ARTIFICIAL INTELLIGENCE MANAGEMENT SYSTEMS

# ISO 42001
# Overview guide

# Contents

# Navigating the AI Landscape

## Understanding the trends reshaping technology, risk and responsibility

**Artificial intelligence (AI)** is increasingly applied across all sectors utilising 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. From finance and manufacturing to healthcare and logistics, AI is driving advances in automation, efficiency, and decision-making. The widespread adoption of generative AI and machine learning has unlocked new possibilities – but it has also accelerated the need for stronger **governance**, greater **transparency** and clearer **accountability**.

### The global AI landscape is being shaped by three converging trends:

#### Accelerated implementation

Businesses are moving fast to embed AI across core operations. According to IBM, 42% of enterprises are already exploring or actively deploying generative AI. However, this pace often outstrips the development of formal governance structures – creating gaps in oversight, quality assurance and risk management.

#### Evolving regulation

Governments and regulators are responding to growing societal concerns with new frameworks to ensure AI systems are safe, fair and explainable. The EU AI Act – passed in 2024 – sets a precedent for risk-based regulation, with similar initiatives underway globally. The message is clear: trust in AI must be earned, not assumed.

#### Rising scrutiny and ethical expectations

From data privacy and intellectual property to bias and accountability, organisations are under pressure to demonstrate that their use of AI is ethical, responsible and secure. Public trust is fragile – and missteps can quickly lead to reputational damage, regulatory consequences and lost opportunities.

These trends signal a turning point. AI has moved from pilot programmes to strategic infrastructure. And with that shift comes a need for structured, system-wide governance that can scale with ambition – and stand up to scrutiny.

# What is ISO 42001?

## The first international management system standard for AI

ISO 42001 is the world's first AI-specific management system standard – providing a structured framework to help organisations manage artificial intelligence responsibly.

Designed for organisations that develop, deploy or rely on AI, the standard sets out the requirements for establishing, implementing, maintaining and continually improving an Artificial Intelligence Management System (AIMS).

Whether you're integrating AI across business operations or delivering AI-enabled products and services, ISO 42001 helps you embed ethical principles, manage risk, and align with global expectations around trustworthy AI.

Key elements of the standard include:

- **Governance and accountability** – Defining roles, responsibilities and oversight for AI-related activities
- **Risk-based controls** – Identifying and addressing risks throughout the AI system lifecycle
- **Transparency and explainability** – Supporting clear communication of how AI systems function and make decisions
- **Continual improvement** – Using feedback, monitoring and performance data to strengthen your AIMS over time

ISO 42001 follows the Annex SL structure, making it easy to integrate with other standards such as ISO 9001, ISO 27001 or ISO 45001 – enabling a consistent and harmonised approach to managing risk across your organisation.

By adopting ISO 42001, organisations can demonstrate a clear commitment to responsible innovation, building trust with clients, partners and regulators in an increasingly AI-driven world.

# Why get certified?



**Certification to ISO 42001 is more than a formality.** It's an independent, globally recognised mark of assurance that your organisation is managing artificial intelligence responsibly and effectively.

**Demonstrates commitment to best practice**
Certification signals that you're serious about building ethical, transparent and well-governed AI systems – in line with international expectations.

**Builds trust and credibility with clients**
For many sectors, certification is becoming a licence to trade. It reassures clients, partners and stakeholders that your AI practices are secure, accountable and well managed.

**Supports privacy, ethics and information security goals**
The certification process helps embed AI governance into your broader risk management systems – strengthening data protection, responsible innovation and ethical oversight.

**Future-proofs your compliance**
As AI regulation accelerates globally, ISO 42001 certification helps position your organisation ahead of evolving legal and industry requirements – reducing risk and supporting long-term resilience.

# ISO 42001 key requirements:

## Annex SL Clause structure

**The ISO Annex SL structure consists of ten clauses. All content in a management system standard, including ISO 42001, must meet the criteria of all ten clauses to follow the Annex SL framework. The clauses are categorised as:**

### Clause 1
### Scope

Defines the intended outcomes of the AI management system and its applicability within the organisation.

