governance of IT characteristics, by category, from ISO/IEC 38500, ISO/IEC TS 38501 and ISO/IEC TR 38502 and is provided for information purposes only.

Assessors shall engage with the governing body and senior management to understand organizational specific governance of IT characteristics and then customize the content in this annex to suit their particular organizational circumstances.

Characteristics can be qualitative or quantitative in nature but should aim to be specific, relevant, realistically achievable and measurable.

Table A.1 — Enabling mechanisms

Governance tasks (EDM) and practices	Evidence of success	Beneficial outcomes

— Governing bodies monitor that appropriate mechanisms for governance of IT are established.
— Governing bodies regularly evaluate the organization's internal conformance to its framework for governance of IT.
	— A governance framework is established, including:
	  — strategies, policies, decision- making structures, terms of reference, charter, etc.
	— A governance steering group is established, including:
	  — administration and documentation, management of the change programme, etc.
	— The governing body considers relevant internal and external requirements in key IT decision making, including:
	  — business goals and strategy, risk appetite, organizational culture, etc.;
	  — regulatory environment, technological advances, generational trends, etc.
	— Business sponsor appointed to lead governance of IT.
	— Stakeholders are appropriately managed, including:
	  — stakeholders identified; stakeholders aware of purpose and their roles and responsibilities;
	  — continual improvement activities are undertaken, including monitoring: governing body's understanding of value of IT; management's appreciation of need for IT to support and enable business; etc.
		— Governance of IT addresses relevant aspects and is effectively administered.
		— There is effective leadership of the governance of IT.
		— Stakeholders are fully engaged and effectively contribute to the governance of IT in the organization.
		— There is continual improvement in the governance of IT.

Assessment	Unknown	Not	Somewhat	Largely	Fully
Are governance tasks and practices being applied?					

Assessment	Unknown	Not	Somewhat	Largely	Fully
Is there evidence of success?					

Assessment	Unknown	Not	Somewhat	Largely	Fully
Are beneficial outcomes being achieved?					

Table A.2 — Responsibility

Governance tasks (EDM) and practices	Evidence of success	Beneficial outcomes

— The governing body directs that plans should be carried out according to the assigned IT responsibilities.
— Governing bodies monitor the performance of those given responsibility in the governance of IT (for example, those people serving on steering committees or presenting proposals to governing bodies).
— The governing body monitors the use of IT to ensure that it is achieving its intended benefits.
— The governing body evaluates the options for assigning responsibilities in respect of the organization's current and future use of IT.
— The governing body evaluates the competence of those given responsibility to make decisions regarding IT.
— The governing body directs that supply arrangements (including both internal and external supply arrangements) support the business needs of the organization.
	— Executive managers lead business process, organization structure and human change when implementing IT solutions.
	— Executive managers treat IT as an investment for return, not solely as a cost to be reduced.
	— Executive managers determine the best IT delivery model, considering:
	  — decision rights and control structures (central, de-central, federal, etc.);
	  — supply: optimizing the provision of IT (sourcing strategy);
	— Reporting of key performance indicators to the governing body, relating to responsibilities for the supply and use of IT.
		— The organization successfully implements IT enabled business change.
		— Organizational value is generated by IT.
		— The organization receives the quality of services it requires in the most effective and efficient manner possible.

Assessment	Unknown	Not	Somewhat	Largely	Fully
Are governance tasks and practices being applied?					

Assessment	Unknown	Not	Somewhat	Largely	Fully
Is there evidence of success?					

Assessment	Unknown	Not	Somewhat	Largely	Fully
Are beneficial outcomes being achieved?					