Building digital trust: AI governance strategies

Seven steps for staying ahead of customer and regulatory demands for sound AI governance

Artificial intelligence (AI) is revolutionizing the way we live and work. It's become an integral part of almost every industry and sector, from healthcare to finance to manufacturing—the list goes on.

While AI brings unprecedented efficiencies and insights to the table, it also holds many potential risks, including ethical concerns, data and privacy breaches, issues involving the quality or integrity of data, and unintended biases. These risks are one of the key reasons that the use of generative AI (GenAI) has stirred up considerable regulatory response worldwide. Regulations such as the European Union (EU) Artificial Intelligence Act (2024) or the National Institute of Standards and Technology's (NIST) AI Risk Management Framework (2022) placed a heightened focus on AI governance rules.

There seems to be almost universal agreement that there's a need to build and enforce governance guardrails that ensure AI's responsible development and deployment. This is the genesis of the International Organization for Standardization's (ISO) enactment of ISO 42001, *Artificial Intelligence Management*.

In this paper, we will explore the requirements of ISO 42001 and other AI governance rules, why they were created, and how to prepare to comply with them in an efficient and effective manner.

Key elements of ISO 42001

- AI policy
- Responsibility for the implementation, operation, and management of AI systems
- Resource allocations of data, tools, systems, and people
- AI risk assessment
- AI impact assessment
- Aligning goals for responsible development and use of AI
- Determining requirements for the AI lifecycle
- Data sources, data quality, and data preparation
- Communication with stakeholders and relationships with third parties

Overview of AI governance guidelines—and inherent AI risks

The new AI requirements set out within the ISO 42001 standard and other comparable frameworks establish an AI management system that should be integrated with an organization's processes and overall management structure. This system should include a comprehensive set of guidelines for developing, evaluating, monitoring, and governing the use of AI.

Specific issues and inherent risks should be considered when designing, developing, and deploying the processes, information systems, and controls related to AI, including:

- Determining organizational objectives, involvement of interested parties, and organizational policy
- Managing risks and opportunities, including addressing concerns related to the trustworthiness of AI systems, such as security, safety, fairness, transparency, data quality, and quality of AI systems throughout their lifecycle
- Managing suppliers, partners, and third parties that provide or develop AI systems for the organization. The AI framework set out in these governance guidelines helps address critical questions such as:
  - What are the risks regarding the use of GenAI?
  - Who are the relevant stakeholders to include in this process?
  - How do we build in the right control measures (e.g., having in place the right team, right people, right processes, right technology) to deploy AI in a way that helps the organization and its stakeholders?
  - What methodologies should we be using to design and implement controls, including guidance on data management, risk assessment, and impact evaluation?

These new AI standards also attempt to address easily overlooked potential risks, such as:

Lack of transparency. The use of AI for automated decision-making can result in a "black box" effect, making it hard to understand how it arrives at its decisions. This makes it difficult to audit and govern the whole AI process effectively with traditional information technology (IT) systems.

Bias. AI models are trained on massive datasets. But if the dataset is biased, then AI will incorporate that bias and perpetuate it. For example, let's say you have a hiring tool that learns from past hiring decisions. If those decisions were biased, then your AI program could continue that bias.

Or if you employ a multiagent system, then an error made by one AI agent can easily be passed on to other agents. This can create a cascading effect where a single mistake can significantly impact the overall system performance.

Benefits of adopting an AI governance system

While compliance with some AI-related rules, like ISO/IEC 42001, is not yet mandatory, adapting their framework for AI governance can yield several benefits:

Risk management

There will be more rigorous and efficient risk management within your organization. It will help you address AI-specific risks, such as treating individuals unfairly (i.e., bias) and making incorrect decisions based on inaccurate information.

Reputation

Your company's reputation can benefit as you increase trust in the products you develop. This can be a critical factor when selling AI products to third parties as well as managing the risks associated with using third-party AI products.

Competitive advantage

Being compliant will instill confidence in customers and stakeholders. It demonstrates a commitment to quality, ethical practices, and adherence to industry-recognized benchmarks that can differentiate your organization from its competitors.

Preparation for the future

Getting ahead of the curve now prepares you for complying with additional regulations that undoubtedly will be introduced in upcoming years, including the EU AI Act, entered into force in August 2024.

Unpredictable AI behavioral changes. AI systems that perform continuous learning may change their behavior during use. They require special consideration to ensure their responsible use continues with changing behavior.

Security threats. GenAI can be misused to create deepfakes or manipulate data, which can also be serious threats. The new AI regulations require organizations to have strong data security controls in place to manage these risks and ensure responsible and trustworthy AI development. It attempts to establish a framework that strikes a balance between innovation and ethical considerations.

Seven keys to a strong, sound AI governance program

Creating an AI policy that meets the requirements of ISO 42001 and the other AI standards can be daunting. And it can't be done overnight. Developing and implementing a sound AI policy will take time and the cooperation and input from multiple stakeholders, including personnel from IT, marketing, operations, finance, audit, legal, and, of course, the approval of senior management.

