

THE EIGHT TIERS · PART 5 · CERTIFIABLE MANAGEMENT STANDARDS

ISO 42001 Certification: What It Actually Proves

Tier 5 of eight: the first AI standard you can be audited against —
and the piece of it that took two more years to show up

9 min read



IN ONE LINE

ISO 42001 certification means an accredited third party has audited your AI management system against ISO/IEC 42001:2023 and found it conformant.

That's it. That's the whole of what the certificate tells anyone.

I'm starting there because I keep watching people conflate it with something much bigger, and the conflation is expensive. A certificate on the wall is not EU AI Act conformity. It's not a presumption of anything. It's an accredited auditor saying you run a management system and it works. Which is genuinely valuable — just not the thing a lot of people think they're buying.

There's also a detail about this standard that I find quietly telling, and we'll get to it.

01 If you've run 27001, you already know this

That's not a throwaway line. ISO/IEC 42001 uses the Harmonised Structure, which means the same high-level clauses you've seen before — context, leadership, planning, support, operation, performance evaluation, improvement — and the same plan-do-check-act cycle underneath.

Context	Leadership	Planning	Support	Operation	Performance evaluation	Improvement
---------	------------	----------	---------	-----------	------------------------	-------------

Anyone who has been through an ISO 27001 or 9001 programme will recognise the shape of it within about ten minutes.

That matters more than it sounds. It means an organisation with an existing management system **extends** rather than rebuilds. In my experience the difference between those two words is roughly nine months and a lot of goodwill. If you already have a certified management system, that's the single strongest argument for making 42001 your governance spine rather than starting somewhere else.

02 What's actually in Annex A

The clauses tell you to have a management system. Annex A is where the work lives. Nine control areas:

1 / 9 Policies for AI A documented AI policy, aligned to your other policies, reviewed on a defined cadence.	2 / 9 Internal organisation Who's responsible for what, and a route for people to raise concerns.	3 / 9 Resources for AI systems A documented understanding of the data, tooling, compute and people each system depends on.
4 / 9 Assessing impacts of AI systems A process for working out the consequences for individuals, groups and society. This is the clause ISO/IEC 42005 goes deep on.	5 / 9 AI system life cycle Objectives for responsible development, the design and development process itself, verification and validation, deployment, operation, monitoring, technical documentation.	6 / 9 Data for AI systems Acquisition, quality, provenance, preparation.
7 / 9 Information for interested parties Documentation for the people using the system, and a way for them to tell you when something's wrong.	8 / 9 Use of AI systems Responsible use policies and defined objectives for use.	9 / 9 Third-party and customer relationships Who carries which responsibility across the supply chain.

If you've read the EU AI Act, most of that will look familiar. The overlap isn't accidental, and it's the reason this standard does so much work across frameworks.

03 The family matters more than the flagship

Three companions worth knowing, because 42001 on its own leaves gaps it expects you to fill elsewhere.

23894 RISK METHODOLOGY ISO/IEC 23894 gives you the risk methodology — essentially ISO 31000 applied to AI. 42001 tells you to have a risk process without specifying one. This is the one.	42005 IMPACT ASSESSMENT ISO/IEC 42005 covers impact assessment. How and when to do one, what to document, how it plugs into your risk process. If you need a fundamental rights impact assessment for Article 27, or you're facing the impact assessment duties in Colorado or Korea, this is the instrument.	42006 CERTIFICATION BODIES ISO/IEC 42006 sets the requirements for the bodies doing the certifying.
---	--	--

That last one is the detail I mentioned, and it's the part of this story people miss. 42001 published in December 2023. For about eighteen months after that, "ISO 42001 certified" was a claim without much behind it, because the standard governing the certification bodies themselves didn't exist yet. 42006 arrived in 2025 and made the whole thing real.

Dec 2023 42001 published	~18 months "Certified" — a claim without much behind it	2025 42006 arrives
--	---	--

It's the least glamorous document in the family and it's the one that turned a standard into a credential.

A CORRECTION	While I'm here — a correction I find myself making constantly. 42005 is impact assessment. 42006 is requirements for certification bodies. A surprising number of commercial guides have those two the wrong way round, including some from firms that should know better.
------------------------------------	---

04 Certification is not conformity

This is where people get hurt, so I want to be unambiguous about it.

ORGANISATION-WIDE · VOLUNTARY

ISO 42001 certification

Demonstrates that you operate a management system, assessed by an accredited third party. It's globally portable. Procurement teams understand it without a briefing. It produces evidence you can reuse across several regulatory frameworks.

PER-SYSTEM · LEGALLY REQUIRED

EU AI Act conformity assessment

Demonstrates that one specific high-risk system meets the Regulation, ending in CE marking and a declaration of conformity. It's legally required. It's per-system, not organisation-wide.

Certification does not confer conformity. What it does — and this is the genuinely useful part — is discharge a large chunk of the underlying work. Article 9 risk management, Article 17 quality management, Article 26 deployer obligations, Article 72 post-market monitoring all draw on artefacts a working 42001 system already produces.

So it's not the answer. It's most of the homework.

05 The thing that just changed, and the thing that didn't

ISO/IEC 42001 is not a harmonised standard under the AI Act. There's a European adoption, EN ISO/IEC 42001:2026, which is a step in that direction but isn't the same thing.

Now the part that's about to be widely misreported.

EN 18286:2026 — the quality management system standard supporting Article 17, and the first JTC 21 deliverable to actually make it over the line — was approved in July and published at the start of October. After years of delay, that's a real milestone and it deserves to be treated as one.

EN 18286:2026 — status

✓ Done

Approved

July

✓ Done

**Published by CEN-
CENELEC**

Start of October

✗ Not yet

**Cited in the Official
Journal**

The only step that does anything
legally

It is not presumption of conformity.

Article 40 attaches the presumption to harmonised standards **whose references have been cited in the Official Journal**. Publication by CEN-CENELEC and citation by the Commission are two separate steps, and only the second one does anything legally. EN 18286 has been published. It has not been cited.

Which means the position is unchanged where it counts:

Nobody currently has presumption of conformity for a high-risk AI system. Not one provider, anywhere.

Build to EN 18286 anyway. It produces audit-ready evidence, and it'll almost certainly be the first thing cited when citation comes. Just don't book the legal shortcut yet. The rest of the pipeline — risk management, cybersecurity, dataset quality, the trustworthiness framework — is still in draft.

Track the Official Journal, not the standard.

06 One practical thing nobody mentions

ISO standards are licensed, not sold.

A typical subscription covers named internal users and excludes external sharing or hosting outside the publisher's platform. Your certification body has its own copies. Your customers need their own.

So if a vendor offers to show you clause text inside their platform, ask them how that's licensed. It's a fair question and the answer is informative.

07 Things people ask me

Is ISO 42001 mandatory?

No. It's voluntary. It's also increasingly requested in enterprise procurement, and it satisfies a lot of the underlying work the regulations require — which is a different kind of mandatory.

Does ISO 42001 certification mean EU AI Act compliance?

No. Certification demonstrates a management system. AI Act conformity assessment is per-system and legally separate. The artefacts carry across; the conclusion doesn't.

What's the difference between ISO 42005 and ISO 42006?

42005 is AI system impact assessment. 42006 sets requirements for the bodies that audit and certify management systems. Worth getting right — plenty of published guidance doesn't.

NEXT IN THE SERIES · PART 6

NIST AI RMF

A voluntary framework that became a statutory safe harbour more or less by accident.