INSIGHT · AI GOVERNANCE & EU AI ACT

# ISO 42001 isn't the EU AI Act, but it's the easiest way to be ready for it

*By Shalini Jhunjhunwala · Aequita Advisory · 9 min read*

Almost every conversation I have with a compliance lead right now contains a version of the same question: *"We've heard about ISO 42001. We've heard about the EU AI Act. Are they the same thing? Different things? Which one do we need to do?"*

The short answer is that they are different things, and ISO 42001 does not satisfy the EU AI Act by itself. The longer and more useful answer is that for most organisations, ISO 42001 is the most practical operational pathway to being ready for the AI Act. The two answers are both true. This piece explains how they fit together.

## What ISO 42001 actually is

Published in December 2023, ISO/IEC 42001 is the world's first international standard for an Artificial Intelligence Management System. It is the AI counterpart to ISO 27001: same management-system architecture (Clauses 4 through 10 covering context, leadership, planning, support, operation, performance evaluation, and improvement), with an Annex A that catalogues controls specific to AI rather than information security.

Annex A organises its controls into nine areas covering AI policies, internal organisation, resources for AI systems, impact assessment of AI systems, AI system lifecycle, data for AI systems, information for interested parties, use of AI systems, and third-party and customer relationships. The standard is certifiable through accredited bodies. The certification process is similar in shape to ISO 27001.

Critically, it is a **management system standard**. It describes how to *manage* AI responsibly. It does not prescribe which AI to build or which use-cases are permitted.

## What the EU AI Act is

The EU AI Act, by contrast, is a regulation with the force of law. It defines categories of AI systems (prohibited, high-risk, limited-risk, minimal-risk), allocates obligations across roles (providers, deployers, importers, distributors), and prescribes specific requirements, particularly for high-risk systems under Annex III. Article 9 requires a risk management system. Article 17 requires a quality management system. Annex IV prescribes specific technical documentation.

The AI Act is enforceable through penalties; ISO 42001 is enforceable through certification audits the organisation has chosen to undergo. The first is a legal obligation. The second is operational discipline.

## The relationship between them, in practice

Here is where the two intersect. The EU AI Act's operational obligations (the risk management systems, the documentation, the human oversight, the post-market monitoring) describe *what* a compliant organisation needs to do. ISO 42001 describes *how* to structure an organisation that can do those things consistently.

A useful analogy: the AI Act says "you must keep your house safe." ISO 42001 is a well-documented housekeeping system. The first one is a legal requirement. The second one is the operational

machinery that makes meeting that requirement repeatable.

Organisations that build an ISO 42001-aligned AI Management System find Article 9 risk management, Article 17 quality management, and Annex IV technical documentation substantially easier to satisfy, because the underlying structure is already in place. Conversely, organisations that try to meet the AI Act's obligations without a management-system backbone tend to produce one-off compliance artefacts that do not hold up to scrutiny over time.

## What ISO 42001 does not do

It is important to be precise here. ISO 42001 certification does not, in itself, demonstrate compliance with the EU AI Act. Three reasons:

- **Scope mismatch.** The AI Act has specific legal definitions and risk classifications that the standard does not directly map to. An ISO 42001-certified organisation can still be missing AI Act-specific obligations.
- **Documentation specificity.** Annex IV technical documentation under the AI Act prescribes particular contents that go beyond what ISO 42001 Annex A requires.
- **Conformity-assessment pathway.** The AI Act has its own conformity-assessment process for high-risk systems, separate from ISO certification audits.

The two are complementary, not substitutable.

## The order I would recommend

For organisations weighing where to start, the practical sequence is usually:

1. **Inventory and classify your AI systems** using the AI Act's risk-tier vocabulary, even if you are not formally subject to it yet. This tells you what scope of work you are actually facing.
2. **Build the management-system foundation** using ISO 42001's clauses 4 through 10 as scaffolding. Define policies, roles, risk methodology, lifecycle controls.
3. **Layer the AI Act-specific obligations** on top: Article 9 risk management against your highest-risk systems, Annex IV documentation, post-market monitoring, human oversight features.
4. **Decide whether to certify.** ISO 42001 certification is a separate decision, justified by procurement requirements, customer expectations, or internal discipline. Many organisations operate aligned-but-uncertified.

This sequence works because each step makes the next one cheaper. Inventory makes classification possible. The management system makes obligations operational. The operational machinery makes certification a documentation exercise rather than a transformation project.

## Where this leaves your organisation

> *"Build the AI Management System, then layer the Act-specific obligations on top. That sequence is cheaper, more durable, and easier to defend than trying to comply with the Act in isolation."*

ISO 42001 is not a shortcut around the EU AI Act. It is a serious operational commitment. But for organisations that need to demonstrate Responsible AI to multiple stakeholders, including regulators, customers, internal governance, and procurement teams downstream, it remains the most practical scaffolding to build on.

The question is rarely *42001 or the AI Act*. It is *in what order, and how do they fit together*. Asking that question early tends to save 12 to 18 months of backtracking later.

**Aequita Advisory**
Privacy & AI Compliance · EU practice

hello@aequita.eu
Shalini Jhunjhunwala, Founder