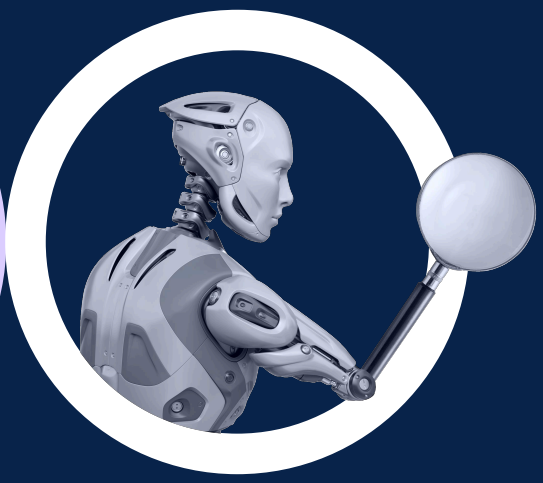


6clicks

ISO 42001 checklist:
The complete compliance guide

Contents

Introduction

The continuous integration of artificial intelligence into the operations and services of more and more organizations necessitates strong governance and regulation to manage the risks associated with these technologies. To ensure the secure use, development, and provision of AI systems, standards such as the ISO/IEC 42001 were established as part of a wider initiative for promoting responsible AI practices.

Achieving ISO 42001 compliance not only enables alignment with global AI standards but also unlocks many benefits for your organization. In this guide, we will explore the components of the ISO 42001 framework and provide you with a comprehensive walkthrough of the compliance process to help you on your journey toward trustworthy AI implementation and audit readiness.

Step 1:
Understanding ISO 42001

Before you go through the compliance and certification process for ISO 42001, first you need to gain an in-depth understanding of the framework and prepare your organization to conduct risk management and compliance activities.

ISO 42001 is the first globally recognized standard for building, implementing, and maintaining an AI Management System (AIMS), which refers to a set of processes, policies, and security measures that constitute an organization's approach to the responsible development, use, or deployment of AI systems. It was established by the International Organization for Standardization to guide organizations using or providing AI-based products or services in addressing AI-related risks.

The main components of ISO 42001 include its mandatory clauses, Annex A – which contains the controls of the framework, and three additional annexes which provide supplementary guidelines and resources for AIMS implementation.

ISO 42001 details specific requirements under Clauses 4 to 10:

Clause 4: Context of the Organization

The organization must identify the purpose of its AI system, internal and external requirements, stakeholders, business objectives, and other dependencies to set the scope of the AIMS.

Clause 5: Leadership

The organization must secure the support of top management in all AIMS-related activities, from AI policy creation to ongoing monitoring and periodic reviews.

Clause 6: Planning

The organization must determine the risks, opportunities, and impacts associated with its AI system, plan actions for addressing them, and set the objectives for the AIMS.

Clause 7: Support

The organization must support the effective implementation of the AIMS through adequate resource allocation, documentation and communication of information, and training and awareness.

Clause 8: Operation

The organization must implement processes and controls for the development, operation, and maintenance of the AIMS.

Clause 9: Performance Evaluation

The organization must monitor, measure, analyze, and evaluate the performance of the AIMS through internal audits and management review.

Clause 10: Improvement

The organization must correct nonconformities and put in place processes for the continuous improvement of the AIMS.

ISO 42001 establishes a structured framework for the secure management of AI systems throughout their life cycle, from planning and design to deployment and monitoring. The goal of ISO 42001 is to balance AI innovation with governance, fostering the development of transparent, ethical, and reliable AI systems. Adopting the ISO 42001 framework enables organizations to:

Facilitate compliance with global regulations like the EU Artificial Intelligence Act

Enhance stakeholder trust by demonstrating commitment to secure AI implementation

Implement effective risk management and AI governance, from risk assessment to treatment and monitoring

Maximize cost savings by eliminating or reducing incidents that could lead to damages and disruptions

