safeshield®

A 12 Step Roadmap to Achieving ISO/IEC 42001 Certification

A step-by-step guide to preparing for and achieving certification under the world's first AI Management System Standard

June 2025

safeshield®

What is ISO/IEC 42001?

ISO/IEC 42001 is the first international standard specifically focused on Artificial Intelligence Management Systems (AIMS). Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), this standard provides a comprehensive framework for businesses to manage AI systems responsibly, ethically, and in alignment with regulatory expectations.

ISO/IEC 42001 offers a structured approach; whether you're building AI technologies or using third-party AI services, to ensure transparency, fairness, accountability, and continual improvement throughout the lifecycle of your AI technologies.

12-Step Roadmap to Certification

To help organizations navigate the journey toward ISO/IEC 42001 certification in a clear and structured way, the 12-step roadmap has been grouped into three distinct phases.

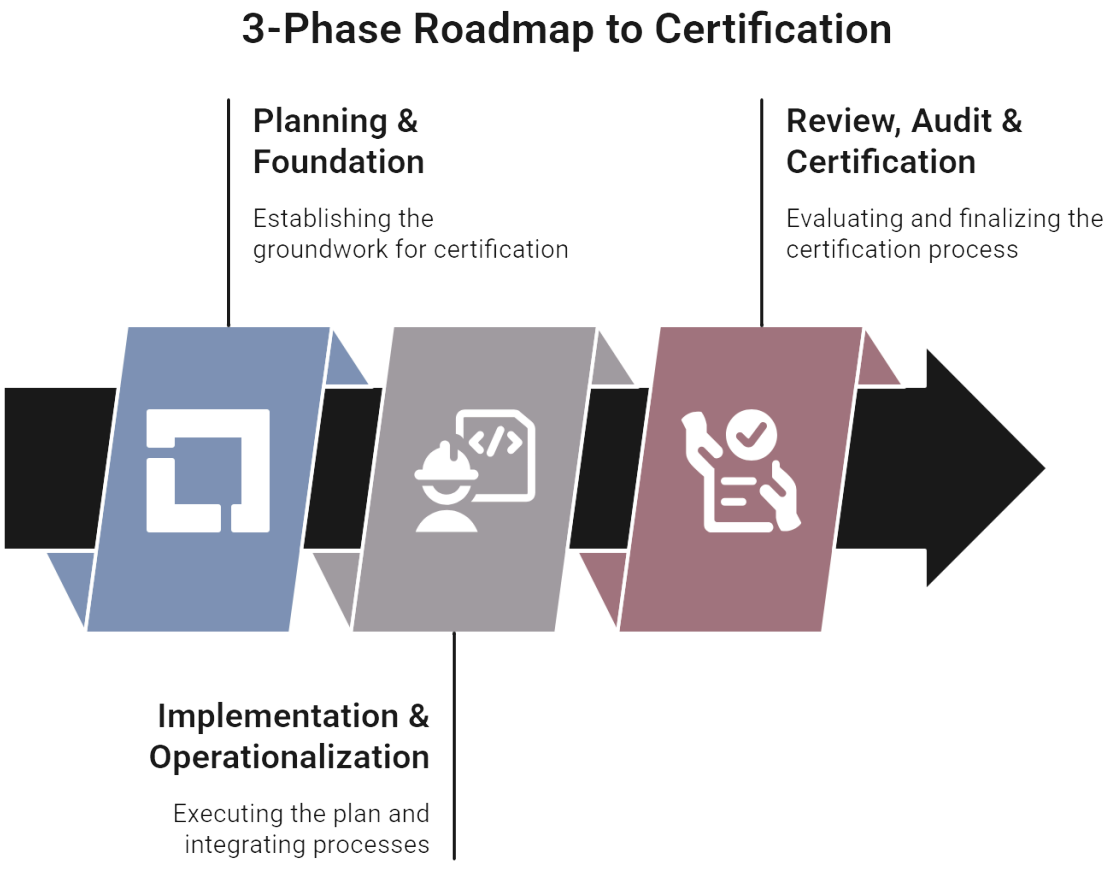

Figure 1: 3-phase roadmap to certification

- **Phase 1:** Planning & Foundation focuses on securing executive buy-in, defining the scope, establishing governance structures, and setting up a risk management approach tailored to AI systems.

- **Phase 2:** Implementation & Operationalization moves from strategy to action, embedding policies into daily operations through data and model governance, transparency measures, documentation controls, and staff training.

- **Phase 3:** Review, Audit & Certification prepares the organization for formal evaluation, including internal audits, corrective actions, management reviews, and the external certification audit.

This phased approach makes the certification process more manageable by aligning activities with natural implementation milestones.

