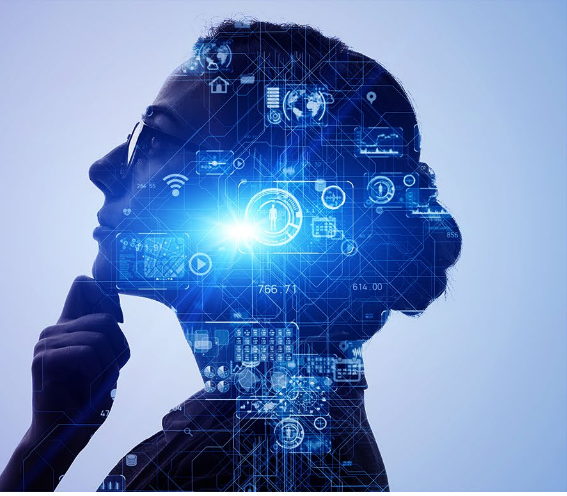
KPMG

Governing AI responsibly

Building an integrated AI governance model



The transformative power and economic potential of generative AI cannot be denied.

According to a recent KPMG survey of 200 business leaders in the U.S., generative AI was rated as the top emerging technology.[1] Survey respondents expected their organization to be impacted "very highly" in the next 12 to 18 months.

80%
Believe generative AI will disrupt their industry

93%
say technology will provide value to their business.

[1] Source: "KPMG Generative AI survey," June 2023

Equally impactful, however, are the risks involving generative AI

- Bias or inaccuracy
- Errors and misinformation
- Privacy concerns with personal data
- Cybersecurity
- Legal, copyright and intellectual property (IP) issues
- Liability
- Transparency

Top considerations for risk organizations while building a governance model for AI

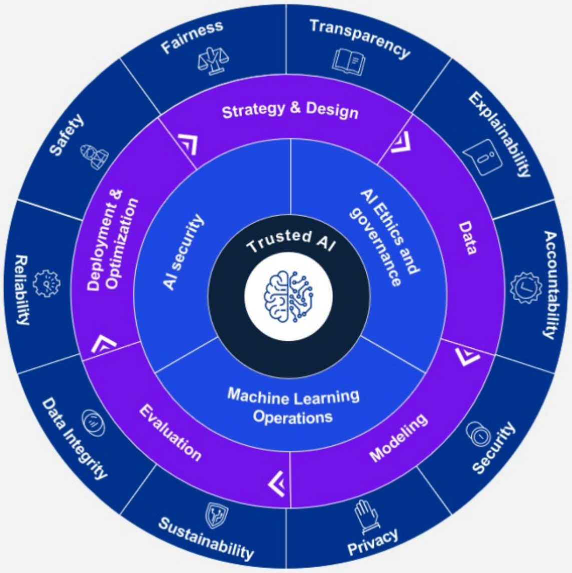
Managing risk related to generative AI begins with developing a solid AI governance model designed to identify, manage, and respond to generative AI risks.

Based on our experience in developing generative AI solutions, both for ourselves internally and our clients, an effective governance model should include essential directives and considerations such as the following:

1 Develop a comprehensive governance model, inclusive of security and privacy

As organizations adopt generative AI, it is critical that they develop a strong governance framework that addresses crucial issues such as data integrity, reliability, and safety. Since AI often involves analyzing and processing large amounts of sensitive data, including personal and financial information, it is crucial for organizations to also implement robust security measures to protect this data from theft or misuse. Moreover, with privacy increasingly becoming a concern for consumers and regulatory bodies, companies that fail to adequately protect the privacy of their customers may face legal and reputational consequences. Implementing security and privacy measures within the AI governance framework can help organizations comply with regulations and protect the data and privacy of their customers.

KPMG's Trusted AI framework



61%
said they were wary about trusting AI systems, reporting either ambivalence or an unwillingness to trust.[2]

[2] Source: "Trust in Artificial Intelligence, A global study, 2023," KPMG, The University of Queensland, Australia

Top considerations for risk organizations while building a governance model for AI (cont.)

2 Consider a risk tiered governance approach

One size or type of governance model does not fit all. Existing models or frameworks that were built for traditional risks might not— and probably do not—apply to all the generative AI risks facing your organization. Develop or update your model to align your organization's risk appetite and tolerance with specific AI use cases and that support how and where governance principles are required and applied. For example, an AI grammar and editing assistant likely will not require the same risk review that a statistical financial risk model.

