INTERNATIONAL STANDARD

ISO/IEC 38507

First edition
2022-04

Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations

Technologies de l'Information — Gouvernance des technologies de l'information — Implications de gouvernance de l'utilisation par des organisations de l'intelligence artificielle

Reference number
ISO/IEC 38507:2022(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

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).

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 jointly by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittees SC40, *IT service management and IT governance* and SC 42, *Artificial intelligence*.

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 objective of this document is to provide guidance for the governing body of an organization that is using, or is considering the use of, artificial intelligence (AI).

This document provides guidance on the role of a governing body with regard to the use of AI within their organization and encourages organizations to use appropriate standards to underpin their governance of the use of AI.

This document addresses the nature and mechanisms of AI to the extent necessary to understand the governance implications of their use: what are the additional opportunities, risks and responsibilities that the use of AI brings? The emphasis is on governance (which is done by humans) of the organization's use of AI and not on the technologies making up any AI system. However, such governance requires an understanding of the implications of the technologies.

Artificial intelligence (AI)

AI embraces a family of technologies that bring together computing power, scalability, networking, connected devices and interfaces, together with vast amounts of data. Reference to 'AI' in this document is intended to be understood to refer to a whole family of technologies and methods, and not to any specific technology, method or application. For AI concepts and terminology, see ISO/IEC 22989:—[1].

Use of AI

"Use of AI" is defined in this document in the broadest sense as developing or applying an AI system through any part of its life cycle to fulfil objectives and create value for the organization. This includes relationships with any party providing or using such systems.

Governance implications of the use of AI

The scope of this document is concerned with the implications for an organization of the use of AI. As with any powerful tool, the use of AI brings new risks and responsibilities that should be addressed by organizations that use it. AI is not inherently 'good' or 'evil', 'fair' or 'biased', 'ethical' or 'unethical' although its use can be or can seem to be so.

The organization's purpose, ethics and other guidelines are reflected, either formally or informally, in its policies. This document examines both governance and organizational policies and their application and provides guidance to adapt these for the use of AI. The operational aspects of the policies are implemented through management. This document refers to other standards for details on related topics including social responsibility, trustworthiness (such as risk management, management of bias, and quality) and compliance management.

[1] Under preparation. Stage at the time of publication: ISO/IEC FDIS 22989:2022.

Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations

1 Scope

This document provides guidance for members of the governing body of an organization to enable and govern the use of Artificial Intelligence (AI), in order to ensure its effective, efficient and acceptable use within the organization.

This document also provides guidance to a wider community, including:

- executive managers;
- external businesses or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies;
- public authorities and policymakers;
- internal and external service providers (including consultants);
- assessors and auditors.

This document is applicable to the governance of current and future uses of AI as well as the implications of such use for the organization itself.

This document is applicable to any organization, including public and private companies, government entities and not-for-profit organizations. This document is applicable to an organization of any size irrespective of their dependence on data or information technologies.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitute 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 22989:—[2], *Information technology — Artificial intelligence —Artificial intelligence concepts and terminology*

ISO/IEC 38500:2015, *Information technology — Governance of IT for the organization*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22989, ISO/IEC 38500 and the following apply.

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

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

[2] Under preparation. Stage at the time of publication: ISO/IEC FDIS 22989:2022.

3.1 Terms related to AI

3.1.1
use of AI
developing or applying an AI system through any part of its life cycle to fulfil an organization's objectives

Note 1 to entry: This term is scoped to any action or activity related to AI that can have governance implications.

3.2 Terms related to governance

3.2.1
oversight
monitoring of the implementation of organizational and governance policies and management of associated tasks, services and products set by the organization, in order to adapt to changes in internal or external circumstances

Note 1 to entry: Effective oversight needs general understanding of a situation. Oversight is one of the 'principles of governance' covered in depth in ISO 37000:2021, 6.4.

3.2.2
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

[SOURCE: ISO 31000:2018, 3.1]

3.2.3
risk appetite
amount and type of *risk* (3.2.2) that an organization is willing to pursue or retain

[SOURCE: ISO Guide 73:2009, 3.7.1.2]

3.2.4
compliance obligations
requirements that an organization mandatorily has to comply with as well as those that an organization voluntarily chooses to comply with

[SOURCE: ISO 37301:2021, 3.25]

3.2.5
compliance
meeting all the organization's *compliance obligations* (3.2.4)

[SOURCE: ISO 37301:2021, 3.26]

4 Governance implications of the organizational use of AI

4.1 General

The governance of organizations is enabled by the application of principles that help the organization fulfil its organizational purpose and, in doing so, generate value for the organization and its stakeholders. According to ISO 31000:2018, 5.3 governance guides the course of the organization, its external and internal relationships, and the rules, processes and practices needed to achieve its purpose. Management structures translate governance direction into the strategy and associated objectives required to achieve desired levels of sustainable performance and long-term viability.