Phase 1: Planning & Foundation

Figure 2: four steps of the project planning and foundation phase

This phase sets the stage for a successful implementation of an Artificial Intelligence Management System (AIMS) by aligning leadership, defining the project's scope, and establishing the foundational structures required by ISO/IEC 42001. During this phase, organizations secure executive commitment, appoint a lead implementer, and build a cross-functional team to guide the initiative. A readiness assessment is conducted to identify gaps

between current practices and the standard's requirements, while the scope of the AIMS is clearly defined to include internal and third-party AI systems. This phase also includes developing a tailored risk management framework and drafting initial governance policies to ensure accountability, ethical AI use, and strategic alignment from the start.

To lead this critical phase effectively, organizations should assign a qualified AIMS Lead Implementer—consider enrolling in a Certified ISO/IEC 42001 Lead Implementer course to gain the expertise needed to guide the project with confidence and ensure alignment with the standard.

Figure 2 above shows 4 different steps of the planning and foundation phase.

- **Step 1:** Executive buy-in and beginning the project
- **Step 2:** Readiness assessment and defining your scope
- **Step 3:** Risk management framework
- **Step 4:** Policy development and governance structure

Let's take a closer look at each of these four steps in this section.

Step 1: Executive Buy-In and Beginning the Project

This first step marks the official launch of the ISO/IEC 42001 implementation journey. In this step, organizations secure commitment from senior leadership by highlighting the strategic, ethical, and regulatory importance of establishing an Artificial Intelligence Management System (AIMS). A Lead Implementer is appointed, and a cross-functional project team is assembled, bringing together key departments such as compliance, IT, HR, and legal. Clear goals, timelines, and responsibilities are defined, ensuring alignment and shared ownership from the outset.

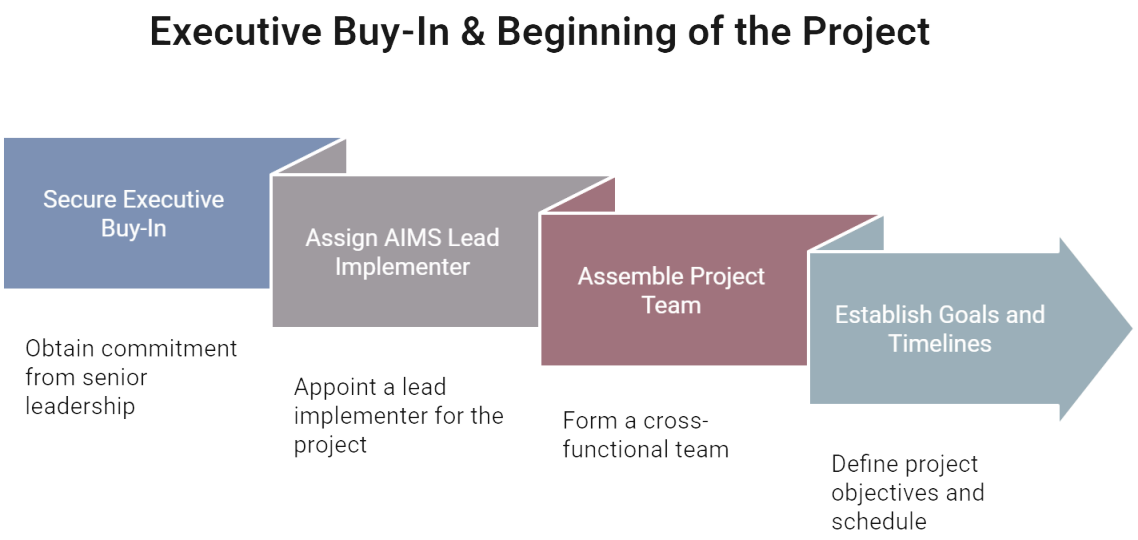

Figure 3: Step 1, phase 1. Executive buy-in & beginning of the project

Step 2: Readiness Assessment & Defining the Scope of your Project

This step focuses on understanding where the organization currently stands and what the AIMS will cover. A gap analysis is conducted to compare existing AI practices against the requirements of ISO/IEC 42001. This helps identify areas needing improvement and sets a baseline for the implementation. At the same time, the scope of the AIMS is defined—clarifying which systems, functions, and locations are included, including both internal and third-party AI. This step also involves identifying key stakeholders, mapping data flows, and documenting known AI systems and their use cases.