Leverage AI technologies securely to increase efficiency and drive growth

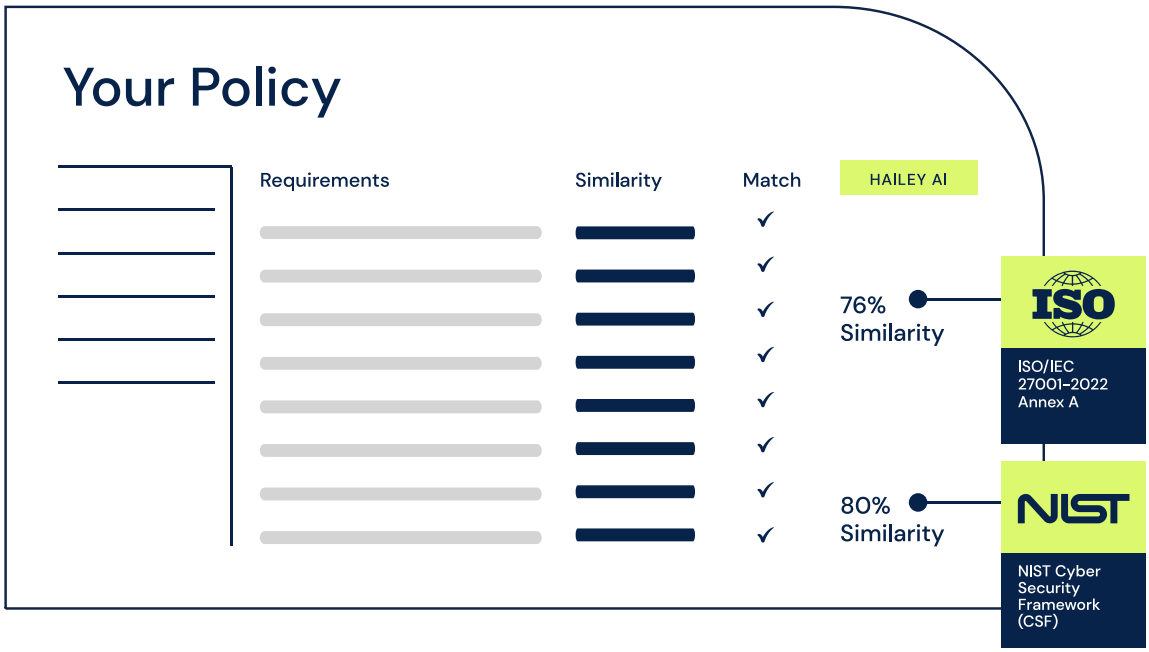
Part of understanding the requirements of the ISO 42001 framework involves identifying whether your organization is an AI provider (deploying AI-based products or services), an AI producer (designing, developing, and operating AI technologies), or an AI customer (the end user of an AI system). This can help you determine the applicability of ISO 42001 to your organization.

Step 2:

Conduct an initial gap analysis

The next step in preparation for the compliance process is to conduct an initial gap analysis to assess your current risk management practices and security implementation against the requirements of the framework. This helps in identifying all points of improvement and areas of non-compliance so you can streamline your efforts and prioritize actions with the most impact.

6clicks can help you automate this step through our ISO 42001-certified platform with AI-powered compliance mapping capabilities. Our AI engine Hailey, can help you map your existing controls to the provisions in ISO 42001 within mere seconds instead of days, automatically calculating similarity scores and providing you with a comprehensive overview of your compliance level.



Step 3:

Develop an AIMS implementation plan

Now that you have determined how much of your processes and controls are in scope of the framework, you can proceed to develop a project plan for the implementation of your AI management system and address the identified compliance gaps. There are a series of actions you can take during this step:

Assemble a team:

Appoint a project manager who will supervise and take ownership of the AIMS implementation. Assign roles and responsibilities to relevant team members who will be in charge of the development, operation, assessment, and maintenance of the AIMS, particularly those who specialize in AI, cybersecurity, risk management, and compliance. This team's job is to drive the entire project, which includes managing resources, coordinating between different departments, and ensuring that the implementation process aligns with the organization's business objectives and fulfills the standard's requirements.

Secure top management support:

One of the main requirements of ISO 42001 is the active involvement of the organization's top management in the AIMS implementation. Aside from playing an advisory role during the planning phase and granting the official authorization needed for the operation of the AIMS, they must also lead the establishment of AI policies and objectives, approve budgets, and oversee the effective distribution of resources. Boards and senior leadership must provide guidance and support throughout the project, and their responsibilities must be clearly defined.

Get down to the details of the project:

List down the resources needed, set timelines, and outline key steps or project milestones to map out the entire AIMS implementation process. Steps should be based on the requirements of the framework. Example steps include defining the context of the organization and determining the scope of your AIMS, setting objectives for the AIMS, formulating an AI policy, and establishing procedures for implementing changes to the AIMS.

Step 4:

Conduct AI system risk & impact assessments

A comprehensive risk assessment is necessary for the effective identification, analysis, prioritization, treatment, and management of risks associated with your AI system. This process involves gathering information across your organization to identify relevant and potential risks, assessing their likelihood and impact, and producing a risk score or risk rating to determine the severity of these risks.

