

# ISO 42001: the management system for responsible AI<sup>1</sup>



Artificial Intelligence (AI) and algorithms are influencing increasingly our daily lives. Maintaining control over these latest developments and responsibly managing this technology is therefore more crucial than ever. Naturally, everyone wants to do the right things and preferably as soon as possible. In this whitepaper, we clarify how implementing a management system (based on ISO 42001) can assist your organization in maintaining control over AI and complying with the AI Act.

## Why an AI management system?

A management system for AI assists an organization in systematically managing the risks associated with AI deployment and enhancing the performance of AI systems. With an AI management system, you can demonstrate that responsible AI deployment is part of your organization's DNA. The management system ensures that your organization effectively deploys AI and similar algorithms in a responsible manner, improves quality, and identifies and controls risks in practice.

The AI regulation requires additional measures for high-risk AI systems. However, when an organization employs multiple AI systems, addressing this on a per-system basis becomes impractical. Instead, organizations must seek a more integrated solution. An AI management system provides this solution in a comprehensive framework for handling AI systems. It offers guidance on meeting various quality requirements, such as description, risk classification, and reporting of executed mitigating measures. By implementing a management system, all AI systems become part of a structured and controlled way of working.

With an effective AI management system, you can centralize information about AI systems and ensure adherence to agreed-upon practices, while also verifying that AI systems function as intended. The configuration of an AI management system is outlined in the ISO 42001 standard.

## What is the ISO 42001 standard?

The international standard ISO 42001 outlines the requirements for a management system for AI and similar algorithms. The foundation of this document describing the management system is the plan-do-check-act approach, which is also evident in other ISO standards such as ISO 9001 for quality, ISO 14001 for environmental management, or ISO 27001 for information security. One of the components of the management system is conducting a risk assessment concerning the deployment of AI systems. To mitigate risks, organizations can utilize the measures outlined in the standard. This encapsulates the immediate value of ISO 42001, which includes relevant and concrete measures outlined in its annexes.

ISO 42001 consists of four annexes. **Annex A** includes a list of management objectives and measures. **Annex B** provides more specific implementation guidelines for these measures. Furthermore, Annex B includes requirements regarding the effects and ongoing monitoring/adaptation of an AI system. **Annex C** serves as a tool for organizations to describe their business objectives for the use of AI systems and potential risk categories. This aids in various analyses such as ethical impact assessments like a Fundamental Rights Impact Assessment (FRIA), which the AI Act obligates for high risk AI systems, and security or privacy analyses like BIA or DPIA. Lastly, **Annex D** addresses the domains and sectors in which an AI system can be used and how ISO 42001 aligns with other standards.

## What are the advantages of ISO 42001?

There are various frameworks for the deployment of AI systems. ISO 42001 offers several advantages:

- The measures outlined in Annex A are comprehensive and align well with other frameworks.
- By adopting a management system approach, an organization streamlines the generic process of developing and utilizing AI systems. Existing standards tend to focus more on unique applications.
- ISO 42001 is an international standard. Many other developed standards are national. This could complicate international collaborations or partnerships with crossborder entities aiding in AI system development. ISO 42001 serves as a good candidate for a unified standard in such scenarios.
- The structure of ISO 42001 aligns with other certifications, such as ISO 9001, ISO 27001, and ISO 27701. Organizations with management systems set up for these standards can relatively easily expand their certification to include ISO 42001.
- It's appealing for organizations to incorporate ISO 42001 requirements into their internal policies and standards for AI system development. The standard serves as a valuable source of inspiration for requirements, allowing organizations to selectively choose and customize as needed.
- Organizations can obtain certification against ISO 42001. This certification provides tangible evidence that all AI systems developed and used within your organization are done so reliably and conscientiously.

## Why certify ISO 42001?

Currently, organizations often demonstrate compliance with requirements and regulations per AI system. With ISO 42001 certification, you demonstrate that you have a way of working that ensures all AI systems you develop and/or deploy meet the requirements and regulations. This means you don't have to individually assess every application, update, or pilot if they fall under the management system. This accounts for all organizations developing AI systems in-house, using them, or procuring them externally.

## How does ISO 42001 help me comply with the AI Act?

The AI Act outlines specific measures that organizations must take when developing an AI system. Depending on the risk assessment of the AI system, measures of different severity are required. The



ISO 42001 management system ensures that with each new AI system and every change to existing applications, there is automatic monitoring to ensure continued compliance with the AI Act.

By working in this structured manner, it becomes much easier to demonstrate compliance with the AI Act. Establishing a management system prevents the need for checking all individual AI systems within your organization. The management system assists you in doing the right things consistently.

### **Is ISO 42001 useful for me if I don't want to certify?**

Certainly. The standard provides concrete management measures in the annexes that are useful as a checklist when developing and deploying individual AI systems. This is always beneficial. Additionally, the requirements from the management system help bridge the gap between, for example, technicians, business professionals, executives, and legal experts. The requirements from the management system contain highly useful measures for conducting risk assessments, involving top management in decision-making, and establishing agreements on accountability for the use of AI systems. This serves as a valuable source of inspiration, even if certification is not the goal.

### **What is the relationship between ISO 42001 and the algorithm registry?**

ISO 42001 serves as a way to support AI governance (in addition to IT/data and privacy governance). This governance includes agreements on who is responsible and how the organization handles AI (processes, guidelines, policies, and scope).

Furthermore, ISO 42001 aligns with the risk approach outlined in the AI regulation and provides room for the results of ethical, security and privacy assessments to be a structured and adequate process component for high-risk AI systems.

Additionally, the AI regulation requires for high-risk AI systems that documentation and metadata is available and published to a European registry. A management system helps centralize this information and ensures it remains consistent and up-to-date.

**More information:** Keep yourself posted on further development and training opportunities by following us on LinkedIn. Feel free to get in touch.

## **About the authors**



**Sabine Steenwinkel-den Daas** Consultant Responsible AI. With her experience in developing, implementing, validating, and testing AI systems, Sabine understands the necessary prerequisites and control measures for successful AI implementations down to the smallest details. In her daily work, she provides concrete advice to responsibly maintain control over AI and algorithms. Sabine also enjoys sharing her knowledge in training sessions and webinars.  
**t +31 6 868 139 31, [sabine.dendaas@highberg.com](mailto:sabine.dendaas@highberg.com)**



**Frank van Vonderen** Partner Privacy, Data en AI. Frank is a specialist in standards at Highberg. He knows precisely how standards like ISO can assist organizations in gaining control. Frank is deployed by various accreditation bodies to assess the quality of certifying institutions, for example, on ISO 27001, ISO 27701, and now also ISO 42001.  
**t +31 6 125 573 58, [frank.vanvonderen@highberg.com](mailto:frank.vanvonderen@highberg.com)**