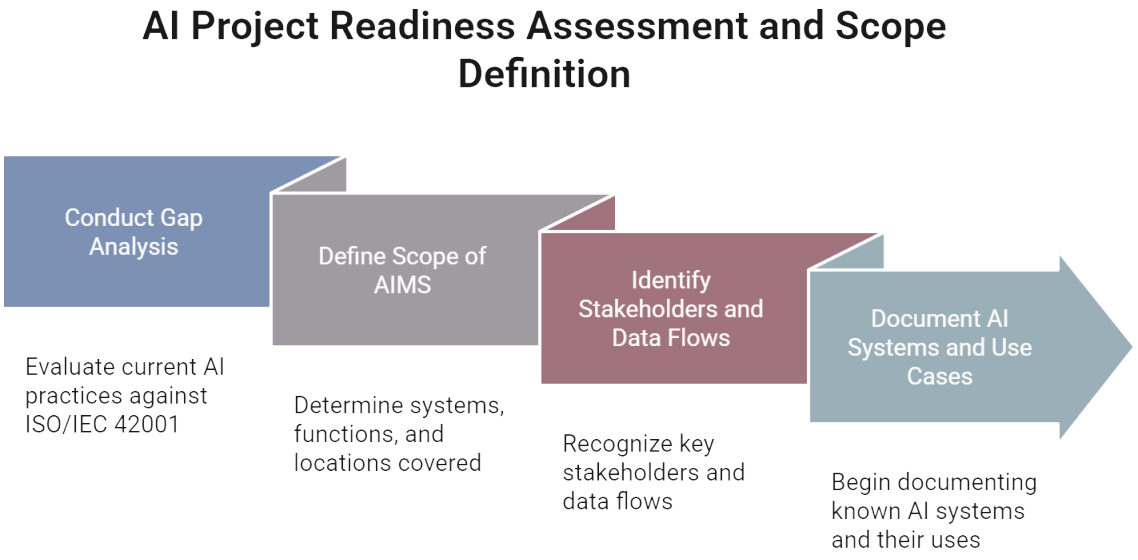

Figure 4: Step 2, phase 1. AI project readiness assessment and scope definition

Step 3: Risk Management Framework

This step introduces a structured approach to identifying, assessing, and mitigating risks associated with AI systems. Organizations define how they will manage risks such as bias, misuse, performance drift, and ethical concerns across the AI lifecycle. This step includes developing a risk methodology tailored to AI, initiating risk assessments for existing or planned systems, and establishing risk registers. It also involves setting thresholds for acceptable risk levels, ensuring that risk treatment aligns with both organizational objectives and ISO/IEC 42001 requirements.

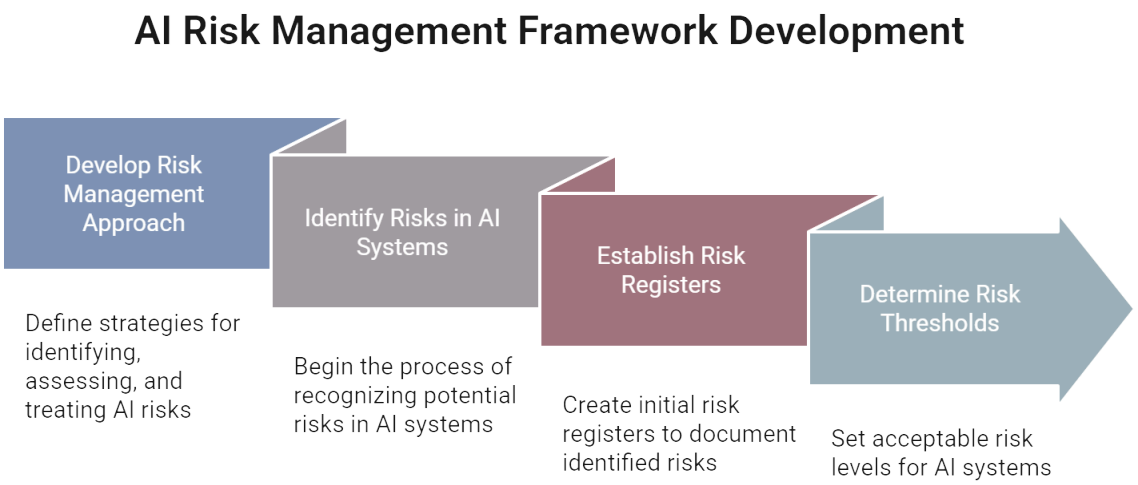

Figure 5: Step 3, phase 1. AI risk management framework development

Step 4: Policy Development & Governance Structure

This step focuses on formalizing the organization's commitment to responsible AI through clear policies and defined oversight. This includes drafting an AI policy that addresses ethical principles, transparency, and compliance with legal and regulatory requirements. Governance structures are established to assign roles and responsibilities across the AI lifecycle—from development to decommissioning. Where appropriate, an AI ethics committee or internal oversight board is formed to guide decision-making and escalate concerns. This step ensures that accountability is embedded into the system from the outset.

