Sensiba

GUIDE

ISO/IEC 42001: Readiness Checklist

Table of Contents

OVERVIEW

Introduction

The ISO/IEC 42001 standard offers guidance and controls to help organizations deploy AI efficiently, and mitigate related security and governance risks, by developing an Artificial Intelligence Management System (AIMS).

The standard is guided by core concepts, including ensuring an organization develops, implements, and manages its AI tools using principles such as transparency, accountability, fairness, explainability, data privacy, and reliability. The standard also emphasizes the integration of AI management with organizational processes, and requires systematic approaches to identifying and mitigating risks throughout the AI lifecycle.

ISO/IEC 42001 is designed to be adaptable to various organizations' needs and use cases, allowing for flexibility in implementation while adhering to core principles of AI governance.

A successful ISO/IEC 42001 audit depends on several steps, starting with careful preparation that includes extensive policy creation and documentation.

We've prepared the following readiness checklist to provide an overview of the audit process, the documents you'll need to prepare, and the steps you can expect. Following the checklist will help you develop a comprehensive plan for the audit and ensure your organization's alignment with the standard's requirements. As a first step, be sure to purchase the standard here.

Note: *This checklist should not be considered a comprehensive guide to ISO/IEC 42001 audit planning. For a deeper dive into ISO/IEC 42001 and its requirements, contact us.*

What Is ISO/IEC 42001?

The standard, published in 2023, addresses the AI system lifecycle from initial concepts to final system deployment and operations. ISO/IEC 42001 is designed to help organizations manage the risks associated with AI and ensure their systems are developed and used responsibly.

ISO/IEC 42001 compliance should be considered by any organization with public-facing products or services leveraging AI.

To evaluate compliance with the standard, an ISO/IEC 42001 certification audit will examine several areas, including AI-specific ethical, security, and operational considerations, system lifecycle management, performance optimization, and documentation.

ISO/IEC 42001 does not offer prescriptive implementation guidance. The standard provides a flexible framework for AI governance rather than detailed requirements. The standard outlines general principles and key components for managing AI systems but allows organizations to adapt the implementation to their specific context, risks, and needs.

RELATED ISO STANDARDS

In addition to ISO/IEC 42001, several standards reference artificial intelligence and various aspects of management systems, data quality, risk management, and governance. Some of the key standards include:

- ISO/IEC 42005, AI System Impact Assessment
- ISO/IEC 23894, AI Risk Management
- ISO/IEC 38507, Governance Implications of AI
- ISO/IEC 22989, Common-language definitions of AI-related terminology
- ISO/IEC 23053, Framework for describing generic AI systems
- ISO/IEC 5259-3, Data quality management requirements for analytics and machine learning

How Long Does ISO/IEC 42001 Certification Take?

The ISO/IEC 42001 audit process typically occurs over several months. Here is an overview of the main phases:

PRE-AUDIT (MONTHS 1-4)

- Define AIMS scope.
- Perform AI impact assessment and gap analysis.
- Design and implement policies and controls.
- Document processes and collect evidence.
- Conduct internal audit and remediation.

POST-CERTIFICATION (MONTHS 9+)

- Monitor AIMS effectiveness.
- Conduct annual internal audit and remediation.
- Undergo annual surveillance audits in years 1 and 2.
- Complete recertification audit prior to end of 3-year certification period.

CERTIFICATION AUDIT (MONTHS 5-8)

Stage 1: Review (Month 5)

- Auditor reviews AIMS documentation and design.
- Existence of key components such as Statement of Applicability (SoA), Impact Assessment, Internal Audit, etc.

Stage 2: Certification (Months 6-8)

- Auditor assesses security controls and business processes.
- Organization receives ISO/IEC 42001 certification (valid for 3 years).

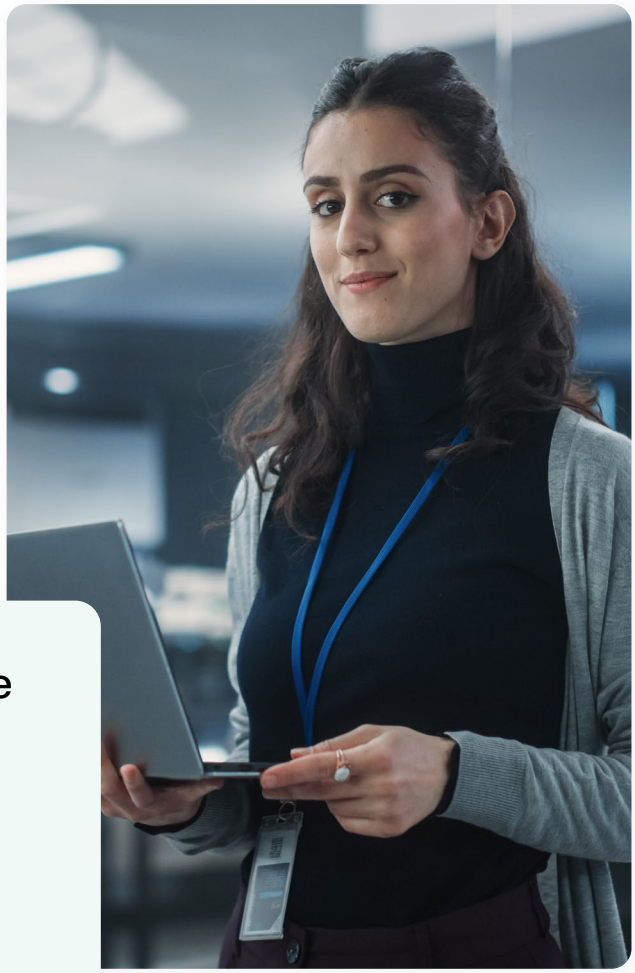
Understanding the ISO/IEC 42001 Standard

