

GUIDE 2025/2026

ISO 42001 guide to AI management

The first international standard for AI management systems, explained plainly

notivia GmbH

Edition 2025/2026

Contents

1 What is ISO 42001? 3

1.1 The standard in plain words 3

1.2 What is an AIMS? 3

1.3 How the standard is built — clauses plus Annex A 4

1.4 How it sits alongside other standards 4

2 Why would you need ISO 42001? 5

3 The road to certification — seven phases 7

4 What does ISO 42001 cost? 9

5 The ten most common mistakes 10

6 Readiness check: are you ready? 12

7 Glossary 14

8 Your next step 16

1 What is ISO 42001?

1.1 The standard in plain words

ISO/IEC 42001:2023 is the world's first international standard for **AI Management Systems (AIMS)**. Published by ISO and IEC in December 2023, it sets out how companies use artificial intelligence systematically and responsibly — with clear governance, risk management and continual improvement.

Think of ISO 42001 as ISO 27001 for AI: the structure is deliberately similar — the harmonised structure — so that companies already running an ISMS can build AI governance **into it** . It is not about prescribing particular AI technologies but about the process: how do you recognise AI risks, how do you manage them, how do you keep improving?

> **The core idea:** ISO 42001 does not ask “which AI do you use?” but “do you have a systematic framework for keeping your AI applications under control — and can you show it?”

Certification is awarded by an independent, accredited certification body — DQS, TÜV or DEKRA, for example. It confirms that your company runs a working AI management system. The certificate is valid for three years and is checked each year by a surveillance audit, just as with ISO 27001.

1.2 What is an AIMS?

AIMS stands for **Artificial Intelligence Management System**. It is the whole of the rules, processes, responsibilities and measures through which you govern the use of AI in your company.

An AIMS covers four objectives:

Fairness
AI that does not discriminate

Transparency
Decisions that can be followed

Safety
Robust, dependable systems

Governance

Clear responsibilities

An AIMS follows the **plan-do-check-act cycle** : you plan your AI governance measures, put them in place, check whether they work and keep improving them. That cycle keeps your AI management in step with the technology.

1.3 How the standard is built — clauses plus Annex A

ISO 42001 follows the same structure as ISO 27001:

- **Clauses 4–10:** the requirements on the management system — context, leadership, planning, support, operation, evaluation, improvement.
- **Annex A:** 38 controls in 9 categories — the concrete safeguards for AI systems.
- **Annex B:** implementation guidance for the controls.
- **Annex C:** organisational objectives and sources of risk.
- **Annex D:** guidance on integrating with other management systems.

> **An easy way to remember it:** ISO 27001 has 93 controls for information security; ISO 42001 has 38 specific to AI. Since the structure is the same — clauses 4–10 plus Annex A — the two management systems integrate seamlessly.

1.4 How it sits alongside other standards

Standard	Focus	Typical audience
ISO 42001	AI management system	Companies that build AI or use it heavily
ISO 27001	Information security	Every industry; the basis for an AIMS
EU AI Act	AI regulation (binding)	Mandatory across the EU
NIST AI RMF	AI risk management framework	Organisations oriented towards the US
ISO 23894	AI risk management (guidance)	Complements ISO 42001

> **Worth knowing:** certification to ISO 42001 is **not** mandatory; the EU AI Act, by contrast, **is**. But a certified AIMS is the most efficient way to evidence AI Act conformity, and a strong signal of trust towards customers and investors.

2 Why would you need ISO 42001?

“Do we really need this?” is a fair question about so young a standard. But the reasons companies increasingly choose it are concrete:

Customer requirements and B2B business

Large companies and groups increasingly examine their suppliers' AI governance. Anyone offering AI-supported products or services is asked more and more often: “how do you make sure your AI is trustworthy?” Certification answers that question with an accepted standard.

> *A real example: a SaaS provider with AI-supported document analysis loses a corporate customer who demands ISO 42001 evidence. Three months later it starts certification; after eight months the certificate is in hand and the customer signs a multi-year contract.*

The regulatory context

The EU AI Act comes into force in stages between 2025 and 2027. Providers of high-risk AI have to implement a quality management system under Art. 17. ISO 42001 is the only international standard that covers those requirements in a structured way. Adopting it early cuts the AI Act implementation effort considerably.

Competitive advantage

AI is a question of trust. Companies that demonstrably manage fairness, transparency and safety enjoy more of it. In finance, health, HR, law and education — where AI decisions affect people directly — the certificate becomes a differentiator.