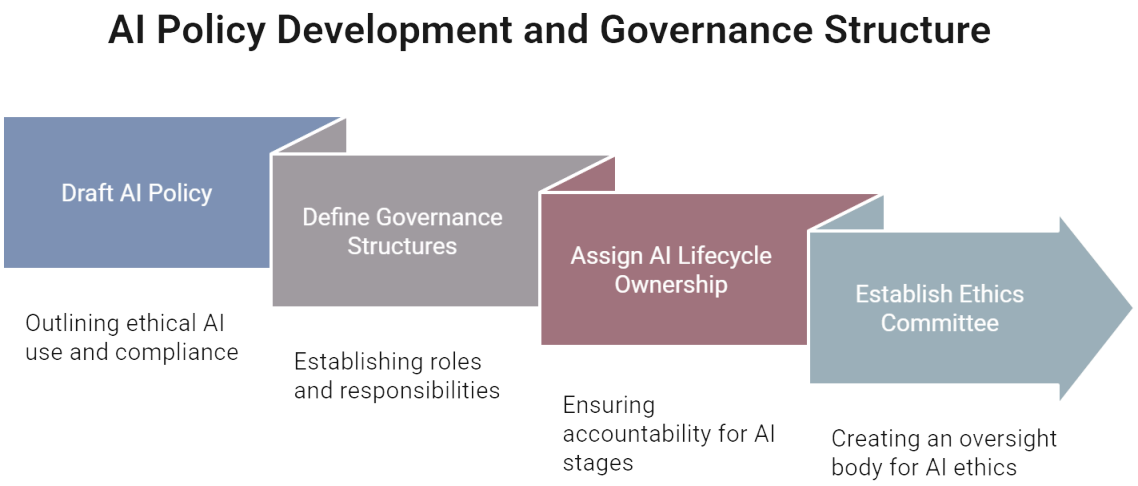

Figure 6: Step 4, phase 1. AI policy development and governance structure

Phase 2: Implementation & Operation

Figure 7: four steps of the implementation and operation phase

Phase 2 focuses on putting the foundational plans into action by embedding AI governance practices across the organization. This phase involves establishing robust data and model governance processes to ensure quality, fairness, privacy, and traceability throughout the AI lifecycle. It also includes implementing

procedures for human oversight and transparency, especially for high-risk AI systems, to maintain accountability and user trust. Organizations begin organizing documentation, setting up centralized record-keeping, and rolling out targeted training programs to build awareness and competence across teams. By operationalizing the principles defined in Phase 1, this phase ensures that responsible AI practices are not only documented but actively integrated into day-to-day activities.

To gain the skills needed to lead this phase effectively and drive real organizational change, consider enrolling in a Certified ISO/IEC 42001 Lead Implementer course and become a recognized expert in AI governance implementation.

Figure 5 above shows the four steps of the implementation and operation phase.

- **Step 5:** Data and model governance
- **Step 6:** Human oversight and transparency
- **Step 7:** Documentation and record keeping
- **Step 8:** Training and building culture

Let's take a closer look at each of these four steps in this section.

+ Step 5: Data and Model Governance

In this step, we ensure that the organization has strong controls over how data is sourced, processed, and used in AI systems. This step involves defining governance policies that address data quality, fairness, bias detection, privacy, and traceability. It also extends to model governance, covering how AI models are trained, validated, deployed, and monitored throughout their lifecycle. For high-impact systems, special attention is given to explainability and reproducibility, ensuring compliance with ISO/IEC 42001 and building trust in AI outcomes.

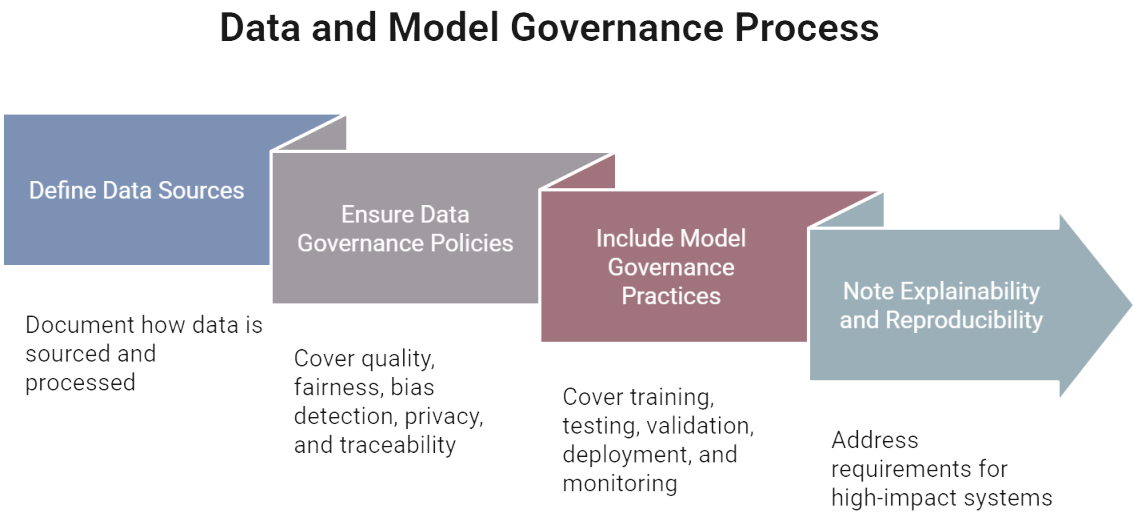

Figure 8: Step 5, phase 2. Data and model governance

Step 6: Human Oversight and Transparency

This step focuses on ensuring that people remain in control of AI systems, especially in high-risk scenarios. This step involves defining clear procedures for when and how human intervention should occur, including thresholds for overriding AI outputs. Organizations also implement transparency measures to inform users when they are interacting with an AI system. Where appropriate, disclosures and opt-out options are provided to employees, customers, or other affected parties, reinforcing trust and accountability in AI use.

