Deloitte.

Demonstrate market readiness of your AI systems with ISO 42001

Lead in the creation of trusted and secure AI systems

Introduction

As artificial intelligence (AI) technologies evolve, so can the risks—ranging from managing biases and safeguarding data privacy, to complying with a patchwork of global regulation. Enter ISO 42001, which provides guidance to assess the maturity of AI management systems. Explore how to get your AI system ready for ISO 42001 certification while building a sustainable risk management program.

As AI becomes integrated into more customer-facing technologies, organizations are recognizing that these tools can introduce risks like inaccuracy and bias, concerns around data privacy and cybersecurity, and challenges with responding to a fragmented US and global regulatory regime.

In Deloitte's *State of Generative AI in the Enterprise* survey, respondents indicated that the top two barriers to developing and deploying Generative AI (GenAI) were worries about complying with regulations (38% of respondents, up 10% from one year prior) and difficulty managing risks (32% of respondents, up 6% from one year prior).[1] These concerns will likely be amplified by the advancements of GenAI and agentic AI use cases expected over the next few years.

In response to the need for guidance and leading practices around AI risk management, the International Organization for Standardization (ISO) Council published its ISO/IEC 42001:2023(E) *Information Technology — Artificial intelligence — Management system* standard ("ISO 42001")[2] in December 2023. ISO 42001 provides a framework for AI governance and risk management across the AI development life cycle, including the following areas:

- **Governance structures** to establish oversight and accountability
- **Risk management protocols** to identify, assess, and mitigate potential risks and impacts
- **Guidelines** to design AI systems that are transparent, fair, and unbiased
- **Compliance mechanisms** to maintain adherence to evolving legal and regulatory standards

Many of these areas overlap with requirements of other regulations and standards, such as the European Union (EU) AI Act and the National Institute of Standards and Technology (NIST) guidelines on AI, and, in certain instances, ISO 42001 includes additional requirements.

Organizations that achieve certification demonstrate how their AI management systems have a way to not only identify and mitigate risks, but also show how they were built with resilience, scalability, and ongoing oversight, which can lead to better outcomes and transparency for their customers.

Certification to build customer trust

AI can be transformative for organizations, but it does not come without risk. Aligning to a standard demonstrates not only risk management, but the maturity of an organization's AI program.

In Deloitte's *State of Generative AI in the Enterprise* survey, 35% of respondents indicated that the biggest obstacle to GenAI's potential marketplace adoption is mistakes or errors with real-world consequences, followed by bias and hallucinations.[3] While 87% of executives claim to have AI governance frameworks within their organization, fewer than 25% have fully operationalized their enterprise governance, according to another study.[4] In such cases, certification becomes an indicator that these programs have been implemented and are operating effectively.

Pursuing an ISO 42001 certification can provide differentiation in the near term and may become a common benchmark in the future. Other ISO standards have become de facto frameworks that are widely used across the world and in various economic sectors. For example, the ISO/IEC 27001 standard describing Information Security Management Systems was published in 2005, and today, there are 70,000 certified organizations in more than 150 countries and in industries ranging from agriculture to manufacturing to social services.[5]

Managing evolving risks and regulation

ISO 42001 aligns with national and international regulatory frameworks related to AI. The following table compares the requirements of the EU AI Act, NIST AI Risk Management Framework (AI RMF), and ISO/IEC 42001:2023(E).

High-level requirement	EU AI Act	NIST AI RMF	ISO 42001
Risk assessments Identifying, assessing, and mitigating risks associated with AI systems	✓	✓	✓
Governance, policies, and standards Establishing processes, policies, and procedures to facilitate adherence to enterprise standards	✓	✓	✓
Alignment with trusted, responsible, and ethical principles Assessing how AI systems operate in a manner that respects ethical principles and human rights	✓	✓	✓
Transparency Making AI system operations and decision-making processes understandable, explainable, and accessible	✓	✓	✓
Human oversight Providing human intervention and control over AI systems when necessary	✓	✓	✓
Risk categorization Classifying AI systems based on their potential impact and risks	✓	NA	✓
Continuous improvement Regularly updating and enhancing AI systems to improve performance and safety	✓	✓	✓
Innovation promotion Encouraging the development and adoption of new and advanced AI tech through internal and external forums	✓	✓	✓
Monitoring and testing on accuracy and reliability Monitoring AI systems' accuracy and reliability, minimizing errors and biases	✓	✓	✓
Evidence and recordkeeping Maintaining evidence and records of AI system development, deployment, and operation	✓	✓	✓

ISO 42001 follows other ISO standards that address risks in technologies. Prominent examples include ISO/IEC 27001:2022,[6] as mentioned above, which provides guidance around establishing, implementing, maintaining, and continually improving an information security management system, and ISO/IEC 27701:2019,[7] which builds on ISO/IEC 27001:2002 to develop a privacy information management system.