### Clause 2
### Normative references

Lists referenced standards that are essential to the application of ISO 42001.

### Clause 3
### Terms and definitions

Provides definitions of core terminology used throughout the standard to ensure shared understanding.

### Clause 4
### Context of the organisation

Considers internal and external factors, stakeholder expectations, and the scope of AI system use.

### Clause 5
### Leadership

Outlines top management's responsibility for policy, resourcing, and promoting a responsible AI culture.

### Clause 6
### Planning

Addresses how the organisation identifies and responds to AI risks and opportunities, and sets AI objectives.

### Clause 7
### Support

Covers the resources, competence, awareness, communication and documentation needed for effective governance.

### Clause 8
### Operation

Defines how AI-related controls are implemented, including risk assessments and system impact evaluations.

### Clause 9
### Performance evaluation

Requires monitoring, measurement, internal audits and management review to evaluate system performance.

### Clause 10
### Improvement

Details the organisation's approach to continual improvement, nonconformity handling, and corrective actions.

**In most cases, these clauses use identical core text, regardless of the standard they are applied to, and share common terms and definitions to promote consistency and compatibility across management systems standards. For ISO 42001, this ensures AI governance is embedded within a familiar and proven management system structure.**

# Addressing ISO 42001 requirements in the context of AI

Like other ISO management system standards, ISO 42001 is built around Clauses 4 to 10 – covering areas such as context, leadership, planning, support and continual improvement. What makes ISO 42001 unique is how these familiar concepts are tailored to the challenges and risks associated with artificial intelligence.

The sections below summarise how the clauses apply in the context of AI – from ethical governance and data transparency to risk management and lifecycle oversight.

## Context of the organisation

ISO 42001 asks organisations to define the scope of their AI management system by understanding their internal and external context. This includes legal obligations, industry-specific AI risks, cultural and ethical norms, stakeholder expectations, and the organisation's role in the AI lifecycle – whether as a developer, deployer, or user. These insights shape how AI is governed and help determine which controls are relevant. Organisations are also encouraged to evaluate whether broader societal issues, such as climate change or digital equity, should inform their approach.

## Leadership and governance

A core requirement of ISO 42001 is visible and sustained leadership commitment to responsible AI use. Senior management must establish a clear AI policy, set objectives aligned with organisational values, and ensure roles and responsibilities are defined across the AI lifecycle. This includes maintaining oversight of risk assessments, impact evaluations and the use of AI, particularly in sensitive or high-risk contexts. Active engagement at the top helps ensure governance is embedded throughout the business – not treated as an afterthought.

## Ethics and transparency

Ethical considerations are embedded throughout ISO 42001. Organisations must demonstrate how they assess and address the potential impacts of AI on individuals and society. This includes considering fairness, non-discrimination, and human autonomy, as well as data privacy and transparency of outcomes. Controls must be in place to identify and mitigate unintended consequences – and evidence of these practices must be documented, monitored and updated regularly.

## Risk and opportunity management

Organisations are required to assess and treat AI-specific risks – including those that affect compliance, reputation, and safety – while also identifying opportunities for innovation and improvement. ISO 42001 recognises that risk appetite and definitions may vary by sector, so the framework is adaptable. What matters is that decisions are made consciously, guided by policy, and evaluated for effectiveness over time.

## Continual improvement

ISO 42001 follows the Plan-Do-Check-Act (PDCA) model. That means continual improvement isn't optional – it's embedded. Organisations must monitor their AI system performance, conduct internal audits, and review governance processes regularly. Whether it's a corrective action or adapting to regulatory changes, the goal is to keep improving the suitability, adequacy, and effectiveness of the AI management system.

# ISO 42001 Annex A Controls

## Translating responsible AI into action

In addition to the 10 main clauses, ISO 42001 includes a set of supporting control objectives in Annex A. These controls are designed to help organisations implement practical, auditable measures that support trustworthy AI development and use.