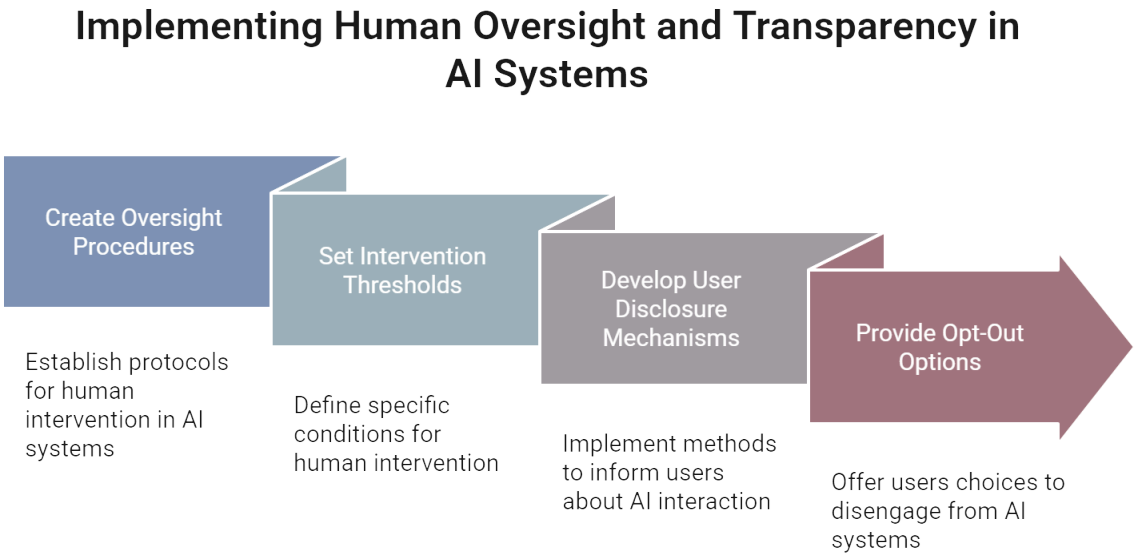

Figure 9: Step 6, phase 2. Human oversight and transparency

Step 7: Documentation and Record-Keeping

This step ensures that all elements of the Artificial Intelligence Management System (AIMS) are properly recorded and traceable. This includes organizing policies, procedures, risk assessments, audit logs, and training records in a centralized repository with version control. Proper documentation not only supports compliance with ISO/IEC 42001 but also provides evidence of due diligence, facilitates audits, and enables continuous improvement. Maintaining clear, accurate, and accessible records is essential for demonstrating transparency and accountability throughout the AI lifecycle.

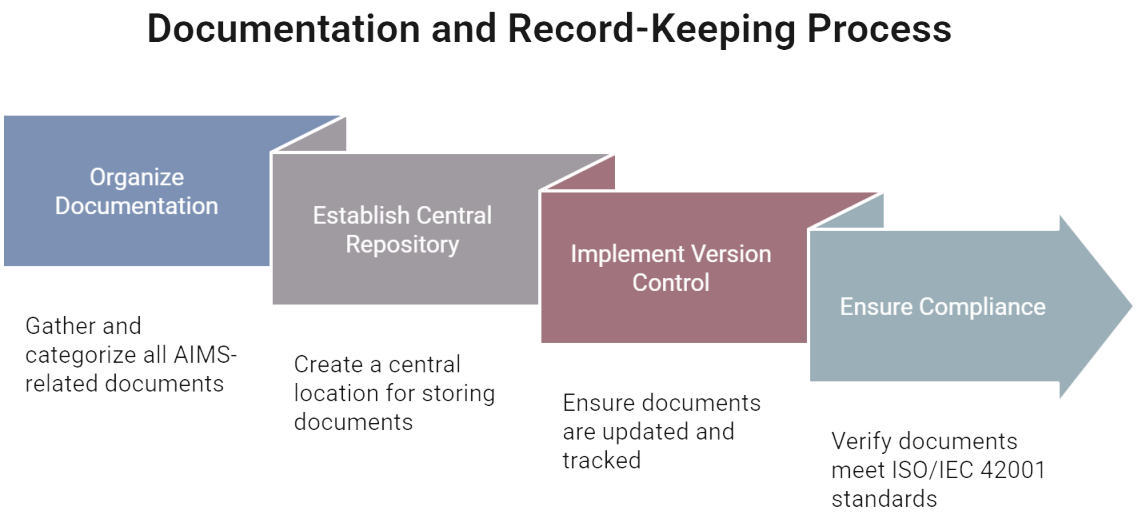

Figure 10: Step 7, phase 2. Documentation and record-keeping

Step 8: Training and Building Culture

Here, we focus on equipping employees with the knowledge and mindset needed to support responsible AI practices. Targeted training is delivered to teams involved in the development, deployment, and oversight of AI systems, while organization-wide awareness initiatives help embed ethical and compliant behavior into the culture. Training programs cover key topics such as AI ethics, transparency, human rights, and security. This step also ensures that leadership reinforces the strategic value of ISO/IEC 42001 certification, creating a unified vision across all levels of the organization.

