BS ISO/IEC 42001:2023

BSI Standards Publication

Information technology — Artificial intelligence — Management system

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 42001:2023

National foreword

This British Standard is the UK implementation of ISO/IEC 42001:2023.

The UK participation in its preparation was entrusted to Technical Committee ART/1, Artificial Intelligence.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 15269 2

ICS 03.100.70; 35.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2023.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 42001:2023

INTERNATIONAL STANDARD

ISO/IEC 42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management

Reference number
ISO/IEC 42001:2023(E)

Documents
Document Sharing Hub
© ISO/IEC 2023

Full document details: BS ISO/IEC 42001:2023

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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 2023 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 42001:2023

Contents

Page

Foreword ... **v**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Context of the organization ... **5**
4.1 Understanding the organization and its context ... 5
4.2 Understanding the needs and expectations of interested parties ... 6
4.3 Determining the scope of the AI management system ... 6
4.4 AI management system ... 6
5 Leadership ... **7**
5.1 Leadership and commitment ... 7
5.2 AI policy ... 7
5.3 Roles, responsibilities and authorities ... 8
6 Planning ... **8**
6.1 Actions to address risks and opportunities ... 8
6.1.1 General ... 8
6.1.2 AI risk assessment ... 9
6.1.3 AI risk treatment ... 9
6.1.4 AI system impact assessment ... 10
6.2 AI objectives and planning to achieve them ... 10
6.3 Planning of changes ... 11
7 Support ... **11**
7.1 Resources ... 11
7.2 Competence ... 11
7.3 Awareness ... 12
7.4 Communication ... 12
7.5 Documented information ... 12
7.5.1 General ... 12
7.5.2 Creating and updating documented information ... 12
7.5.3 Control of documented information ... 13
8 Operation ... **13**
8.1 Operational planning and control ... 13
8.2 AI risk assessment ... 13
8.3 AI risk treatment ... 14
8.4 AI system impact assessment ... 14
9 Performance evaluation ... **14**
9.1 Monitoring, measurement, analysis and evaluation ... 14
9.2 Internal audit ... 14
9.2.1 General ... 14
9.2.2 Internal audit programme ... 14
9.3 Management review ... 15
9.3.1 General ... 15
9.3.2 Management review inputs ... 15
9.3.3 Management review results ... 15
10 Improvement ... **15**
10.1 Continual improvement ... 15
10.2 Nonconformity and corrective action ... 16
Annex A (normative) **Reference control objectives and controls** ... **17**

Documents
Document Sharing Hub

© ISO/IEC 2023 – All rights reserved

Full document details: BS ISO/IEC 42001:2023

Annex B (normative) **Implementation guidance for AI controls** **21**
Annex C (informative) **Potential AI-related organizational objectives and risk sources** **46**
Annex D (informative) **Use of the AI management system across domains or sectors** **49**
Bibliography **51**

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

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 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 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

Introduction

Artificial intelligence (AI) is increasingly applied across all sectors utilizing information technology and is expected to be one of the main economic drivers. A consequence of this trend is that certain applications can give rise to societal challenges over the coming years.

This document intends to help organizations responsibly perform their role with respect to AI systems (e.g. to use, develop, monitor or provide products or services that utilize AI). AI potentially raises specific considerations such as:

— The use of AI for automatic decision-making, sometimes in a non-transparent and non-explainable way, can require specific management beyond the management of classical IT systems.

— The use of data analysis, insight and machine learning, rather than human-coded logic to design systems, both increases the application opportunities for AI systems and changes the way that such systems are developed, justified and deployed.

— AI systems that perform continuous learning change their behaviour during use. They require special consideration to ensure their responsible use continues with changing behaviour.

This document provides requirements for establishing, implementing, maintaining and continually improving an AI management system within the context of an organization. Organizations are expected to focus their application of requirements on features that are unique to AI. Certain features of AI, such as the ability to continuously learn and improve or a lack of transparency or explainability, can warrant different safeguards if they raise additional concerns compared to how the task would traditionally be performed. The adoption of an AI management system to extend the existing management structures is a strategic decision for an organization.

