Vanta | A-LIGN

The ISO 42001 Compliance Checklist

The ISO 42001 Compliance Checklist

As AI (artificial intelligence) companies and the adoption of their technologies grows, so does the need for ethical governance due to the inherent risks of these technologies. The ISO 42001 framework addresses these risks by defining the requirements of an Artificial Intelligence Management System (AIMS), which helps organizations demonstrate their commitment to responsible development and usage of AI.

By educating your organization on the requirements for ISO 42001 and using an automated compliance software, you can set your organization up for success. This ISO 42001 compliance checklist helps to lay the foundation for what your organization should expect when working towards certification.

STEP 1

Pre-work for your ISO 42001 compliance

Understand ISO 42001 requirements

- □ Decide on what is the scope of the AIMS
- □ Familiarize yourself with key AI concepts, principles, and lifecycle based on ISO frameworks
- □ Determine if you are a provider, developer, or user of AI systems

Perform initial gap analysis

- □ Using Vanta, asses your in-scope ISO 42001 controls
- □ Identify areas of requirement, development, or adjustment

Secure top management support

- □ Present a business case highlighting the benefits of ISO 42001 certification
- □ Define roles and responsibilities for top management in AIMS implementation
- □ Involve various department heads in the analysis to ensure comprehensive coverage

STEP 2

Work for your ISO 42001 compliance

Appoint a Project Manager

- □ Designate an owner for the ISO 42001 implementation project

Develop a project plan

- □ Outline steps, timelines, and resources needed for AIMS implementation
- □ Integrate the AIMS implementation project within existing organizational processes

Establish the AIMS framework

- □ Define the scope and objectives of the AIMS within the organization
- □ Develop and document AI policies and risk management processes
- □ Based on gap analysis, implement necessary controls for AIMS
- □ Ensure integration of AIMS with other management systems and requirements
- □ Create an AIMS statement of applicability (SOA)

Promote competence and awareness

- □ Conduct training for stakeholders on AI concepts and ISO 42001 requirements
- □ Raise awareness about the importance and benefits of AIMS

Implement AIMS controls

- □ Create an AI policy
- □ Define the process for reporting concerns about AI systems
- □ Identify, document, and manage resources for AI systems
- □ Ensure tooling and computing resources for AI systems are adequately documented
- □ Conduct an AI system impact assessment exercise
- □ Ensure that objectives are documented for the design and development of AI systems
- □ Create a process for responsible design and development of AI systems
- □ Ensure that AI system deployment, operation, and monitoring are documented and executed according to your AIMS
- □ Define and implement data management processes for AI systems
- □ Assess and document the quality of data for AI systems
- □ Ensure that system documentation and information for users is provided and accessible
- □ Document and follow the processes for the responsible use of AI systems
- □ Clearly allocate and document responsibilities with third parties

Conduct internal audits

- □ Regularly assess compliance with ISO 42001 and the effectiveness of AIMS

Management review

- □ Review AIMS performance and compliance with top management
- □ Address any non-conformities and areas for improvement

STEP 3

Prepare for your external audit

Work with A-LIGN as your ISO 42001 certification body

- □ Engage A-LIGN, a leading ISO certification body, to conduct your audit

Prepare documentation

- □ Ensure all AIMS documentation is up-to-date and accessible

Pre-audit meeting

- □ Prepare a list of questions and clarifications regarding the audit process

Initial sales process

- □ Discuss the scope of the audit in detail to ensure full preparedness

Conduct a pre-certification audit (optional)

- □ Consider a pre-certification audit to identify any remaining gaps

STEP 4

The ISO 42001 audit

Engage in the certification audit

- □ Collaborate with A-LIGN auditors, providing necessary information and access
- □ Designate a team member as the point of contact for auditors to streamline communication
- □ Organize walkthroughs to discuss your AIMS processes and procedures, including facilities (if applicable)

Address audit findings

- □ Plan for immediate, short-term, and long-term corrective actions based on the audit report
- □ Celebrate the audit success with your team and publicly promote your certification

Continuous improvement

- □ Establish a continuous improvement team to oversee progress post-certification
- □ Continuously improve the AIMS, leveraging lessons learned and feedback
- □ Integrate ISO 42001 compliance metrics into regular management reviews

EXTRA

Keys to success

- □ Leverage Vanta's readiness capabilities and A-LIGN's expertise for an efficient and high-quality audit experience from readiness to report
- □ Incorporate AIMS within the business strategy and daily operations
- □ Apply continuous improvement to enhance AIMS over time
- □ Avoid integrating new technologies during the initial AIMS implementation
- □ Engage interested parties and maintain their support throughout
- □ Highlight the completion of the audit to demonstrate trust with customers, partners, and other key stakeholders

Vanta

Automate compliance. Simplify security. Demonstrate trust.

Vanta is the leading trust management platform that helps simplify and centralize security for organizations of all sizes. Thousands of companies rely on Vanta to build, maintain and demonstrate their trust—all in a way that's real-time and transparent. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, New York, San Francisco and Sydney.

For more information, visit: www.vanta.com | sales@vanta.com

A-LIGN

A-LIGN is the leading provider of high-quality, efficient cybersecurity compliance programs. Combining experienced auditors and audit management technology, A-LIGN provides the widest breadth and depth of services including SOC 2, ISO 27001, HITRUST, FedRAMP, and PCI. A-LIGN is the number one issuer of SOC 2 and HITRUST and a top three FedRAMP assessor.

To learn more, visit: a-lign.com