An overview of the concepts of governance and organizational decision-making (and in particular, references to existing standards) that shall be followed, is given in Annex A.

The governing body's responsibility to set goals in traditional contexts extends to both financial objectives and non-financial outcomes including culture, values and ethical outcomes. Organizational and governance policies are generally created and enforced through a combination of controls, business plans, strategies, position descriptions, professional discipline accepted practice, regulation, training, key performance indicators and a variety of executive communications.

The governing body remains accountable for all activities of an organization. This accountability cannot be delegated.

The governing body of an organization has an ongoing responsibility to consider the implications on the organization of any new tool, technique or technology being introduced.

The members of the governing body should assure themselves and be able to demonstrate to stakeholders that their policies (together with the implementation of those policies) are sufficient for the organization, its products and interactions, and the human resources, processes and technology the organization uses. In this respect, the responsibility for and resulting from the introduction of AI is not new. However, AI has the potential to enable new organizational objectives, and to fulfil or extend existing ones, and do so more effectively and more efficiently.

4.2 Maintaining governance when introducing AI

The governing body sets the purpose of the organization and approves the strategies necessary to achieve that purpose. However, it is possible that existing governance is no longer fit-for-purpose when AI is being used within that organization. The specific choice of tools, e.g. AI systems, should be a management decision, made in light of and in line with guidance from the governing body. In order to establish such guidance, the governing body should inform itself about AI in general terms because its use can bring:

— significant benefit to the organization strategically;

— significant risk to the organization, with the potential for harm to its stakeholders;

— additional obligations to the organization.

The governing body should assess its intended use of AI as part of its risk appetite. Risk can change rapidly. New insights and a proactive approach provide an organization with the means to respond to risk. The organization should therefore demonstrate willingness to modify or abort projects, if deemed necessary. For further guidance see ISO/IEC 38506.

New implications arise from the use of AI, including but not limited to:

— increased reliance on technology and systems for the acquisition of data and assurance of its quality;

— transparency and explainability of AI systems (including insight into the objectives, assumptions and rules included in them) when partly or fully automated systems are used for addressing tasks and problems that were previously performed by humans (e.g. credit scoring) together with adequate processes to modify and update those algorithms;

— the possibility that existing direction and controls are not appropriate to ensure required outcomes (and mitigate the risk of undesirable consequences) or can even be compromised. This is due to the differences in assumptions that can be made when delegating to a human, as opposed to when making use of, or acquiring support from, AI.

EXAMPLE 1 An instruction to "defer credit repayment until after the holidays" is sufficiently clear in context to another human operator but insufficiently precise for an AI system to execute correctly.

- competitive pressure due to the sales and operations of an organization not using AI;
- accepting the use of AI systems without awareness or consideration of potential bias, error or harm, or of the implications of embedding AI within existing complex systems;
- the growing disparity between the speed of change in automated learning systems and the corresponding human controls of compliance;
- the impact of AI on the workforce, including concerns about discrimination, harm to the fundamental rights of workers, redundancy due to automation or de- and re-skilling, and the possible loss of organizational knowledge, but also leveraging AI to increase human creativity, increased quality of work by delegating repetitive, trivial or dangerous tasks to an AI system;
- the impact on commercial operations and to brand reputation.

The use of AI can also reduce or eliminate certain existing risks and the governing body should review and adjust its risk assessment accordingly.

EXAMPLE 2 An AI system can reduce the risk of error when deployed to complement humans engaged in repetitive tasks, or where humans are required to continuously monitor systems looking for rare anomalies (e.g. security guards).

4.3 Maintaining accountability when introducing AI

Members of the governing body are responsible for oversight and outcomes of the organization as well as for the systems and practices that enable such assurances to be made. They are accountable for the decisions made throughout the organization, including those that are made through the use of AI and for the adequacy of governance and controls where AI is being deployed. They are thus accountable for the use of AI considered acceptable by the organization.

The governing body should take responsibility for the use of AI, rather than attributing responsibility to the AI system itself. Members of the governing body are responsible for informing themselves about the possibilities and risks raised by using AI systems. Members of the governing body should be conscious of the risk of anthropomorphising AI, a phenomenon by which human characteristics (e.g. thinking, emoting, judging, moralizing) are unduly attributed to AI systems, out of proportion, or in a manner inappropriate, to that which is necessary in order to understand the role played by the use of AI.

Members of the governing body can be held to account for the mis-actions of the organization in cases where inadequate diligence, care, guidance, training, oversight and enforcement within the organization allow issues to arise. Such accountability can be ensured by the governing body itself or imposed by stakeholders or through other means. Members of the governing body can face a penalty, removal from office, or legal redress.

