International Standard

ISO/IEC 38500

Third edition
2024-02

Information technology — Governance of IT for the organization

Technologies de l'information — Gouvernance des technologies de l'information pour l'entreprise

Reference number
ISO/IEC 38500:2024(en)

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

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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*.

This third edition cancels and replaces the second edition (ISO/IEC 38500:2015), which has been technically revised.

The main changes are as follows:

— the principles for governance of IT and alignment to the principles of governance in ISO 37000 have been elaborated;

— the model has been updated to include "engage stakeholders";

— a framework for the governance of IT has been updated from ISO/IEC TR 38502.

A list of all parts in the ISO/IEC 38500 series can be found on the ISO and IEC websites.

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

The use of information technology (IT) is critical to the success of most organizations, not only as a supporting function, but also as part of the organization's capability to transform the organization. IT enables new business models and can substantially improve the organization's outcomes to meet the organization's stakeholder needs and expectations. The growing threat of cybersecurity and risks emanating from emerging technologies increases this focus.

The increasing potential of current and future IT requires the appropriate application of governance of IT to ensure that it fulfils the purpose of the organization in an effective, responsible and ethical manner, and that it aligns with the organization's strategic direction.

The objective of this document is to provide guidance to governing bodies on the responsible, innovative, sustainable and strategic use of IT, data and digital capabilities, so their organizations can fulfil their purpose in a manner expected by their stakeholders. This document provides principle-based guidelines and therefore does not include specific implementation detail.

It utilizes three tools for the governing body and associated governance and management practices to achieve good governance of IT:

1) Principles for the governance of IT — applying these principles to the responsible and strategic use of IT can lead to an organization that is more agile and adaptive.

2) Model for the governance of IT — the model shows the main governance tasks and interactions throughout the organization, leading to a clarity of decision-making and responsibilities for all aspects of the use of IT.

3) Framework for the governance of IT — the framework describes the elements through which the organization's governance of IT arrangements operate, which helps to ensure the critical actions of governance are considered and applied to the use of IT by the organization.

As the governance of IT is a domain of the governance of organizations, this document aligns to ISO 37000 and its principles of governance. This document can also be used in conjunction with other governance codes and principles for effective governance. This document can be used independently or to upgrade current governance based on the previous edition of ISO/IEC 38500.

This document is addressed primarily to the governing body but recognizes that governance occurs throughout the organization. It therefore provides guidance on the practice of governance of IT across the organization including the interaction and collaboration of all personnel, regardless of their job description.

Information technology — Governance of IT for the organization

1 Scope

This document provides guiding principles for members of governing bodies of organizations and those that support them on the effective, efficient and acceptable use of information technology (IT) within their organizations.

This document is applicable to:

— the governance of the organization's current, and future, use of IT;

— the governance of IT as a domain of governance of organizations.

In terms of audience, this document is applicable to:

— all organizations, including public and private companies, government entities, and not-for-profit organizations;

— organizations of all sizes, from the smallest to the largest, 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 37000, *Governance of organizations — Guidance*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 37000 and the following 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
direct
communicate desired purposes and outcomes

Note 1 to entry: Within the context of the governance of IT, directing involves setting objectives, strategies and policies to be adopted by the members of the organization, to ensure that the use of IT meets business objectives.

Note 2 to entry: Objectives, strategies and policies can be set by management if they have the relevant authority delegated to them by the governing body.

3.2
evaluate
consider and make informed judgements

Note 1 to entry: Within the context of the governance of IT, evaluating involves making judgements about the circumstances and opportunities (internal and external, current and future) relating to the organization's current, and future use of IT.

3.3
governance
human-based system comprising directing, overseeing and accountability

3.4
governance of IT
system by which the current and future use of IT is governed

Note 1 to entry: Governance of IT is a component or a domain of governance of organizations.

Note 2 to entry: The term "governance of IT" is equivalent to the terms "corporate governance of IT", "enterprise governance of IT" and "organizational governance of IT".

3.5
information technology
IT
resources used to acquire, process, store and disseminate information or data

Note 1 to entry: Resources can include computer or communication equipment, sensors, software, cloud computing and other software-based services.

3.6
investment
allocation of resources to achieve defined objectives and other benefits

3.7
management
fulfilment of the organization’s objectives within the authority and accountability established by governance

Note 1 to entry: The term "management" is often used as a collective term for those with responsibility for controlling an organization or parts of an organization.

3.8
monitor
review as a basis for appropriate decisions and adjustments

Note 1 to entry: Monitoring involves routinely obtaining information about progress against plans as well as the periodic examination of overall achievements against agreed strategies and outcomes to provide a basis for decision-making and adjustments to plans.

Note 2 to entry: Monitoring includes reviewing compliance with relevant legislation, regulations and organizational policies.

