GovLoX | Executive Briefing

ISO 42001:

A Practical Guide

What the AI management system standard requires and how to implement it

Executive Summary

ISO/IEC 42001:2023 is the international standard for AI management systems. Published in December 2023, it provides a structured framework for organisations to govern the development, deployment, and use of AI in a responsible, transparent, and accountable way.

Unlike the EU AI Act, which is a legal obligation with enforceable penalties, ISO 42001 is a voluntary standard. But voluntary does not mean unimportant. ISO 42001 is rapidly becoming a baseline expectation in enterprise procurement, a benchmark for regulatory readiness, and a practical framework that organisations can implement regardless of size or sector.

This guide explains what ISO 42001 requires, how it relates to other frameworks, and what a realistic implementation programme looks like - without the jargon.

> **Key finding**
> ISO 42001 is the most practical starting point for organisations building an AI governance programme. It is structured, internationally recognised, auditable, and directly complementary to EU AI Act compliance requirements. Organisations that implement ISO 42001 are building the governance infrastructure they will need regardless of which specific regulations apply to them.

What ISO 42001 Is

An AI management system standard

ISO 42001 defines the requirements for an AI Management System (AIMS) - the set of policies, processes, roles, and controls that an organisation uses to govern AI throughout its lifecycle. It follows the same high-level structure (HLS) as other ISO management system standards, including ISO 27001 (information security) and ISO 9001 (quality management).

This means organisations that already hold ISO 27001 or ISO 9001 certification will find the structure familiar. Many of the foundational elements - context of the

organisation, leadership commitment, risk assessment, internal audit, management review - carry over directly.

> **Who it is for**
> ISO 42001 applies to any organisation that develops, provides, or uses AI systems - regardless of size, sector, or whether AI is central or incidental to its business. A law firm using AI for document review, a manufacturer using AI for quality control, and an AI software company building foundation models are all in scope.

What it is not

ISO 42001 is not a technical specification for how AI systems must be built. It does not prescribe algorithms, architectures, or performance thresholds. It is a management system standard - it governs how an organisation manages AI, not how AI systems work internally.

It is also not a replacement for legal compliance. ISO 42001 certification does not confer EU AI Act compliance, GDPR compliance, or any other regulatory clearance. It is a governance framework that complements and supports regulatory compliance - not a substitute for it.

The Structure of ISO 42001

ISO 42001 is organised into ten clauses. Clauses 1–3 are introductory. Clauses 4–10 contain the requirements that organisations must meet to achieve conformance.

Clause	Title	What it requires
4	**Context**	Understand the organisation's internal and external context, identify interested parties and their expectations, define the scope of the AIMS
5	**Leadership**	Top management must demonstrate commitment, establish an AI policy, and assign roles and responsibilities for AI governance
6	**Planning**	Conduct AI risk and impact assessments, set objectives for the AIMS, and plan how to achieve them
7	**Support**	Provide resources, ensure competence of personnel involved in AI, raise awareness, manage documentation
8	**Operation**	Implement the AI risk assessment and treatment process, manage AI system lifecycle, control third-party AI
9	**Performance**	Monitor and measure the AIMS, conduct

	evaluation	internal audits, undertake management review
10	**Improvement**	Address nonconformities, take corrective action, pursue continual improvement of the AIMS

Annex A: AI-specific controls

In addition to the main clauses, ISO 42001 includes Annex A - a set of AI-specific controls that organisations select based on their context and risk profile. These controls cover areas including:

- **AI system impact assessment:** Evaluating the potential impact of AI systems on individuals and society before and during deployment
- **Data governance for AI:** Ensuring training, validation, and operational data is appropriate, documented, and managed
- **Human oversight of AI:** Defining when and how human review, intervention, and override applies to AI outputs
- **AI system transparency:** Documenting how AI systems make decisions and ensuring appropriate explainability
- **Responsible AI use policy:** Establishing organisational principles for the ethical and responsible development and use of AI
- **Supplier and third-party AI:** Managing governance obligations that arise when AI is procured from or shared with third parties

How ISO 42001 Relates to Other Frameworks

One of ISO 42001's practical strengths is how well it maps to other governance and compliance frameworks that organisations are likely to be working with simultaneously.

