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/IEC 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2022 – All rights reserved

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**
3.1 Terms related to AI ... 2
3.2 Terms related to governance ... 2

4 Governance implications of the organizational use of AI ... **2**
4.1 General ... 2
4.2 Maintaining governance when introducing AI ... 3
4.3 Maintaining accountability when introducing AI ... 4

5 Overview of AI and AI systems ... **6**
5.1 General ... 6
5.2 How AI systems differ from other information technologies ... 6
5.2.1 Decision automation ... 6
5.2.2 Data-driven problem-solving ... 7
5.2.3 Adaptive systems ... 7
5.3 AI ecosystem ... 8
5.4 Benefits of the use of AI ... 9
5.5 Constraints on the use of AI ... 10

6 Policies to address use of AI ... **11**
6.1 General ... 11
6.2 Governance oversight of AI ... 12
6.3 Governance of decision-making ... 13
6.4 Governance of data use ... 14
6.5 Culture and values ... 15
6.6 Compliance ... 16
6.6.1 Compliance obligations ... 16
6.6.2 Compliance management ... 17
6.7 Risk ... 17
6.7.1 Risk appetite and management ... 17
6.7.2 Risk management ... 18
6.7.3 Objectives ... 19
6.7.4 Sources of risk ... 20
6.7.5 Controls ... 21

Annex A (normative) **Governance and organizational decision-making** ... **23**

Bibliography ... **27**

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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

© ISO/IEC 2022 – All rights reserved