3.9
use of IT
planning, design, development, deployment, operation, management and application of IT to fulfil business objectives and create value for the organization

Note 1 to entry: The use of IT includes both the demand for, and the supply of, IT.

3.10
digital capability
IT to enable or support a service, product or process of the organization

4 Good governance of IT

4.1 Outcomes of good governance of IT

4.1.1 Overview

This document provides guidance on the governance implications of the use of IT, data and digital capabilities by an organization. Throughout the concept, this term is simplified as the phrase “the governance of IT”. While the governing body retains ultimate accountability for the whole organization, the practice of governance of IT can occur throughout the organization.

The governance of IT in this context is applied broadly to the use of information technology including emerging technology, data and digital capabilities. Information technology includes computers, sensors, software, cloud computing services and techniques which are used to gather, store, process, disseminate and transform data. Digital capabilities, often innovative, enable or support the services, products or processes of the organization that can create value for stakeholders. Digital capabilities of the organization are supported, or enabled, by using information technology and data.

The governance of IT is a domain of the governance of organizations, so this document aligns to ISO 37000 and its principles for governance. This document provides guidance on how the governance outcomes are realized by the organization as a result of effective governance of IT.

ISO 37000 describes governance of organizations as laying the foundation for the fulfilment of the purpose of the organization in an effective, responsible and ethical manner in line with stakeholder expectations. It sets out eleven governance principles to guide governing bodies in discharging their duties such that the organizations realize the three intended governance outcomes, which are defined as:

— effective performance,

— responsible stewardship, and

— ethical behaviour.

IT and the data from which it creates and unlocks value, have become increasingly effective and strategically significant to most organizations. This makes the governance of IT increasingly important for the organization – and stakeholders have high expectations of the outcomes of effective governance of IT.

4.1.2 Effective performance

What constitutes effective performance of IT by the organization is determined by the governing body and its understanding of the organization’s context and stakeholder expectations. To achieve effective performance, clearly stated performance expectations are established as a basis for operational management, oversight of delivery and use of IT.

The effective performance of IT by the organization can also be measured by evaluating the following points:

— alignment of digital capabilities to support and enable the fulfilment of organizational purpose;

— appropriate investment in IT, including degree of digitalization and innovation required by the organization;

— appropriate value extraction from resources, including IT assets such as computers and software, but also the data and digital services used and the people creating, maintaining and using the digital capabilities;

— the linkage between data costs and how data use delivers better decision-making in the organization and its stakeholders;

— the degree to which digital capabilities are delivering agility and adaptability to the organization so it can sense, learn and adapt to address future opportunities, potential risks and new obligations.

4.1.3 Responsible stewardship

The resources under the stewardship of the organization include the digital capabilities of the organization as well as the data it has created and data from others (such as vendors, customers, employees and other stakeholders).

Expectations for responsible stewardship should be clearly stated and can include:

— consideration for ensuring that automated decisions are reasonable and justified (see ISO/IEC 38507);

— ensuring that data relating to stakeholder information is appropriately protected and used;

— ensuring the security and resilience of the digital capabilities and data;

— demonstrating appropriate risk governance, duty of care and good decision-making in the usage of digital capabilities;

— adapting to the changing stakeholder requirements of transparency, explainability and impact assessments.

4.1.4 Ethical behaviour

The organization relies on stakeholder engagement and international norms of behaviour to define its ethical practices and drive appropriate conduct. In the context of the use of IT, this means that such use is appropriately governed and expectations are clearly stated to ensure that use remains within these parameters (including human behaviour), and any impact from such use does not adversely affect relevant stakeholders or the economic or natural environment.

By adhering to the principles of the governance of IT and applying the model and framework to the organization's use of IT, the governing body ensures that ethical behaviour is supported and encouraged.

Expectations for ethical behaviour can include:

— consideration of IT asset ownership and data rights and obligations;

— consideration of access and rights of use;

— consideration of social and environmental issues;

— maintenance of confidentiality;

— integrity and transparency in fulfilling obligations and commitments;

— compliance to regulations.

4.2 Principles, model and framework

This document provides three tools for the governing body and associated governance and management practices to use to achieve effective governance of IT. Table 1 describes these tools, how they are used and the benefits of using them.

