Rhymetec

ISO 42001 Checklist

In this guide, you'll find the resources to help you prepare for your ISO 42001 audit.

rhymetec.com

Introduction

Whether you're just getting started on your journey with ISO 42001 or are currently in the process of implementation, you're probably aware the road to compliance isn't easy. Thankfully, it can be simplified. As cybersecurity experts, our team has helped hundreds of CEOs, CTOs, and other decision-makers at SaaS companies achieve compliance across a wide spectrum of frameworks, laws, and regulations.

In this guide, you'll find the following resources to help you prepare for your ISO 42001 audit:

- **ISO 42001 Checklist** to break down the readiness process
- **ISO 42001 Timelines** to help you assess how long your readiness and audit phases will take
- **ISO 42001 FAQ** to answer the most common questions we see about ISO 42001

Written with busy SaaS and tech leaders in mind, our goal is to help you shorten your timelines, reduce your team's level of effort, and successfully guide your company through ISO 42001 compliance so you can continue to move your business forward.

If you need some help with your ISO 42001 journey, book a no-obligation chat with our team.

Our method, as outlined in this guide, transforms compliance into a business enabler by allowing you to align control implementation with your business goals and manage both risks and opportunities associated with AI.

> **"Rhymetec was amazing! Couldn't have done it without you guys! I loved that we could integrate via Slack. It made it feel even more like Rhymetec was just a natural extension of Truthset."**
>
> – Head of Data Science, Truthset

Table of Contents

ISO 42001 Checklist

Although every company's journey to ISO 42001 compliance will be a little different, this checklist breaks down the steps most organizations will deal with during the ISO 42001 process. Use it to educate yourself on the road ahead before guiding your organization through ISO 42001 compliance.

Phase 1: Build A Strong Base For ISO 42001 Compliance

This first phase prepares you for successful ISO 42001 certification. These steps will lay the groundwork from which to build an Artificial Intelligence Management System (AIMS) for your organization. Establishing AIMS is not just about compliance; it's about crafting a concrete strategy to improve decision-making and risk management around AI technologies. After accomplishing these items, you'll have a clear direction for responsible AI usage that aligns with global standards and be on the right path to work towards ISO 42001 compliance:

☐ Understand Your ISO 42001 Requirements

Make Sure you Understand AI Concepts, Principles, and Lifecycle as Established in ISO Frameworks.

- It's important to understand terms like "AI systems" and "machine learning models" from ISO/IEC 22989 to plan out your roadmap for ISO 42001.
- Familiarizing yourself with the terminology helps you understand every step of the compliance process, speak the same language as your auditors, and prevent miscommunications.
- A glossary of terms can be easily found here under "Terms related to AI."

Clarify Whether your Organization Acts as a Provider, Developer, or User of AI Systems.

- This is important to clarify from the onset, as the AIMS and control implementation must be tailored to your organization's specific operational needs and risks.

Define Which AI Systems, Processes, and Technologies your AI Management System (AIMS) will Cover.

- Identify the locations, assets, and technologies included to map out the AIMS boundaries.

☐ Conduct An Initial Gap Analysis

Evaluate Your Current ISO 42001 Controls.

- Compare your existing AI management practices against ISO 42001 controls. This initial gap analysis will direct future improvements.

Identify Where You Need to Develop New Controls or Adjust Existing Ones.

- Focus on areas such as AI risks, data integrity, and ethical compliance.
- Align each focus area with the corresponding ISO 42001 controls to fully address all facets of AI management.

Conduct A Risk Assessment

Identify all potential hazards associated with AI systems and development.

- Consider your organization's AI risks related to products, services, and all other activities.
- Assess the likelihood and potential consequences of each identified risk. You will need this documentation later down the road in your ISO 42001 journey.

Prioritize risks based on their level and determine corresponding controls.

- Develop an action plan to remediate risks, focusing on the highest risks first.
- Assess existing controls and their effectiveness in mitigating risks.

