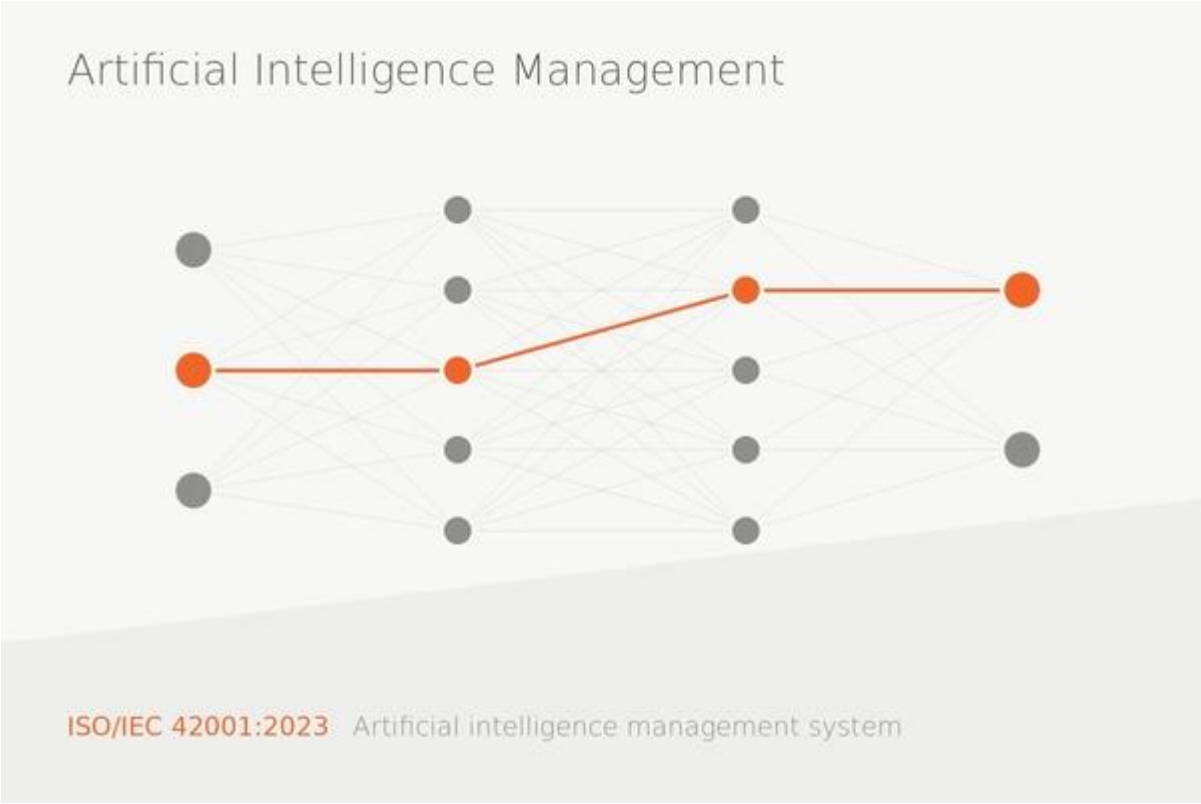
ISO 42001 Overview and Guidance

This guidance document provides an overview of the **ISO 42001:2023 Artificial Intelligence Management System** standard.



Introduction

The ISO 42001:2023 Artificial intelligence (AI) management system standard details the requirements for an AI management system (AIMS) - the arrangements an organisation puts in place to make sure the artificial intelligence it develops, provides or uses is managed responsibly.

It is the first certifiable management system standard for artificial intelligence, and it follows the same Annex SL high-level structure as ISO 9001, ISO 14001 and ISO 45001, so it can be integrated into an existing management system rather than run as a separate system.

The standard applies to any organisation that develops, provides or uses products or services that use AI systems, whatever its size or sector. It sits alongside the organisation's other obligations - data protection, equality, product safety, sector regulation and contractual commitments - and does not replace any of them.

The requirement that sets ISO 42001 apart from the other management standards is that the organisation must consider the effect of its AI systems on individuals, groups of individuals and societies, not only the risk to the organisation itself. This is done through an AI system impact assessment.

The Organisation's Role in Relation to AI

Before anything else the organisation needs to be clear about the role or roles it holds, because the requirements that apply follow from it. The standard recognises the organisation may be:

- an AI developer - designing, building or training AI systems
- an AI provider - supplying an AI system or an AI-based product or service to others
- an AI user - using an AI system, including third-party or off-the-shelf tools, within its own operations

Most organisations seeking certification are users of third-party AI. An organisation can hold more than one role, and the role can differ from one AI system to another. The role held should be stated in the scope of the AI management system.