The organization's needs and objectives, processes, size and structure as well as the expectations of various interested parties influence the establishment and implementation of the AI management system. Another set of factors that influence the establishment and implementation of the AI management system are the many use cases for AI and the need to strike the appropriate balance between governance mechanisms and innovation. Organizations can elect to apply these requirements using a risk-based approach to ensure that the appropriate level of control is applied for the particular AI use cases, services or products within the organization's scope. All these influencing factors are expected to change and be reviewed from time to time.

The AI management system should be integrated with the organization's processes and overall management structure. Specific issues related to AI should be considered in the design of processes, information systems and controls. Crucial examples of such management processes are:

— determination of organizational objectives, involvement of interested parties and organizational policy;

— management of risks and opportunities;

— processes for the management of concerns related to the trustworthiness of AI systems such as security, safety, fairness, transparency, data quality and quality of AI systems throughout their life cycle;

— processes for the management of suppliers, partners and third parties that provide or develop AI systems for the organization.

This document provides guidelines for the deployment of applicable controls to support such processes.

This document avoids specific guidance on management processes. The organization can combine generally accepted frameworks, other International Standards and its own experience to implement crucial processes such as risk management, life cycle management and data quality management which are appropriate for the specific AI use cases, products or services within the scope.

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

An organization conforming with the requirements in this document can generate evidence of its responsibility and accountability regarding its role with respect to AI systems.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are implemented. The list items are enumerated for reference purposes only.

Compatibility with other management system standards

This document applies the harmonized structure (identical clause numbers, clause titles, text and common terms and core definitions) developed to enhance alignment among management system standards (MSS). The AI management system provides requirements specific to managing the issues and risks arising from using AI in an organization. This common approach facilitates implementation and consistency with other management system standards, e.g. related to quality, safety, security and privacy.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

Documents
Document Sharing Hub

Information technology — Artificial intelligence — Management system

1 Scope

This document specifies the requirements and provides guidance for establishing, implementing, maintaining and continually improving an AI (artificial intelligence) management system within the context of an organization.

This document is intended for use by an organization providing or using products or services that utilize AI systems. This document is intended to help the organization develop, provide or use AI systems responsibly in pursuing its objectives and meet applicable requirements, obligations related to interested parties and expectations from them.

This document is applicable to any organization, regardless of size, type and nature, that provides or uses products or services that utilize AI systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 22989:2022, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22989 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
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.6)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: If the organization is part of a larger entity, the term "organization" refers only to the part of the larger entity that is within the scope of the AI *management system* (3.4).

3.2
interested party
person or *organization* (3.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity

Note 1 to entry: An overview of interested parties in AI is provided in ISO/IEC 22989:2022, 5.19.

© ISO/IEC 2023 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

3.3
top management
person or group of people who directs and controls an *organization* (3.1) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.4) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

3.4
management system
set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.5) and *objectives* (3.6), as well as *processes* (3.8) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The management system elements include the organization's structure, roles and responsibilities, planning and operation.

3.5
policy
intentions and direction of an *organization* (3.1) as formally expressed by its *top management* (3.3)

3.6
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as finance, health and safety, and environment). They can be, for example, organization-wide or specific to a project, product or *process* (3.8).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, as a purpose, as an operational criterion, as an AI objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of AI *management systems* (3.4), AI objectives are set by the *organization* (3.1), consistent with the AI *policy* (3.5), to achieve specific results.

3.7
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential events (as defined in ISO Guide 73) and consequences (as defined in ISO Guide 73), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (as defined in ISO Guide 73) of occurrence.

3.8
process
set of interrelated or interacting activities that uses or transforms inputs to deliver a result

Note 1 to entry: Whether the result of a process is called an output, a product or a service depends on the context of the reference.

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

3.9
competence
ability to apply knowledge and skills to achieve intended results

3.10
documented information
information required to be controlled and maintained by an *organization* (3.1) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.4), including related *processes* (3.8);

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

3.11
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to managing activities, *processes* (3.8), products, services, systems or *organizations* (3.1).

Note 3 to entry: In the context of this document, performance refers both to results achieved by using AI systems and results related to the AI *management system* (3.4). The correct interpretation of the term is clear from the context of its use.