The ISO/IEC 42001 standard contains 10 clauses outlining the requirements for the management system. The clauses provide guidance for aligning AI initiatives with business objectives, stakeholder expectations, and regulatory requirements.

The first three clauses provide an overview of the standard including general information, the standard's scope, references, and terms and definitions. They also set the context for the requirements outlined in Clauses 4-10.

The mandatory clauses outline requirements in the following categories:

- Clause 4: Context of the Organization
- Clause 5: Leadership
- Clause 6: Planning
- Clause 7: Support
- Clause 8: Operation
- Clause 9: Performance Evaluation
- Clause 10: Improvement



Annex A provides a comprehensive set of 38 optional reference control objectives and controls to help organizations manage AI system risks and achieve business objectives.

CLAUSES 4-10 (MANDATORY)

4 - Context of the Organization

- [ ] Identify external and internal issues relevant to the organization's purpose. (Clause 4.1)
- [ ] Understand the needs and expectations of interested parties. (Clause 4.2)
- [ ] Determine the scope of the AI management system (AIMS). (Clause 4.3)
- [ ] Establish, implement, maintain, continually improve, and document an AI management system. (Clause 4.4)

5 - Leadership

- [ ] Ensure top management demonstrates leadership and commitment to the AIMS. (Clause 5.1)
- [ ] Establish an information security policy. (Clause 5.2)
- [ ] Define and communicate roles, responsibilities, and authorities. (Clause 5.3)

6 - Planning

- [ ] Address risks and opportunities. (Clause 6.1)
- [ ] Define and establish an AI risk assessment process. (Clause 6.1.2)
- [ ] Define and establish an AI risk treatment process. (Clause 6.1.3)
- [ ] Produce a Statement of Applicability: controls and justification for inclusion/exclusion. (Clause 6.1.3.f)
- [ ] Define a process for assessing the potential consequences of AI systems. (Clause 6.1.4)
- [ ] Establish AI relevant objectives. (Clause 6.2)
- [ ] Define a process for planning and implementing changes. (Clause 6.3)

7 - Support

- [ ] Provide necessary resources for the AIMS. (Clause 7.1)
- [ ] Ensure personnel competence. (Clause 7.2)
- [ ] Ensure awareness about information security policies and procedures. (Clause 7.3)
- [ ] Establish internal and external communication protocols. (Clause 7.4)
- [ ] Documented information. (Clause 7.5)
- [ ] Document information required by the standard and the organization. (Clause 7.5.1)
- [ ] Create and update documented information. (Clause 7.5.2)
- [ ] Control documented information. (Clause 7.5.3)

8 - Operation

- [ ] Plan, implement, and control required processes. (Clause 8.1)
- [ ] Assess AI risks regularly or when system changes. (Clause 8.2)
- [ ] Implement and assess the AI risk treatment plan. (Clause 8.3)
- [ ] Perform AI system impact assessments regularly or when system changes. (Clause 8.4)

9 - Performance Evaluation

- [ ] Monitor, measure, analyze, and evaluate the AIMS performance. (Clause 9.1)
- [ ] Conduct internal audit. (Clause 9.2)
- [ ] Conduct Management Review. (Clause 9.3)

10 - Improvement

- [ ] Continually improve the AIMS. (Clause 10.1)
- [ ] Manage nonconformities and take corrective actions. (Clause 10.2)

ANNEX A: REFERENCE CONTROL OBJECTIVES AND CONTROLS

2 - Policies related to AI

- [ ] AI policy (Annex A 2.2)
- [ ] Alignment with organizational policies (Annex A 2.3)
- [ ] Review of the AI policy (Annex A 2.4)

3 - Internal organization

- [ ] AI roles and responsibilities (Annex A 3.2)
- [ ] Reporting of concerns (Annex A 3.3)

4 - Resources for AI systems

- [ ] Resource documentation (Annex A 4.2)
- [ ] Data resources (Annex A 4.3)
- [ ] Tooling resources (Annex A 4.4)
- [ ] System and computing resources (Annex A 4.5)
- [ ] Human resources (Annex A 4.6)

5 - Assessing impacts of AI systems

- [ ] AI system impact assessment process (Annex A 5.2)
- [ ] Documentation of AI system impact assessments (Annex A 5.3)
- [ ] Assessing AI system impact on individuals or groups of individuals (Annex A 5.4)
- [ ] Assessing societal impacts of AI systems (Annex A 5.5)