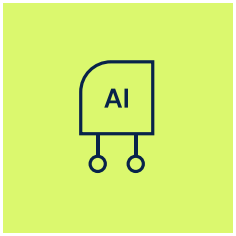
Your risk assessment should cover risks specific to AI technologies, focusing on areas such as:

Data privacy

The ability of the AI system to access, process, or disclose sensitive or confidential information

Algorithmic transparency

The traceability and explicability of the logic and processes behind the decision-making capabilities of the AI system



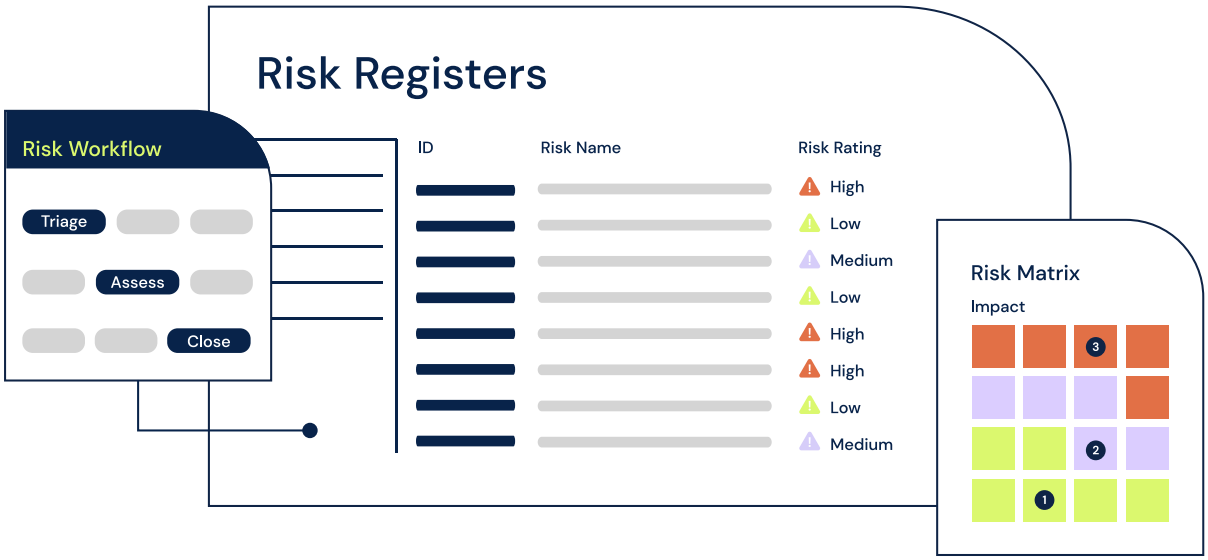
Bias and manipulation

The quality and integrity of the training data used for the AI system to ensure accurate and fair outcomes

On the other hand, an AI system impact assessment refers to the process of identifying and evaluating the potential impacts of an AI system on individuals, communities, and society. While a risk assessment focuses on evaluating cybersecurity threats and vulnerabilities as well as operational risks, an impact assessment examines the broader social, economic, environmental, and ethical impacts of the AI system. For both assessments, the organization must identify and analyze potential risk sources, events, and consequences, determine which risks or impacts are acceptable, and develop treatment plans to mitigate significant risks and negative impacts.

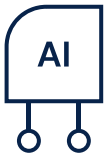
Identifying and evaluating AI-related risks and impacts can help you define the right objectives for your AIMS and ensure that your AI system aligns with ethical principles and upholds human rights and safety.

6clicks also makes this step 10x easier through its ready-to-use AI risk library and AI system impact assessment template, allowing you to expedite your risk and impact assessments. Meanwhile, 6clicks' risk management solution equips you with a powerful risk register featuring custom fields and workflows, automatic risk rating calculation, data visualization tools, and task management functionality for simplifying risk assessment and treatment. With the integrated modules of the 6clicks platform, you can identify and manage information on your AI system within the Assets Register and link your AI system to their associated risks for a holistic view of your risk profile.



Step 5:

Establish AI policies and objectives



Moving away from the planning stage and on to the AIMS development phase, this step involves determining the objectives of your AIMS and establishing AI policies to directly address the risks and impacts identified during earlier assessments. Objectives for your AIMS should encompass responsible AI principles such as fairness, privacy and security, and accountability, and detail the specific actions you plan to take to achieve them, which could include your risk management processes and security controls.