Table 1 — Governance of IT — Overview of tools

Tool	Explanation	Use	Benefit(s)
Principles for the governance of IT	Provides the fundamental truth and assumptions that serve as the foundation for beliefs, behaviours and reasoning.	Application of these principles in tasks, interactions and framework elements allows faster and more aligned decision-making, particularly in the absence of clearly-defined rules (e.g. new markets, business rules, technologies or innovations in any of these areas).	A more agile, adaptive, responsible and strategic use of IT to support and enable the objectives of the organization.
Model for the governance of IT	Shows the main tasks and interactions throughout the organization that are necessary for the implementation of the governance of IT.	The model is used to clearly delineate governance responsibilities and decisions from those of management, while understanding how these two practices interact within an overall framework for the governance of IT.	Clarity of decision-making and responsibilities for all aspects of the use of IT.
Framework for the governance of IT	Describes the elements through which the organization's governance of IT arrangements operate.	The governance practice collaborates throughout the organization to detail the six elements of the framework. The principles are applied throughout the collaboration and the model guides the responsibilities and decision-making throughout.	Helps to ensure the critical actions of governance are considered and applied to the use of IT by the organization.

5 Principles for the governance of IT

5.1 Overview

The benefit of a principle-based document is that such an International Standard can identify the outcomes of applying the principles without specifying explicit methodologies, structures, processes and techniques. As the foundational document for the governance of IT, it is essential that the document can be applied with no consideration to the specific implementation for an organization. The system of governance adopted by the organization should be outcome-driven to best fit the organization, including but not limited to, its compliance needs.

The principles for the governance of IT provide the fundamental truth and assumptions that serve as the foundation for beliefs, behaviours and reasoning (see Table 1). They provide a useful foundation for the governance of IT and will provide particular value when new or innovative use of IT is considered. The principles can be applied to individual situations and elements of IT, as well as across the whole ecosystem of an organization.

As the governance of IT is a domain of the governance of organization, the "principle" statements (Table 2, 5.2 to 5.12) are those of ISO 37000:2021, Clause 6. Table 2 details the category and grouping of the principles and is taken from ISO 37000:2021, Table 1.

The governance implications of the use of IT and consequent outcomes are detailed, highlighting both the specific and unique aspects of the principles for an organization with respect to IT.

Table 2 — Organizational governance principles overview

Category	Category description	Principle
Primary	The pursuit of purpose is at the centre of all organizations and is of primary importance for the governance of organizations. Therefore, this principle is the primary consideration for governance and the central point of all the other principles in this document. All other principles are to be read in the context of the application of this principle.	Purpose (5.2)
Foundational	The four foundational governance principles are the essence to ensuring that effective governance of an organization takes place. Core to the ability to effectively govern an organization is: — determining the organization's approach to value generation; — directing and engaging with strategy to generate that value; — overseeing that the organization performs and behaves according to the expectations set by the governing body; — demonstrating accountability for the organization's performance, behaviour, decisions and activities.	Value generation (5.3)
		Strategy (5.4)
		Oversight (5.5)
		Accountability (5.6)
Enabling	The six enabling principles address the governance responsibilities pertinent to today's organizations: to meet evolving stakeholder expectations and the changing natural environment, social and economic context.	Stakeholder engagement (5.7)
		Leadership (5.8)
		Data and decisions (5.9)
		Risk governance (5.10)
		Social responsibility (5.11)
		Viability and performance over time (5.12)

5.2 Purpose

5.2.1 Principle

"The governing body should ensure that the organization's reason for existence is clearly defined as an organizational purpose. This organizational purpose should define the organization's intentions towards the natural environment, society and the organization's stakeholder. The governing body should also ensure that the associated set of organizational values is clearly defined." [SOURCE: ISO 37000:2021, 6.1.1]

5.2.2 Governance implications for use of IT

When defining the purpose of the organization, the governing body should consider how the use of IT can enable or enhance the organizational purpose as well as the values of the organization. Consideration should be given to the implications of new and emerging technologies, communicated in a way that makes appropriate use of IT and is embedded through continued, demonstrated commitment.

As technology changes, the purpose of the organization should be reviewed to address the potential for a wider, more focussed or stronger purpose by leveraging these changes. Additionally, the use of new technology services should be reviewed to ensure such use remains aligned to the agreed organization's purpose.

5.2.3 Outcomes

The expected outcomes of the use of IT for the application of the principle are as follows.

— **Extended or improved purpose**: by leveraging the use of IT appropriately, the organization can enhance its value offerings.

— **Alignment of IT to purpose**: addressing the use of IT along with the organizational purpose and values helps to align the use of IT.

— **Empower personnel**: clarifying the alignment of the use of IT to the organizational purpose empowers personnel to make decisions and act in alignment with the purpose.

5.3 Value generation

5.3.1 Principle

"The governing body should define the organization's value generation objectives such that they fulfil the organizational purpose in accordance with the organizational values and the natural environment, social and economic context within which it operates." [SOURCE: ISO 37000:2021, 6.2.1]

5.3.2 Governance implications for use of IT

IT plays an important role in an organization's value generation as it can provide new or improved products or services in a timely, cost-effective and high-quality manner. It can also be used to differentiate the organization's value to its stakeholders including customers and suppliers. The use of IT can have significant impacts, both positive and negative, on the organization's value generation model and therefore, the role of IT in the definition and generation of organizational value should be determined and communicated. The concept of a value generation model is defined in ISO 37000:2021, 6.2.3.

