

5 Steps to Achieve ISO 42001 Compliance

Quick Start Guide

Why ISO 42001 Compliance Matters Now

ISO 42001 compliance is crucial as AI becomes more embedded in business processes. The standard provides a framework for managing AI responsibly, covering key requirements for the safe development and use of AI technologies. By following the seven clauses that outline how to establish and maintain an Artificial Intelligence Management System (AIMS), companies can show their commitment to ethical AI practices. Annex A further supports this with controls to meet the requirements. As AI regulations evolve, ISO 42001 compliance helps organizations manage risks, build trust, and stay compliant with emerging standards.

The adoption of AI in businesses is rapidly increasing, but consumer concerns have drawn the attention of legal and regulatory bodies seeking to regulate high-risk AI systems. ISO 42001 establishes requirements for responsible AI and data management, addressing key concepts such as ethical use, fairness, bias, and trustworthiness. It helps organizations enhance the quality, security, and reliability of AI systems while ensuring ethical development and use.

The AI market size is expected to reach **\$1,339 billion** by 2030

72% of business have already adopted AI for at least one business function

Over **75% of consumers** are concerned about misinformation from AI

Key Benefits of ISO 42001



Validates AI Management: Provides organizations with independent corroboration that AI systems are being managed ethically and responsibly.



Enhances Trust with Stakeholders: Demonstrates an organization's commitment to both responsible AI practices and ethical, transparent, and accountable AI development and usage.



Enhances Risk Management: Can aid in the improved identification and mitigation of risks associated with AI, as the process and required lifecycle helps ensure organizations identify and address potential ethical, security, and compliance issues proactively; and to help ensure organizational objectives are consistently met.



Competitive Advantage / Market Differentiator: Currently, ISO 42001 is the only certifiable standard which allows organizations to gain an edge in the market and signal to clients, partners, and regulators that responsible AI usage is a priority.

Five Essential Steps to Achieve ISO 42001 Compliance

1. Understanding the Requirements of ISO 42001

This step is often overlooked but is crucial when starting the compliance journey. Begin by familiarizing yourself with the standard's seven clauses and Annex A, which lists controls to meet AI management objectives. Annex B offers guidance for implementing these controls, while Annex C outlines potential AI-related objectives and risk sources. Annex D provides insights into applying an AI Management System (AIMS) across different sectors.

2. Determining the Scope of the Certified AIMS

Define the boundaries of your AIMS to establish its focus. Consider key questions:

- What AI capabilities have we implemented?
- Are we developing AI or using off-the-shelf models?
- Do we design and deploy AI systems, or just use AI in business processes?
- How many people are involved in the AI lifecycle?

3. Establishing an AI Management System (AIMS)

Once you understand the requirements and scope, the next step is setting up the necessary policies, procedures, systems, and personnel to manage the AIMS.

3A. Performing a Readiness Assessment (Optional)

While not mandatory, a readiness assessment helps identify any gaps in meeting ISO 42001 requirements. The effort needed depends on your existing systems and controls.

4. Selecting a Certification Body

Choose a certification body that meets your needs. Accredited bodies are evaluated for competence and consistency, but non-accredited bodies can also be reputable.

5. Undergoing an ISO 42001 Certification Review

The certification audit follows a familiar two-stage process:

- Stage 1: Reviews AIMS design effectiveness.
- Stage 2: Evaluates operational effectiveness and Annex A controls.

Nonconformities must be addressed before certification is granted. Once issued, the certification is valid for three years, with annual surveillance reviews to ensure ongoing effectiveness and incorporation of any changes.

Secuvy's Data Classification Technology Supports ISO 42001 Compliance

Secuvy's Data Classification solution enables assessors to effectively evaluate an organization's risk management practices within their Artificial Intelligence Management System (AIMS). Our goal is to streamline the audit process, allowing businesses to quickly identify potential gaps or areas of concern in their data handling practices. Comprehensive reports provide the necessary documentation for data quality, integrity, and bias mitigation, helping organizations meet compliance

requirements for the EU AI Act, NIST RMF, and HITRUST.

Secuvy's technology supports on these ISO 42001 controls.

- Data Resources Documentation (A.4.3)
- Data Considerations (A.7)
- Data Acquisition (A.7.3)
- Data Quality (A.7.4)
- Data Provenance (A.7.5)
- Data Preparation (A.7.6)

For more information on Secuvy email at info@secuvy.com

For more information on Schellman reach out at [contact us](#)

About Schellman

Schellman is a leading provider of attestation and compliance services. We are a globally licensed PCI Qualified Security Assessor, an ISO Certification Body, HITRUST CSF Assessor, and a FedRAMP 3PAO. Renowned for expertise tempered by practical experience, Schellman's professionals provide superior client service balanced by steadfast independence. Our approach builds successful, long-term relationships and allows our clients to achieve multiple compliance objectives through a single project team.

About Secuvy

Secuvy makes data protection easy, efficient, and trusted with a next-generation privacy, data security, and AI data governance platform. The self-learning AI automates the inventory of any type of data, in any format, in any environment, at record speed and highest accuracy in the market. The era of AI governance is here.