Organizations applying for multiple certifications can leverage common controls, frameworks, and evidence for overlapping areas insofar that the management systems are connected and dependent on the same processes. Additionally, common functions—such as internal teams testing compliance with other ISO standards and governance, risk, and compliance technologies—can be leveraged for additional efficiencies.

Getting started

An ISO 42001 certification affords organizations the ability to stay ahead of costly risks, build customer trust, and make strides toward compliance with other AI frameworks. However, understanding and implementing the standard requires an investment of time and effort across the enterprise. The following list provides three areas for organizations exploring where to start their ISO 42001 compliance journeys.

1. **Assess overlapping capabilities:** Many organizations already have a head start toward ISO 42001 compliance. The standard's approach to AI management builds upon control frameworks that many organizations already have in place, including data governance, IT, security, privacy, enterprise risk management, and internal audit. An initial assessment can help organizations to understand where they can expand existing capabilities to meet ISO 42001 requirements and minimize the introduction of new processes.

2. **Align on ownership over AI risk management responsibilities:** The complexity of AI risk management typically involves a variety of teams across an organization, including product management, data and model engineering, infrastructure, legal and compliance, trust and safety, and training teams. Given the number of stakeholders, this may lead to fragmented ownership and unclear responsibilities. Organizations obtaining their certification should identify leadership that can champion, resource, coordinate, and drive compliance and risk management efforts, and determine an operating model to coordinate among the teams involved.

3. **Evidence operational effectiveness:** To obtain an ISO 42001 certification, organizations need to demonstrate that their AI management system operates effectively and sustainably. Organizations should retain evidence, such as AI model design requirements, accuracy and performance monitoring logs, data audit trails, and product launch approvals, to demonstrate sustained compliance. Tools like governance, risk, and compliance platforms specifically built for AI risk management needs can support these processes.

How Deloitte can help

Leading organizations find value in working with Deloitte to recommend sustainable risk and compliance programs and proactively unlock AI's value. We have assisted organizations as they manage risks related to AI for more than a decade, ranging from early machine learning adoption to—more recently—risks from GenAI and agentic AI technologies. We bring the combination of practical experience with AI development, as well as perspectives in large-scale risk and compliance programs across a variety of industries. This includes supporting organizations while not disrupting their operations as they scale and mature their products.

Our services include the following:

- **Readiness evaluations:** ISO 42001 readiness evaluations identify critical capabilities throughout your enterprise and measure potential gaps to certification
- **AI model testing:** AI model testing for qualitative and quantitative benchmarks, guardrails, and outcomes
- **Governance, risk, and compliance program development:** Program development for enterprise AI risk management, including AI policies, procedures, governance, operating model, and controls frameworks
- **Tooling:** Configuration and integration of tools and technologies, such as governance, risk, and compliance platforms, to support AI risk management, AI model monitoring, and discovery of AI models across the enterprise
- **Talent:** Development of talent strategies, including alignment of roles and responsibilities for enterprise AI risk management and upskilling talent on AI practices
- **Regulatory compliance:** Regulation tracking, analysis, and change management, as well as mock regulatory/internal audit examinations and regulatory response
- **Security risk:** Program development for strategy, governance, risk assessment, and secure/privacy by design, including AI threat assessments, system security, and red teaming

Contact us

Please reach out to our team if you would like to discuss these topics in more detail.

Rich Tumber
Principal
Deloitte & Touche LLP
ritumber@deloitte.com

Alison Hu
Managing Director
Deloitte & Touche LLP
aehu@deloitte.com

Don Williams
Managing Director
Deloitte Transactions and Business Analytics LLP
dowilliams@deloitte.com

Brendan Maggiore
Senior Manager
Deloitte Transactions and Business Analytics LLP
bmaggiore@deloitte.com

Endnotes

1. Jim Rowan et al., *State of Generative AI in the Enterprise: Quarter four report*, Deloitte, January 2025.
2. International Organization for Standardization (ISO), ISO/IEC 42001:2023 *Information technology—Artificial intelligence—Management system* (ed. 1), 2023.
3. Rowan et al., *State of Generative AI in the Enterprise: Quarter four report*.
4. IBM, "IBM study: AI spending expected to surge 52% beyond IT budgets as retail brands embrace enterprise-wide innovation," press release, January 7, 2025.
5. ISO, ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (ed. 3), 2022.
6. Ibid.
7. ISO, ISO/IEC 27701:2019 *Security techniques—Extension to ISO/IEC 27001 and IOS/IEC 27002 for privacy information management—Requirements and guidelines* (ed. 1), 2019.

Deloitte.