Below are some key steps to get you started:

- **Take an AI inventory:** An AI inventory should be created by your organization, including both active and developing AI projects, with details on their status and risk management considerations.
- **Conduct a readiness assessment:** Evaluate your organization's existing AI policies, procedures, and security standards against the ISO 42001 standard. This assessment must consider the technical and societal impact of your AI system, including the potential consequences for users of the system. For example, ask yourself whether your AI program is aligned with principles of fairness, transparency, privacy, etc.

  These assessments—and what they involve—can be broken down as follows:

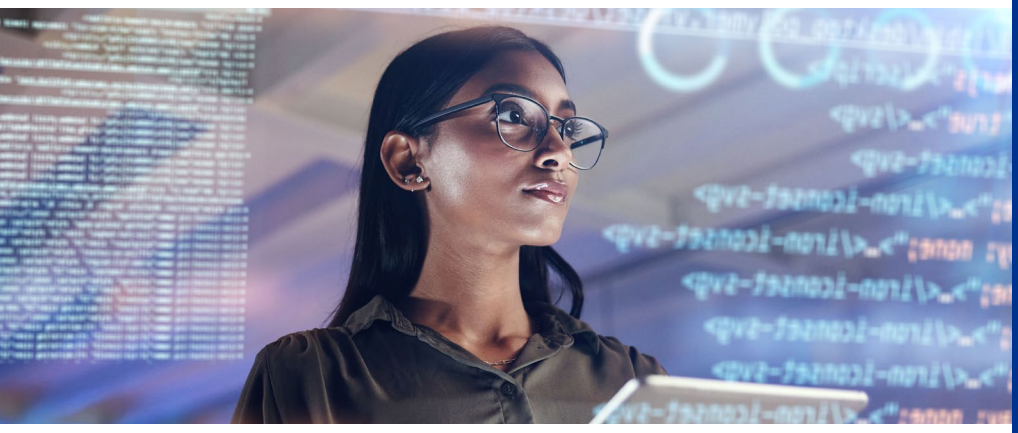
  - AI risk assessment: This is a systematic evaluation of the potential risks associated with the use of AI models and systems.

This process involves identifying, analyzing, and mitigating risks to ensure the safe and effective deployment of AI technologies.

- AI impact assessment: An AI impact assessment evaluates the potential effects that an AI system may have on people, organizations, and society. The process involves identifying, analyzing, and mitigating the actual and potential impacts of AI to ensure that AI technologies are developed and deployed in a fair, transparent, explainable, responsible, robust, secure, and safe manner.
- AI gap assessment: This assessment is used to identify and analyze the differences between the current state of an organization's AI capabilities and its desired state. The gap assessment enables an organization to evaluate its AI maturity and reveals where it is lacking in terms of AI technology, skills, processes, and governance.

  Equally important, it provides a roadmap for improvement. For example, AI-powered skills gap assessment tools can analyze employee skills, identify deficiencies, and recommend targeted training programs.

- **Craft or refine AI policies and procedures:** Based on your risk assessment results and insights gained, modify your overall AI risk and governance framework as needed to create/design appropriate controls to mitigate risks.
- **Develop a detailed roadmap:** This will help you visualize what needs to be done and implement the needed changes as effectively and efficiently as possible.
- **Get approval of senior management:** Make sure you run key program and policy decisions by senior management and your AI steering committee, focusing on any changes that were made and the reasons for the changes.
- **Monitor and optimize performance:** Organizations must look to continually maintain, monitor, and improve their AI management systems. This process calls for identifying analyzing, testing, evaluating, monitoring, and remediating risks during the entire AI system's lifecycle.
- **Manage your suppliers:** Having your organization in compliance with ISO 42001 is not enough. Your suppliers must also be aligned with your AI principles and approach.



Case study

Achieving ISO 42001 readiness

A global technology company aimed to achieve ISO 42001 readiness to bolster its global compliance, risk management, and documentation processes. The company enlisted the expertise of KPMG to assist with this critical initiative.

Approach

Initially, our team conducted a thorough evaluation of the existing documentation and processes to assess the company's compliance with ISO 42001 standards. Subsequently, we developed the necessary compliance documentation, including Impact Assessments, Statements of Applicability, Risk Assessments, and the AIMS. Then, through multiple iterations and collaborative feedback sessions with the client, we fine-tuned the documentation to meet stringent ISO 42001 requirements.

Results

We successfully delivered comprehensive and compliant documentation for the client, ensuring preparedness for ISO 42001 certification. Additionally, we revamped the risk management process, integrating various open-source repositories to update and enhance the client's risk library.