Organizations are faced with an environment of continuous change, often driven by IT, data and digital capabilities. The governing body should consider the impact of technology change on its value generation model and ensure that implications are well understood and appropriate for the organization's purpose, values and ability or necessity to change or transform.

In determining the impacts of IT, data and digital capabilities on the value generation model, the competitive environment, emerging and future technology trends, alternative technology solutions and trends in stakeholder expectations should be considered.

Organizations should also ensure the opportunities and threats to the organization's value generation model from digital innovation or transformation are monitored. Opportunities for innovation should be identified and assessed.

Governance should ensure that the digital capabilities of the organization are appropriate for both current use and the desired future use, at a pace of change required by the organization. Investment in IT, data and digital capabilities is critical and significantly impacts the value generation model for an organization. Investment in both the organization's current environment and its future plans should be considered for impact on value for the organization.

5.3.3 Outcomes

The expected outcomes of the use of IT for the application of the principle are as follows.

— **Defined value generation objectives**: there are defined objectives as to how the organization proposes to use IT to support and enable its value generation model and to guide the organizational priorities and investment in IT.

— **Communicated value generation objectives**: the contribution and integration of the organization's digital capabilities as a critical enabler to the value generation model are understood and aligned to its strategy and communicated to its relevant stakeholders.

— **Adaptability**: there are mechanisms in place to regularly assess the potential impact of new technology solutions and to leverage these for the organization's value generation model and competitive solutions.

5.4 Strategy

5.4.1 Principle

"The governing body should direct and engage with the organizational strategy, in accordance with the value generation model, to fulfil the organizational purpose." [SOURCE: ISO 37000:2021, 6.3.1]

5.4.2 Governance implications for use of IT

The overall organizational strategy should consider the impact of IT on the organization's current and future needs and expectations. The potential value and role that emerging IT can provide to the organization in a timely manner as well as the pace and approach used to integrate new or emerging IT should form fundamental elements of the organizational strategy.

The IT strategy should align with, and be included in, the organizational strategy. It should identify where the strategic choices impact on the use of IT, the increasing demand for digital services and the impact of cyber security, resilience, total cost of ownership, flexibility and resources. Particular attention should be given to whether the organization can adapt its strategy to integrate new technology opportunities and to adapt to changing internal and external demand. The IT strategy for the supply and use of IT should be critically reviewed, considering the ecosystem within which the organization operates now and into the future.

Essential IT services, such as online identity management, data storage and communications should be examined to ensure a reasonable balance between costs, flexibility and organizational autonomy and independence.

5.4.3 Outcomes

The expected outcomes of the use of IT for the application of the principle are as follows.

— **Digital capability**: the organizational strategy provides current and effective guidance for the use and delivery of the organization's IT, data and digital capabilities.

— **Digital readiness**: the organization makes effective use of new digital capabilities as appropriate, planning for the appropriate resources, including personnel.

— **Digital innovation**: the strategy identifies the appropriate level of investment for digital innovation to enable the organization to accelerate its strategic objectives.

— **Digital currency**: the organization's IT is and remains current and in line with the organizational strategy. The organization has strategies for resolving IT degradation and obsolescence over time.

5.5 Oversight

5.5.1 Principle

"The governing body should oversee the organization's performance to ensure that it meets the governing body's intentions for, and expectations of, the organization, its ethical behaviour and its compliance obligations." [SOURCE: ISO 37000:2021, 6.4.1]

5.5.2 Governance implications for use of IT

Policies and practices provide the enumeration of intentions and direction within which an organization operates to achieve its objectives. Some are based on the requirements of mandatory legislation and regulations. Others are based on best practices and will guide the organization in terms of risk reduction or improvements in efficiency and effectiveness in the delivery and use of IT. It is noteworthy that with

the fast evolution of advances in digital technologies, legislation can be unclear, underdeveloped or even contradictory. In such a case, the governing body should address the compliance elements it requires of the organization.

The governing body should have the assurance that appropriate policies are in place, are being followed and that it is informed of any significant breaches or patterns of breach. Open communication and the ability to demonstrate or verify conformance with an applicable set of regulatory or voluntary framework requirements assists the organization in being considered trustworthy. The governing body should define their expectations and the mechanisms through which the overall performance is assessed and through which significant modifications for improvement are made, focussed on organizational value generation.

Awareness of the governing body's responsibilities and expectations are key so that all members are effective in their role and duties.

The governing body should have oversight of management's progress in implementing the IT strategy and any risks to the organization that might arise. This requires that the governing body be informed about progress in implementing the organization's IT strategy, as well as the impact of changes to the organization's external and internal environments, to identify areas in which the strategy needs to be adjusted.