3.12
continual improvement
recurring activity to enhance *performance* (3.11)

3.13
effectiveness
extent to which planned activities are realized and planned results are achieved

3.14
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.1) and *interested parties* (3.2) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.10).

3.15
conformity
fulfilment of a *requirement* (3.14)

3.16
nonconformity
non-fulfilment of a *requirement* (3.14)

3.17
corrective action
action to eliminate the cause(s) of a *nonconformity* (3.16) and to prevent recurrence

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

3.18
audit
systematic and independent *process* (3.8) for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the *organization* (3.1) itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.19
measurement
process (3.8) to determine a value

3.20
monitoring
determining the status of a system, a *process* (3.8) or an activity

Note 1 to entry: To determine the status, there can be a need to check, supervise or critically observe.

3.21
control
<risk> measure that maintains and/or modifies *risk* (3.7)

Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO 31000:2018, 3.8, modified — Added <risk> as application domain]

3.22
governing body
person or group of people who are accountable for the performance and conformance of the organization

Note 1 to entry: Not all organizations, particularly small organizations, will have a governing body separate from top management.

Note 2 to entry: A governing body can include, but is not limited to, board of directors, committees of the board, supervisory board, trustees or overseers.

[SOURCE: ISO/IEC 38500:2015, 2.9, modified — Added Notes to entry.]

3.23
information security
preservation of confidentiality, integrity and availability of information

Note 1 to entry: Other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

[SOURCE: ISO/IEC 27000:2018, 3.28]

3.24
AI system impact assessment
formal, documented process by which the impacts on individuals, groups of individuals, or both, and societies are identified, evaluated and addressed by an organization developing, providing or using products or services utilizing artificial intelligence

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

3.25
data quality
characteristic of data that the data meet the organization's data requirements for a specific context

[SOURCE: ISO/IEC 5259-1:—[1)], 3.4]

3.26
statement of applicability
documentation of all necessary *controls* (3.23) and justification for inclusion or exclusion of controls

Note 1 to entry: Organizations may not require all controls listed in Annex A or may even exceed the list in Annex A with additional controls established by the organization itself.

Note 2 to entry: All identified risks shall be documented by the organization according to the requirements of this document. All identified risks and the risk management measures (controls) established to address them shall be reflected in the statement of applicability.

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its AI management system.

The organization shall determine whether climate change is a relevant issue.

The organization shall consider the intended purpose of the AI systems that are developed, provided or used by the organization. The organization shall determine its roles with respect to these AI systems.

NOTE 1 To understand the organization and its context, it can be helpful for the organization to determine its role relative to the AI system. These roles can include, but are not limited to, one or more of the following:

— AI providers, including AI platform providers, AI product or service providers;

— AI producers, including AI developers, AI designers, AI operators, AI testers and evaluators, AI deployers, AI human factor professionals, domain experts, AI impact assessors, procurers, AI governance and oversight professionals;

— AI customers, including AI users;

— AI partners, including AI system integrators and data providers;

— AI subjects, including data subjects and other subjects;

— relevant authorities, including policymakers and regulators.

A detailed description of these roles is provided by ISO/IEC 22989. Furthermore, the types of roles and their relationship to the AI system life cycle are also described in the NIST AI risk management framework.[29] The organization's roles can determine the applicability and extent of applicability of the requirements and controls in this document.

NOTE 2 External and internal issues to be addressed under this clause can vary according to the organization's roles and jurisdiction and their impact on its ability to achieve the intended outcome(s) of its AI management system. These can include, but are not limited to:

a) external context related considerations such as:

   1) applicable legal requirements, including prohibited uses of AI;

   2) policies, guidelines and decisions from regulators that have an impact on the interpretation or enforcement of legal requirements in the development and use of AI systems;

1) Under preparation. Stage at the time of publication ISO/IEC DIS 5259-1:2023.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

3) incentives or consequences associated with the intended purpose and the use of AI systems;

4) culture, traditions, values, norms and ethics with respect to development and use of AI;

5) competitive landscape and trends for new products and services using AI systems;

b) internal context related considerations such as:

1) organizational context, governance, objectives (see 6.2), policies and procedures;

2) contractual obligations;

3) intended purpose of the AI system to be developed or used.