Impact is categorized as low, medium, or high based on factors like financial loss, legal repercussions, and damage to customer trust. As an example, if your AI handles sensitive or critical data, the risk of a data breach would be considered **high risk** (as a breach could result in substantial legal and reputational damage).

A **medium risk** could be data bias in functions that are not critical to core operations but could impact user satisfaction or minor decision-making processes. A threat with a **low-risk** level could be any potential minor AI performance fluctuations. If you use an AI-driven customer support chatbot, for example, the risk of users experiencing minor delays in response time or slight inaccuracies in non-critical responses could be considered low risk.

Obtain Executive Support

Build a Business Case for ISO 42001 Certification.

- Create a compelling business case that outlines the strategic benefits of ISO 42001 certification.
- Include how it will enable AI governance, help your organization comply with regulations, and build stakeholder trust.
- Showcase the long-term value and innovation potential a formalized AI management system can offer.

Assign Responsibilities to Senior Management for AIMS.

- Assign senior management responsibilities to align the AIMS with your goals and provide them with the necessary resources.

Engage Department Heads in the Analysis.

- Bring department heads from IT, legal, operations, and human resources into the gap analysis process. Their involvement ensures all potential impacts of AI systems are considered.

> **"I appreciate the weekly operational calls which are very organized. I also appreciate my account rep who meets with me monthly to organize our company's goals and executes on our planned testings and compliance prep. This has greatly helped me both accelerate our implementation of compliance frameworks and keeps the plates spinning on new ones that we need to plan for."**
>
> – VP of Security & Compliance, Orum

Phase 2: Execute Your ISO 42001 Compliance Blueprint

In this second phase, your organization will activate the plans laid out above. This involves hands-on tasks such as appointing a project manager, setting up the structure for your AIMS, and implementing controls. This phase culminates with your internal audit to assess your ISO 42001 certification readiness before moving into external evaluations:

☐ Designate a Compliance Project Leader

Select a Qualified Compliance Leader.

- Appoint a project manager with a solid understanding of AI and compliance issues.
- This individual will coordinate all activities related to achieving ISO 42001 certification and act as the point of communication between departments and external auditors.

☐ Draft An Implementation Roadmap For AIMS

Develop a Detailed Project Plan.

- Create a project plan that includes deadlines and resource allocations.
- Your plan should cover everything from the initial assessment to the final audit stages.

Budget Appropriately.

- Allocate sufficient financial and human resources to support the project.
- This includes funding for training, external consultants, auditing costs for certification, and technology upgrades necessary to comply with ISO 42001.

*__TIP:__ *When implementing ISO 42001, you should not rely on checklists alone from external sources, purchasing the standard should be in your budget for successful implementation.*

Set Up The AIMS Structure

Define Your AI Management System Structure.

- Set up a structure for your AIMS that integrates with existing organizational processes.
- The structure should support all stages of AI lifecycle management, from development to deployment and maintenance.

Document All Processes.

- Document workflows, decision-making processes, and control measures.

Create Organization-Wide Awareness

Develop Training Programs.

- Organize training sessions to improve your employees' AI and compliance knowledge base.
- Focus on ethical AI use, data security, and the legal implications of AI technologies.

Circulate Information Across The Organization.

- Distribute informational materials and regular updates about AIMS and its importance to encourage organization-wide understanding and engagement.
- Internal communications channels such as newsletters, intranets, and staff meetings are all good avenues for dissemination.

> **"Rhymetec has been a great security partner for us! They feel like they are on the Modern Health security team and they provide a ton of value for different aspects of Modern Health's information security and compliance program"**
>
> – Head of Information Security, Modern Health

Apply Necessary AIMS Controls

Implement Controls.

- ISO 42001 controls address risk management, data protection, system reliability, and transparency.
- The way controls are implemented will vary depending on your organization's industry, needs, risks, and the types of AI applications you use. (A complete control list can be found in ISO/IEC 42001:2023, Annex A).
- Consulting with a compliance expert at this step may be necessary.

