ATLAS AI GOVERNANCE

ISO 42001 for Companies That Already Have ISO 27001:

What's Net-New

Control overlap, what's unique to 42001, and what most companies underestimate when adding AI governance to an existing information security program.

travis@atlasaigovernance.com | atlasaigovernance.com

V.2 | April 2026

01

Why This Matters Right Now

Twelve months ago, ISO 42001 was a nice-to-have. Today, it's becoming a gate in enterprise procurement, investor due diligence, and regulatory compliance. Here's what changed:

Enterprise procurement

Large enterprises are adding ISO 42001 to vendor security questionnaires. If you sell AI-powered software into enterprise accounts, expect the question "Are you ISO 42001 certified?" in your next procurement cycle. Without it, you're not disqualified on paper, but you're at a disadvantage against vendors who have it.

Microsoft SSPA

Microsoft's Supplier Security and Privacy Assurance program now requires ISO 42001 for suppliers with sensitive AI use cases (Section K). If you're a Microsoft vendor and your product involves AI, this isn't optional.

EU AI Act

Enforcement begins August 2, 2026. If your AI system touches hiring, lending, credit scoring, or workplace monitoring, you're classified as high-risk under the Act. ISO 42001 certification maps directly to EU AI Act obligations around risk assessment, documentation, transparency, and human oversight. Getting certified now puts you ahead of the deadline rather than scrambling to meet it.

Investor due diligence

VCs and PE firms are asking portfolio companies about AI governance. ISO 42001 is the clearest signal that your organization takes AI risk seriously. It's showing up in due diligence checklists alongside SOC 2 and ISO 27001.

> **The bottom line:** The companies getting certified now are doing it proactively, before their buyers force the issue. The companies that wait will be doing it reactively, on a compressed timeline, at a premium.

02

What Carries Over from ISO 27001

Both standards use the ISO Harmonized Structure (Annex SL). Your management system foundation carries over. Here's what you can reuse directly or with minor modifications:

ISO 27001 Element	42001 Equivalent	Effort
Information Security Policy	AI Policy (extend scope to cover AI)	Modify
Risk Assessment Process	AI Risk Assessment (new risk criteria needed)	Modify

Risk Treatment Methodology	AI Risk Treatment (AI-specific treatments)	Modify
Internal Audit Program	Same process, expanded to include AIMS	Reuse
Management Review	Same process, add AI-specific inputs	Reuse
Document Control	Same requirements apply	Reuse
Competence / Training	AI-specific competence requirements added	Extend
Corrective Actions	Same process	Reuse
Statement of Applicability	New SoA for Annex B (AI-specific controls)	New

> **Key distinction:** Clauses 4-10 (the management system structure) carry over. Annex A controls (information security) do not map directly to Annex B controls (AI-specific). That's where the new work lives.

Roughly 30-40% of the total certification effort is reduced by having ISO 27001 in place. That's meaningful, but it means 60-70% of the work is still ahead of you.

03

What's Net-New

These are the areas where ISO 27001 gives you no head start. This is where companies underestimate the work.

AI Management System (AIMS)

ISO 42001 requires a dedicated AI Management System. This is not an extension of your ISMS. The AIMS has its own scope, its own policy, and its own risk treatment plan specific to AI systems. The two systems integrate and share infrastructure, but auditors will verify the AIMS has independent substance.

AI Impact Assessment

This is the single biggest new requirement. You must assess the potential impact of each AI system on individuals, groups, and society — before deployment and on an ongoing basis. This goes well beyond information security risk. It covers bias, fairness, transparency, human oversight, and societal impact.

Annex B: AI-Specific Controls

Annex B contains AI-specific controls with no equivalent in ISO 27001. Key areas include:

Control Area	What It Covers	Key Controls

AI System Lifecycle	Development, testing, deployment, monitoring, and decommissioning	Design docs, validation, deployment procedures
Data for AI Systems	Data acquisition, quality, labeling, provenance, governance	AI05: Data governance
AI Impact Assessment	Consequences of AI decisions on individuals and society	AI03: Impact assessment
AI Documentation	System behavior, decisions, design rationale, performance	AI07: Traceability
Third-Party AI	Risk from AI components, APIs, models, services from vendors	AI10: Supply chain mgmt

Documentation requirements

ISO 42001 requires documented evidence for: a complete AI system inventory, impact assessments for each in-scope system, AI risk treatment plans, lifecycle documentation from design through decommissioning, data provenance and quality records, and third-party AI component assessments.

Companies that breeze through 27001 documentation often stall here. Most organizations don't have structured records of how their AI systems were designed, trained, tested, and deployed.