6 - AI system lifecycle

- [ ] Management guidance for AI system development (Annex A 6.1)
- [ ] Objectives for responsible development of AI system (Annex A 6.1.2)
- [ ] Processes for responsible AI system design and development (Annex A 6.1.3)
- [ ] AI system lifecycle (Annex A 6.2)
- [ ] AI system requirements and specification (Annex A 6.2.2)
- [ ] Documentation of AI system design and development (Annex A 6.2.3)
- [ ] AI system verification and validation (Annex A 6.2.4)
- [ ] AI system deployment (Annex A 6.2.5)
- [ ] AI system operation and monitoring (Annex A 6.2.6)
- [ ] AI system technical documentation (Annex A 6.2.7)
- [ ] AI system recording of event logs (Annex A 6.2.8)

7 - Data for AI systems

- [ ] Data for development and enhancement of AI system (Annex A 7.2)
- [ ] Acquisition of data (Annex A 7.3)
- [ ] Quality of data for AI systems (Annex A 7.4)
- [ ] Data provenance (Annex A 7.5)
- [ ] Data preparation (Annex A 7.6)

8 - Information for interested parties of AI systems

- [ ] System documentation and information for users (Annex A 8.2)
- [ ] External reporting (Annex A 8.3)
- [ ] Communication of incidents (Annex A 8.4)
- [ ] Information for interested parties (Annex A 8.5)

9 - Use of AI systems

- [ ] Processes for responsible use of AI systems (Annex A 9.2)
- [ ] Objectives for responsible use of AI (Annex A 9.3)
- [ ] Intended use of the AI system (Annex A 9.4)

10 - Third-party and customer relationships

- [ ] Allocating responsibilities (Annex A 10.2)
- [ ] Suppliers (Annex A 10.3)
- [ ] Customers (Annex A 10.4)

Additional Considerations

While an ISO/IEC 42001 audit can be a detailed process, the following suggestions will help you increase the efficiency of the audit while reducing the potential for interruptions to your teams and their daily functions. Here are some key tips and best practices to make ISO/IEC 42001 audits easier:

- ☐ Document everything thoroughly. Maintain clear, up-to-date documentation of your AIMS, policies, procedures, and controls.
- ☐ Conduct regular internal audits and management reviews to address any issues before the external audit.
- ☐ Perform a comprehensive impact assessment and create an appropriate treatment plan. This is crucial to ISO/IEC 42001 compliance.
- ☐ Familiarize employees with the ISO/IEC 42001 process and their roles.
- ☐ Appoint an ISO manager or representative to oversee the certification process and provide a central contact for your auditor.
- ☐ Create a central hub to store and share audit-related tasks, requests, and evidence.
- ☐ Consider the use of a GRC platform for storing and sharing documents.
- ☐ Automate task assignments and evidence collection where possible.
- ☐ Monitor audit preparation and progress using dashboards and reporting features.
- ☐ Collaborate closely with auditors, providing them access to relevant information in a controlled environment.
- ☐ Maintain a comprehensive risk registry to track and prioritize identified risks. Continue to maintain and monitor your AIMS after passing the audit.

Common Mistakes to Avoid

As companies undergo or prepare for an ISO/IEC 42001 audit, there are some common mistakes that leaders should keep an eye out for:

- Inadequate preparation and planning
- Incorrect scope definition
- Vague language in documentation that can create confusion
- Lack of management commitment and involvement, or not allocating necessary resources
- Poor documentation and record-keeping
- Staff not following established processes and procedures
- Failing to update risk assessments or treatments to address new or evolving threats
- Insufficient employee training and awareness
- Not conducting regular internal audits to identify issues before certification audits
- Trying to conduct an internal audit with inexperienced personnel
- Failing to maintain standards after certification

By being aware of these common pitfalls, organizations can better prepare for their ISO/IEC 42001 audits and improve their chances of a successful certification process.

Conclusion

Careful planning and consistent documentation are among the key steps to planning for an ISO/IEC 42001 certification or recertification audit. Understanding the standard's requirements, identifying and mitigating applicable risks, developing a realistic timeline, and creating accurate documentation are among the important steps in getting your organization ready for this important milestone.

Above all, be sure your plans include an in-depth internal audit conducted by a competent, experienced, and independent internal auditor. This is the best predictor of success during the certification audit. In many cases, an internal audit is conducted by a third party to ensure objectivity and provide an unbiased perspective.

By following the steps outlined in this checklist, you can increase customer trust, enhance information security, improve regulatory compliance, and highlight your commitment to security with ISO/IEC 42001 certification.

About Sensiba

Whether you're a venture-backed start-up or a public company, we're here to help you through your ISO certification. Sensiba is ANAB-accredited, and our in-house team is composed of experienced auditors who carry relevant professional designations, including Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), and Certified Cloud Security Professional (CCSP). Additionally, our ISO auditors hold the ISO/IEC 27001:2022, 27701:2019 and 42001:2023 Lead Auditor designations.

Contact Us