Regularly Update Control Measures.

- Continuously monitor and update the controls to adapt to new technologies, changes in organizational processes, and shifts in regulatory requirements.

*__TIP:__ *Many startups choose to work with a Managed Security Services Provider (MSSP) at this stage. Rhymetec's vCISO program provides hands-on managed security services, taking the complexity of compliance off your plate, and doing the readiness and audit phases for you.*

Conduct Executive AIMS Evaluations

Organize Regular Review Meetings.

- Hold management review meetings periodically to assess the AIMS's performance.
- Reviews should involve top management and key stakeholders to help AI systems & applications continue to align with broader organizational goals.

Update Executive Team Regularly.

- Keep the executive team informed about the outcomes of management reviews, including challenges, achievements, and the overall effectiveness of the AIMS.

Phase 3: Preparation for External ISO 42001 Audit

This stage serves as preparation for the external audit. It's where you make sure everything is in perfect order for your audit. Choosing the right auditor is important - you want to choose a reputable certification body that will conduct a rigorous and fair audit, providing credible validation of your AIMS. Each step in this phase is an opportunity to solidify stakeholder confidence and demonstrate your proactive approach to responsible AI management and compliance:

☐ Select an ISO 42001 Certification Body

Choose a Qualified Auditor.

- Select an auditing firm that has been certified to offer ISO certifications and has demonstrated experience in assessing AI management systems.
- Your certification body must be accredited to guarantee a legitimate audit.

☐ Conduct Internal Audits

Schedule and carry out internal audits.

- Internal audits serve to identify any gaps in compliance and provide recommendations for improvements before your external audit.
- An internal review serves as a trial run, providing insights into potential audit challenges and giving you a chance to address any issues.

Prepare Documentation

Organize Essential Documents.

- Gather all necessary documentation that demonstrates your compliance with ISO 42001.
- Documents are to include policies, procedures, control implementation records, and evidence of continuous improvement efforts.
- Make things as easy as possible for your auditors. Documents should be in a format that is readily available and organized for easy reference during the audit.

*__TIP:__ *Using a compliance automation tool at this point can be tremendously helpful. Compliance automation platforms allow you to easily organize your documentation. When it comes time for your audit, it makes your auditor's job easier and more efficient to be able to see everything clearly laid out in one central place.*

Review and Update Documentation Regularly.

- Regularly review your AIMS documentation to make sure it accurately reflects current AI management practices and that all modifications are recorded.
- Keep this documentation accessible to all relevant personnel and the auditing team for transparency and ease of verification.

Pre Audit Meeting

Set Up an Initial Audit Meeting.

- Arrange a meeting with the selected certification body to discuss the audit process.
- Use this as an opportunity to understand the audit scope, methodology, and specific focus areas.
- Use the meeting to align expectations and clarify the audit schedule.

Compile Key Audit Questions.