The organization's digital capabilities are often composed of IT delivered by third parties through contractual arrangements, such as service agreements or business process outsourcing. These policies should cover the governing body's intentions and expectations of ethical use of IT, as well as its compliance obligations. Oversight of the overall sourcing strategy and these arrangements and responsibilities can be a key governance issue for the organization. See the ISO/IEC 20000 series and the ISO/IEC 30105 series respectively for related management guidance.

The governing body should have oversight of the end-to-end life cycle of technology provision from embracing new technologies to the retirement of outdated technology and data. Consideration should be given to the resilience of digital capabilities and the effective and optimized use of technical and data capital within the organization.

5.5.3 Outcomes

The expected outcomes of the use of IT for the application of the principle are as follows.

— **Compliance:** IT-related obligations both, internal and external (regulatory, legislation, common law, contractual,) have been identified with planned actions.

— **Informed:** the governing body should be informed in a timely manner of any material breaches, particularly in regulatory or contractual compliance, and any risks to the organization that relate to IT.

— **Effective performance:** processes are in place to ensure transparency and that the flow of information and associated performance measurements aids governance and decision-making.

5.6 Accountability

5.6.1 Principle

"The governing body should demonstrate its accountability to the organization as a whole and hold to account those to whom it has delegated." [SOURCE: ISO 37000:2021, 6.5.1]

5.6.2 Governance implications for use of IT

The governing body should ensure that respective responsibilities and accountabilities for delivery and use of IT are clear. There should also be a clear strategy to ensure those who use IT, those who are responsible for the products and services IT enables and those who have the appropriate IT knowledge are engaged in IT-related decision-making applicable to their responsibilities, with appropriate support mechanisms. This maximizes the benefits while minimizing the associated risk of delivery.

The governing body should have assurance that where necessary, the formulation and translation of its intentions are supported by personnel with the appropriate competence across the organization. Accountability for the governance of IT remains with the governing body regardless of implementation strategies and delegation of responsibilities.

5.6.3 Outcomes

The expected outcomes of the use of IT for the application of the principle are as follows.

— **Governing body accountability**: accountability for the governance of IT remains with the governing body regardless of delegation.

— **Integrated decision-making:** the design of the decision-making structures and oversight arrangements include those in the organization responsible for delivering as well as those using the IT services, with authority delegated to those best placed to exercise it.

— **Assurance:** there is assurance that the framework for the governance of IT is effective and there is the appropriate oversight control of the use of IT.

5.7 Stakeholder engagement

5.7.1 Principle

"The governing body should ensure that the organization's stakeholders are appropriately engaged and their expectations considered." [SOURCE: ISO 37000:2021, 6.6.1]

5.7.2 Governance implications for use of IT

The organization's use of IT should be aligned to the organization's stakeholder requirements. Stakeholder satisfaction in digital capabilities is a critical factor in achieving the benefits from investment in IT. Customer retention and personnel engagement are essential factors for the successful use of the IT. The organization's approach to design, implementation and operation of IT and associated support arrangements should address stakeholder expectations to increase satisfaction and trust.

Stakeholder engagement involves not just the interface of one system but the whole of organization approach though which stakeholders, including customers, suppliers, regulators and personnel, interact with the organization through IT. Increasingly, there is a need for a clear strategic approach to design, implementation and operation of systems and support arrangements to meet or exceed stakeholder expectations and achieve increased stakeholder and end-user satisfaction and loyalty. It is critical that IT investment is aligned with stakeholder requirements and organizational goals.

The governing body should identify the stakeholders including those using the IT of the organization, and consider the entire stakeholder journey in order to monitor overall satisfaction of the use of IT. There should be an effective stakeholder engagement strategy in place.

The governing body should also ensure that the organization's culture enables the successful achievement of strategic objectives, particularly when introducing change. Culture influences the way individuals and groups within the organization interact with IT. Culture can thus impact the ability of the organization to use IT to achieve its objectives. The effectiveness of an individual's participation in all aspects of IT are influenced by the organization's culture.

5.7.3 Outcomes

The expected outcomes of the use of IT for the application of the principle are as follows.

— **Stakeholder-centric approach**: there is a planned approach to stakeholder engagement so that those affected by decisions can influence the outcome. The organization's policies, models and frameworks support a stakeholder-centric approach.

— **Supportive culture:** organization leadership, policies and practices positively influence human and organization behaviour in the delivery and use of IT.

5.8 Leadership

5.8.1 Principle

"The governing body should lead the organization ethically and effectively and ensure such leadership throughout the organization." [SOURCE: ISO 37000:2021, 6.7.1]

5.8.2 Governance implications for use of IT

The governing body should ensure ethical leadership across the organization's use of IT in a manner consistent with its organizational values.