Reducing risk

- **Liability risk:** AI errors can cause harm — discrimination, wrong diagnoses, bad decisions. A systematic AIMS reduces both the risk and the liability.
- **Reputational risk:** a public AI scandal — bias in a recruitment tool, hallucination in a customer chatbot — can damage a brand. An AIMS helps prevent it.
- **Operational risk:** drift, data decay, models falling out of date — without monitoring, AI systems get worse over time. An AIMS keeps them steady.

Synergies with other standards

ISO 42001 is designed to combine with ISO 27001, ISO 9001 or other management systems. Introduced together they cost 30 to 50 % less. If you are already certified to ISO 27001, you can add ISO 42001 in three to five months.

3 The road to certification — seven phases

Depending on where you start, the road to certification takes **three to ten months**. With ISO 27001 as the basis and structured planning, four to six months is realistic.

1 Gap analysis and AI inventory

Take stock: which AI systems exist in the company, and are you the provider or the deployer? Which parts of an AIMS are already there — use what ISO 27001 gives you. What is missing against ISO 42001? Two to three weeks.

2 Set the scope and context

Define what the AIMS covers: which systems, processes and sites. Put the organisation in place: appoint an AI officer, settle responsibilities, set up reporting to management. Two weeks.

3 Analyse the AI risks

A systematic analysis per system: bias, hallucination, security, privacy and ethical risk. For each one: treat, accept, transfer or avoid, recorded in a risk register. Four to six weeks.

4 Implement the controls

Work through the 38 controls in Annex A step by step, not all at once, prioritised by risk. The usual focus: data governance, model lifecycle, impact assessment and human oversight. Two to four months.

5 Documentation and policies

An AI policy, usage guidelines, an impact assessment process, a lifecycle procedure. Every document has to fit your company — do not adopt generic templates without thinking. Three to four weeks, alongside phase 4.

6 Training and internal audit

Train management on their governance responsibility and staff on AI literacy. Run an internal audit to test effectiveness, then a management review with concrete decisions on what comes next. Three to four weeks.

7 External audit (stages 1 and 2)

The external audit comes in two stages. Stage 1 is a document review by the auditor; stage 2 checks the practice on site. If no serious deviations are found,

> you receive your certificate. Four to six weeks.

> **Tip:** If you already hold ISO 27001 or plan to, go for a **combined audit**. Auditing both together, internally and externally, saves around 40 % of the effort — and the controls overlap considerably, particularly data governance, asset management and access control.

4 What does ISO 42001 cost?

One of the questions we are asked most. Here are concrete figures, from market analysis and from our own projects:

Company size	Total cost*	Timeframe	Internal effort
1–5 staff	**€6,900–9,500**	3–5 months	6–10 hrs/week
6–20 staff	**€9,500–13,500**	4–6 months	8–12 hrs/week
21–50 staff	**€13,500–19,000**	5–7 months	10–16 hrs/week
51–150 staff	**€16,000–24,000**	6–9 months	14–22 hrs/week
150+ staff	**€24,000–38,000**	8–12 months	½-1 FTE

* The total includes consulting and implementation support, the AIMS platform and tooling, and the certification audit by an accredited body.

What drives the cost?

- **How many AI systems are in scope:** each one needs a risk analysis, an impact assessment and monitoring.
- **Provider or deployer:** a provider developing its own AI faces far more than a pure deployer.
- **An existing ISMS:** an ISO 27001 basis cuts the cost by 30 to 40 %.
- **Your industry:** health, finance and education face additional requirements under the sectoral parts of the AI Act.

Costs after the first certification

The certificate is valid for three years, with a surveillance audit in years two and three and recertification in the third. For keeping it running, allow around **20 to 25 % of the initial cost per year**.

> **In the interest of transparency:** combining ISO 27001 and ISO 42001 saves around 30 % when introduced together, and around 40 % when introduced one after the other. Our integrated ISMS platform lets you manage both efficiently.

5 The ten most common mistakes

1. **Building ISO 42001 without ISO 27001**
   Inefficient. ISO 42001 is built structurally on ISO 27001. Without an ISMS to start from, the work on data governance, access control and incident response doubles.

2. **An incomplete AI inventory**
   Shadow AI — staff tools such as ChatGPT — gets overlooked. In an audit that is a finding straight away.

3. **A risk analysis that stays abstract**
   Generic risks such as “AI can make mistakes” are not enough. Per system: concrete risks of bias, hallucination, security and ethics.

4. **No commitment from management**
   An AIMS is strategic. Without management taking an active part — resources, decisions, visibility — the audit fails.

5. **Human oversight for form's sake**
   “Someone looks at it sometimes” is not enough. The control points have to be documented, trained and auditable.

6. **Neglecting lifecycle management**
   Models degrade over time through data drift. Without monitoring, a model that started out fair becomes biased.

7. **No AI literacy training**
   Like the AI Act, ISO 42001 requires staff using AI to be qualified. Without evidence of training, that is a deviation.