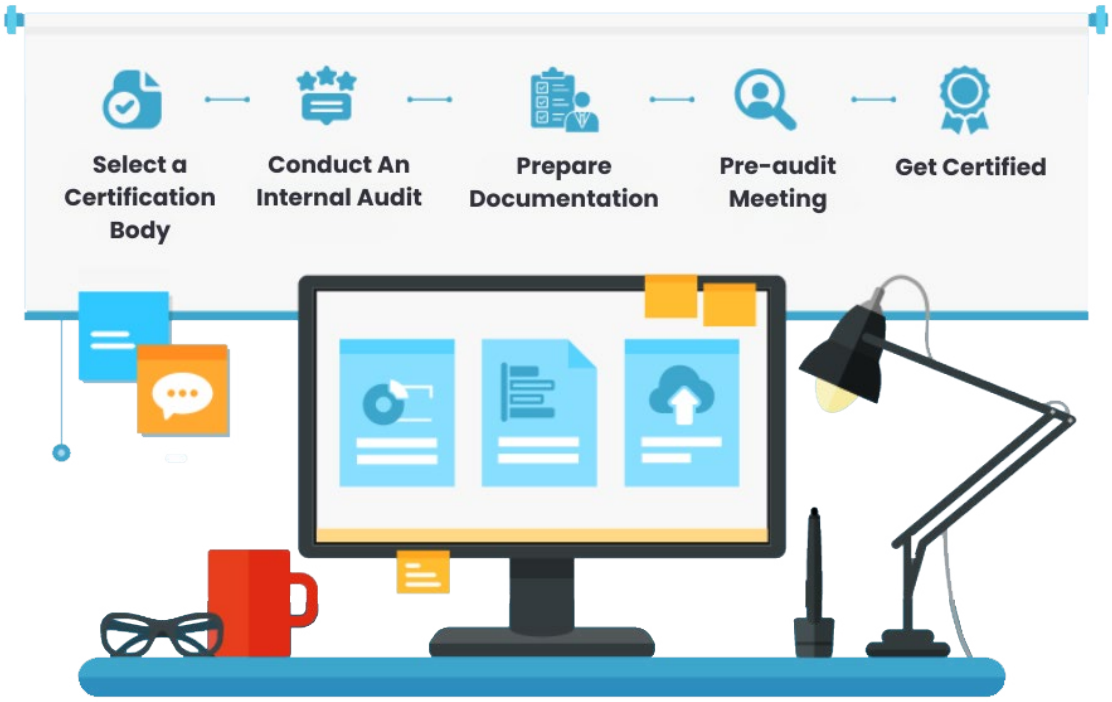
- Prepare a list of questions and points needing clarification to address during the pre-audit meeting.
- Cover logistical details, specific compliance queries, and any concerns about the AIMS implementation.

Discuss Audit Scope.

- Engage with the certification body to discuss a detailed scope of the audit. The scope must cover all relevant areas of your AIMS.
- Confirm that both parties have a mutual understanding of the audit boundaries.

ISO 42001

Certification Process Overview



Phase 4: Obtaining your ISO 42001 Certification

This final phase is where all of your preparation pays off.

Engaging fully with auditors transforms this process from a compliance exercise to a powerful tool for improving your operations and reputation. Undergoing this audit isn't just a badge for your business to put on your website; it's a statement that you take AI risks seriously and are ahead of the curve in managing AI responsibly. Lastly, continually improving after the audit shows you're not just "checking a box" to get through an audit. Ongoing improvements post-audit strengthen trust among clients and partners:

☐ Undergo Your Audit

Facilitate Auditor Access.

- Auditors need to have full access to all relevant sites, personnel, and documentation.
- Designate a team member to serve as a point of contact and participate in discussions with auditors to streamline the process and clarify any misunderstandings.

☐ Address Any Identified Issues

Develop Corrective Actions.

- Promptly create action plans for any non-compliance issues identified during the audit.
- Assign clear responsibilities and timelines for these actions.

Implement and Document Corrective Actions.

- Execute the necessary corrective measures and document the processes.
- You will need this documentation during follow-up audits.

Ongoing Improvement & Post-Audit Plan

Review Audit Outcomes.

- Analyze the results and feedback from the certification audit. Review all findings to pinpoint areas for improvement.
- Examine both strengths and weaknesses highlighted during the audit.

Plan for Continuous Improvement.

- Develop a plan for continuous improvement based on audit findings.
- Your post-audit plan should include updating training programs and communication with employees to address any changes.
- Schedule regular intervals to review the AIMS and identify opportunities to improve.