ISO 42001 requirement	EU AI Act equivalent	GDPR equivalent
Cl.6: AI risk assessment	Conformity assessment (Art.43)	DPIA (Art.35)
Cl.8: AI system lifecycle management	Technical documentation (Art.11)	Records of processing (Art.30)
Annex A: Human oversight controls	Human oversight obligation (Art.14)	Art.22 automated decision-making
Cl.5: AI policy and leadership	Provider/deployer obligations (Art.16/26)	Accountability principle (Art.5(2))
Cl.9: Internal audit and review	Post-market monitoring (Art.72)	Ongoing compliance review
Annex A: Data governance for AI	Data and data governance (Art.10)	Data minimisation, accuracy (Art.5)

Cl.10: Corrective action	Incident reporting (Art.73)	Breach notification (Art.33)

The mapping is not perfect - the EU AI Act has specific legal requirements that ISO 42001 does not replicate exactly, and GDPR has data subject rights obligations that go beyond what ISO 42001 addresses. But the overlap is substantial enough that organisations building an ISO 42001-conformant AIMS are also building the infrastructure needed for EU AI Act and GDPR compliance.

Certification: Do You Need It?

ISO 42001 can be implemented in two ways: as a self-declared conformance, where the organisation assesses itself against the standard without external verification; or as third-party certified conformance, where an accredited certification body audits the organisation and issues a certificate.

When certification makes sense

- **Customer and procurement requirements:** Enterprise customers and public sector procurement processes are increasingly requiring ISO 42001 certification as a supplier qualification criterion
- **Regulatory positioning:** Certification provides auditable evidence of governance maturity that regulators and data protection authorities find credible
- **Market differentiation:** For AI-adjacent businesses - technology vendors, consultancies, data processors - certification is becoming a commercial differentiator
- **Internal discipline:** The certification process imposes a discipline on implementation that self-assessment often does not - external auditors ask harder questions

When self-assessment is the right starting point

- **Early-stage programmes:** Organisations beginning their AI governance journey should build and operate their AIMS for at least 6–12 months before pursuing certification - auditors will expect evidence of sustained operation
- **Resource constraints:** Certification requires management time, documentation effort, and audit fees. Organisations with limited governance resources may get more value from a well-implemented self-assessed AIMS than a rushed certification
- **Internal clarity first:** The primary value of ISO 42001 is the governance structure it creates, not the certificate. Organisations should not optimise for certification at the expense of building something that actually works

> **Practical guidance**
> Start with self-assessment against the standard. Build your AIMS. Run it for a full

cycle - including an internal audit and management review. Then pursue certification when the programme is mature and the business case for external validation is clear.

A Practical Implementation Roadmap

The following roadmap reflects what works in practice for organisations building an ISO 42001-conformant AIMS. It assumes no existing formal AI governance programme. Organisations with existing governance infrastructure can compress the earlier phases.

Phase	Key actions
Phase 1 Months 1–2: Foundation	Define AIMS scope. Identify interested parties and their expectations. Establish AI policy with top management sign-off. Assign governance roles: AI Governance Officer, AI System Owners, DPO. Conduct initial AI system inventory.
Phase 2 Months 2–4: Risk and Impact Assessment	Conduct AI risk assessment for each system in scope. Complete AI impact assessments for high-risk systems. Select and apply relevant Annex A controls. Document risk treatment decisions and residual risk acceptance.
Phase 3 Months 4–6: Controls Implementation	Implement selected Annex A controls. Establish data governance processes for AI training and operational data. Build human oversight mechanisms. Create and publish approved AI tool registry. Develop AI-specific training for relevant staff.
Phase 4 Months 6–9: Operation and Evidence	Operate the AIMS for a full cycle. Maintain records of AI system approvals, assessments, and incidents. Run supplier AI due diligence process. Handle any AI-related incidents through the documented process.
Phase 5 Month 9–12: Audit and Review	Conduct internal audit against ISO 42001 clauses 4–10 and selected Annex A controls. Complete management review. Address nonconformities. Identify improvement opportunities. Decision point: proceed to third-party certification or continue self-assessment cycle.