Figure 11: Step 8, phase 2. AI training and culture building

Phase 3: Review, Audit and Certification

Figure 12: four steps of the review, audit and certification phase

Phase 3 prepares the organization for formal evaluation and external certification. Building on the processes established in earlier phases, this stage begins with internal audit preparation, including selecting qualified auditors, reviewing compliance evidence, and conducting pre-audit checks. A full internal audit follows, helping to identify any nonconformities and drive

corrective actions. Management then conducts a formal review to assess the effectiveness of the Artificial Intelligence Management System (AIMS), address remaining gaps, and confirm readiness for certification. The phase concludes with the certification audit conducted by an accredited body. Successful completion results in ISO/IEC 42001 certification, validating the organization's commitment to trustworthy and accountable AI practices.

To play a key role in this critical phase and lead organizations through successful audits, consider taking a course to become a Certified ISO/IEC 42001 Lead Auditor.

Figure 5 above shows the four steps of the review, audit, and certification phase.

- **Step 9:** Internal audit preparation
- **Step 10:** Internal audit and corrective actions
- **Step 11:** Final review and certification readiness
- **Step 12:** Certification audit

Let's take a closer look at each of these four steps in this section.

Step 9: Internal Audit Preparation

This step lays the groundwork for evaluating the effectiveness of the Artificial Intelligence Management System (AIMS) before the formal certification audit. Organizations begin by reviewing ISO/IEC 42001 requirements and identifying qualified internal auditors—either by training existing staff or engaging external experts. An audit plan is developed to ensure comprehensive and impartial review, with auditors independent from the implementation team. Pre-audit checks are conducted to verify that processes are in place and evidence is properly documented, helping identify any gaps before the internal audit begins.

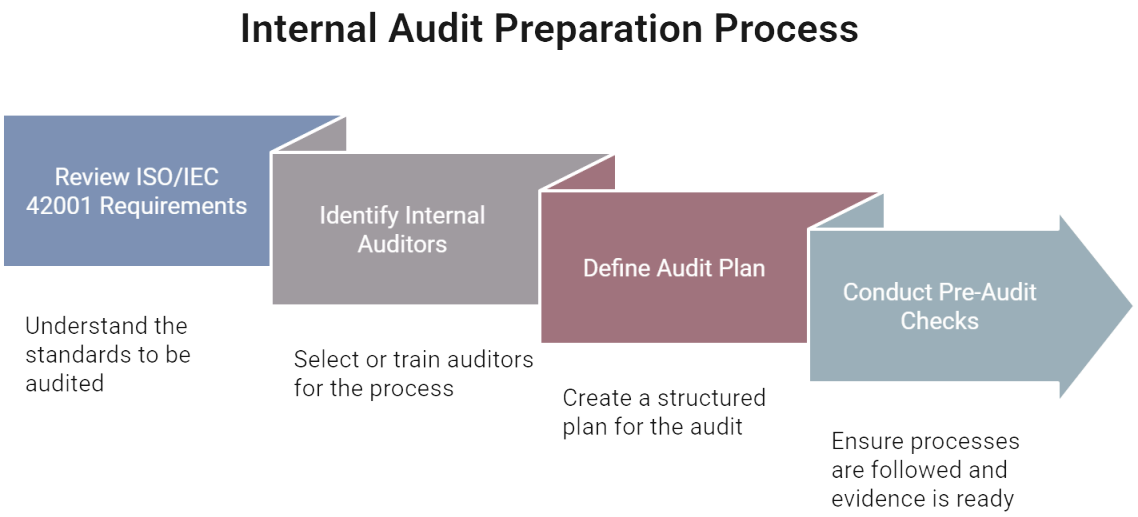

Figure 13: Step 9, phase 3. Internal audit preparation process

Step 10: Internal Audit and Corrective Actions

This step involves conducting a thorough internal audit to assess compliance with ISO/IEC 42001 and identify any nonconformities or areas for improvement. Audit findings are documented, and corrective actions are assigned to address root causes, not just symptoms. This step is essential for validating the effectiveness of the AIMS and ensuring that all processes are functioning as intended. It also reinforces accountability across departments and provides an opportunity to share lessons learned and highlight early successes before moving to the certification stage.

