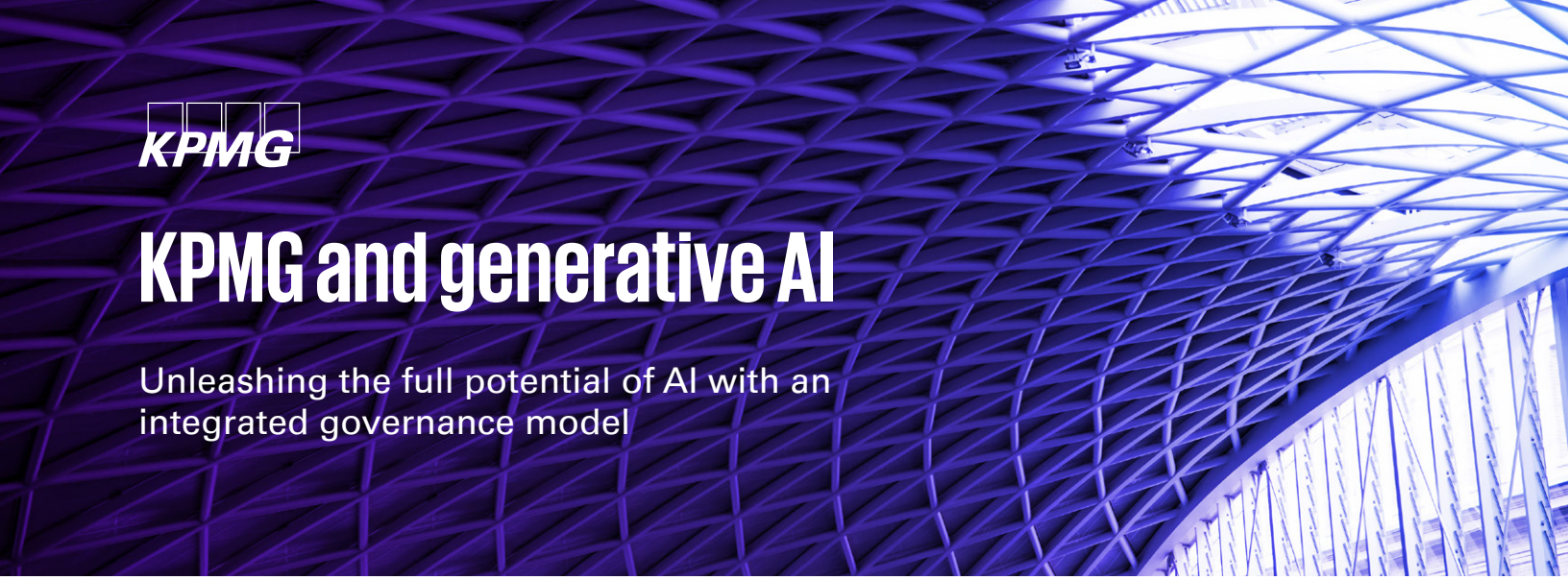


KPMG and generative AI

Unleashing the full potential of AI with an integrated 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. Additionally, 80 percent believed that generative AI will disrupt their industry, and 93 percent are certain that this technology will provide value to their business.

The benefits are clear in generative AI solutions, including:

- Gaining efficiency and improving productivity
- Improving decision making based on data and analytics
- Generating reports, presentations, and other communication
- Enhancing user experiences
- Optimizing costs
- Building and improving business models
- Enabling innovation and transformation initiatives.

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

Equally clear, however, are the risks involving generative AI. Even the best-run organizations can develop or adopt generative AI solutions that unintentionally present major risks in the following areas:

Bias or inaccuracy: perpetuating and even amplifying societal biases present in the data used to train algorithms

Lies and misinformation: inadvertently creating fake, distorted, or misleading content

Privacy concerns with personal data: generating sensitive information, such as personally identifiable data or protected health information

Cybersecurity: allowing the unintended introduction of vulnerabilities into infrastructures and applications through generated code or configurations