Common Implementation Pitfalls

Organisations that struggle with ISO 42001 implementation tend to make the same mistakes. Avoiding these will save significant time and effort.

Treating it as a documentation exercise

ISO 42001 requires evidence of operation, not just documentation of intent. An AI policy that has never been communicated, a risk assessment template that has

never been used, and governance roles that exist on paper but not in practice will not satisfy an auditor - and will not deliver governance value.

Scoping too broadly too early

The AIMS scope does not have to cover every AI system in the organisation from day one. Organisations that attempt to bring all AI systems into scope simultaneously often find the programme becomes unmanageable. A well-defined, narrower scope - one business unit, one category of AI system - implemented well is more valuable than a broad scope implemented poorly.

Underestimating the inventory challenge

You cannot manage what you cannot see. Organisations consistently underestimate how many AI systems are in use until they conduct a structured discovery exercise. Shadow AI - tools adopted informally without governance oversight - is the most common gap. The inventory must come before the assessment, and it must be kept current.

Missing the leadership requirement

Clause 5 is not optional and cannot be delegated entirely to compliance teams. ISO 42001 explicitly requires top management commitment and involvement. Organisations where AI governance is owned exclusively by IT or compliance, without visible leadership sponsorship, will have difficulty demonstrating conformance - and are likely to have weaker governance in practice.

> **The most common gap**
> Annex A control selection is where most organisations get stuck. The standard requires organisations to justify which controls they have selected and why - and to document controls they have excluded and the rationale for exclusion. This Statement of Applicability (SoA) is one of the most important documents in the AIMS. Treat it as a living document, not a one-time exercise.

The Statement of Applicability

The Statement of Applicability (SoA) is a document that lists every Annex A control, states whether the organisation has selected it, and explains the rationale for inclusion or exclusion. It is required for ISO 42001 conformance and is the central reference document for any certification audit.

A well-structured SoA includes:

- **Control reference and title:** Each Annex A control identified by clause number and name
- **Applicability decision:** Whether the control is applicable to the organisation's context - and if not, a clear rationale for exclusion
- **Implementation status:** Whether the control has been implemented, partially implemented, or is planned
- **Evidence reference:** A pointer to the policy, procedure, or record that demonstrates implementation

- **Risk linkage:** Which risks or impact assessment findings the control addresses

The SoA is not a static document. It should be reviewed and updated as the organisation's AI portfolio evolves, as new systems are onboarded, and as the risk landscape changes. At minimum, it should be reviewed as part of the annual management review cycle.

Three Things to Do This Week

For organisations that have not yet started their ISO 42001 journey, the following three actions provide the most effective starting point:

1	**Build your AI system inventory** List every AI system your organisation uses, has developed, or procures from a third party. Include systems you suspect are in use but have not been formally approved. This inventory is the foundation of your AIMS and the starting point for every assessment that follows.
2	**Assign an AI Governance Officer** ISO 42001 requires leadership commitment and defined roles. Name the person accountable for AI governance in your organisation. This does not have to be a full-time role - but it must be an explicit, documented accountability, not an implied one.
3	**Read the standard** ISO/IEC 42001:2023 is available from ISO and national standards bodies. It is not long. The normative requirements (Clauses 4–10 and Annex A) can be read in an afternoon. Understanding what the standard actually says - rather than working from summaries - is the most reliable way to build a conformant programme.