Why Should ISO/IEC 27001 Certified Organizations Also Look to Pursue ISO/IEC 42001?

Artificial Intelligence (AI) is now embedded in how organizations operate – driving decisions, processing data and shaping outcomes. But **AI introduces risks that go far beyond information security: bias, lack of transparency, ethical impact** and lifecycle accountability.

ISO/IEC 27001 secures your data.

ISO/IEC 27001 is a starting point for information security, one that should be built on.

ISO/IEC 42001 governs your AI.

ISO/IEC 42001 is the international management system standard for AI. It governs how AI systems use information, make decisions, and create impact, providing a structured framework for organizations that produce, provide, or use AI systems.

The Scope of Certification Is Not the Same

ISO/IEC 27001 and ISO/IEC 42001 are **harmonized approach management system standards**, each with a specific focus.

	ISO/IEC 27001	ISO/IEC 42001
Focus	Governance of information security and cyber risks	Governs how AI systems are developed, deployed, and managed and used
Covers	Risk management, cyber resilience and operational excellence in information security	Bias, transparency, societal impact, lifecycle accountability and intended use
Scope	Defines which information assets are in scope and ensures the appropriate level of confidentiality, integrity and availability	Defines which AI systems, components and roles are included

What this means:

A separate scope statement is needed:
Your ISO/IEC 27001 scope does not automatically extend to AI governance.

AI systems and assets must be identified:
Models, datasets, pipelines, and decision processes all fall within scope.

Coverage extends across AI roles:
Whether you produce, provide, or use AI, each role carries distinct responsibilities.

ISO/IEC 27001 protects your information.
ISO/IEC 42001 governs how your AI processes and uses it.

Establishing Clear AI Governance and Accountability

AI governance is a critical organizational responsibility, not solely an IT issue. Today, **AI oversight is often fragmented** across functions without unified leadership, **increasing risks and accountability gaps.**

ISO/IEC 42001 addresses this directly by providing:

- ☑ Defined roles and responsibilities for AI management across every level of the organization
- ☑ Documented decision-making ensuring traceability and accountability for every AI system
- ☑ Clear purpose and scope to define intended use, prohibited use and decision rights
- ☑ Cross-functional alignment connecting IT, legal, compliance, and operations under one governance model
- ☑ Board-level visibility into AI risks through structured enterprise risk frameworks

This framework enables **informed leadership decisions, outlines clear ownership, and builds lasting confidence** with regulators, customers, and stakeholders alike.

Confident Compliance in an Evolving Regulatory Landscape

AI regulation is **rapidly evolving globally.**

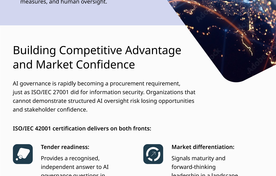
EU AI Act:
The world's first comprehensive AI law. It classifies AI systems by risk level and imposes strict requirements on high-risk applications, including conformity assessments, transparency obligations, and human oversight mandates.

United States:
Executive orders, the NIST AI Risk Management Framework, and growing state-level legislation are building a patchwork of requirements that organizations must navigate.

United Kingdom:
A sector-led, principles-based approach. Regulators such as the FCA, ICO, and Ofcom are embedding AI expectations into existing frameworks.

Global momentum:
Canada, Brazil, Singapore, China, and others are advancing their own AI governance frameworks. Multinational organizations face a complex and evolving compliance landscape.

The standard does not guarantee compliance with any single regulation. But it provides **the management system foundation** that most regulations expect: documented risk assessments, defined controls, transparency measures, and human oversight.



Building Competitive Advantage and Market Confidence

AI governance is rapidly becoming a procurement requirement, just as ISO/IEC 27001 did for information security. Organizations that cannot demonstrate structured AI oversight risk losing opportunities and stakeholder confidence.

ISO/IEC 42001 certification delivers on both fronts:

Tender readiness:
Provides a recognised, independent answer to AI governance questions in procurement processes

Market differentiation:
Signals maturity and forward-thinking leadership in a landscape where most organizations are still catching up

Stakeholder assurance:
Gives customers, investors, and partners independently verified evidence of responsible AI practices

Future-proofed positioning:
Establishes the governance foundation now, before certification becomes a baseline expectation

Trust is earned before scrutiny arrives. Certification protects both **competitive position and reputation.**

Accelerating Innovation Through Structured Governance

Without governance, organizations face two risks simultaneously. Externally, AI incidents **damage reputations rapidly.** Internally, **uncertainty creates paralysis.** Leaders delay approvals, teams operate without shared standards, and high-potential projects stall indefinitely.

ISO/IEC 42001 solves both problems through one unified framework:

Pre-deployment risk assessments:
Potential harms are identified and addressed before systems go live

Human oversight mechanisms:
Critical AI decisions include defined checkpoints for human judgement

Ongoing performance monitoring:
Systems are continuously evaluated for accuracy, fairness, and behavioural drift

End-to-end lifecycle management:
Every phase, from design to decommissioning, follows structured, repeatable processes

Data Governance:
Provenance, quality, representativeness and privacy

Proportionate controls:
Governance scales with risk; streamlined for routine applications, rigorous for high-stakes systems

The outcome is clear: **organizations with embedded AI governance move faster, not slower.** Innovation accelerates because the difficult questions are resolved upfront, not mid-crisis.

Your Journey to Trusted AI Starts Here

Responsible AI demands more than ambition. It demands structure. ISO/IEC 42001 provides the framework. BSI provides the pathway.

Four steps to certification:

1. **Get the standard:**
   Obtain the ISO/IEC 42001standard and understand the requirements.
2. **Build capability:**
   Enrol in BSI's dedicated ISO/IEC 42001 training courses.
3. **Assess readiness:**
   Undertake a pre-certification assessment to identify gaps.
4. **Achieve certification:**
   BSI can audit your organization to ISO/IEC 42001. We are the first certification body to achieve triple accreditation for ISO/IEC 42001, with accreditation from UKAS, RvA, and ANAB.

Let's work together on trusted and responsible AI.

Harness the full power of AI and reassure stakeholders of your responsible development and use of AI systems, with ISO/IEC 42001.

Click here to start your journey today