IT-enabled organizational change should be supported through a clear vision of the desired outcomes, together with the capacity to deliver the change required to achieve planned outcomes. The level to which the organization adopts business transformation, through and supported by digital transformation, should be defined and enacted throughout the leadership of the organization. The governing body should establish the organization's purpose, value generation model and organizational values to achieve IT objectives to ensure stakeholder satisfaction.

The digital landscape to address the organization's purpose should be clearly identified and communicated throughout the organization.

The delivery of value from IT-enabled change is often complex. The governing body should have the assurance that the organization has the organizational and IT knowledge and skills needed to implement change in a timely fashion. The governing body should consider its own competencies in respect to IT and the impact of the use of IT on all stakeholders. It should continuously improve and align their IT knowledge in line with the societal and organizational requirements. It should ensure that oversight is performed appropriately and there is ongoing evaluation to ensure accountability and oversight of strategic decision-making and use of IT.

5.8.3 Outcomes

The expected outcomes of the use of IT for the application of the principle are as follows.

— **Transformational capability**: the organization has organizational and IT change capability appropriate to the level of organizational change, complexity and rate of change.

— **Technology adaptability:** a disciplined, flexible approach to acquiring or changing IT services supports IT-enabled organizational change.

— **Learning culture**: the organization has a learning culture with integrated IT competency and skills strategy for future needs to achieve the organization's goals.

5.9 Data and decisions

5.9.1 Principle

"The governing body should recognize data as a valuable resource for decision-making by the governing body, the organization and others." [SOURCE: ISO 37000:2021, 6.8.1]

5.9.2 Governance implications for use of IT

Gathering data and processing it into information to be used for decision-making is one of the primary objectives of IT and is increasingly an essential enabler of organizational value. Through access to data from various sources and using tools such as Artificial Intelligence (AI), organizations can make better and faster

strategic and operational decisions to drive value through improved services, more immediate responses or reduced costs.

As data are used to make decisions, by machines and people, they are valuable not only for the organization itself but also as a resource that can be bought, sold or otherwise distributed. For example, data are a resource used in products and their design, market and customer insights, and supply chain and product usage information.

The role of data in the value generation model should be clear and aligned to the organization's strategy. It should ensure that the organization can effectively acquire, use and protect data. The governing body should ensure there is clear data strategy that addresses the following:

a) the strategic objectives for the use of data;

b) data governance and data protection responsibilities;

c) strategies for data assets, including classification, sharing and use;

d) ensuring the obligations and restrictions placed on data use by others;

e) ensuring the data rights concerning use are respected when those data are disseminated to others;

f) that data are used in line with the organizational purpose and values.

5.9.3 Outcomes

The expected outcomes of the use of IT for the application of the principle are as follows.

— **Strategic use of data:** the role of the use of data is clearly defined in the organization's strategy. Data are used in every aspect of the organization, including its products, services and value generation. It is therefore important to understand how it adds value, risk and obligations to the organization's goals.

— **Responsible use of data:** the organization can demonstrate its responsible use of data. This includes ensuring that the data are appropriate for their use (including respect for obligations such as privacy and copyright), that they are of requisite quality (including an absence of unwanted bias) and that they are protected from theft, corruption and malicious use.

— **Requisite data quality:** the quality requirements are understood and mechanisms are in place to ensure the data meets these requirements.

5.10 Risk governance

5.10.1 Principle

"The governing body should ensure that it considers the effect of uncertainty on the organizational purpose and associated strategic outcomes." [SOURCE: ISO 37000:2021, 6.9.1]

5.10.2 Governance implications for use of IT

The governance of risk is critical to the effective governance and management of the delivery and use of IT. An understanding of the IT-related risks, threats and opportunities for the organization should guide the focus of governance of IT and should provide a basis for the governance framework for IT. Cybersecurity risks, the level of uncertainty of emerging technologies and the risks and consequences of adverse impact to accidental or intentional unethical use of IT would be areas of attention for risk governance of IT.

The governing body should ensure that it is kept aware of the strategic or critical risks associated with IT and that a sound process for management of IT-related risks is in place. Having a risk-based approach provides flexibility and agility for adopting and adapting to changing conditions. Furthermore, it provides a mechanism for prioritization of resource allocation.

5.10.3 Outcomes

The expected outcomes of the use of IT for the application of the principle are as follows.

— **Appropriate risk oversight:** critical or strategic risk associated with the use of IT is recognized and acted upon promptly.

— **Acceptable risk appetite:** the level of risk that the organization is prepared to accept with regard to the use of IT in pursuit of its objectives is defined and managed.

— **Digital resilience:** the organization is able to respond and recover from internal IT failures or adverse external events in line with stakeholder expectations.

