

Coalfire ISO/IEC 42001 Readiness Assessment Checklist

What is ISO 42001?

With the global AI market set to grow by 38% in 2025 ([Teneo](#)), adapting to and understanding AI is no longer just a helpful additive to your business, but a critical move to allow your company to stay up to date.

However, with the rapid development of diverse AI-powered products and services, there's been a growing need to establish regulatory frameworks for adopting AI responsibly.

ISO/IEC 42001:2023 — or simply ISO 42001 — is the first international, certifiable standard focusing on the governance of an Artificial Intelligence Management System (AIMS). AIMS refers to the interconnected set of policies and procedures that contribute to the oversight function necessary for regulating AI applications. The primary purpose of ISO 42001 is to help organizations build a structured management system and demonstrate trust among customers through the ethical and transparent use, development, deployment, and upkeep of AI systems.



This readiness checklist helps assess your current state, identify gaps, and guide your path toward certification.

Step 1: Understand the Standard and Define the Scope

- ☐ **Acquire and study ISO 42001 and related AI standards:**
 - ISO 42001 – AIMS Standard
 - ISO/IEC 22989:2022 – AI Concepts and Terminology
 - ISO/IEC 23894:2023 – AI Risk Management
 - ISO/IEC 5338:2023 – AI System Lifecycle Processes
 - ISO/IEC 42005 – AI Impact Assessment (Not Yet Published)
 - ISO/IEC TR 24368:2022 – Ethical and Societal Concerns
- ☐ **Define the scope of your AIMS**
- ☐ **Determine your AI role: customer, provider, developer, or producer**
- ☐ **Familiarize stakeholders with the AI lifecycle and governance principles**
- ☐ **Secure executive sponsorship and leadership alignment**
- ☐ **Conduct a baseline gap analysis/readiness assessment (internal or with Coalfire Certification)**
- ☐ **Present the business case for certification**

Step 2: Build Your AIMS Framework

- ☐ Appoint a project lead and assemble a cross-functional team
- ☐ Create a project roadmap with clear milestones
- ☐ Align AIMS with existing management systems (e.g. ISO 27001, ISO 31000)
- ☐ Define and document AI policies and acceptable use protocols
- ☐ Develop a Statement of Applicability (SOA)
- ☐ Conduct an AI impact and risk assessment
- ☐ Implement ISO 42001 Annex A controls:
- ☐ Train internal teams on AI risks and governance
- ☐ Document all resource and tooling requirements for AI systems

Step 3: Implement Controls and Validate Performance

- ☐ Launch organization-wide AIMS policy and reporting structure
- ☐ Establish data governance controls specific to AI
- ☐ Ensure system transparency for users and stakeholders
- ☐ Conduct internal audits and address nonconformities
- ☐ Hold executive-level reviews of AIMS effectiveness
- ☐ Centralize documentation with secure access controls

Step 4: Prepare for Certification

- ☐ Select a certification partner (e.g., Coalfire Certification)
- ☐ Finalize audit scope and timeline
- ☐ Designate a point of contact for auditors
- ☐ Designate a point of contact for auditors
- ☐ Ensure audit artifacts are current and accessible
- ☐ Conduct audit simulations and walkthroughs

Step 5: Post-Certification – Continuous Improvement

- ☐ Form a continuous improvement team
- ☐ Define and monitor AIMS KPIs
- ☐ Maintain a corrective action process
- ☐ Re-assess AI technologies and update documentation regularly
- ☐ Stay informed through:
 - Additional ISO AI Standards Roadmap
 - OECD AI Policy Observatory
 - [NIST AI Risk Framework](#)

Why Coalfire?

At Coalfire, we help organizations lead with trust.

As one of the most trusted cybersecurity and compliance advisors to modern enterprises and cloud providers, Coalfire brings deep expertise in complex frameworks like ISO 27001/9001, SOC, HITRUST, FedRAMP, and now ISO 42001. With decades of experience in regulated industries and a pulse on emerging tech risks, we guide you through the process to certify your AIMS.

Here's why Coalfire is the ideal partner:

- ☑ **Proven success with enterprise compliance and AI governance frameworks**
- ☑ **Cross-disciplinary expertise in cloud, privacy, security, and ethical AI**
- ☑ **Deep familiarity with ISO frameworks and pre-certification readiness assessments**
- ☑ **A collaborative, strategic approach that aligns AIMS with your business goals**

Coalfire doesn't just help you meet ISO 42001 standards—we help you lead the market in responsible AI innovation.