The governing body therefore should ensure that its practices are fit-for-purpose for the specific uses to which AI is being applied within the organization. This can include review and, where necessary, enhancement of:

- **Direction**: through policy, strategy, allocation of resources, codes of ethics, statements of values, purpose or other instruments relating to the use of AI in the organization;
- **Oversight**: through an evaluation of AI, an assessment of its value to the organization and the organization’s risk appetite, and assurance of implementation, monitoring, measurement, decision assurance and other mechanisms relating to the use of AI in the organization;
- **Evaluation**: considering different elements, e.g. the internal and external factors relating to the organization, current and future threats and opportunities, outcomes achieved, effectiveness and efficiency of the governance mechanisms in place, and judgements about decisions and options taken.

- **Reporting**: to demonstrate to stakeholders that the use of AI is being effectively governed by those accountable (compare this with the tasks of ‘evaluate’, ‘direct’ and ‘monitor’ in ISO/IEC 38500:2015, 4.2).

The governing body should also ensure that it has sufficient capabilities to deal with the implications of the use of AI. Actions to address this can include:

- improving AI-related skills among its members;
- increasing the frequency of review of the organization’s use of IT and AI in particular;
- examining and updating the criteria used to monitor both the internal and external environment;
- ensuring that staff interests and concerns (e.g. workplace safety, staff training, quality of work) are represented;
- strengthening oversight by establishing or enhancing subcommittees dealing with strategy, risk, assessment or audit, and ethics.

The governing body’s accountability should be established across all aspects of intended or actual use of AI and in a manner that is sufficient to ensure the intended outcomes, notably:

- when considering the potential impacts of the use of AI;
- when crafting business strategies that incorporate the use of AI;
- at purchase, implementation, configuration, deployment, testing and other project phases throughout an AI system’s life cycle;
- changes in the environments to which the AI is exposed, the learning and actions, decisions and outputs of the AI system, as well as its impacts on stakeholders;
- that appropriate security controls are in place to protect the organization, its stakeholders and its data;
- at decommissioning, including the knowledge and data that are contained in the AI system.

Alongside issues associated with AI itself, there are other issues associated with newly introduced technologies that can affect the organization and its stakeholders, including:

- misunderstanding the nature of the technologies;
- making inappropriate governance decisions;
- omitting appropriate governance oversight of AI;
- failing to include AI in the scope of existing governance;
- applying the technologies inappropriately or ubiquitously without context-specific awareness, appropriate planning, policy or training;
- failing to protect and secure information and assets against automated attacks that use AI to identify vulnerabilities;
- failing to address the implications of emerging relationships between humans and AI systems.

5 Overview of AI and AI systems

5.1 General

AI systems come in a range of forms and warrant different degrees of oversight by the governing body. As such, the governing body should understand what the “use of AI” entails and at what stage in its use the governing body should be involved either directly or through appropriate governance mechanisms.

AI systems build on existing IT capabilities including networking, Internet of things devices, e.g. sensors and actuators, big data and cloud computing.

Most of the recent advances in the field of AI technologies relate to the domain of machine learning (ML). ML is an AI technique that gives computers the ability to “learn” without being explicitly programmed. Data are key: they can represent, e.g. text, numbers, pictures, symbols, formulae, graphs, images, speech, sound or videos. A model of an existing data set is created and applied to new data to solve a particular problem, predict an outcome or to categorize new input data.

The nature of AI systems based on ML, including the objective of their use, the choice of algorithms, data driven approach, training methodologies and probability-based outputs, is such that there is potential for additional risk to, and opportunities for, the organization (see also 6.7).

AI systems can automate decision-making by analysing data to provide a potentially probabilistic outcome and, in many cases, acting on that outcome. AI systems can change the nature of products, processes and relationships as well as how an organization operates. This can have material impacts across most industries.

As with any powerful tool that offers benefits, the potential for harm also exists. Therefore, the use of AI should be included in the organization’s risk assessment.

The use of AI can result in new obligations for the organization. These can be legal requirements or as a consequence of the adoption of voluntary codes of practice, whether directly within an AI system’s automation of decision-making processes or indirectly through its use of data or other resources or processes. The potential for an AI system to cross the boundary between presenting options for action and executing the action itself, without a human involved, should be a major consideration for the governing body.

AI can be distinguished from other technologies by the sheer volume and complexity of data gathered from various sources that can be too complex for humans to handle or adequately process, and specifically, from the perspective of governance implications, by:

- the capability for decision automation;
- the use of data analysis, insights and learning rather than explicit human coded logic to solve problems;
- the capability to adapt as the AI system’s environment changes, in ways that are not explicitly coded and necessarily known in advance.

These three elements have wide ranging implications for the organization and its governance.

5.2 How AI systems differ from other information technologies

5.2.1 Decision automation

AI systems generally create output based on historical and current data chosen for the tasks for which the AI system is designed. In modern AI systems, in particular those based on ML, the resultant prediction is usually represented as a probability. For example:

- there is a 97 % probability that this part does not meet the quality requirements;