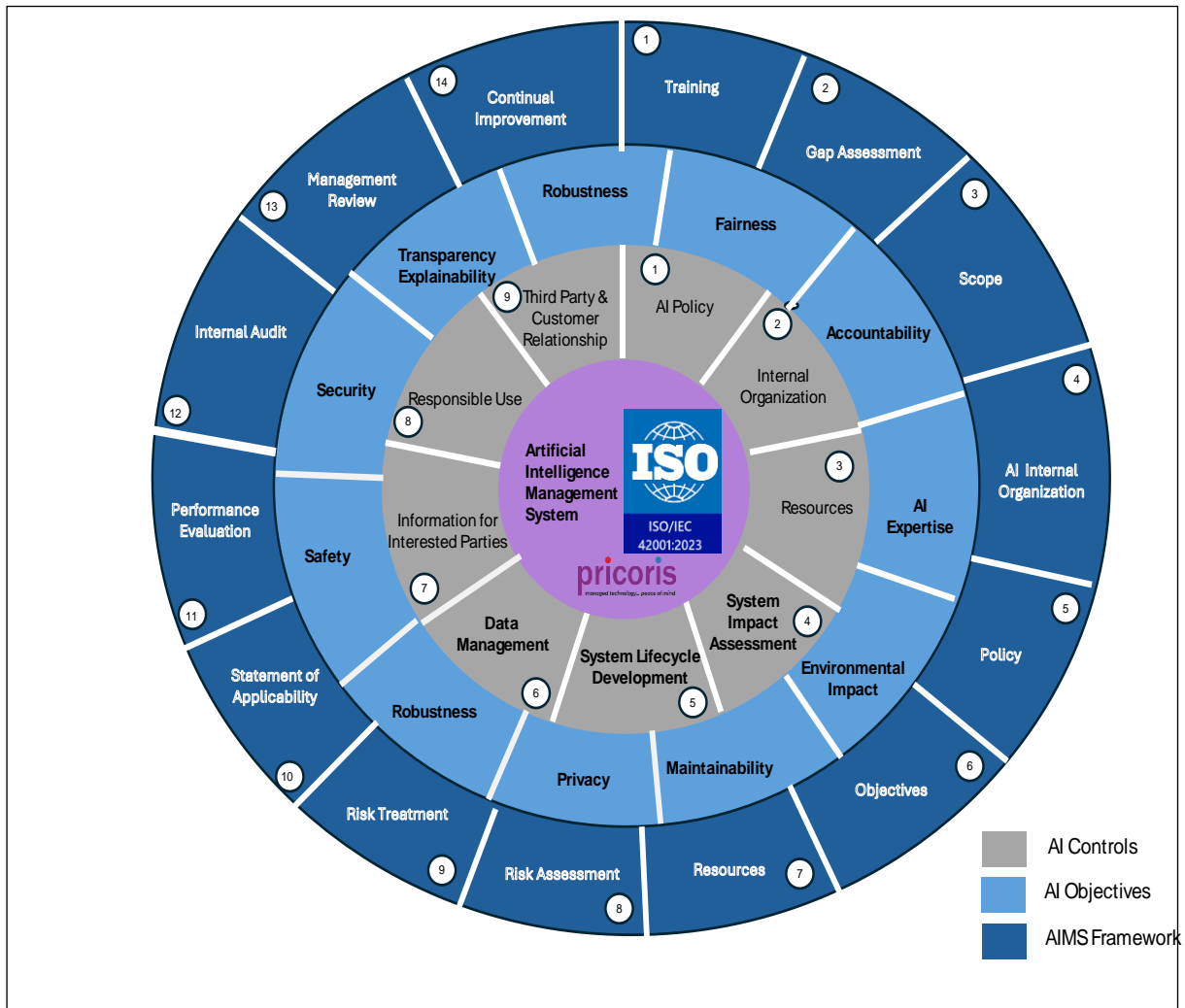


Artificial Intelligence Management System – ISO/IEC 42001:2023



Diagrammatic Representation of AIMS ISO/IEC 42001:2023

Artificial Intelligence Management System – ISO/IEC 42001:2023

Part 1 of 3 of Artificial Intelligence Management System

1. Are you assured that your AI algorithms are making the most effective decisions?
2. Do you have mechanisms in place to manage your AI's influence on society?
3. Are you comfortable with the potential risks involved in utilizing third-party AI systems
4. Is your organization prepared to adapt to evolving AI regulations and standards?
5. Can you effectively monitor and control the ethical implications of your AI systems?

