FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
38500**

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

Secretariat: **SA**

Voting begins on:
2023-06-28

Voting terminates on:
2023-08-23

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 FDIS 38500:2023(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 v
Introduction vi
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Good governance of IT 2
4.1 Outcomes of good governance of IT 2
4.1.1 Overview 2
4.1.2 Effective performance 3
4.1.3 Responsible stewardship 3
4.1.4 Ethical behaviour 4
4.2 Principles, model and framework 4
5 Principles for the governance of IT 5
5.1 Overview 5
5.2 Purpose 6
5.2.1 Principle 6
5.2.2 Governance implications for use of IT 6
5.2.3 Outcomes 6
5.3 Value generation 7
5.3.1 Principle 7
5.3.2 Governance implications for use of IT 7
5.3.3 Outcomes 7
5.4 Strategy 7
5.4.1 Principle 7
5.4.2 Governance implications for use of IT 8
5.4.3 Outcomes 8
5.5 Oversight 8
5.5.1 Principle 8
5.5.2 Governance implications for use of IT 8
5.5.3 Outcomes 9
5.6 Accountability 9
5.6.1 Principle 9
5.6.2 Governance implications for use of IT 9
5.6.3 Outcomes 10
5.7 Stakeholder engagement 10
5.7.1 Principle 10
5.7.2 Governance implications for use of IT 10
5.7.3 Outcomes 10
5.8 Leadership 11
5.8.1 Principle 11
5.8.2 Governance implications for use of IT 11
5.8.3 Outcomes 11
5.9 Data and decisions 11
5.9.1 Principle 11
5.9.2 Governance implications for use of IT 11
5.9.3 Outcomes 12
5.10 Risk governance 12
5.10.1 Principle 12
5.10.2 Governance implications for use of IT 12
5.10.3 Outcomes 13
5.11 Social responsibility 13
5.11.1 Principle 13

5.11.2 Governance implications for use of IT 13
5.11.3 Outcomes 13
5.12 Viability and performance over time 13
5.12.1 Principle 13
5.12.2 Governance implications for use of IT 14
5.12.3 Outcomes 14

6 Model for the governance of IT 14
6.1 Introduction 14
6.2 Governance of IT practice 15
6.2.1 Engage stakeholders 15
6.2.2 Evaluate 15
6.2.3 Direct 16
6.2.4 Monitor 16
6.3 Management of IT practice 16
6.4 Framework for the governance of IT 16

7 Framework for the governance of IT 16
7.1 General 16
7.2 Elements of the framework 17
7.2.1 General 17
7.2.2 Direction 18
7.2.3 Capability 18
7.2.4 Policy 18
7.2.5 Delegation 19
7.2.6 Performance 19
7.2.7 Accountability 20

Bibliography 21

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 version of ISO/IEC 38500:2015.

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 applies to the governance of the organization's current, and future, use of IT.

This document applies to the governance of IT as a domain of governance of organizations.

This document is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. This document is applicable to 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 for enabling or supporting 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. For 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 clearly stated to ensure that it 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.