NOTE 3 Role determination can be formed by obligations related to categories of data the organization processes (e.g. personally identifiable information (PII) processor or PII controller when processing PII). See ISO/IEC 29100 for PII and related roles. Roles can also be informed by legal requirements specific to AI systems.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

— the interested parties that are relevant to the AI management system;

— the relevant requirements of these interested parties;

— which of these requirements will be addressed through the AI management system.

NOTE Relevant interested parties can have requirements related to climate change.

4.3 Determining the scope of the AI management system

The organization shall determine the boundaries and applicability of the AI management system to establish its scope.

When determining this scope, the organization shall consider:

— the external and internal issues referred to in 4.1;

— the requirements referred to in 4.2.

The scope shall be available as documented information.

The scope of the AI management system shall determine the organization's activities with respect to this document's requirements on the AI management system, leadership, planning, support, operation, performance, evaluation, improvement, controls and objectives.

4.4 AI management system

The organization shall establish, implement, maintain, continually improve and document an AI management system, including the processes needed and their interactions, in accordance with the requirements of this document.

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the AI management system by:

— ensuring that the AI policy (see 5.2) and AI objectives (see 6.2) are established and are compatible with the strategic direction of the organization;

— ensuring the integration of the AI management system requirements into the organization's business processes;

— ensuring that the resources needed for the AI management system are available;

— communicating the importance of effective AI management and of conforming to the AI management system requirements;

— ensuring that the AI management system achieves its intended result(s);

— directing and supporting persons to contribute to the effectiveness of the AI management system;

— promoting continual improvement;

— supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE 1 Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

NOTE 2 Establishing, encouraging and modelling a culture within the organization, to take a responsible approach to using, development and governing AI systems can be an important demonstration of commitment and leadership by top management. Ensuring awareness of and compliance with such a responsible approach and in support of the AI management system through leadership can aid the success of the AI management system.

5.2 AI policy

Top management shall establish an AI policy that:

a) is appropriate to the purpose of the organization;

b) provides a framework for setting AI objectives (see 6.2);

c) includes a commitment to meet applicable requirements;

d) includes a commitment to continual improvement of the AI management system.

The AI policy shall:

— be available as documented information;

— refer as relevant to other organizational policies;

— be communicated within the organization;

— be available to interested parties, as appropriate.

Control objectives and controls for establishing an AI policy are provided in A.2 in Table A.1. Implementation guidance for these controls is provided in B.2.

NOTE Considerations for organizations when developing AI policies are provided in ISO/IEC 38507.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

5.3 Roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the AI management system conforms to the requirements of this document;

b) reporting on the performance of the AI management system to top management.

NOTE A control for defining and allocating roles and responsibilities is provided in A.3.2 in Table A.1. Implementation guidance for this control is provided in B.3.2.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the AI management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

— give assurance that the AI management system can achieve its intended result(s);

— prevent or reduce undesired effects;

— achieve continual improvement.

The organization shall establish and maintain AI risk criteria that support:

— distinguishing acceptable from non-acceptable risks;

— performing AI risk assessments;

— conducting AI risk treatment;

— assessing AI risk impacts.

NOTE 1 Considerations to determine the amount and type of risk that an organization is willing to pursue or retain are provided in ISO/IEC 38507 and ISO/IEC 23894.

The organization shall determine the risks and opportunities according to:

— the domain and application context of an AI system;

— the intended use;

— the external and internal context described in 4.1.

NOTE 2 More than one AI system can be considered in the scope of the AI management system. In this case the determination of opportunities and uses is performed for each AI system or groupings of AI systems.

The organization shall plan:

a) actions to address these risks and opportunities;

b) how to:

1) integrate and implement the actions into its AI management system processes;

2) evaluate the effectiveness of these actions.

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

The organization shall retain documented information on actions taken to identify and address AI risks and AI opportunities.

NOTE 3 Guidance on how to implement risk management for organizations developing, providing or using AI products, systems and services is provided in ISO/IEC 23894.

NOTE 4 The context of the organization and its activities can have an impact on the organization's risk management activities.