Trusted AI Governance

Core Guiding AI Principles	○ AI Principles
Policies governing AI Principles	○ Policy
Representative standards defined based on frameworks such as NIST, OECD, SR11-7, ISO (42001) & ENISA	○ Standards
AI Best Practices Guide	○ Process
Self Assessment, RACI, Risk Scoring	○ Controls & Metrics

3 Develop and publicize a company wide Artificial Intelligence Charter

Aligned with the organization's core principles, the Artificial Intelligence Charter states the ethical vision for artificial intelligence at the organization, building the foundation for responsible and trusted use of generative AI.

4 Reimagine your AI intake process

In terms of generative AI, the intake process should include how new AI models are considered, reviewed, and approved prior to development and implementation. This is an important step because generative AI has the potential of introducing new risks such as access to confidential data by third parties, IP risks, or liability issues that are often not considered in current intake processes.

5 Re-evaluate your third-party risk exposure and contracts

Implement a process for re-evaluating existing contracts and evaluating recently added AI features to third party products to identify any contractual gaps or potential risks to your organization from using new AI product features. Further, review your vendors' AI charter against your own to gain comfort that both organizations align on responsible and trusted use guidelines.

6 Align existing policies for AI

Organizations should review and align their policies for generative AI models to ensure suitability and applicability for generative AI implementation. Alignment activities include, but are not limited to, examining the impact of regulations on the use of generative AI and assessing the impact of AI on various areas of the organization, such as operations, human resources, and legal compliance.

7 Implement controls to manage risks across the entire AI lifecycle

Implement appropriate safeguards and controls to manage risks across the entire AI lifecycle. Such safeguards include, but are not limited to, ongoing monitoring of outputs for model drift and hallucinations.

8 Engage a diverse and representative group of stakeholders

It is important to engage a broad set of stakeholders in these efforts and within your AI Steering Committee. For instance, consider diversity, equality, and inclusion (DEI), human resources (HR), legal and compliance in addition to other stakeholder groups such as Finance and IT. A diverse steering committee, through advancing training and educational programs for example, can help ensure that all perspectives are incorporated, and all risks are considered in the finished model.

Considerations for risk professionals to get started on the AI governance journey

The rapid evolution and adoption of generative AI creates significant challenges for business leaders responsible for helping to ensure adequate governance and oversight.

1 Operational Risk

Is my existing governance process agile enough to ensure that generative AI risks are identified, managed, mitigated in a timely manner?

Are my existing risk appetite metrics aligned to risks related to generative AI?

Are our processes to bring generative AI to market to cumbersome and impeding our ability to capitalize on opportunities?

Have we created an inventory of the existing AI technology landscape?

Are controls appropriate for each stage of the generative AI lifecycle and are controls commensurate to different risk levels?

Do automated workflows or tools maintain and enhance control postures?

2 Third Party Risk

How do I evaluate the risk profile of third party risk vendors we are using for AI applications?

How do I ensure that my vendors are not camouflaging their use of AI in supporting my existing needs?

How do our AI third party providers map against our AI principles?

How do we monitor and manage for ongoing risks after the vendor has been approved?

What is the contingency plan in case my third party is not in compliance?

3 Security Risk

How are we safeguarding our AI systems from potential cyber attacks?

Have we addressed security issues and opportunities by providing a suite of services to specifically address the issues and opportunities discovered within an organization's AI ecosystem?

How do we ensure the robustness and resiliency of our systems in event of an attack?

Have we performed an assessment of our current state of AI Security Pipelines, including technical components of AI pipeline and related vulnerabilities?

4 Data Risk

How is data accuracy and integrity being maintained while using AI systems?

Is there a continonous monitoring mechanism of data usage and processing within AI to prevent data misuse?

Are the current data classification schemas relevant for the Gen AI risks?

What are my controls and measures on data leakage and loss?

Do our data and privacy policies ensure compliance with the data protection laws and regulations?

How KPMG can help

With every generative AI project, at KPMG, we strive to combine our deep industry experience, modern technical skills, leading solutions, and robust partner ecosystem to help business leaders harness the power of generative AI in a trusted manner—from initial strategy and design to ongoing activities and operations. We are actively involved in helping our clients manage risks associated with generative AI solutions such as performing rapid assessments of existing generative AI frameworks, maturity and benchmarking analysis, and implementing a generative AI governance process from intake to production.

Contact us

Bryan McGowan
US Trusted AI Leader
KPMG LLP
T: 816-802-5856
E: bmcgowan@kpmg.com

Vivek Mehta
Solution Leader,
Technology Risk KPMG LLP
T: 212-872-6548
E: vivekmehta@kpmg.com

Learn more at: **visit.kpmg.us/TRMCOE**

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

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

MADE: MDE200155 | October 2023