04

What Auditors Actually Look For

Certification body auditors approach ISO 42001 differently than ISO 27001. Here's what we've seen auditors focus on during Stage 2 assessments:

AI system inventory completeness

Auditors will ask for a complete inventory of AI systems in scope. If you can't produce one quickly, or if they find AI systems in your environment that aren't on the list, that's a nonconformity. They want to see that you know what AI you're running and where.

Impact assessment depth

Shallow impact assessments are the most common finding. Auditors want to see that you've genuinely assessed impact on individuals, not just checked boxes. If your AI system makes decisions affecting people (hiring, lending, access, recommendations), the impact assessment needs to reflect that specificity.

AIMS independence from the ISMS

Auditors check that your AI Management System has its own substance and isn't just your ISMS with "AI" added to the headers. They'll look for AI-specific policy language, AI-specific risk criteria, and AI-specific treatment plans that go beyond information security.

Evidence of ongoing monitoring

42001 isn't point-in-time. Auditors want evidence that you're continuously monitoring AI system performance, reviewing impact assessments when systems change, and updating risk treatments. A

governance program that was built for the audit but isn't being maintained will not pass surveillance audits.

Third-party AI management

If you use third-party AI models, APIs, or services (and most companies do), auditors will look for evidence that you've assessed the risks those third parties introduce. This includes how you evaluate vendor AI practices, what contractual controls you require, and how you monitor third-party AI behavior in production.

> **The pattern:** Companies that struggle in audits are the ones that treated 42001 as a documentation exercise. Auditors are looking for evidence that your AI governance program is real and operational, not just a set of policies that sit in a SharePoint folder.

05

Self-Assessment: How Ready Are You?

Answer these 10 questions honestly. Every "no" represents a gap between where you are and ISO 42001 certification.

01	Do you have a complete, documented inventory of every AI system your organization operates or uses?	☐ Yes ☐ No
02	Have you conducted a formal impact assessment for each AI system that evaluates effects on individuals and society — not just information security risk?	☐ Yes ☐ No
03	Do you have an AI-specific policy that is separate from (but integrated with) your information security policy?	☐ Yes ☐ No
04	Do you have a defined AI risk assessment process with risk criteria that go beyond confidentiality, integrity, and availability?	☐ Yes ☐ No
05	Can you produce lifecycle documentation for each AI system — from design and training through deployment and monitoring?	☐ Yes ☐ No
06	Do you have documented data governance practices for AI training data, including provenance, quality controls, and labeling standards?	☐ Yes ☐ No
07	Have you assessed the AI-specific risks introduced by third-party AI models, APIs, or services you use?	☐ Yes ☐ No
08	Do you have defined competence requirements for personnel involved in AI system development, deployment, and governance?	☐ Yes ☐ No
09	Is there an ongoing monitoring process for AI system performance, bias, and impact — not just a point-in-time assessment?	☐ Yes ☐ No

10	Could you demonstrate all of the above to an external auditor within two weeks?	☐ Yes ☐ No

Your Score	What It Means
8-10 Yes	You're close. A gap assessment confirms readiness and identifies final gaps. Expect 2-4 months to certification.
4-7 Yes	You have a foundation but significant work remains. Most ISO 27001 companies land here. Expect 4-6 months.
0-3 Yes	Your AI governance program needs to be built, not just extended. Expect 6-12 months, but having ISO 27001 still saves you time on the management system foundation.

06

Realistic Timeline

For companies with a mature ISO 27001 program:

Phase	Duration	What Happens
Gap Assessment	2-3 weeks	Map existing controls to 42001, identify gaps, scope the AIMS, build remediation roadmap
AIMS Build	6-10 weeks	AI policy, risk framework, impact assessments, Annex B controls, documentation
Internal Audit	2 weeks	Audit AIMS against 42001, identify nonconformities, remediate
Management Review	1 week	Leadership review of AIMS effectiveness, risk status, audit results
Stage 1 Audit	1-2 weeks	Certification body reviews documentation, confirms readiness
Stage 2 Audit	1-2 weeks	Implementation audit: interviews, evidence review, effectiveness assessment

> **Total for ISO 27001 companies:** 3-6 months from kickoff to certification. The variable is the AIMS build phase. Companies with well-documented AI systems move faster. Companies that haven't inventoried their AI usage take longer.

Starting from scratch with no ISO 27001? Add 3-6 months for the management system foundation. Some organizations pursue both certifications simultaneously through an integrated management system.

07

Your Next Step

Every company's path to ISO 42001 is different. The gap between where you are and where you need to be depends on your existing certifications, how your AI systems are documented, and what your stakeholders are requiring.

We offer a free 30-minute gap assessment call to review your current posture, identify your specific gaps, and give you a realistic timeline.

Book a Free Gap Assessment Call

30 minutes. No obligation. We tell you exactly where you stand and what it takes to get certified.

calendly.com/travis-atlasaigovernance/30min

travis@atlasaigovernance.com

atlasaigovernance.com