Structured across 10 categories, the Annex A controls cover:

- **Policies related to AI** – ensuring clear leadership intent and direction
- **Internal organisation** – defining governance roles and responsibilities
- **Resources** – managing tools, data and infrastructure used in AI
- **Impact assessments** – evaluating risks to individuals and society
- **Lifecycle oversight** – aligning system design with ethical and regulatory goals
- **Data for AI systems** – ensuring quality, provenance and relevance
- **Information for interested parties** – promoting transparency and accountability
- **AI system usage** – managing scope, intent and safeguards
- **Third-party relationships** – setting expectations for suppliers and partners
- **Documentation and traceability** – supporting explainability and auditability

These control areas provide the practical foundation for implementing ISO 42001. They can be adapted to different levels of AI maturity and complexity – and form a key part of readiness assessments and certification.

# Implementing ISO 42001

## Focus areas for operationalising your AI Management System

ISO 42001 provides a framework for implementing responsible and effective AI management practices using the Plan-Do-Check-Act (PDCA) model – a core foundation shared across all Annex SL-based ISO standards.

The standard supports the development of an Artificial Intelligence Management System (AIMS) through interconnected management processes, including:

- **Awareness**

  Organisations should build awareness by training teams to understand the benefits, risks and ethical considerations of AI – from developers to decision-makers.

- **Responsibility**

  Clearly defined roles and responsibilities must be assigned, ensuring that AI governance is understood and embedded across the system lifecycle

- **Response**

  There should be timely and coordinated action to manage risks, respond to AI system impacts, and apply corrective actions where needed.

- **Risk assessment**

  Risks associated with AI systems – including technical failure, unintended outcomes, or misuse – must be assessed in a structured, evidence-based way.

- **System design and development**

  AI systems must be developed and deployed in line with documented policies and processes – supporting ethical use, transparency and lifecycle accountability.

- **Governance and control**

  Organisations should adopt a holistic approach to managing AI, covering data quality, explainability, fairness, reliability and human oversight.

- **Reassessment and continual improvement**

  As part of the PDCA model, performance should be monitored and reviewed regularly. Internal audits and management reviews help ensure the AIMS continues to meet objectives and adapts to emerging risks and regulations.

# Building your roadmap with ISO 42001

## Laying the groundwork for effective AI governance

**Implementing ISO 42001 begins with clarity of purpose and strong leadership support. These early steps help ensure your AI Management System (AIMS) is both practical and aligned to your organisation's goals.**

### 1. Gain leadership commitment

Senior management must lead the AIMS – setting clear objectives that define what success looks like for your organisation. Whether it's enhancing oversight, meeting regulatory expectations or building trust, leadership should allocate the resources and direction needed to embed responsible AI use throughout the business.

### 2. Understand your AI context

Assess how AI is developed, deployed or used across your organisation. Consider legal obligations, sector-specific risks and stakeholder expectations. This understanding should inform your resourcing – including the time, skills and budget needed to manage AI responsibly and effectively.

### 3. Assess training requirements

AI governance spans technical, ethical, legal and operational domains. Engage cross-functional teams and ensure tailored training is in place – from awareness for wider teams to audit training for specialists. Building capability across roles is key to effective, scalable implementation.

### 4. Define the AIMS scope

Clarify which teams, systems and geographic locations your AIMS will cover – including internally developed AI, third-party tools and high-risk use cases. A well-defined scope will keep your governance focused and fit for purpose.

### 5. Plan and implement your AIMS

Develop a realistic implementation plan that covers timelines, responsibilities and required resources. Introduce the necessary controls, documentation and governance processes. Build in regular reviews, feedback loops and performance monitoring to ensure your AIMS evolves with your business and the AI landscape.

### 6. Conduct a gap analysis

Review your current governance, risk and compliance frameworks to identify where your organisation already meets the standard – and where gaps or vulnerabilities exist. This insight will help prioritise improvements and avoid duplication.

### 7. Book your certification audit

Once your AIMS is in place, schedule your ISO 42001 certification audit with LRQA. Our two-phase process will assess your system design and implementation – helping you demonstrate accountability, integrity and responsible innovation to your stakeholders.