For your AI policy, include guidelines on the ethical use and development of AI technologies, risk management procedures, legal and regulatory considerations, policies on data governance and how to preserve the quality and integrity of data used in the AI system, and mechanisms such as documentation and reporting for transparency and accountability.

Step 6:

Conduct training & awareness programs

As mandated by Clause 7 in ISO 42001, the effective allocation of resources, including human resources, is critical in supporting the implementation of your AIMS. This means educating all employees on the proper use of the AI system and equipping personnel with AIMS-related duties with the knowledge, skills, and competencies necessary for the successful operation of the AIMS.

Organizations can do this by conducting training programs on AIMS and ISO 42001 compliance and raising awareness of responsible AI principles. Part of providing support for the AIMS also involves maintaining accurate, up-to-date, and accessible documentation of all AIMS-related data and establishing reliable communication lines and channels to facilitate the effective communication of AI policies, regulatory requirements, and other essential information across the organization.

Step 7:

Implement ISO 42001 controls

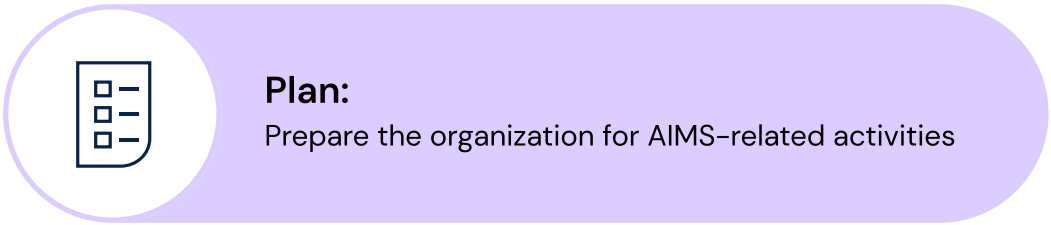
To finalize the implementation of your AI management system, the standard provides controls including implementation guidelines to help organizations put in place safeguards or security measures for mitigating AI-related risks.

ISO/IEC 42001:2023 Annex A has a list of controls grouped into 9 control objectives:

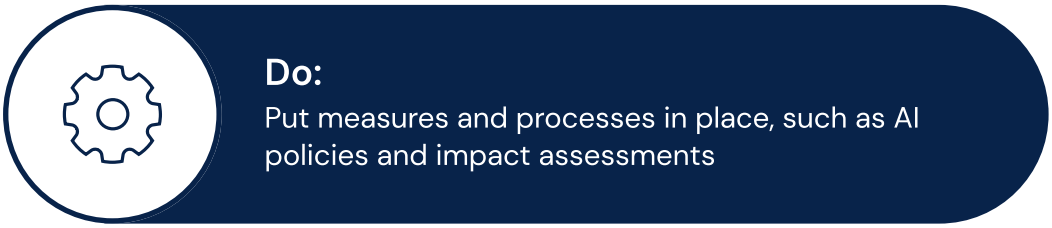
Control A.2: Policies Related to AI	The establishment and documentation of an AI policy that aligns with business objectives and responsible AI principles to guide the use, development, or deployment of the AI system Integration of the AI policy into existing organizational processes Maintaining the relevance and effectiveness of the AI policy through regular reviews by the organization's top management
Control A.3: Internal Organization	Definition and allocation of roles and responsibilities throughout the development, deployment, operation, and maintenance of the AIMS to ensure traceability and foster a culture of accountability across the organization Establishment of reporting mechanisms for AI concerns
Control A.4: Resources for AI Systems	Identification and documentation of resources critical to the AI system, such as data resources, tooling resources, AI system components, computing resources, and human resources at each stage of the AI system life cycle
Control A.5: Assessing Impacts of AI Systems	Identification, evaluation, and management of the impacts including potential benefits of the AI system on individuals, communities, and societies throughout its life cycle Mitigation of potential harms Documentation of the intended use of the AI system and the process and results for risk and impact assessments

Control A.6: AI System Life Cycle	Documentation of the organization's objectives for the development of the AI system Documentation of design and development processes for the AI system Identification and documentation of AI system requirements and specifications Documentation of the AI system's architecture, interface, and other design and development components Maintaining the integrity of the AI system through verification and validation processes Documentation of a deployment plan for the AI system Documentation of the performance of the AI system throughout its life cycle to facilitate management and continuous improvement: from development, to deployment, operation, and monitoring Technical documentation of the AI system including information on functionality, usage, and limitations Recording of event logs throughout the AI system's life cycle
Control A.7: Data for AI Systems	Definition and documentation of requirements for ensuring the quality of data used in the AI system to maintain reliable and fair outputs and prevent errors and biases Documentation of the origin, transformation, and usage of data throughout the AI system's life cycle Documentation of data acquisition, selection, and preparation methods to ensure suitability for use in the AI system
Control A.8: Information for Interested Parties of AI Systems	Provision of documentation and essential information about the AI system by the organization to users and other interested parties, including its purpose, instructions for use, and technical limitations Establishment of mechanisms for external reporting of AI-related issues by users and other interested parties Timely communication of AI-related incidents to internal and external stakeholders to build trust and reinforce the organization's commitment to ethical AI implementation Identification and documentation of the organization's obligations for communicating information about the AI system to users and other interested parties
Control A.9: Use of AI Systems	Definition and documentation of processes to guide other organizations in the responsible use of the AI system Documenting and monitoring the use of the AI system to ensure it is operated and deployed according to its intended purpose Incorporating human oversight into the development and operation of the AI system
Control A.10: Third-Party & Customer Relationships	Clear allocation of responsibilities between the organization and its partners, suppliers, customers, and other third parties regarding the use of the AI system Establishing assessment processes for suppliers to ensure that the AI system your organization will use or provide meets ethical standards and compliance requirements Aligning the development of the AI system with customer needs and expectations

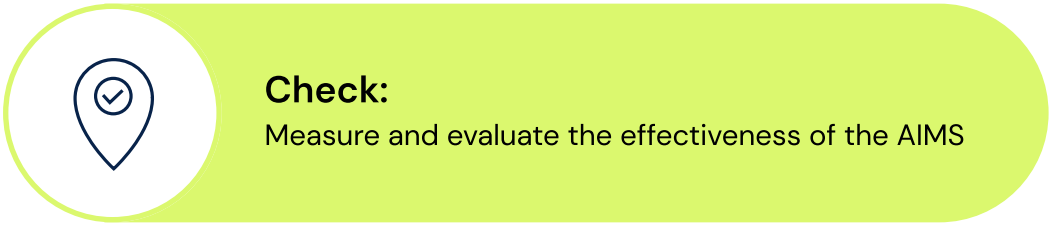
ISO 42001 provides guidance for the implementation of these controls through the Plan-Do-Check-Act (PDCA) methodology. The standard prescribes that organizations utilize the PDCA cycle to adopt a continuous approach to AI governance, treating the development, implementation, operation, monitoring, and improvement of an AIMS as an iterative process:



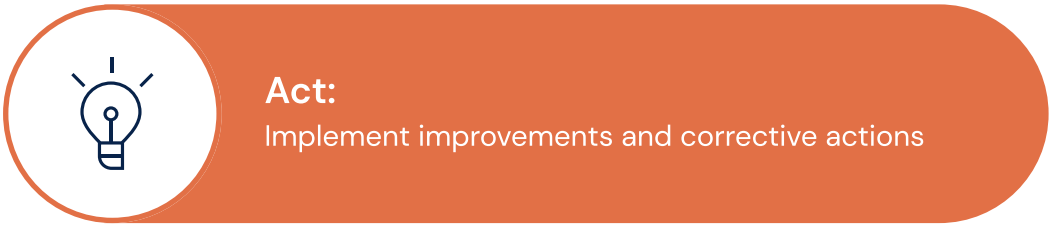
Plan:
Prepare the organization for AIMS-related activities



Do:
Put measures and processes in place, such as AI policies and impact assessments

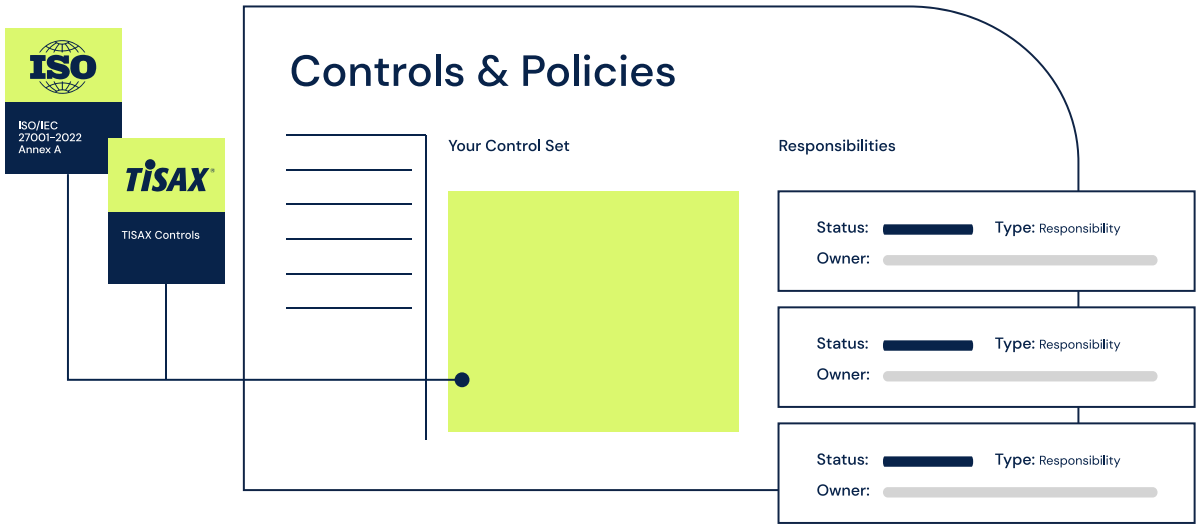


Check:
Measure and evaluate the effectiveness of the AIMS

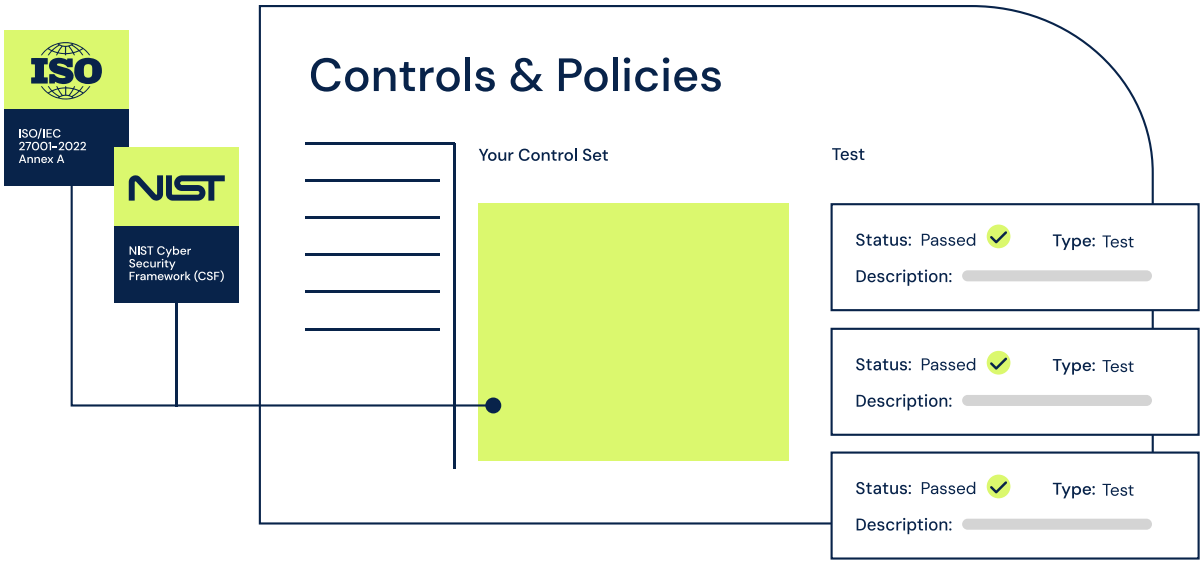


Act:
Implement improvements and corrective actions

Streamline the implementation and management of your AI controls using 6clicks' compliance management solution. You can use our turnkey AI control set to fast-track the process or build your own within the Controls module. Catalog and organize your controls, create control responsibilities and assign tasks to team members, and directly link AI controls to provisions in ISO 42001 as well as to risks, issues, and assessments, enabling seamless control management and evidence collection.



Then, using our Continuous Control Monitoring feature, you can perform manual and automated tests to verify the effectiveness of AI controls and get real-time alerts for non-conformities, configuration errors, and control failures. With this capability, your organization can proactively address issues, allowing you to ensure robust control implementation for your AI system that is consistent with the requirements of ISO 42001.

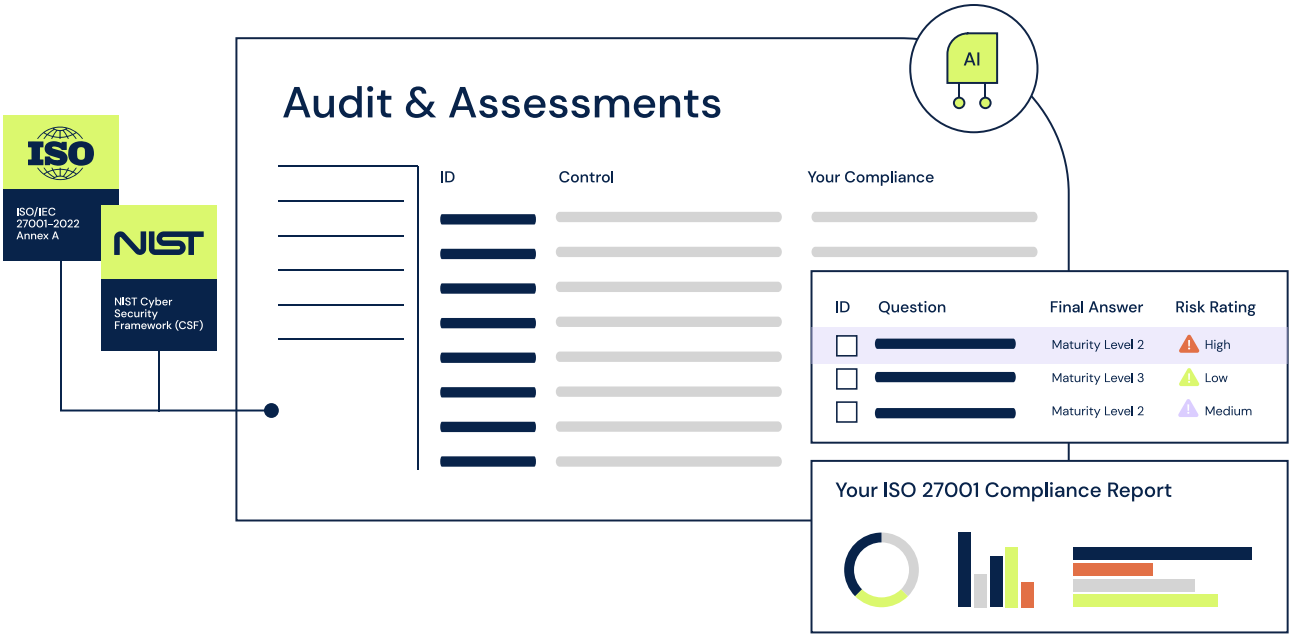


Step 8:

Perform internal audits

With controls now in place, it's time to assess your organization's compliance with ISO 42001 and determine whether you have fulfilled the requirements for an effective AIMS. Perform internal audits to validate the implementation of controls, AI policies, risk management procedures, and roles and responsibilities, covering all processes and components associated with your AIMS. Based on the findings, implement improvements or corrective actions to address any issues or areas of non-compliance.

Audits don't have to be a demanding task with 6clicks' AI-powered audit & assessment capabilities. Our AI engine Hailey automates audit and assessment responses by analyzing previous data, saving valuable time and resources. Meanwhile, you can create question-based or requirement-based audits and assessments, customize and automate workflows, and generate board-ready audit and assessment reports to optimize your audit process.



Step 9:

Establish continuous monitoring and review

Monitoring and evaluating your AIMS is another key requirement in ISO 42001. The organization must define methods for monitoring, measuring, analyzing, and evaluating the performance of the AIMS, such as regular audits and assessments and management reviews, to continuously identify and respond to evolving risks and regulatory demands. A process for collecting, documenting, and analyzing performance data must also be developed and implemented.

Top management must conduct periodic reviews of the AIMS, including AI policies, audit and assessment results, and whether the objectives initially set by the organization are being fulfilled. The organization must then address non-conformities or opportunities for improvement found during audits or management reviews. By establishing continuous monitoring and review processes, you can foster ongoing improvement of your AIMS and continuously enhance AI governance.

Step 10:

Prepare for ISO 42001 certification

Now that your AIMS is fully implemented and operational, with monitoring and review systems in place, your organization is ready to go through the next step: preparing for the ISO 42001 certification process.

To prepare, compile the necessary documents for the external audit that will be conducted by a certification body. This includes all documentation for your AIMS, such as records of your AI policies, risk and impact assessments, and internal audits, as well as the technical documentation of the AI system.

A main requirement for ISO 42001 certification is the Statement of Applicability (SoA), which is a document that specifies the different Annex A controls included in your AI management system. To create the Statement of Applicability, identify which of the controls in ISO 42001 Annex A have been implemented and not implemented and provide justification as to why each control is applicable or not applicable to your organization. Your SoA must also document all identified risks along with the equivalent measures (controls) that your organization has established to mitigate and manage them.

Breeze through your ISO 42001 audit by centralizing all evidence and documentation in a single location. With the 6clicks platform, you can conduct risk and impact assessments, perform audits, manage tasks, and coordinate with team members all in one place, and be able to export complete reports and documentation for all AIMS-related activities, streamlining the preparation needed for the audit and certification process. Meanwhile, you can upload your SoA, assessment results, technical documentation, and other compliance evidence to the 6clicks Trust Portal to provide easy access for both internal and external stakeholders.

Step 11:

Undergo an external audit and address audit findings

Once documentation is ready, organizations can proceed to go through an external audit with an accredited certification body. This process typically takes a few months and is split into two stages. During the initial review, auditors perform a comprehensive examination of the organization's fulfillment of ISO 42001 controls and requirements by reviewing its policies, procedures, and operations through the provided documentation.

Afterward, during the certification assessment stage, the audit body will conduct onsite or virtual audit including interviews with leadership and technical teams to assess the practical implementation of the AIMS and determine the organization's eligibility for certification. A detailed compliance report will then be produced following these procedures, including a formal evaluation of the AIMS' compliance with the standard. If no major nonconformities are found, the organization will be granted ISO 42001 certification.

Step 12:

Address audit findings and maintain continuous compliance

During the external audit is also when compliance gaps are identified and opportunities for improvement are provided by the certification body. To attain certification, the organization must plan immediate as well as long-term actions, such as updating policies or introducing new controls, to address these gaps and continuously improve its AIMS.

Once certification is achieved, the organization is responsible for renewing its ISO 42001 compliance certification every three years, accompanied by an annual surveillance audit, to maintain ongoing compliance and ensure its AIMS remains aligned with the latest regulatory requirements and cybersecurity best practices.

Best practices for compliance

The journey to compliance requires commitment and consistent efforts to ensure success and make the process of AIMS implementation, deployment, and maintenance easier. Here are some best practices you can adopt for an effective compliance process:

Preparation

- **Incorporate AIMS into core business operations**

  AI policies, risk management procedures, and documentation and monitoring processes must be deeply integrated into your organizational culture to enable seamless adoption of responsible AI practices.

- **Leverage technology**

  Utilize powerful technology that can streamline risk management, automate control and compliance validation and monitoring, and expedite audit readiness. The 6clicks platform provides all these capabilities and more to help you build a robust AIMS and achieve ISO 42001 compliance faster.

Audit

- **Facilitate engagement and communication**
  Make sure that documents are easily accessible and submitted within the allotted time to avoid delays. Assign a team member who will serve as the point of contact between your organization and the audit body for smooth communication and coordination.

Post-certification

- **Publish audit findings and certification**
  Provide real-time visibility of your compliance posture and build trust by making the results of your external audit and certification readily available. The 6clicks Trust Portal is where you can publicly or privately share certifications and other documents to demonstrate your compliance and foster assurance with stakeholders.
- **Embrace continuous improvement**
  Conduct regular audits and assessments, policy reviews and updates, and staff training to maintain the effectiveness of security controls and risk management processes and continually improve your AIMS.

Learn more about 6clicks

Book a demo

Ready to build resilient cyber GRC programs powered by AI? Explore the 6clicks platform today.

Book a demo

See 6clicks in action

Watch exclusive demonstrations of our AI and cyber capabilities through our on-demand webinars.

Watch webinar

Explore helpful resources

Get access to the latest cybersecurity, risk, and compliance news and thought leadership by industry experts.

Access all resources

6clicks

6clicks is transforming cyber risk and compliance management with its AI-powered platform, featuring the pioneering Hub & Spoke architecture tailored for federated businesses, advisors, and managed service providers (MSPs). As the first platform to introduce an AI engine specifically designed for GRC, 6clicks delivers a smarter approach to managing cyber risk and compliance. The 6clicks business model is channel-aligned, and SaaS licensing is transparent and straightforward with unlimited user access and access to frameworks. With sales and support operations presence across APAC, EMEA, and NA, and private cloud hosting options on Microsoft Azure, 6clicks equips cyber leaders and professionals to build resilient, trusted, and scalable cyber risk and compliance programs, disrupting traditional GRC solutions and setting a new standard in the industry.

Request a demo