5.11 Social responsibility

5.11.1 Principle

"The governing body should ensure that decisions are transparent and aligned with broader societal expectations." [SOURCE: ISO 37000:2021, 6.10.1]

5.11.2 Governance implications for use of IT

The governing body should ensure that their societal responsibilities are addressed in all IT decisions, providing transparency and addressing impacts to all stakeholders. With the growth of increasingly automated decision-making, the governing body should ensure that the impact of these automated decisions are as intended and any unintended consequences are addressed swiftly while maintaining appropriate human oversight.

The governing body should ensure that the organization's responsibility and possible legal duty of care, to its stakeholders, including customers, is maintained.

The organization should be sensitive to, and anticipate, community expectations of the use of IT, including the need for transparency of decision-making, the impact of increasing automation and equitable access to essential online services.

The environmental impact of the use of IT should also be considered, both at an organizational level and also across organizations.

5.11.3 Outcomes

The expected outcomes of the use of IT for the application of the principle are as follows.

— **Appropriate social responsibility:** alignment with overall organization principles of decision-making and policies for IT. The organization takes responsibility for the use and consequences of the IT utilized by the organization.

— **Impact assessed and addressed:** clear recognition and understanding of the potential impact of the use of IT on stakeholders is considered and planned prior to implementation.

— **Ethical checks and balances:** ethical checks and balances are considered in decisions to ensure acceptable use of IT, data and algorithms.

5.12 Viability and performance over time

5.12.1 Principle

"The governing body should ensure that the organization remains viable, and performs over time, without compromising the ability of the current and future generations to meet their needs." [SOURCE: ISO 37000:2021, 6.11.1]

5.12.2 Governance implications for use of IT

Effective digital capabilities now and into the future are vital to the viability of an organization. A clear direction and path to the future should be identified while maintaining a reliable and sustainable current environment. The direction should include resilience for the future of the organization from a technology perspective. The governing body should understand and respond, through good governance of IT, to the needs of the ecosystem in which the organization operates to remain viable and perform over the longer term.

In a rapidly changing environment, organizations need to have a clear understanding of technology options. The governing body should understand the reliance of critical functions on IT and have the assurance that the provision of the IT services is well managed and resilient. They should be informed of any potential IT-related issues that can impact the organization's performance.

IT should be suitable for the task for which it is designed in supporting the organizational purpose and objectives, providing services, levels of service and service quality required to meet current and future organizational requirements.

The governing body should minimize any negative impact of the organization's use of IT on the natural, social and economic systems within which the organization operates.

5.12.3 Outcomes

The expected outcomes of the use of IT for the application of the principle are as follows:

— **IT ecosystem remains valid for the needs of the organization**: the provision of IT is managed to ensure that business requirements are identified, agreed upon and provided in line with organizational priorities.

— **Infrastructure management:** the essential operational components, such as policies, processes, equipment, data, human resources and external contacts are managed for overall effectiveness.

— **Protection:** the organization's policies and practices ensure that the operations and information are protected in an increasingly complex and vulnerable environment.

6 Model for the governance of IT

6.1 Introduction

Governance involves setting and being accountable for the purpose and parameters for the organization. While the governing body retains ultimate accountability for the whole organization (and this document focuses on the accountability for the current and future use of IT by the organization), the practice of governance occurs throughout the organization.

Management is about fulfilling the associated objectives by making choices within the parameters set by the governing body.

The distinction between the roles will vary between organizations, but it is important to differentiate between the various responsibilities, decisions and actions required by each role. Even if a person is tasked with both governance and management roles, this separation and clarity of roles assists with effective governance outcomes.

The whole organization operates within a governance framework, and this document focuses on the framework for the governance of IT – that is, the strategies, policies, decision-making structures and accountabilities through which the organization's use of IT operates today and plans for its future.

Responsibility for specific aspects of IT may be delegated to management within the organization. However, accountability for the effective, efficient and acceptable use of IT by an organization remains with the governing body and cannot be delegated.

Figure 1 shows the model for the governance of IT. This model consists of:

1) **governance of IT practice**, comprising the four main tasks of "engage stakeholders", "evaluate", "direct" and "monitor" (as depicted by the triangle);

2) **management of IT practice** (as depicted by the rectangle); and

3) **framework for the governance of IT** (as depicted by the circle), within which the whole organization operates.