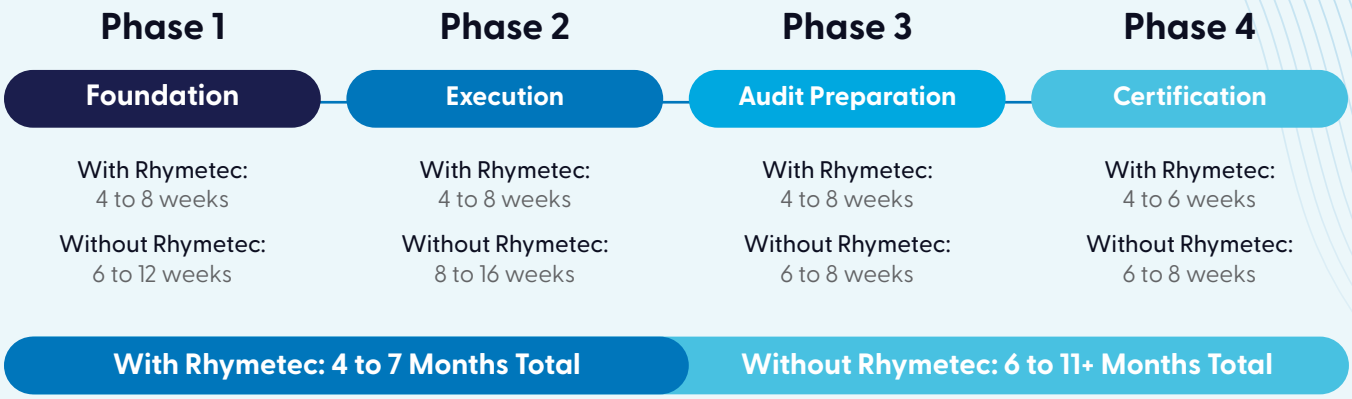
Conduct Surveillance Audits In Preparation to Recertify Every 3 Years.

- ISO 42001 requires recertification every 3 years to remain compliant.
- Surveillance audits are needed in between to ensure your organization is ready for the next official audit.

“We are now on our second year of ISO and third year for SOC 2 certifications with Rhymetec vCISO services. For startups that would rather focus efforts on their core business, bringing in Rhymetec vCISO services was the most efficient and cost effective way to become ISO and SOC 2 compliant.”

– Security and Data Analyst, MetaMap

ISO 42001 Implementation & Audit Timeline



How Long Does ISO 42001 Readiness Take?

With managed security services providers like Rhymetec, it takes anywhere from **4 to 6 months** for the preparation and readiness portion of ISO 42001 compliance. This timeline varies depending on your organization's size and the complexity of your AI systems.

What If I Already Have ISO 27001?

If you have already implemented ISO 27001, the good news is that the process will be on the faster end of the timeline. Many controls will need to be tweaked rather than built from scratch.

How Long Does The Audit Take?

Several scoping factors determine how long your timeframe will be for the audit. Scoping factors include: the number of employees, complexity factors, and organizational role (producer, provider, developer, or user of AI). As a rough estimate, you can expect the certification audit by an accredited body to take **4 to 8 weeks.**

Working With Rhymetec

Rhymetec can help you save time and costs while obtaining ISO 42001 certification.

Our mission is to make cutting-edge cybersecurity and compliance services available to SaaS companies and startups. Traditionally, ISO frameworks can take hundreds of hours to implement. We help companies simplify the process and achieve ISO 42001 compliance in record time.

What we do for you:

- ✓ Conduct a gap analysis for you
- ✓ Conduct your risk assessment
- ✓ Draft an implementation roadmap for you
- ✓ Set up your AIMS structure
- ✓ Implement all necessary controls
- ✓ Conduct internal audits to prepare you for your official audit
- ✓ Work with an ISO 42001 certification body on your behalf
- ✓ Prepare all documentation for your audit
- ✓ Work closely with you for your pre-audit meeting and attend
- ✓ Remediate any issues from your audit
- ✓ Support ongoing improvement and your post-audit plan
- ✓ Keep you compliant with ISO 42001 for recertification every 3 years

Our team of experts acts as an extension of your team to work in the best interest of your company. With years of experience working among some of the most complex compliance regulations, we can provide you with strategic direction and hands-on support to simplify your ISO 42001 readiness and audit. We help you save time and money and focus on what really matters - moving your business forward.