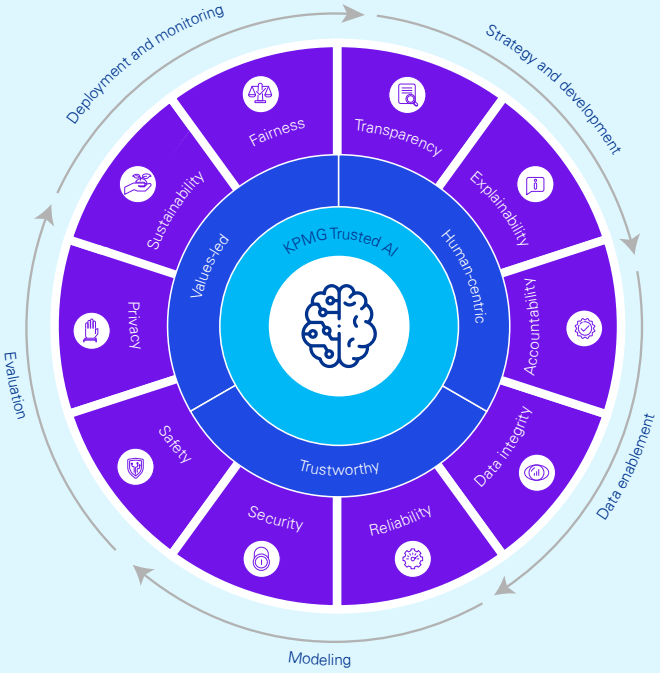
Legal, copyright and intellectual property (IP) issues: creating ambiguities over the authorship, ownership, and responsibility of the data input and content generated by AI

Liability: acting on wrong information or taking detrimental actions (such as a wrong diagnosis or the deletion of IP) that leave the organization open to legal liability

Transparency: failing to understand input data or how generative AI makes decisions, sometimes because of "black box" technology provided by third-party suppliers

In a survey conducted by KPMG and The University of Queensland, Australia, 17,000 people from 17 countries were asked about the potential risks of AI solutions. Three out of five respondents (61 percent) said they were wary about trusting AI systems, reporting either ambivalence or an unwillingness to trust.[2]

KPMG Trusted AI framework



Fairness
AI solutions should be designed to reduce or eliminate bias against individuals, communities, and groups.

Transparency
AI solutions should include responsible disclosure to provide stakeholders with a clear understanding of what is happening in each solution across the AI lifecycle.

Explainability
AI solutions should be developed and delivered in a way that answers the questions of how and why a conclusion was drawn from the solution.

Accountability
Human oversight and responsibility should be embedded across the AI lifecycle to manage risk and comply with applicable laws and regulations.

Data integrity
Data used in AI solutions should be acquired in compliance with applicable laws and regulations and assessed for accuracy, completeness, appropriateness, and quality to drive trusted decisions.

Reliability
AI solutions should consistently operate in accordance with their intended purpose and scope and at the desired level of precision.

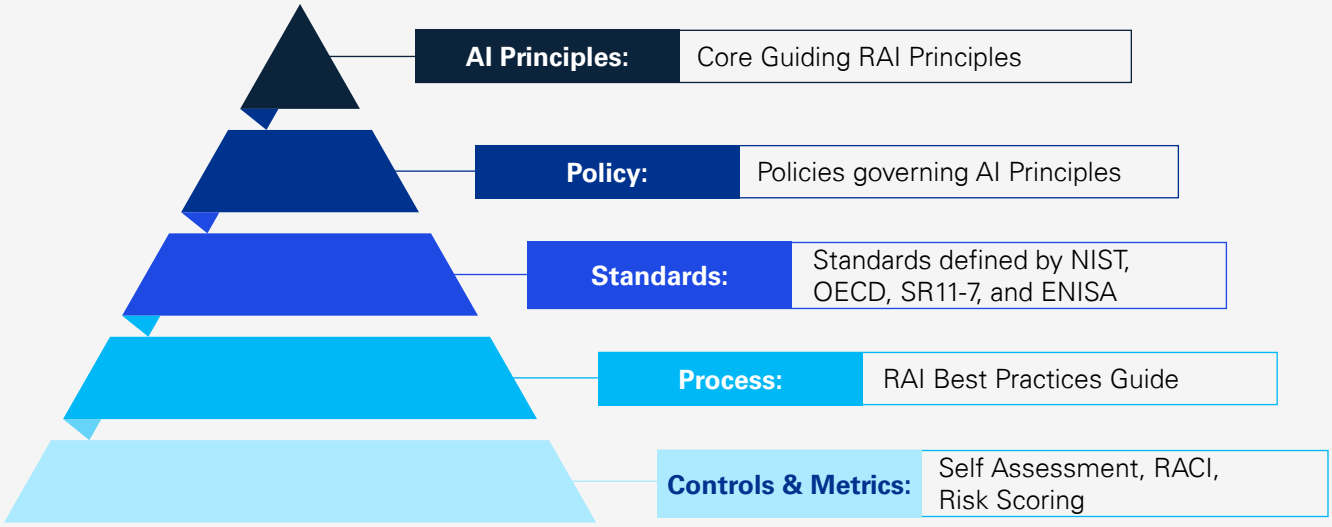
Security
Robust and resilient practices should be implemented to safeguard AI solutions against bad actors, misinformation, or adverse events.