If answer to any one of these questions is no, please consider ISO 42001 – Artificial Intelligence Management System.

- ISO 42001 is a best practise framework which sets the baseline for organizations which use, develop, monitor or provide products or services that utilize AI). – Introduction to ISO 42001:2023).
- **This is Part 1 of the 3 series of articles on AIMS.**

Introduction and Overview

- ISO/IEC 42001 which was released on 18th December 2023 is an international standard on Artificial Intelligence- Management System.
- As stated in the introduction to the standard its purpose is 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).
- It applies to organizations providing or using products or services that utilize AI systems.
- Considerations which are unique to AI which called for a separate management system for AI are as follows:
 - Use of AI for Automatic Decision-making systems (ADMS) with consequential concerns on transparency and explainability
 - Use of data analysis which depends on machine learning changes the complexity of the AI system lifecycle and considerations of data management including data bias.
 - Ensuring responsible use with continuous learning resulting in change in behaviour.
- It is a Requirements and Guidelines standard. The requirements are 'shall' statements contained in the main body of the standard. This comprises clause 1 to 10 and the 38 controls of Annexure A which are spread across 9 domains.

Artificial Intelligence Management System – ISO/IEC 42001:2023

- Annexure B are the Implementation Guidance for AI controls. These are 'should', 'could' or 'may' statements and are an extension to Annexure A.
- Annexure C which is informative in nature, provides 11 potential AI related organizational objectives and also mentions risk sources for AI systems and specific reference to ISMS (ISO 27001), PIMS (ISO27701) and QMS (ISO9001). Since the standard follows Annex SL it is easy to integrate this with other management systems.
- Annexure D is also informative and specifies some of the industry sectors where AI is used and also mentions integration with other management systems.

2. Normative References

- This standard refers to ISO 22989:2022 (AI – concepts and terminology) as a referenced document.

3. Terms & Definitions

- ISO 22989 define AI systems as engineered systems that generate outputs such as content, forecasts, recommendations or decisions for a given set of human defined objectives.
- ISO 42001 also defines various terms including AI system impact assessment, data quality.

4. Context of the Organization

- The organization has to determine the context of the organization and consider whether climate change is a relevant issue.
- It has to consider the purpose for which AI is developed and used within the organization.
- It has to determine its role in relation to AI system – AI provider, producer, customers (users), partners, AI subjects, relevant authorities.
- The organization shall determine **external and internal factors** that are relevant to the AI context and that affect its ability to achieve the intended outcome(s) of its AIMS. These can include:
 - applicable legal requirements including prohibited use of AI.
 - applicable regulations.
 - incentives or consequences associated with the intended purpose
 - competitive landscape and trends for new products and services using AI systems.
 - organizational context, governance, policies and procedures.
 - applicable contractual obligations.
 - intended purpose of the AI systems to be developed or used.
- The interested parties for AI have to be identified and their needs and expectations from AIMS arrived at. Interested Parties can include
 - AI provider,

Artificial Intelligence Management System – ISO/IEC 42001:2023

- producer,
 - customers (users),
 - partners,
 - AI subjects,
 - relevant authorities.
- Scope of AIMS has to be determined and documented.