Ready to learn more?
Book a no-obligation chat with our team to learn how we can help.

Rhymetec has been a terrific resource in helping us accomplish our security and compliance goals. It has been good to work with a competent vCISO who has the experience and knowledge that we need to answer our questions and help us feel compliant. It is also nice to know that he has a team of other experts backing him up for when we need it. Rhymetec's established relationships has helped us navigate the sometimes confusing, and often stressful, audit processes."

– VP of Regulatory Affairs, Fullpower Technologies, Inc.

ISO 42001 Compliance FAQ – 5 Frequently Asked Questions

1. What Is ISO 42001?

ISO 42001 is a certifiable international standard providing guidelines for building and managing AI tools. It offers a repeatable framework from which organizations can build solid operational governance and management systems while promoting responsible AI usage.

It covers areas including security, privacy, and ethical practices. It specifies the requirements for creating a reliable AI program that, when developed with overall business goals and daily functions top of mind, can improve the safety of AI systems while also serving as a business enabler.

2. Why Is ISO 42001 Compliance Important?

Certification serves as a Marketing & Reputation Management Tool:
Organizations can use their certification to reassure clients and prospects that they adhere to the highest standard in AI use and development. ISO 42001 certification acts as a mark of credibility, signaling that the organization has taken steps to implement best practices as laid out by an industry gold standard framework. If a prospect asks about your organization's AI practices, being able to show a certification is a powerful tool.

To Guide Strategic Implementation of AI:
ISO 42001 certification not only supports compliance with other regulatory and legal requirements but also positions you to fully reap the business benefits of responsible AI use. By following ISO 42001, companies reduce security risks, optimize decision-making processes, foster customer trust, and ultimately drive business growth and sustainability.

3. Who Needs ISO 42001 Compliance?

ISO 42001 is particularly useful for companies in the early stages of developing AI features in their products or those creating new products that offer AI services.

The AI ecosystem can be categorized into three roles:

AI Producers: Companies like Microsoft, OpenAI, and Anthropic that build and sell foundational AI models.

Service Providers: Organizations that consume these models from producers, customize them, and then sell them downstream.

Customers and Users: The end-users and businesses that utilize AI services and products.

ISO 42001 can apply to any business interacting with others in this ecosystem.

4. How Different Is ISO 42001 Vs. ISO 27001?

ISO 42001 is fundamentally different from ISO 27001, despite their complementary nature from a high-level structure perspective.

While ISO 27001 centers around information security management systems (ISMS), ISO 42001 is highly specialized in the scoping of AI systems. The good news is that ISO 42001 is designed to integrate smoothly with existing ISO frameworks, including ISO 27001.

ISO frameworks are designed to act as building blocks for each other, but there are many areas in which they diverge in control implementation. For example, both ISO 27001 and 42001 require a risk assessment. However, even if you've completed your risk assessment for ISO 27001, you would still need to identify risks specific to AI systems for 42001.

5. How Much Does ISO 42001 Certification Cost?

Direct Costs: Hiring an accredited certification body to conduct the audit is a primary cost. Depending on the size and complexity of your organization, this can range from $5,000 – $20,000. This fee typically covers the initial certification audit and any follow-up assessments.

You may need to allocate significant internal resources to manage the project, which can translate into measures like hiring temporary staff to handle regular duties. For this reason, many startups choose to hire consultants.

Consulting fees can range from $10,000 – $50,000, depending on the level of support you need. Consultants can assist with gap analysis, control implementation, and preparation for your audit.

Indirect Costs: There are potential costs around employee training and awareness and technology upgrades. You may need to invest in new software or upgrade existing systems. Costs here can vary greatly depending on your technology stack.

Lastly, maintaining ISO 42001 certification requires regular audits and continuous improvement. Budget for annual internal audits and surveillance audits, which can cost between $3,000 – $10,000 per audit per year, and allocate resources for ongoing training and process updates.

Rhymetec

Get In Touch

sales@rhymetec.com

rhymetec.com