8. **Skipping the impact assessment**
   A structured impact assessment before introducing a new system is mandatory. Leave it out and the AIMS stops being preventive.

9. **Inadequate data governance**

Training, validation and test data have to be quality-checked and documented. The most common audit finding: unchecked data sources.

10 **Choosing the wrong consultant**

ISO 42001 is new. Many consultants know ISO 27001 but little about the AI-specific questions. Check their references.

6 Readiness check: are you ready?

1. **Do you have a complete inventory of every AI system in your company?**
   Including the AI your staff use — ChatGPT, Copilot and the like.
2. **Is there someone responsible for AI governance?**
   An AI officer, chief AI officer, or an equivalent named role.
3. **Do you have a documented AI policy?**
   Which AI may be used, how and by whom?
4. **Do you run a systematic risk analysis for every AI system?**
   Bias, hallucination, security, ethical risk.
5. **Do you have a process for AI impact assessments?**
   A structured assessment before a new system goes in.
6. **Are lifecycle management processes in place?**
   Design, deployment, monitoring, decommissioning.
7. **Do you have data governance processes for training and operational data?**
   Quality assurance, provenance, currency.
8. **Is there a human oversight process for critical AI decisions?**
   Documented control points and a trained person overseeing them.
9. **Have your staff had AI literacy training?**
   Regular training, with attendance recorded.
10. **Do you have ISO 27001 or a comparable ISMS?**
    It reduces the effort for ISO 42001 considerably.

Your yes answers	Assessment	Recommendation
0–3 × yes	**New ground**	Building up in a structured way, with support, is advisable. Eight to twelve months combined with ISO 27001.

Your yes answers	Assessment	Recommendation
4–6 × yes	**Partly prepared**	Focus on the gaps, usually the risk analysis and the documentation. Five to eight months.
7–10 × yes	**A good basis**	With audit preparation you can be ready for certification in three to five months.

> Whatever your result: **every company using AI can achieve ISO 42001.** It is a question of planning properly, not of company size.

7 Glossary

ISO 42001

The international standard ISO/IEC 42001:2023, “Artificial intelligence — Management system”. The first certifiable AI management system standard.

AIMS

AI management system — the whole of the policies, processes, responsibilities and measures through which AI is governed systematically.

Annex A

The normative annex of ISO 42001, with 38 controls in 9 categories — the concrete safeguards.

Controls

Measures such as data governance, model testing, impact assessment, human oversight and security testing.

AI officer

The person responsible for AI governance. The role can be filled internally or brought in from outside.

AI impact assessment

A structured assessment of the effects of a new AI system before it is introduced. A mandatory element of the AIMS.

Human Oversight

Human oversight of AI decisions — a core principle in both ISO 42001 and the EU AI Act.

Lifecycle Management

Managing an AI system systematically from design through deployment to decommissioning.

Data Governance

Quality-checked, documented use of data for training, validation and testing.

Bias / Unfairness

Systematic distortion in AI decisions — a central risk in recruitment, lending and the like.

Data Drift

A shift in the distribution of the data over time, which degrades performance. Monitoring is mandatory.

Stage 1 / Stage 2

The two stages of the external certification audit. Stage 1 is a document review, stage 2 an on-site audit.

Surveillance audit

The annual check by the certification body in the years after the first certification.

Recertification

Renewing the certificate after three years through a full re-audit.

Nonconformity

A deviation found in the audit. Major non-conformities block certification.

combined audit

Auditing several management systems together — ISO 27001 and 42001, for example. It saves time and money.

8 Your next step

You have read this guide — that is the first step already. Tackling ISO 42001 systematically is an investment that pays off: in customer trust, in AI Act conformity, in reduced risk, and in a real competitive advantage on a subject that is only going to matter more.

A free first conversation

In 30 minutes, with no obligation, we work out together:

- ✓ Which AI systems are you using today?
- ✓ What scope makes sense for your certification?
- ✓ What timeframe and budget are realistic?
- ✓ Which next steps make sense?

No sales pitch, no pressure — just an honest assessment.

> **The quick ISO 42001 check**
> At **iso-easy.de** you will find our free ISO 42001 check. In a few clicks you get a first view of your maturity, the cost and the timeframe.

Contact

Web: iso-easy.de

Phone: +49 711 35 15 705

E-mail: feedback@iso-easy.de

iso-easy.de

iso-easy is part of notivia GmbH.

With more than 30 years of experience in IT consulting and compliance we support mid-sized companies in implementing ISO 42001, the EU AI Act, ISO 27001 and neighbouring standards — pragmatically, transparently and as equals.

© 2025/2026 notivia GmbH — **iso-easy.de** | All rights reserved.