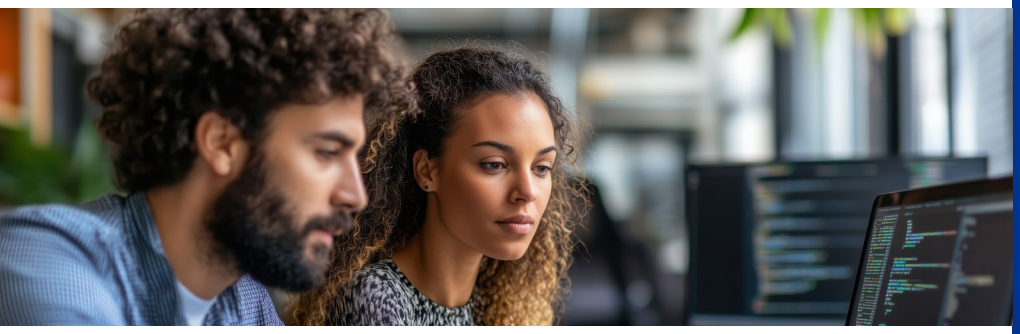
This holistic approach not only ensured ISO 42001 compliance but also optimized overall risk management procedures, reinforcing the company's position as a global leader in technology and innovation.

Getting a jump start for what lies ahead

Organizations that position themselves as leaders in the AI space will gain a competitive advantage in an increasingly AI-driven marketplace. The fact is that AI has proven its business case; in many situations, the consistency, efficiency, and results generated by an AI model can't be matched.

Establishing customer and stakeholder trust in AI products and services is table stakes for business growth. An even bigger potential challenge will be staying on top of this rapidly changing and developing area as the regulatory landscape involving AI continues to shift and evolve.

While there's general uncertainty and inconsistency across jurisdictions on AI rules and regulations, we strongly believe that it's not too soon to get a head start in determining the best course of action for your organization. Building a robust AI risk and governance structure will be crucial in helping your organization understand and meet the requirements of ISO 42001 and other AI-related regulations that are sure to be coming in the future.



How KPMG can help you

Creating and implementing trustworthy and ethical AI is a complex business, regulatory, and technical challenge. KPMG can help you develop and deploy an extensive trusted AI program that will enable you to meet these challenges across the AI lifecycle.

Scope and AIMS awareness

The first step in your ISO 42001 journey involves defining a clear scope statement and obtaining stakeholder buy-in. We facilitate this through a series of educational sessions, stakeholder interviews, and meticulous crafting of your AIMS scope statement document.

Practicing what we preach: KPMG Australia becomes first organization to achieve AI management system certification

KPMG Australia became the first company in the world to achieve ISO 42001 (AI) certification for establishing, implementing , maintaining, and continually improving an Artificial Intelligence Management System (AIMS). In doing so, KPMG Australia received certification to the ISO 42001 standard, which is intended to assist organizations in using AI responsibly.

Approach

Following the release of the ISO 42001 standard in December 2023, KPMG began it path on the certification process. This involved a detailed audit by a BSI auditor of how the firm approached AI, from governance to project management to embedding trusted AI practices in the way that KPMG's people work. The auditor also examined our system to ensure that we maintained adequate guardrails.

Result

Our robust AI management system met an extremely high bar, and we demonstrated that we are living and breathing our trusted AI commitment. With a focus on safe management and responsible use of AI, the BSI accreditation demonstrates KPMG's dedication to ethical AI, high-level governance, and ingraining a culture of continuous improvement.

Perspectives: Perceptions of Consulting in the US in 2024, Source Global Research (March 2024).

Readiness assessment

Our highly skilled team will conduct a comprehensive readiness assessment to evaluate your organization's current standing against the ISO 42001 framework. This involves reviewing your risk assessment, drafting the statement of applicability, conducting interviews, and testing a sample of controls. Upon completion, we will provide you with a detailed readiness assessment report, including observations and recommendations to help you prepare for certification.

AIMS elements development

ISO certification necessitates the documentation and implementation of specific mandatory documents, such as the RACI chart, risk assessment framework, implementation manual, AI policy, internal control monitoring approach, and internal audit plan. We will collaborate with you to draft each required document, ensuring you have everything needed for your certification journey.

Certification Advisory

Navigating an external certification audit can be daunting and stressful. Your organization does not have to face this challenge alone. Our KPMG professionals will support you at every step, from audit preparation and meeting attendance to debriefing, reviewing documentation and evidence packages, and providing overall guidance to your key stakeholders throughout the audit process.

According to senior buyers of consulting services who participated in the Perceptions of Consulting study in the US in 2024 , KPMG ranked No. 1 for quality in AI advice and implementation services. The KPMG global organization operates in 142 countries and territories and has more than 275,000 partners and employees working in member firms around the world - including technology professionals, data scientists, data engineers, and developers. We are consistently recognized as a global leader in AI/GenAI. What's more, propelled by the innovation and dedication of our AI solutions team, KPMG has developed one of the most trusted AI security solutions in the market. Discover more here.

Contact us

Bryan McGowan
Principal, Advisory, Cybersecurity & Tech Risk – Global and US Trusted AI Leader
KPMG US
T: 816-802-5826
E: bmcgowan@kpmg.com

Ussamah Ahmed
Managing Director, Cybersecurity & Tech Risk
KPMG US
T: 408-367-4992
E: ussamahahmed@kpmg.com

Charlie Murray
Managing Director, Cybersecurity & Tech Risk – Tech Compliance Leader
KPMG US
T: 313-230-3074
E: cmurray@kpmg.com

Some of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**