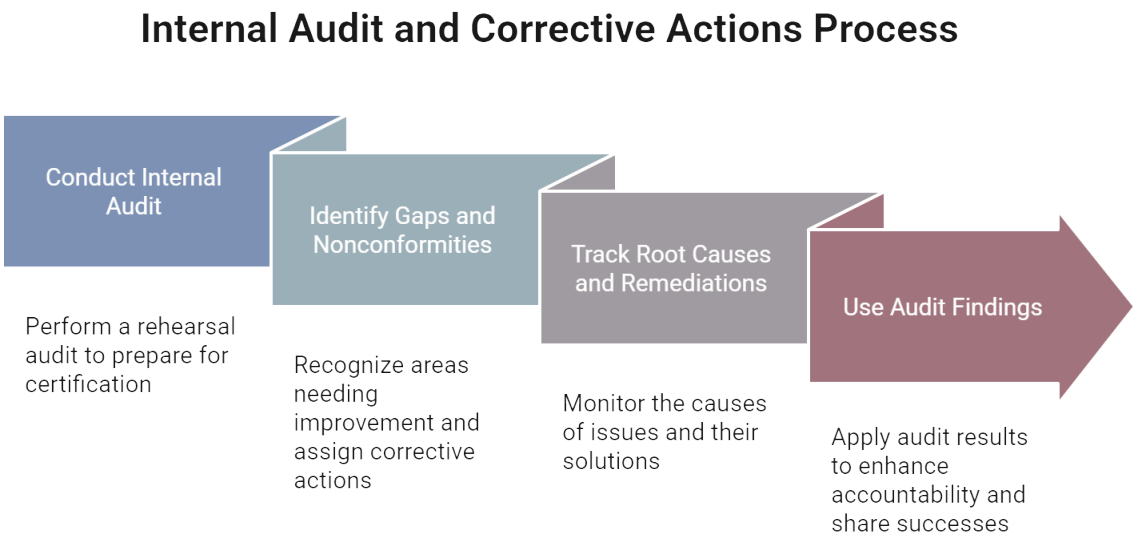

Figure 14: Step 10, phase 3. Internal audit and corrective actions process

Step 11: Final Review and Certification Readiness

This is the last internal checkpoint before engaging with a certification body. In this step, the organization conducts a formal management review to evaluate the overall performance of the Artificial Intelligence Management System (AIMS). This includes reviewing audit findings, corrective actions, key performance indicators, and risk assessments. Any final adjustments to documentation or processes are made to ensure full alignment with ISO/IEC 42001 requirements. A final internal review or dry run may be conducted to confirm that the organization is fully prepared for the external certification audit.

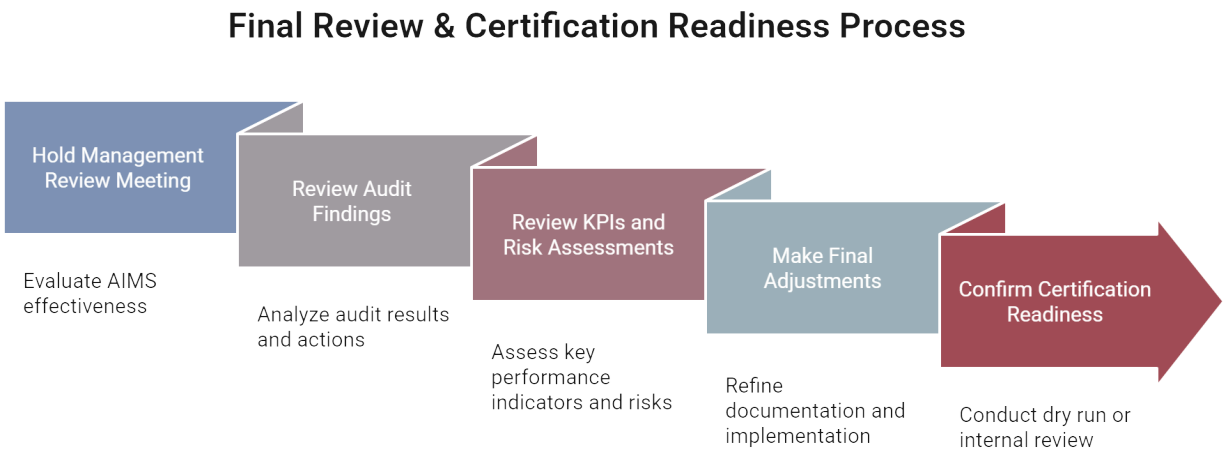

Figure 15: Step 11, phase 3. Final review and certification readiness process

Step 12: Certification audit

This is the final step in the ISO/IEC 42001 journey, where an accredited certification body formally assesses the organization's AIMS for compliance. This step involves preparing documentation, scheduling audit activities, and ensuring that relevant personnel are available to support the audit process. During the audit, the organization must demonstrate how its policies, procedures, and practices align with the standard's requirements. Any observations or minor findings are addressed promptly. Upon successful completion, the organization receives ISO/IEC 42001 certification—an important milestone that validates its commitment to responsible, ethical, and compliant AI governance.