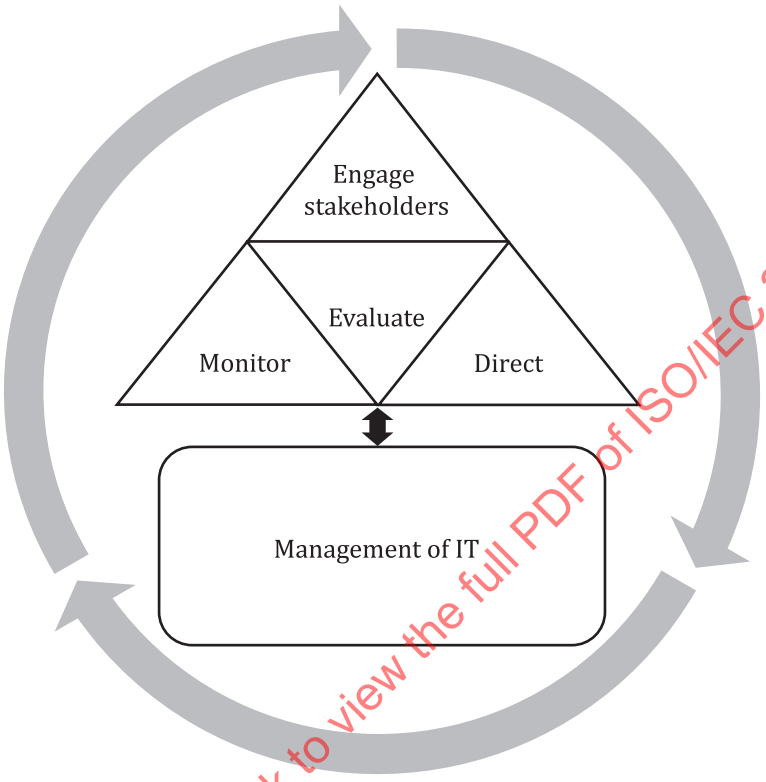

Figure 1 — Model for the governance of IT

6.2 Governance of IT practice

6.2.1 Engage stakeholders

The relevant stakeholders of the use of IT by the organization should be identified, consulted and appropriately engaged. Such stakeholders are likely to be internal to the organization (e.g. users of IT, employees and developers) as well as external (e.g. customers, suppliers, governments).

Understanding the expectations of relevant stakeholders helps the organization to set appropriate policy and behaviour so that the desired governance outcomes are understood and its accountability obligations can be set. In particular, the organization should ensure that there is a clear statement of commitments regarding the use of IT and data and that any breaches in these commitments are communicated promptly to allow the organization and its stakeholders to deal with the consequences.

Engaging with the relevant stakeholders also allows the potential capabilities of the use of IT to be discussed, and the understanding of that potential can change the expectation of stakeholders.

6.2.2 Evaluate

Governing bodies should examine and make judgement on the current and future use of IT, including plans, proposals and supply arrangements (whether internal, external or both).

In evaluating the use of IT, governing bodies should consider the external or internal pressures acting upon the organization, such as technological change, economic and social trends, regulatory obligations, legitimate stakeholder expectations and political influences. Governing bodies should undertake evaluation continually as circumstances change. Governing bodies should also take account of both current and future business needs, i.e. the current and future organizational objectives that they intend to achieve, such as maintaining competitive advantage, as well as the specific objectives of the plans and proposals they are evaluating.

6.2.3 Direct

Governing bodies should assign responsibility for, and direct preparation and implementation of strategies and policies. Strategies should set the direction for investments in IT and what IT should achieve. Policies should establish acceptable behaviour in the use of IT.

Governing bodies should encourage a culture of effective governance of IT in their organization by requiring management to provide timely information, to comply with direction and to conform to the eleven principles of effective governance.

If necessary, governing bodies should direct the submission of proposals for approval to address identified needs.

6.2.4 Monitor

Governing bodies should monitor, through appropriate measurement systems, the performance of IT. They should assure themselves that performance is in accordance with strategies, particularly with regard to business objectives.

Governing bodies should also ensure that IT complies with external obligations (regulatory, legislation, contractual) and internal work practices.

6.3 Management of IT practice

Given the direction and parameters in which the organization will operate, the management practice uses a management system of interrelated or interacting elements to establish management policies, objectives and processes to achieve those objectives. Additionally, there is a commitment of continual improvement to the management system.

6.4 Framework for the governance of IT

Governance and management should not operate separately or independently. The collaboration between the two practices is essential for effective governance outcomes, including the pursuit of the organization's purpose, achieving its goals, and delivering the performance and behaviour expected by its stakeholders.

The framework for the governance of IT (see Clause 7) describes this collaboration as well as other mechanisms for establishing policy, ensuring good decision-making across the organization and ensuring that the governing body can remain accountable for the use of IT by the organization.

7 Framework for the governance of IT

7.1 General

Figure 2 shows the framework for the governance of IT, which includes six elements through which the organization's governance of IT arrangements operate. This includes establishing and maintaining the policies, decision-making structures, behaviours and accountability mechanisms that are required to ensure the operational model is delivering value, the risks are managed and other expectations of stakeholders can be met. The six elements are further described in 7.2.2 to 7.2.7.