5. Leadership

- Demonstration and commitment for AI Policy, Objectives, integration of AIIMS within organization, resource provision for AIMS, communication of importance of AIMS, intended result(s) achievement of AIMS including setting direction and control for effectiveness of AIMS and promoting continual improvement of AIMS and supporting relevant roles by the leadership has to be demonstrated.
- Developing a culture of responsible AI systems within the organization is a demonstration of commitment.
- Control objectives and controls for establishing the AI Policy have been defined in Annexure A
- Artificial Intelligence Management Systems roles along with responsibilities and authorities are to be defined by the leadership.

6. Planning

- For planning of AIMS, risks and opportunities have to be considered in relation to the context determined earlier.
- Since AI can be used in different sectors, risks may be defined as per the sectoral definition of risks.
- Risk criteria for acceptable and unacceptable risks, when to perform AI risk assessment, criteria for determination of risk treatment and assessing likelihood and impact of risks are to be determined in the methodology.
- Since the usage of AI systems can be many, the Risk assessments may be grouped or separate depending on the opportunities and usage.
- Controls determined as a result of Risk Assessment shall be compared with controls in Annexure A of ISO 42001 (guidance contained in Annexure B. Additional controls may also be implemented.
- The statement of Applicability will include Controls from Annexure A of ISO 27001, ISO 27701 – annexure A (where organization is controller) and from ISO 27701 Annexure B (where organization is processor).
- Organizations may include controls beyond the ones specified in these standards.
- Justification for the inclusion and exclusions (not within the acceptable risk criteria, not required by legislation or regulation or not applicable is also to be documented.
- AI system Impact Assessment (AISIA) to be conducted, documented and shared with interested parties (where required) to assess the potential

Artificial Intelligence Management System – ISO/IEC 42001:2023

consequence for the deployment, use and foreseeable misuse on individuals, or groups of individuals, or both, and societies.

- The results of the AISIA to be incorporated in the risk assessment.
- Technical context, societal context and legal context are to be considered.
- AI objectives are to be determined for relevant functions and levels. Objectives plan is to be made.
- List of AI Objectives are provided in Annexure C of the standard. Control objectives for responsible development and use of AI systems is also required.
- All changes to AI systems are to be planned.

7. Support

- Organizations, now, have to identify and provide resources for AIMS. Control objective A.4 also refers to resources.
- Competence (education, experience and training) of people, with roles, responsibilities and accountabilities, who will impact AI performance have to be defined.
- Awareness of AI Policy, contribution to effectiveness of AIMS and implication of non-conformance to AIMS requirements must be spread in the organization (employees and contractors) and beyond - relevant interested parties
- Communication Procedures (both internal and external) must be determined. Information for interested parties including communication of incidents is also a control objective A.8.
- Documented Information for AIMS is to be maintained with special consideration on changes, retention and disposition including documents of external origin.

8. Operation

- Implementation of controls for Risk Treatment for AIMS, and monitoring the effectiveness of these controls to be ensured. Controls on outsourced processes to be ensured. Risk assessments shall be performed as per the defined process and risk treatment implemented. Besides, AI System Impact Assessments shall be performed at planned intervals or when significant changes happen.

9. Performance Evaluation

- Performance Evaluation of AIMS Performance and its effectiveness including criteria for measuring controls implemented under Annexure A, including the monitoring plan, must be defined and evidence of the monitoring has to be documented.
- Internal audits to include AIMS and included in the audit program and criteria for selection of AIMS auditors to be defined.
- Management Review to include AIMS in the agenda and minutes of meetings to contain decisions made on AIMS.

Artificial Intelligence Management System – ISO/IEC 42001:2023

10. Improvements

- Non-Conformities arising in the AI Management System must be actioned upon and evaluate the need for corrective action and implementation of the same to be ensured and tracked. Continual Improvement of AIMS to ensure its suitability, adequacy and effectiveness to be ensured.

Part 2 from this series will consider the second layer- the AI objectives from the standard.

If you are interested in learning more, please join our course on AIMS – which is a 5-day course.

We offer both online and offline classes.

Please contact Akanksha Chordia for details.

Email: akanksha.chordia@pricoris.in or info@pricoris.com call at +91 8058877450.