NOTE 5 The way of defining risk and therefore of envisioning risk management can vary across sectors and industries. The definition of risk in 3.7 allows a broad vision of risk adaptable to any sector, such as the sectors mentioned in Annex D. In any case, it is the role of the organization, as part of risk assessment, to first adopt a vision of risk adapted to its context. This can include approaching risk through definitions used in sectors where the AI system is developed for and used, such as the definition from ISO/IEC Guide 51.

6.1.2 AI risk assessment

The organization shall define and establish an AI risk assessment process that:

a) is informed by and aligned with the AI policy (see 5.2) and AI objectives (see 6.2);

NOTE When assessing the consequences as part of 6.1.2 d) 1), the organization can utilize an AI system impact assessment as indicated in 6.1.4.

b) is designed such that repeated AI risk assessments can produce consistent, valid and comparable results;

c) identifies risks that aid or prevent achieving its AI objectives;

d) analyses the AI risks to:

1) assess the potential consequences to the organization, individuals and societies that would result if the identified risks were to materialize;

2) assess, where applicable, the realistic likelihood of the identified risks;

3) determine the levels of risk;

e) evaluates the AI risks to:

1) compare the results of the risk analysis with the risk criteria (see 6.1.1);

2) prioritize the assessed risks for risk treatment.

The organization shall retain documented information about the AI risk assessment process.

6.1.3 AI risk treatment

Taking the risk assessment results into account, the organization shall define an AI risk treatment process to:

a) select appropriate AI risk treatment options;

b) determine all controls that are necessary to implement the AI risk treatment options chosen and compare the controls with those in Annex A to verify that no necessary controls have been omitted;

NOTE 1 Annex A provides reference controls for meeting organizational objectives and addressing risks related to the design and use of AI systems.

c) consider the controls from Annex A that are relevant for the implementation of the AI risk treatment options;

d) identify if additional controls are necessary beyond those in Annex A in order to implement all risk treatment options;

© ISO/IEC 2023 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023

e) consider the guidance in Annex B for the implementation of controls determined in b) and c);

NOTE 2 Control objectives are implicitly included in the controls chosen. The organization can select an appropriate set of control objectives and controls from Annex A. The Annex A controls are not exhaustive and additional control objectives and controls can be needed. If different or additional controls are necessary beyond those in Annex A, the organization can design such controls or take them from existing sources. AI risk management can be integrated in other management systems, if applicable.

f) produce a statement of applicability that contains the necessary controls [see b), c) and d)] and provide justification for inclusion and exclusion of controls. Justification for exclusion can include where the controls are not deemed necessary by the risk assessment and where they are not required by (or are subject to exceptions under) applicable external requirements.

NOTE 3 The organization can provide documented justifications for excluding any control objectives in general or for specific AI systems, whether those listed in Annex A or established by the organization itself.

g) formulate an AI risk treatment plan.

The organization shall obtain approval from the designated management for the AI risk treatment plan and for acceptance of the residual AI risks. The necessary controls shall be:

— aligned to the objectives in 6.2;

— available as documented information;

— communicated within the organization;

— available to interested parties, as appropriate.

The organization shall retain documented information about the AI risk treatment process.

6.1.4 AI system impact assessment

The organization shall define a process for assessing the potential consequences for individuals or groups of individuals, or both, and societies that can result from the development, provision or use of AI systems.

The AI system impact assessment shall determine the potential consequences an AI system's deployment, intended use and foreseeable misuse has on individuals or groups of individuals, or both, and societies.

The AI system impact assessment shall take into account the specific technical and societal context where the AI system is deployed and applicable jurisdictions.

The result of the AI system impact assessment shall be documented. Where appropriate, the result of the system impact assessment can be made available to relevant interested parties as defined by the organization.

The organization shall consider the results of the AI system impact assessment in the risk assessment (see 6.1.2). A.5 in Table A.1 provides controls for assessing impacts of AI systems.

NOTE In some contexts (such as safety or privacy critical AI systems), the organization can require that discipline-specific AI system impact assessments (e.g. safety, privacy or security impact) be performed as part of the overall risk management activities of an organization.

6.2 AI objectives and planning to achieve them

The organization shall establish AI objectives at relevant functions and levels.

The AI objectives shall:

a) be consistent with the AI policy (see 5.2);

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 42001:2023