### 8. Embed continuous improvement and response

A mature AIMS includes more than initial implementation – it requires mechanisms for continuous learning and improvement. Establish feedback loops, regular audits and performance metrics to adapt to evolving AI risks and technologies. Implement an AI-specific incident response plan to ensure that errors, bias or system failures are addressed quickly, transparently and effectively.

# Integrating ISO 42001 with existing management systems

## Build on what's already working. Strengthen your governance across AI and information security.

For many organisations, ISO 42001 is not a starting point – it's a natural extension. If you already hold ISO 27001 certification, you're in a strong position to integrate ISO 42001 efficiently and effectively.

ISO 27001 provides a proven framework for managing information security risks, and its controls around data confidentiality, integrity and availability directly support many of the requirements in ISO 42001. By combining the two standards, you can create a unified governance approach that addresses both your information and AI-related risks.

## Why integration makes sense

### Shared structure

ISO 42001 follows the Annex SL framework – the same high-level structure used in ISO 27001, ISO 9001, ISO 45001 and others. This enables consistency across policy, leadership, planning, operation and evaluation.

### Efficient resource use

Integration helps reduce duplication across audits, documentation and internal reviews. Teams can align reporting, objectives and controls – streamlining compliance and improving oversight.

### Aligned risk management

Both standards require a risk-based approach. Where ISO 27001 focuses on information assets, ISO 42001 extends this to AI systems – including how data is used to train, validate and operate them.

### Stronger system resilience

An integrated approach makes it easier to spot systemic issues, resolve them holistically, and demonstrate a joined-up governance model to clients, regulators and partners.

# Our ISO 42001 services



## Training

Build your knowledge of ISO 42001 with a range of courses designed for different experience levels – delivered via multiple learning styles.

View available courses

## Gap analysis

An optional service where one of our expert auditors will help you identify any critical, high-risk or weak areas of your system prior to certification.

## Certification

We assess your AI Management System (AIMS) in line with the requirements of ISO 42001.

## Integrated assessments

If you've implemented multiple management systems, you could benefit from an integrated audit and surveillance programme – a more efficient and cost-effective way to manage risk.

# Why work with us?



At LRQA, we help organisations develop robust, future-ready risk management programmes that enable the safe, responsible and effective adoption of AI and technology.

From ensuring compliance with evolving AI regulations to strengthening data security and embedding best practices in governance, we provide the assurance needed to drive innovation with confidence – helping businesses integrate AI and technology while managing risks proactively.

## On the ground expertise

Our solutions are delivered by a global team of experts specialising in cybersecurity, compliance, and supply chain risk management, helping you navigate AI-related risks, meet evolving regulatory requirements, and integrate responsible AI practices into your operations.

## Continuous assurance

AI-driven risks require continuous oversight. Our approach to real-time risk management enables proactive issue resolution, reducing business disruption and enhancing resilience. Our connected portfolio of risk management solutions helps businesses go beyond regulatory requirements and embed AI risk management into day-to-day operations.

## Solution-based partnerships

We don’t just certify – we work alongside you to integrate AI governance into your wider risk and compliance strategy. Our tailored approach ensures AI and technology help drive sustainable growth while meeting evolving legal and ethical expectations.

## Data-driven decision-making

We leverage digital platforms and analytics to provide deeper insights into AI risks across your business. Our human intelligence, enhanced by data-driven tools, helps organisations identify vulnerabilities, predict future risks and make informed decisions with confidence.

## About LRQA

LRQA is the leading global assurance partner, bringing together decades of unrivalled expertise in assessment, advisory, inspection and cybersecurity services.

Our solutions-based partnerships are supported by data-driven insights that help our clients solve their biggest business challenges. Operating in more than 150 countries with a team of more than 5,000 people, LRQA's award-winning compliance, supply chain, cybersecurity and ESG specialists help more than 61,000 clients across almost every sector to anticipate, mitigate and manage risk wherever they operate.

In everything we do, we are committed to shaping a better future for our people, our clients, our communities and our planet.

## Get in touch

Visit **lrqa.com** for more information or email **enquiries@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom