hyperproof | BDO

GUIDE

ISO 42001:

Paving the Way Forward for AI Governance

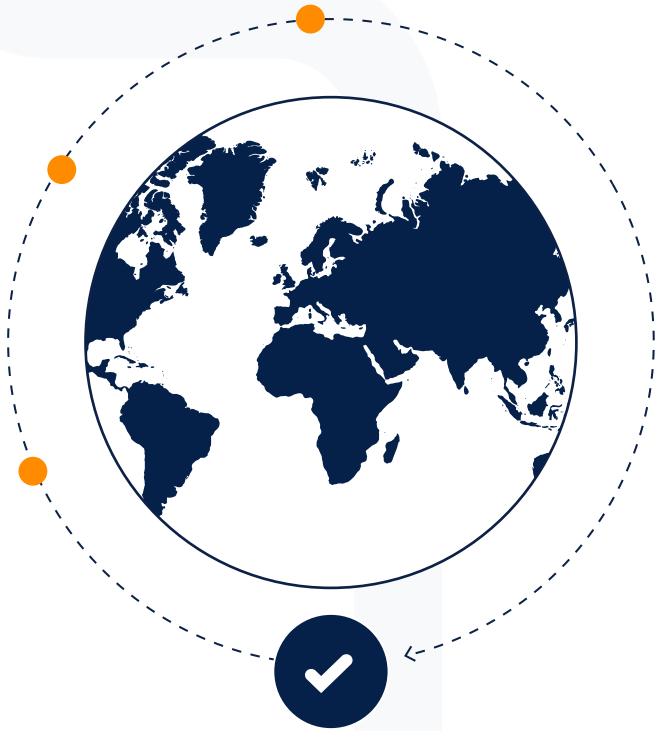
hyperproof.io // info@hyperproof.io

Introduction

Artificial intelligence (AI) is shaping and reshaping our world every day, both in our daily routine and at work. Whether you're using generative AI to create content, and images, write code, or more advanced work, AI impacts your world. In addition to its powerful capabilities comes an influx of new and unique risks. How can you better govern AI technologies and build, operate, and manage fair, transparent, accountable, and trustworthy systems?

ISO/IEC 42001, also known as **ISO 42001**, provides a structured framework to address these challenges. It offers a roadmap for organizations to manage AI-related risks and opportunities and includes appropriate controls to help manage and mitigate AI risks.

In this guide, we'll outline everything you need to know about the world's first artificial intelligence framework: ISO 42001. Whether you're a small startup or a large enterprise, this guide will equip you with the knowledge and resources to navigate the complex landscape of AI governance.



What is ISO 42001?

Developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), the ISO 42001 standard provides a structured approach to managing the risks and opportunities associated with AI technologies.

This comprehensive standard outlines the requirements for an Artificial Intelligence Management System (AIMS).

> According to ISO, an AI management system is "a set of interrelated or interacting elements of an organization intended to establish policies and objectives, as well as processes to achieve those objectives, in relation to the responsible development, provision or use of AI systems."

ISO 42001 follows a similar structure as other ISO management system standards, including:

- Documenting the intended use of AI systems and the role of the organization
- Completing an AI risk assessment and creating a statement of applicability to denote the inclusion and exclusion of Annex A controls
- Requiring the conduct of periodic internal audits and management reviews

At its core, ISO 42001 is designed to help organizations of all sizes:

- Establish clear policies and objectives for AI development and use
- Implement robust processes for AI system lifecycle management
- Ensure ethical considerations are integrated into AI decision-making
- Maintain transparency and accountability in AI operations
- Continuously improve the management and operations of AI systems

The ISO 42001 standard serves as a reference framework for AI governance that companies can implement to create a solid baseline of controls to manage AI-specific risks. Implementing the standard will also help organizations to comply with other AI-related laws and regulations.

Just like your SOC 2® report builds trust in your organization, ISO 42001 is a way for organizations to demonstrate that they have strong controls protecting against AI. **Trust matters**, especially when AI enters the equation.

How do I get ISO 42001 certified?

To obtain an ISO 42001 certification, you'll need to undergo an external audit by an approved auditing firm. That means being audited against the ISO 42001 framework.

Preparing for an ISO 42001 audit

As with any ISO audit, you should first define the scope. To start, define the purpose of AI in the organization. Are you *developing* or are you using AI? What does AI mean within the context of your company? What are the specific objectives or use cases for AI within the company? Note that not every department or product/service needs to be included within the scope. Focus on the ones significantly leveraging AI as a part of their operations.

Note: Even the most mature companies do not have auditable controls for AI. If you feel as if your company is lagging behind, keep this in mind.

ISO 42001: A Deep Dive

ISO 42001 Clauses

The clauses of the ISO 42001 standard define the scope and language in which the standard is written. Terminology is defined and context for the framework is given, along with guidance for leadership, planning, support, operation, performance evaluation, and improvement.

Let's dive into an overview of each clause:

Clause 1: Scope

Clause 1 defines the scope of the standard, outlining what the document shares, including requirements, guidance, and intended use. Most notably, the standard emphasizes that ISO 42001 is designed to be universally applicable, encompassing organizations of all sizes, types, and characteristics that either produce or employ AI-powered products or services.

Clause 2: Normative references

Clause 2 is short and explains which documents are referred to within the text, primarily ISO/IEC 22989:2022.

Clause 3: Terms and definitions

Clause 3 defines terms used throughout the standard, ensuring that all readers are using shared terminology and definitions, which helps with the overall clarity of the document. Refer to pages 1-5 of the official documentation for these terms and definitions.

Clause 4: Context of the organization

Clause 4 sets up the context of the organization, providing an overview of considerations the organization should undertake to determine the organization's objectives for developing or using AI systems. It also describes the types of possible roles, with further details available in ISO 22989 (Clause 4.1).

According to Clause 4, it is also vital to understand the needs and expectations of interested parties (Clause 4.2), to determine the scope of the AI management system (Clause 4.3), and to define and document the AI management system (Clause 4.4).

The most fundamental step is for the organization to identify and document the scope of the ISO 42001 standard. First, identify your internal and external stakeholders and understand their specific requirements. Then, consider the requirements of any AI-specific laws or regulations you must comply with.

As noted earlier, the scope for implementing the requirements of the standard doesn't need to be considered for your entire company. Alternatively, you can consider:

- A specific department
- A single team
- An application, product, or service
- Modules or features of an app that leverages AI

These are just a few examples. There are many other business areas that you could consider for the scope of ISO 42001 instead of your entire company's operations.

Note: Organizations must consider both outside factors and internal matters when dealing with AI management. These factors can differ depending on the company's role, jurisdiction, and impact on the company's ability to reach its AI management goals (Clause 4.1).

Clause 5: Leadership

Clause 5 handles leadership, describing how top management should ensure, direct, and support the AI management system. The subclauses include leadership and commitment (Clause 5.1), AI policy (Clause 5.2), and roles, responsibilities, and authorities (Clause 5.3).

This clause ensures sufficient management support to establish, operate, and manage an AIMS. An appropriate level for leadership commitment and buy-in is evidenced by:

- Periodic oversight
- Formulating and publishing an AI policy
- Allocation of resources, including creation of specialized groups, roles or defining responsibilities for managing AI governance, risk, and controls-related activities

Clause 6: Planning

Clause 6 tackles the planning for the AI management system and describes what to consider. This includes actions to address risks and opportunities (Clause 6.1), AI objectives and planning to achieve them (Clause 6.2), and planning of changes (Clause 6.3).

Clause 6.1 is broken down into multiple subclauses that outline general planning (Clause 6.1.1), AI risk assessment processes (Clause 6.1.2), and AI system impact assessment processes (Clause 6.1.4).

The organization is required to have a formal process for carrying out an AI risk assessment and system impact assessment. Based on the results of the risk assessment, a statement of applicability is created that denotes which of the Annex A controls will be applicable or not applicable to the organization and the reasons.

AI RISK ASSESSMENTS VS. AI SYSTEM IMPACT ASSESSMENTS

Creating both a risk and system impact assessment is unique to the ISO 42001 standard, but there are key differences between the two. The AI risk assessment process takes you through analyzing and then evaluating AI risks. AI system impact assessments, on the other hand, help determine the potential consequences of deploying an AI system, its intended use, foreseeable misuse, and the impact of these aspects on individuals, groups, and/or societies.

The AI system impact assessment takes into account the technical and societal context in which the AI system is deployed. By defining the potential consequences of AI use and misuse, you can better understand the impact of AI on individuals, groups, and/or societies.

Additional information regarding AI risk and impact assessments can be found in the Annexes of the ISO 42001 standard.

Clause 7: Support

Clause 7 provides prescriptive instructions for the organization to take regarding AI management systems. It is broken into five subclauses:

- Resources (Clause 7.1)
- Competence (Clause 7.2)
- Awareness (Clause 7.3)
- Communication (Clause 7.4),
- Documented information (Clause 7.5)

Of these, Clause 7.5 is the most complex, further broken into three subclauses covering general documentation (Clause 7.5.1), creating and updating documented information (Clause 7.5.2), and control of documented information (Clause 7.5.3).

The clause requires the organization to identify and nominate individuals with the right competence to carry out various responsibilities related to the AI system. You must have a plan and process to communicate and disseminate appropriate information related to the AIMS and its associated activities to internal and external parties.

Further, the trove of documentation required by this standard including policies, standards, procedures, templates, and other completed artifacts should be created, updated, stored, and archived using a standardized process.

Clause 8: Operation

Clause 8 demonstrates how to operationalize ISO 42001 through operational planning and control (Clause 8.1), AI risk assessments (Clause 8.2), AI risk treatments (Clause 8.3), and AI system impact assessments (Clause 8.4). This clause requires the effective implementation of the applicable controls from Annex A and periodically conducting risk and system impact assessments.

This clause works closely with Clause 6, as well as the controls in Annex A and the implementation guidance in Annex B. The results of AI risk treatments, AI system impact assessments, and AI risk assessments should all be kept documented.

Clause 9: Performance evaluation

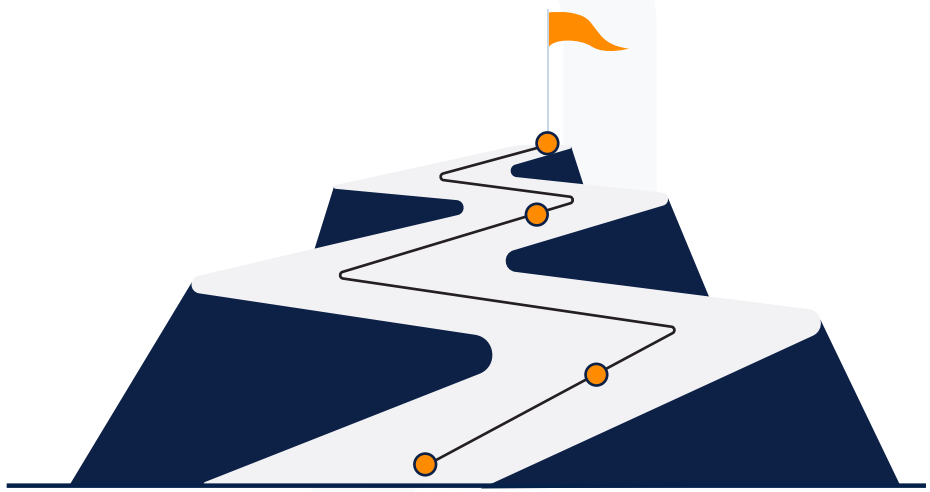
Clause 9 guides readers through performance evaluation, with the clause broken down into:

- Monitoring, measurement, analysis, and evaluation (Clause 9.1)
- Internal audit (Clause 9.2)
- Management review (Clause 9.3)

Clause 9.2 and 9.3 are longer, broken into two and three subclauses, respectively.

Internal audit, Clause 9.2, covers general information for internal audits, helping organizations plan, establish, implement, and maintain audit programs. This includes the frequency, methods, responsibilities, planning requirements, and reporting aspects of internal audits (Clause 9.2.1). It also guides organizations to define objectives, criteria, and scope for each audit, select auditors, conduct audits, and ensure results are reported to the necessary stakeholders (Clause 9.2.2).

Management review, or Clause 9.3, is organized into three subclauses: general (Clause 9.3.1), management review inputs (Clause 9.3.2), and management review results (Clause 9.3.3). Generally, the clause refers to how top management should regularly review the outputs and relevant metrics from the AI management system to maintain its suitability, adequacy, and effectiveness (Clause 9.3.1).



Clause 10: Improvement

Clause 10 consists of two subclauses covering the improvement of AI management systems. These clauses focus on continual improvement (Clause 10.1) and nonconformity and corrective action (Clause 10.2).

Clause 10.1 covers general improvement of the “suitability, adequacy, and effectiveness” by introducing planned changes and improvements over time for the AI management system, while Clause 10.2 dives deeper into managing issues, nonconformities, and how to take corrective action. For more information on nonconformities, please refer to Clause 10.2 of the ISO 42001 standard.

ISO 42001 Annexes

Annex A: Reference control objectives and controls

The reference control objectives and controls annex, known as Annex A, defines all controls in the ISO 42001 standard.

Organizations have the flexibility to select and implement control objectives and controls that are most relevant to their specific needs. They are not obligated to use all the control objectives and controls outlined in Table A.1. Furthermore, companies can develop and put into practice their own custom controls tailored to their unique requirements.

For more information, please refer to the section of this guide on statements of applicability (SOA).

Annex B: Implementation guidance for AI controls

While Annex A defines controls, Annex B provides guidance for implementing AI-specific controls within an organization. It helps you understand and write AI policies (A.2.2), and defines lines of accountability within your business (A.3.1). It also contains valuable guidance for performing an AI risk assessment, allowing you to evaluate your AI control design.

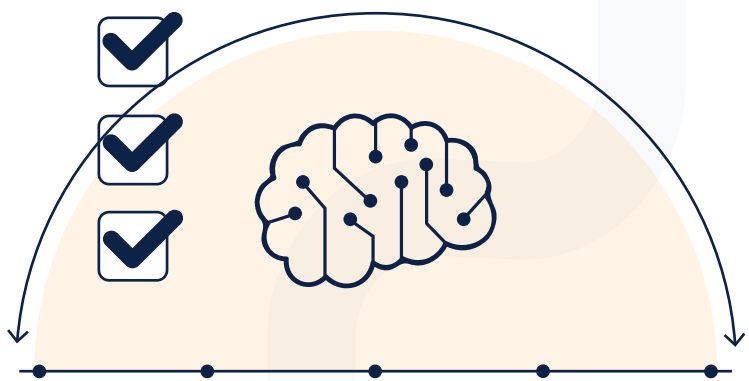
Annex B gives detailed instructions for implementing the standard, from defining AI life cycles (Clause B.6.2) to analyzing the quality of data used in AI training (Clause B.7.4). Annex B colors in the framework and provides essential background information about why AI governance matters.

Annex C: Potential AI-related organizational objectives and risk sources

This annex presents a range of organizational objectives, risk sources, and descriptions for consideration in risk management. It's important to note that this list is not all-encompassing and may not apply universally. Each organization should identify the objectives and risk sources most relevant to their specific context.

For a more comprehensive understanding of these objectives and risk sources, as well as their connection to risk management, refer to ISO/IEC 23894. This standard provides in-depth information on the subject.

Regular assessment of risks for AI systems is crucial. By evaluating these systems initially, periodically, and when circumstances warrant, organizations can gather evidence to ensure their AI systems align with organizational objectives. This ongoing evaluation process is key to maintaining effective risk management and compliance.



Annex D: Use of the AI management system across domains or sectors

Annex D outlines the applicability of ISO 42001, especially as it relates to various domains and sectors of a business. It also provides guidance for holistically assessing and understanding AI management systems (AIMS).

By adopting this holistic perspective, organizations can better identify interdependencies, mitigate risks, and optimize performance across the entire system. This approach aligns with best practices in risk management and compliance, promoting a more robust and resilient operational framework.

ISO 42001 controls

To better understand ISO 42001's controls, we've broken them out into categories reflecting their most common themes: policies and governance controls, data controls, AI system life cycle controls, and system impact assessment controls.

Note: Because we have categorized the following controls, they may appear out of order within this guide.

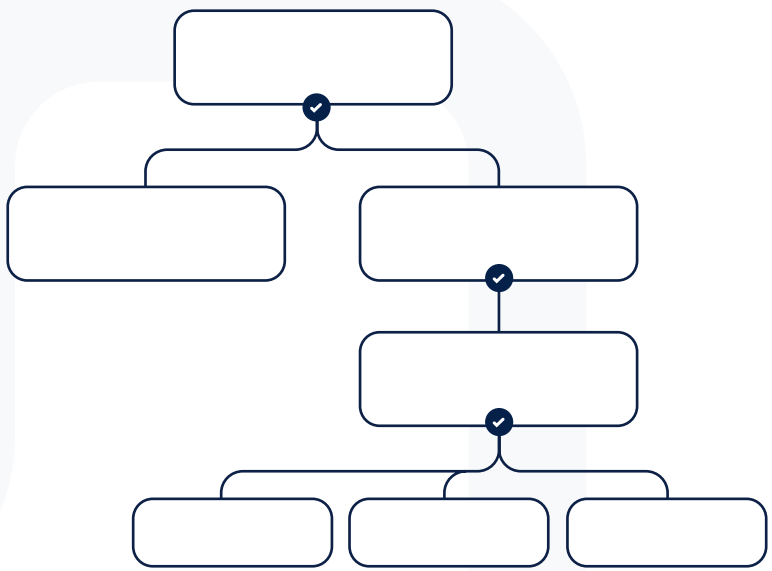
POLICIES AND GOVERNANCE CONTROLS

Annex A Control A.2 – Policies Related to AI

A.2's objective is to ensure that AI systems receive appropriate direction and support from leadership, aligning them with the company's business needs and strategic goals. This control emphasizes the importance of management's role in directing AI initiatives to meet specific business requirements.

A.2 is broken down into three areas: AI policy (A.2.1), alignment with other organizational policies (A.2.3), and review of the AI policy (A.2.4). These controls cover documenting an overarching company-wide policy that outlines:

- The rules for and guides the development and use of AI systems
- Determining where other existing organizational policies can be affected by the use of AI or the policies apply to business objectives with regards to AI systems
- Regular review of AI policy at planned intervals and as needed to ensure suitability, adequacy, and effectiveness



Annex A Control A.3 – Internal Organisation

A.3's objective is to help establish lines of accountability in order to uphold a responsible approach to implementing, operating, and managing AI systems.

A.3 has two controls: AI roles and responsibilities (A.3.2) and reporting of concerns (A.3.3). These controls help determine responsibilities within your organization as it pertains to AI throughout its lifecycle and process for reporting concerns.

Annex A Control A.8 – Information for Interested Parties of AI Systems

A.8's objective is to provide relevant stakeholders with essential information to comprehend and evaluate both the positive and negative risks and impacts associated with AI systems. This aims to ensure transparency and informed decision-making regarding AI systems by ensuring relevant stakeholders have crucial information.

This set of controls requires the organization to provide detailed instructions on how to use and work with the AI system and also, provide a mechanism for users to report any bugs, errors, or problems with the AI system. The organization must have a formal process in place to communicate relevant information about the features, capabilities, and incidents pertaining to the AI system.

A.8 is broken down into four areas: system documentation and information for users (A.8.2), external reporting (A.8.3), communication of incidents (A.8.4), and information for interested parties (A.8.5). These requirements aim to create a framework for open and responsible communication about AI systems. By clearly defining what information needs to be shared, how users can report issues, and how incidents will be communicated, organizations can build trust and transparency with their stakeholders.

This approach helps manage expectations, address concerns promptly, and maintain positive relationships with those affected by AI technologies. Ultimately, these practices contribute to more responsible AI development and deployment, ensuring that all parties have a clear understanding of the AI system's capabilities, limitations, and potential impacts.

Annex A Control A.10 - Third-Party and Customer Relationships

A.10's objective is to make sure the organization knows what its responsibilities are, stays accountable for its actions, and shares risks fairly when working with third parties at any stage of the AI system life cycle.

A.10 is broken into three controls: allocating responsibilities (A.10.2), suppliers (A.10.3), and customers (A.10.4). These controls help the organization ensure responsibilities are distributed between the organization, partners, suppliers, customers, and third parties (A.10.2), as well as establish processes to ensure usage or development of the AI system aligns with the organization's approach to responsible AI systems (A.10.3).

Lastly, the organization must ensure a responsible approach to developing and using AI systems and consider customer expectations and needs (A.10.4). This domain will cover only the third parties or vendors who are involved in establishing and maintaining the AI system and not all of the suppliers used by the company,

DATA CONTROLS

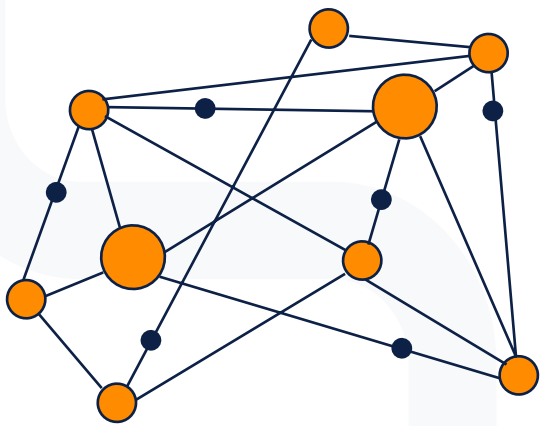
Annex A Control A.7 – Data for AI Systems

A.7's objective is to help the organization understand the role and impact of data used by – and to create – AI systems, throughout the entire AI life cycle. A.7 is broken down into five controls: data for the development and enhancement of AI systems (A.7.2), acquisition of data (A.7.3), quality of data for AI systems (A.7.4), data provenance (A.7.5), and data preparation (A.7.6).

These controls help define and implement data management practices, addressing topics like privacy and security implications due to the use of data, security and safety threats that can arise from data-dependent AI system development, transparency and explainability aspects including data provenance and the ability to explain how data are used for determining an AI system's output, representativeness of training data compared to operational domain of use, and accuracy and integrity of the data.

Data acquisition (A.7.3) regards the documentation processes for acquisition and selection of data used in AI systems, including:

- Data sources and categories of data
- Characteristics of data source and data subject demographics
- Data rights and metadata



A.7.4 documents requirements for data quality to ensure data used in the AI system life cycle meets the requirements. Additionally, it is important to consider the impact of bias on system performance and system fairness.

Lastly, data provenance and preparation controls document a process for recording the provenance of data and document details of data preparation methods used, respectively.

These are important controls as the **accuracy of the AI system depends on the type and quality of data used to train the underlying model**. It is critical to identify the correct data types and sources from where it will be obtained.

Further, the raw dataset must be prepared and cleaned for consistency and to remove any errors. Lastly, the quality of the data must be verified to ensure it is exhaustive and diverse to prevent the introduction of bias in the system outputs. The entire workflow of the data from source to its eventual destruction must be captured and logged.

AI SYSTEM LIFECYCLE CONTROLS

Annex A Control A.4 – Resources for AI Systems

A.4's objective is to ensure the organization maintains a comprehensive inventory of all AI system resources, encompassing both components and assets, to facilitate a thorough understanding and management of associated risks and impacts.

A.4 is broken down into five parts, including resource documentation (A.4.2), data resources (A.4.3), tooling resources (A.4.4), system and computing resources (A.4.5), and human resources (A.4.6).

ISO 42001 notes that it is important to identify and document all relevant resources for all AI system life cycle stages and any other AI-related activities relevant to the organization. Resources for the purpose of this standard include people, processes, tools, and technology required for the AIMS. It broadly comprises personnel with niche skill sets; tools and utilities; application software and database needs and hardware specifications like compute, storage, and memory.

Annex A Control A.6 - AI System Life Cycle

A 6.1

A.6.1's objective is to guide organizations in establishing and recording clear goals for responsible AI creation. It requires companies to set up and implement specific processes that ensure AI systems are designed and developed ethically and responsibly.

This approach aims to embed accountability and thoughtful practices into the early stages of AI development, helping to create AI systems that are aligned with ethical standards and organizational values from the outset.

A.6.1 is broken down into two areas that cover the responsible development of AI systems (A.6.1.2) and the processes for responsible design and development of AI systems (A.6.1.3).

A.6.1.2 instructs organizations to document steps to incorporate objectives into every stage of system development from requirements specification, data acquisition, data conditioning, model training, verification, and validation.

A.6.1.3 is similar to the software development lifecycle (SDLC), in that it documents the lifecycle stages, approval and testing requirements, training data expectations and rules, release criteria, and usability and change control for AI systems.

A.6.2

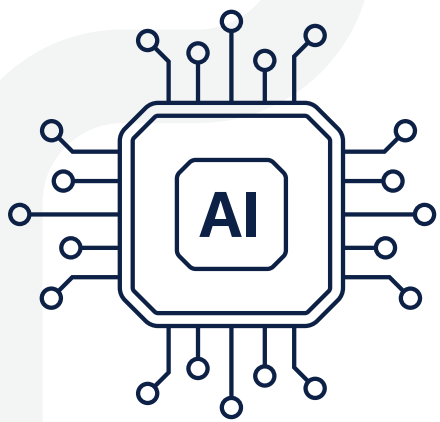
The objective of A.6.2 aims to establish clear guidelines and specifications for every phase of an AI system's existence. This comprehensive approach ensures that each stage of the AI lifecycle is governed by well-defined standards and requirements.

A.6.2.2 includes details of why the AI system is being developed and how the model can be trained, all while data requirements are achieved.

A.6.2.3 includes architecture details including hardware and software components. The key details must cover your machine learning approach and learning algorithms, as well as the type of machine learning models to be used.

A.6.2.4 covers model verification and validation. Given the far-reaching impacts of AI systems, it is critical to ensure the models are tested adequately before deploying them for use. The organization has to define the type, level, and extent of testing that will have to be done, in addition to specifying criteria thresholds for metrics like accuracy, drift, bias, and so on. Further, the organization must document the test results clearly for every AI-related system change.

A.6.2.5 instructs the organization to create a deployment plan for the AI system. Appropriate requirements should also be met before the deployment of the system.



Annex A Control A.9 – Use of AI Systems

A.9's objective hones in on the responsible usage of AI systems, per your organization's policies.

A.9 is broken down into three controls: processes for responsible use of AI systems (A.9.2), objectives for responsible use of AI systems (A.9.3), and intended use of the AI system (A.9.4).

Per this control, organizations must establish and document processes for the responsible use of AI systems, including defining clear objectives to guide responsible AI usage. Further, appropriate monitoring processes – including a review of relevant logs – must be implemented to ensure that the system was deployed and used according to its intended objectives.

This approach aims to promote the ethical and appropriate use of AI technologies within the organization, aligning actual usage with predetermined goals and guidelines. By documenting processes and objectives, the organization creates a framework for accountability and consistency in AI system deployment and operation.

SYSTEM IMPACT ASSESSMENT CONTROLS

Annex A Control A.5 – Assessing Impacts of AI Systems

A.5's objective focuses on evaluating the effects of AI systems on both individual users and broader societal groups throughout the entire life cycle of the system. This assessment aims to comprehensively understand how AI technologies influence people and communities from development to deployment and beyond. The evaluation process considers the potential impacts, both positive and negative, that AI systems may have on various stakeholders and social structures.

A.5 is broken down into four areas:

1. AI system impact assessment process (A.5.2)
2. Documentation of AI system impact assessments (A.5.3)
3. Assessing AI system impact on individuals or groups of individuals (A.5.4)
4. Assessing societal impacts of AI systems (A.5.5)

To evaluate this control, it is important to first establish a policy/process to assess the potential consequences resulting from AI systems. From there, you must define the scope of the impact assessment. You can do this by asking if individuals and societies are likely to be affected by the purpose and use of AI systems. Then, you can document procedures to perform the AI system impact assessment, including the detailed steps, frequency of the assessment, and how it will be used.

PERFORMING AND DOCUMENTING RESULTS OF THE AI SYSTEM IMPACT ASSESSMENT

System impact assessments should consider the intended use of the system, consequences of misuse, demographics the system applies to, and the role of humans in relation to the system.

KEY AREAS OF INDIVIDUAL OR GROUP IMPACT

When assessing whether the system impacts individuals or groups of individuals, it's vital to address the expectations of individuals using the system around the trustworthiness of the system. Areas of impact include fairness, accountability, transparency and explainability, security and privacy, safety and health, financial consequences, accessibility, and human rights.

KEY AREAS OF SOCIETAL IMPACT

When assessing the societal impact of AI systems, it is important to consider several key areas. These include:

- Environmental sustainability
- Economic considerations
- Government
- Health and safety
- Traditions, culture, and values

Guidance for writing AI policies

Writing policy is a vital part of governing AI. To begin writing AI policy, we recommend:

- Documenting principles that guide all activities of the organization related to AI
- Gathering general requirements for AI system impact assessments and system development
- Calling out alignment with other organizational policies
- Determining a process for reporting concerns related to AI

When writing your documentation, be sure to outline all aspects, including documenting AI-specific roles and responsibilities, the process for hiring, managing, and staffing AI-related roles, data resource requirements, system tooling requirements, and system and computing resource requirements.

For more information on AI policies in ISO 42001, refer back to control A.2.

ISO 42001 statement of applicability

A statement of applicability (SoA) in the context of ISO 42001 is very similar to that of ISO 27001. You'll need to document all of your necessary controls (as determined by the results of the risk assessment), along with justifications for the inclusion and exclusion of controls.

Like ISO 27001, you are required to explain why or why not a control is necessary to your organization and can add additional controls unique to your organization. While the controls in Annex A of the standard serve as a reference baseline, you can include similar and applicable controls from other frameworks or standards like the NIST SP 800-53 and the ISACA AI Audit Toolkit to meet the specific control requirement outlined in Annex A.

For more information on the statement of applicability produced by ISO 42001, please refer to Clause 6.1.3 of the official documentation.

Challenges and considerations for ISO 42001

Implementing ISO 42001 can have some challenges you need to take into consideration. These include:

- Lack of buy-in from management
- Lack of resources with the right skill set
- The right tooling and automation
- Increased documentation requirements
- Not knowing where to start

Because this is a new standard, it's easy to feel like you don't know quite where to get started. You are not alone! Whether you're battling executive buy-in, policy- and documentation-writing, or simply do not have the resources, ISO 42001 can be a lot to take on.

Remember that ISO 42001 is modeled after ISO 27001 and can play nicely with many other frameworks and standards, like NIST CSF. The documentation is similar to that of ISO 27001, which can help you more easily understand the standard.

GRC maturity should also be taken into account by your organization. By understanding your GRC maturity level, you can better assess where your gaps are, so you can be more resilient against AI risks.

For now, auditing firms and organizations implementing ISO 42001 can concentrate on understanding and getting controls in place to prepare for certification, as well as conducting ISO 42001 readiness assessments.

RELATED CONTENT

The GRC maturity model

Not sure where you're at on the GRC maturity ladder? Maybe you don't understand the concept of GRC maturity and want to get started. In this whitepaper, we outline everything you should know about the varying levels of GRC maturity – traditional, initial, advanced, and optimal – and how to achieve them.

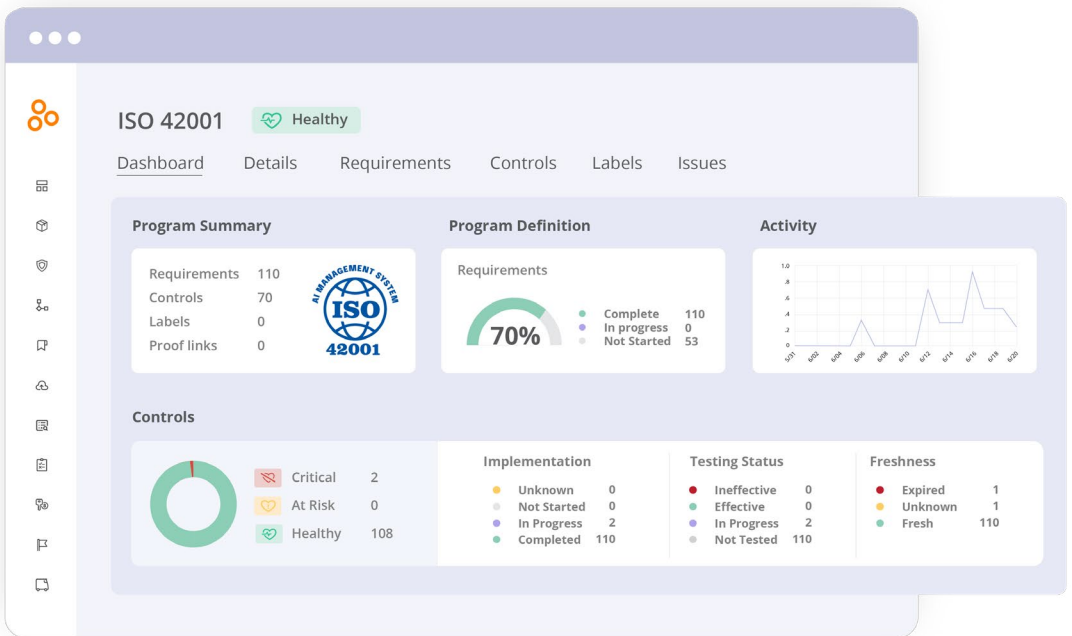
GET THE MODEL

Discover your GRC maturity level

Explore your GRC maturity in the areas of governance, risk, compliance, and compliance operations with our quizzes.

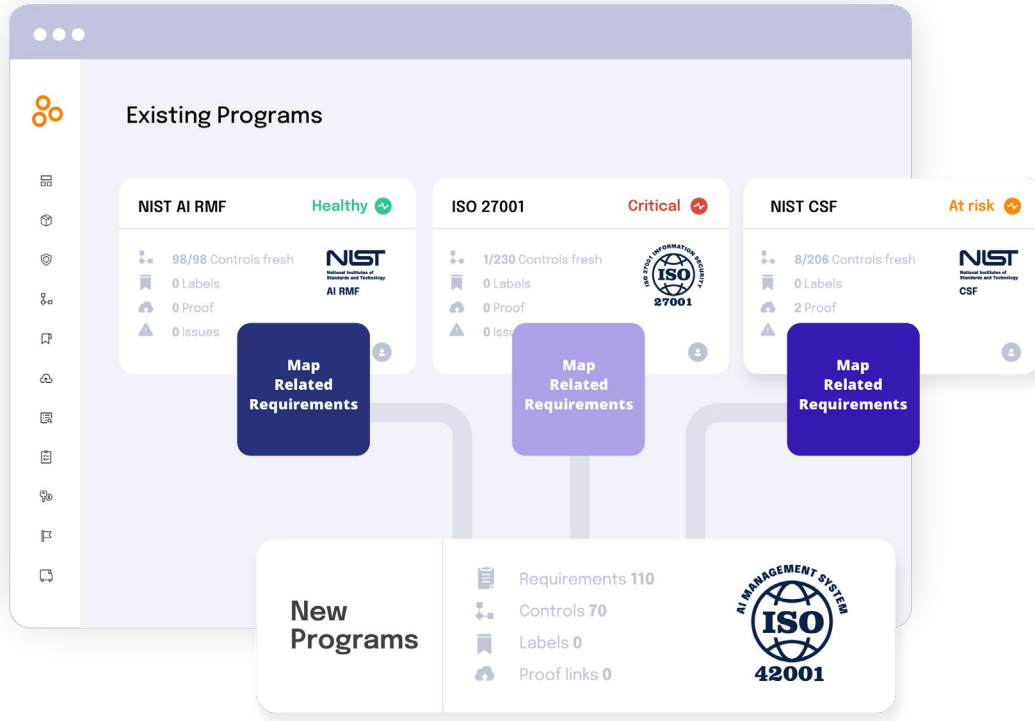
TAKE A QUIZ

Jumpstart ISO 42001 compliance with Hyperproof



Explore the benefits of Hyperproof when implementing ISO 42001. With an out-of-the-box template, you can easily start your ISO 42001 journey with a comprehensive program template, including controls and requirements outlined in Annex A.

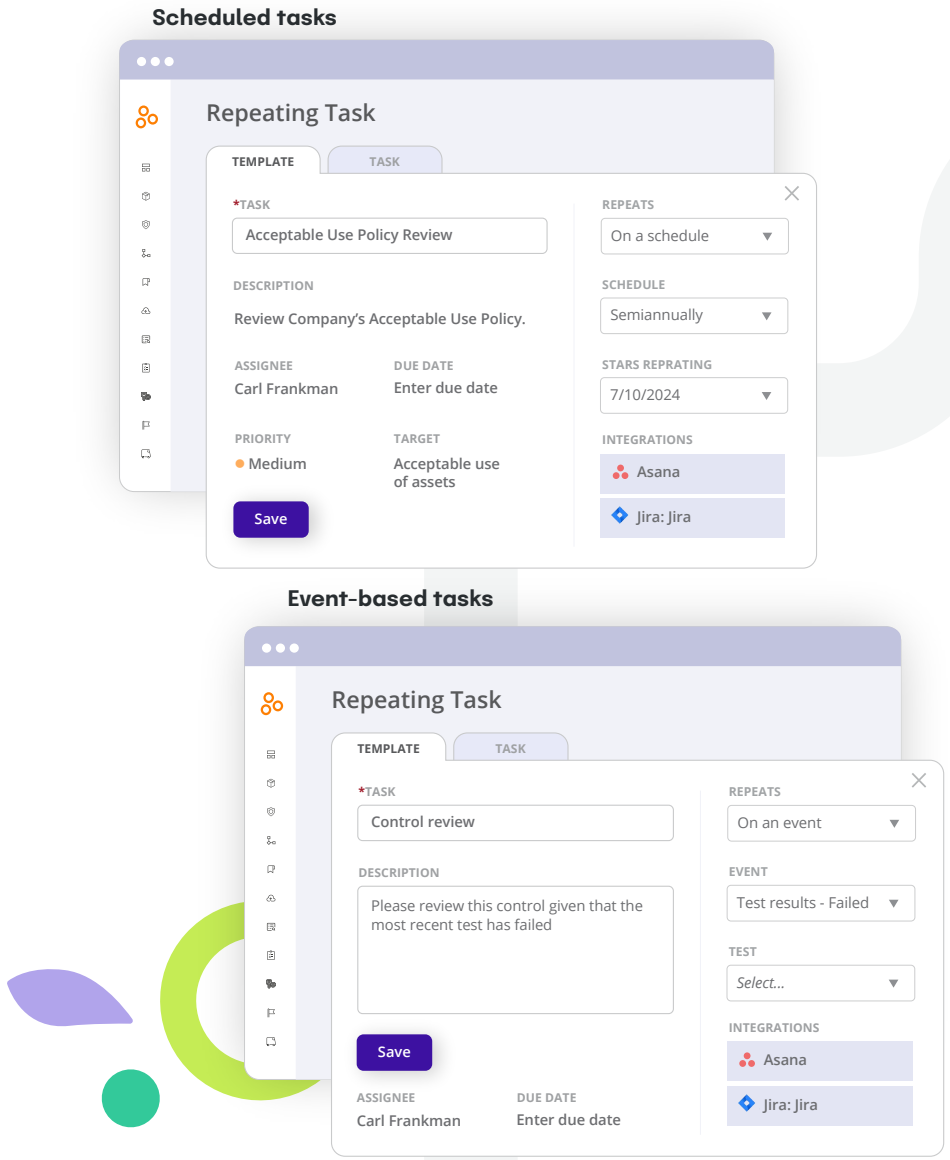
Add new frameworks quickly with control crosswalking



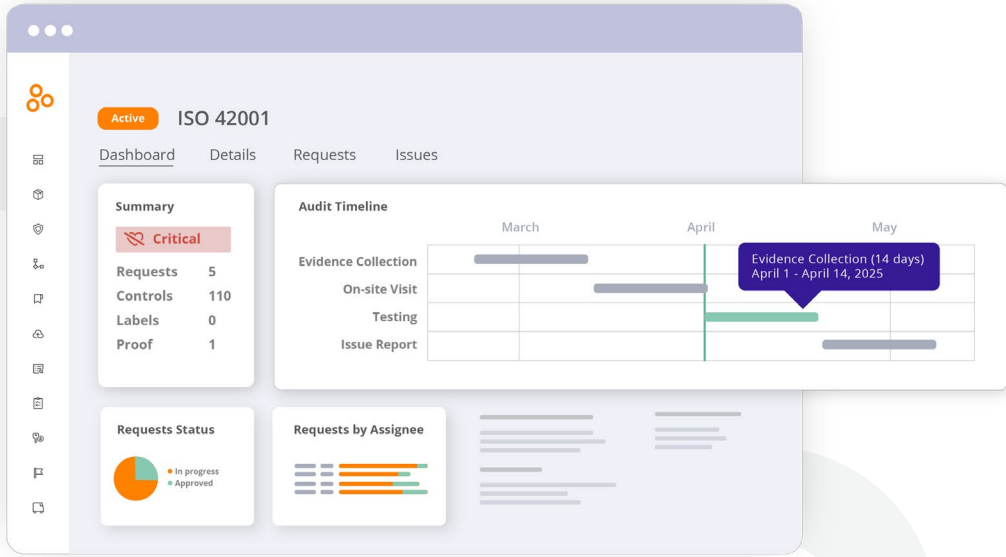
Make adding new frameworks a breeze with control crosswalks, including NIST CSF, NIST AI RMF, ISO 27001, and many more. Get rid of duplicative work and reuse controls across frameworks so you save time and resources.

Task management made easy

Hyperproof's bi-directional task integrations with popular project management systems like Jira, ServiceNow, and Asana help GRC professionals create and assign tasks. Task assignees receive notifications in the project management systems they use and love and complete their tasks in their tool of choice. Hyperproof then automatically syncs updates to proof, taking the manual work off your plate and keeping stakeholders happy.



Seamlessly manage your ISO 42001 audit



Manage your ISO 42001 audit with Hyperproof's Audit Module. Invite your auditor to work alongside your team in Hyperproof's dedicated audit space to make information sharing easy while ensuring they only have access to what they need.

With Hyperproof, you can seamlessly connect controls to audit requests and their associated evidence to speed up the audit readiness process. This also helps you reuse work for your next audit.

Hyperproof's Audit Module enables you to know the status of your audit at all times. Easily understand what requests still need to be done, what's in progress, what's under review, and what's completed with Hyperproof's audit dashboard.

About the authors

hyperproof

COURTNEY CHATTERTON

Courtney Chatterton is a Sr. Email and Content Marketing Specialist at Hyperproof, with over two years of experience writing in the fields of risk management, compliance, and information security, with a growing emphasis on AI frameworks and standards. She is a known subject matter expert for email marketing in the cybersecurity industry, leading monthly email marketing calls with the Cybersecurity Marketing Society, as well as presenting at the Society's annual conference, CyberMarketingCon.

Her career has run the gamut from on-site and service desk technical support for faculty, staff, and guests in the Information Technology department at Northwestern University to highly-technical roles within business-to-business (B2B) Software as a Service (SaaS) companies. In the past, she has served as a key member of Revenue Operations teams, writing documentation and serving as a subject matter expert for various marketing automation platforms, including Salesforce Pardot and HubSpot Marketing Hub.

At Hyperproof, she has served as a leader for Hyperpride, the LGBTQ+ employee resource group, as well as a Culture Ambassador on the Culture Committee, working with the People team and various departments to ensure positive steps are being taken toward diversity, equity, inclusion, and belonging (DEI&B).

VARUN PRASAD

Varun Prasad is a Managing Director with BDO's Third Party Attestation practice, an MSECB auditor, and an IT audit and risk management professional with more than 14 years of progressive experience.

He has managed and executed a variety of IT audit-based projects from end to end. Varun has provided various types of audits, advisory, and assurance services, such as SOC 1, SOC 2, gap assessment and examination, internal audits, compliance audits (NIST frameworks, etc.), risk assessments, financial external audit support, agreed-upon procedures, business continuity and disaster recovery planning, system security reviews, and privacy.

He is a lead auditor for ISO/IEC 27001, ISO/IEC 42001, and ISO 22301 and has led multiple ISMS audits for large multinational tech companies and SaaS providers. Varun has experience working with a wide range of industries, including technology, financial services, insurance and benefits, and manufacturing, with a strong focus on cloud services.

About Hyperproof

Hyperproof is a risk and compliance management platform that empowers IT, security, and compliance teams to automate and scale their workflows without the burden of jumping between multiple legacy platforms and spreadsheets. The Hyperproof platform enables teams to get complete visibility into their organizational risks, streamline the audit process, and reduce their ever-growing compliance workloads. Hyperproof is trusted by leading organizations like Veeva Systems, Fortinet, Motorola, Outreach, and Solventum.

To learn more about Hyperproof, visit **hyperproof.io**

To learn more, visit hyperproof.io