AI Risk Assessment and Risk Treatment

The organisation is required to define and apply an AI risk assessment process which:

- establishes and maintains AI risk criteria, including criteria that distinguish acceptable risk from risk that is not acceptable
- identifies the risks that could affect the intended outcomes of the AI management system
- analyses and evaluates those risks, taking account of the likelihood and the potential consequences
- prioritises the risks for treatment

Risk treatment then requires the organisation to select the treatment options, determine the controls needed, compare that set of controls against Annex A of the standard to confirm nothing necessary has been overlooked, and produce a Statement of Applicability. A risk treatment plan is required, and both the plan and the acceptance of any residual AI risk must be approved by the designated management.

The risk assessment must be carried out at planned intervals and repeated when significant changes are proposed or occur.

AI System Impact Assessment

This is specific to ISO 42001 and has no equivalent in ISO 9001, ISO 14001 or ISO 45001.

The organisation must define a process for assessing the potential consequences for individuals, groups of individuals and societies of each AI system it develops, provides or uses. The assessment has to take into account:

- the deployment of the AI system, its intended use and its foreseeable misuse
- the technical and societal context in which the system is used
- the jurisdictions that apply to it

The results must be documented and retained, and made available to interested parties where that is appropriate. The assessment must be performed at planned intervals and repeated when the system, the way it is used, or its context changes.

Leadership, Policy and Responsibilities

The standard sets out the requirements for the organisation's leadership. Top management is required to:

- establish an AI policy that is appropriate to the organisation and its use of AI, and that commits to meeting applicable requirements and to continual improvement
- ensure the AI management system is integrated into the organisation's business processes
- ensure the resources needed for the AI management system are available
- assign and communicate the roles, responsibilities and authorities relevant to the AI management system, including responsibility for reporting on its performance
- promote continual improvement and support other management roles in demonstrating leadership

The AI policy must be documented, communicated within the organisation, available to interested parties where appropriate, aligned with the organisation's other policies and reviewed at planned intervals.

Responsibilities need to be defined across the whole life cycle of each AI system - who authorises a system into use, who owns it, who oversees its outputs and who is accountable for the decisions it supports. Where activities are shared with a supplier, provider or customer, the allocation of responsibilities between the parties has to be understood and recorded.

Awareness, Competence and Training

The standard requires the organisation to determine the competence needed by anyone whose work affects AI performance, to ensure those people are competent, and to retain evidence of it. Separately, it requires that all workers are made aware of the AI policy, of their own contribution to the effectiveness of the AI management system, and of the implications of not conforming to it.

Awareness training should therefore be completed by everyone who uses an AI system or who relies on its output, and repeated when the policy, the tools in use or the way they are used change. New starters should complete it before they use any AI system. A certification auditor will ask to see the training records.

Annex A Controls and the Statement of Applicability

Annex A of the standard lists 38 controls under nine headings:

- A.2 Policies related to AI
- A.3 Internal organization
- A.4 Resources for AI systems
- A.5 Assessing impacts of AI systems
- A.6 AI system life cycle
- A.7 Data for AI systems
- A.8 Information for interested parties
- A.9 Use of AI systems
- A.10 Third-party and customer relationships

The controls are not a checklist to be adopted wholesale. The organisation determines the controls it needs from its own risk assessment and impact assessment, compares that set against Annex A to check nothing has been missed, and then records the decision on each control in a Statement of Applicability - whether it applies, the justification for including or excluding it, and whether it has been implemented. Controls that are not in Annex A can be added where the organisation needs them.

Annex B of the standard provides implementation guidance for each of the 38 controls. Annex C lists potential AI-related organisational objectives and risk sources which are useful prompts when

completing the risk assessment. Annex D covers use of the AI management system across sectors and alongside other management system standards.

Overall Requirements

Summary of the overall requirements of the ISO 42001:2023 standard:

- **Context of the organisation** - internal and external issues, interested parties
- **Leadership and commitment** - AI policy, roles, responsibilities and authorities
- **Planning** - actions to address risks and opportunities, AI system impact assessment
- **AI objectives** and planning to achieve them
- **Planning of changes**
- **Support and resources**
- **Competence** of persons whose work affects AI performance
- **Awareness** of the AI policy, of each person's contribution to the AI management system
- **Communication** - internal and external communication relevant to the AI management system
- **Documented information** (creation, control and update)
- **Operational planning** and control
- **AI system life cycle** - objectives for responsible development, life cycle processes
- **Data for AI systems** - data management, provenance, quality and preparation
- **Information for interested parties** - system documentation, information provided to user
- **Use of AI systems** - processes and objectives for responsible use, including human oversight
- **Third-party and customer relationships** - suppliers and customer expectations
- **Performance evaluation** - monitoring, measurement, analysis and evaluation
- **Internal audit**
- **Management review**
- **Nonconformity and corrective action**
- **Continual improvement** of the AI management system

ISO 42001 Certification

Information about the ISO 42001 audit process and guidance for preparing for a certification audit is available at the following pages;

- **ISO 42001 Certification Guidance**
- **ISO Certification Guidance**