Figure 16: Step 12, phase 3.Certification audit

Why ISO/IEC 42001 Matters

Certification not only makes your AI systems more reliable; it also builds trust with both stakeholders and customers. It demonstrates that your AI systems are ethical, transparent, and safe. ISO/IEC 42001 provides a formalized, internationally recognized structure to prove that you've put the work in.

If you are leading an implementation project or preparing to assess compliance, becoming a Certified ISO/IEC 42001 Lead Implementer or Lead Auditor equips you with the skills and credentials to drive responsible AI practices within your organization. Enroll in one of our certification courses and position yourself at the forefront of AI governance, risk management, and compliance.

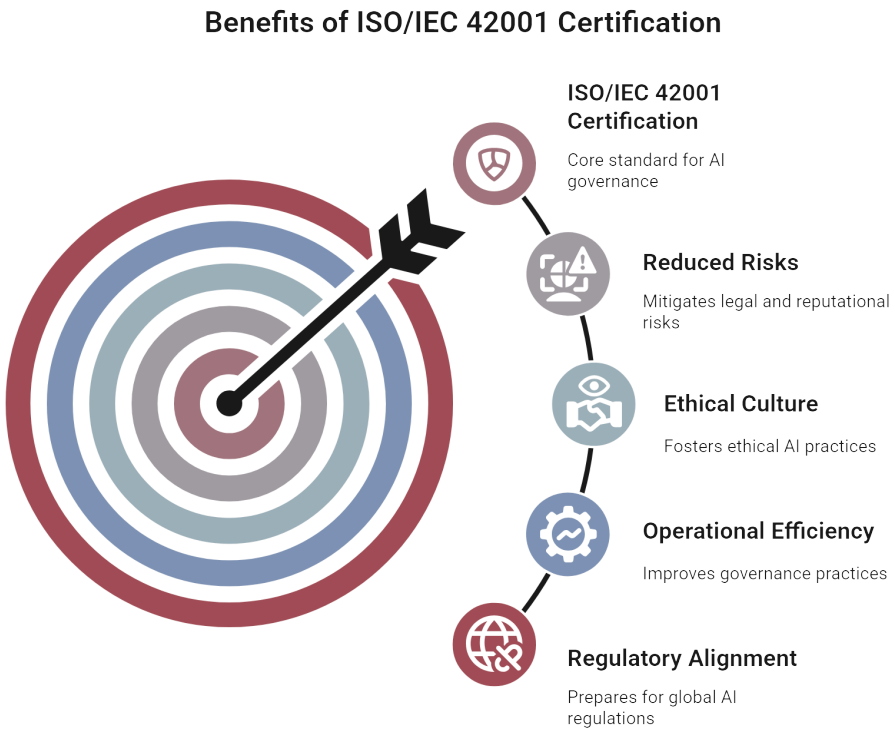

Figure 17: The benefits of ISO/IEC 42001 certification

safeshield

FAQs

+ Does ISO/IEC 42001 apply to organizations that use third-party AI tools?

Yes. Even if you're using SaaS platforms or embedded AI, you're responsible for ensuring proper oversight and governance under ISO/IEC 42001.

+ Is certification mandatory?

Not yet. But adoption is highly recommended, especially as global regulations evolve. Certification can futureproof your business through responsible AI implementation.

+ How long does the certification take?

Most mid-sized businesses take anywhere from 8 to 12 months to get certified.

+ Can ISO/IEC 42001 help my business integrate with the other standards I have adopted?

This is a common concern. Luckily, many businesses have successfully adopted ISO/IEC 42001 alongside standards and frameworks they already comply with, such as ISO/IEC 27001 or SOC 2.

If you're wondering how, our next guide in this series explores integrating ISO/IEC 42001 with other standards and frameworks you may already follow.

How can I get better prepared to lead or participate in the implementation of an AIMS alighned with ISO/IEC 42001?

Consider enrolling in a professional training program, such as the ISO/IEC 42001 Lead Implementer certification. This equips you with the knowledge and tools needed to plan, execute, and manage an Artificial Intelligence Management System, while aligning with global best practices and regulatory expectations.

How can I get better prepared for readiness assessments and internal audits of an ISO/IEC 42001-compliant audit?

Pursuing an ISO/IEC 42001 Lead Auditor certification is a strong step. This training helps you understand audit principles, assess compliance against the standard, and identify nonconformities effectively—whether you're conducting internal audits or preparing for third-party assessments.

Ready to get started?

Whether you're preparing for certification or just exploring responsible AI management, Safeshield offers expert ISO/IEC 42001 training to equip you with the right tools for your business' needs. Explore our AIMS certification courses here.

Thank You

About Us

SafeShield specializes in cybersecurity and compliance consulting, providing comprehensive solutions to help businesses safeguard against potential cyber threats and compliance risks. Our services include:

- ISMS Implementation
- Risk assessments
- Security audits
- Security training for employees and executives
- More

Visit us at https://www.safeshield.cloud for more information or to view our library of training courses and personalized services.