Safety
AI solutions should be designed and implemented to safeguard against harm to people, businesses, and property.

Privacy
AI solutions should be designed to comply with applicable privacy and data protection laws and regulations.

Sustainability
AI solutions should be designed to be energy efficient, reduce carbon emissions, and support a cleaner environment.

Trusted AI Goverance - The Framework



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

Developing an effective AI governance model: What should risk professionals know

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:

01 **Maintain security and privacy as core components of any governance model.** The generative AI risk landscape includes data poisoning and backdoor detection, model theft or ransom, model evasion, and data extraction, to name a few. Develop governance that addresses key issues such as data integrity, reliability, and safety by using frameworks such as Trusted AI, a tested approach to the development, and deployment of AI systems in a safe, trustworthy, and ethical manner. Consider enhancing your existing AI policies, such as codes of conduct, to include the protection of confidential information in accordance with applicable legal requirements, professional standards, and contractual obligations.

02 **Consider a single consistent governance model.** 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 a model that aligns your organization's risk appetite and tolerance with specific AI use cases and supports how and where governance principles are required and applied. For example, an AI grammar and editing assistant might not require the same risk review that a statistical financial risk model would.

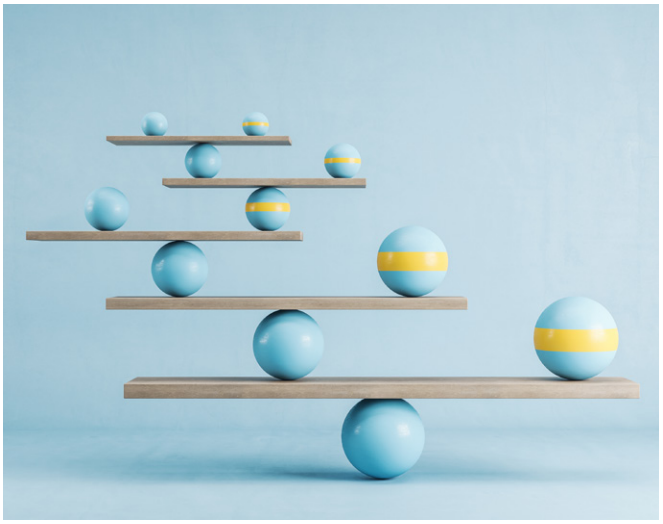
03 **Reimagine your work intake process.** In terms of generative AI, the intake process should include how new AI models are considered, reviewed, and approved prior to development and implementation. This is important because generative AI has the potential of introducing new risks such as access to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

04 **Re-evaluate your third-party risk management process.** Review your vendors' Trusted AI principles against those supported by your organization to identify any gaps. Furthermore, consider re-evaluating existing contracts with vendors that have recently adopted AI technologies.

05 **Develop sustainable solutions.** Organizations with ESG commitments need to consider how their AI solutions can be energy efficient, reduce carbon emissions, and support a cleaner environment.

06 **Help ensure that a diverse and representative group of stakeholders are involved in governance and model development.** It is necessary to engage diversity, equality, and inclusion (DEI) and human resources (HR) teams in these efforts. Steering committees should also advance training and education programs.

07 **Build appropriate safeguards and measures to manage risks across the entire AI lifecycle, including ongoing monitoring.** Solutions need to continuously test for risks such as model drift involving results that stray away from initial project parameters, or hallucinations where AI generates a convincing but completely made-up answer.



Engage your board for better oversight over AI initiatives

The rapid evolution and adoption of generative AI creates significant challenges for business leaders responsible for helping to ensure adequate governance and oversight. Board members and other senior executives can consider the following questions to help them assess their organization's state of readiness and maturity regarding generative AI issues:

- 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 my stakeholders in business and IT frustrated by the slow risk review process?
- Are controls appropriate for each stage of the generative AI lifecycle and are controls commensurate to different risk levels?
- Do automated workflows maintain and enhance control postures?
- Does your organization provide a safe zone for development?
- Is experimentation appropriately supported with access to training data for use cases?
- Is monitoring and measuring post-deployment supported?
- Can the organization's generative AI solutions scale up effectively while still managing risk?

5 steps for risk organizations to get started on the AI Governance journey

- Establish your principles for AI that will guide your process in building the governance model and consider an enterprise-wide AI mission statement.
- Reimagine your existing governance model including your risk assessment process to uncover the risks of AI.
- Ensure that your AI office is inclusive of relevant stakeholders across Business, Technology, HR, Diversity amongst others.
- Align your AI deployments against appropriate standards and regulatory guidelines.
- Monitor your existing third and fourth parties to determine compliance against your trusted AI principles including existing low risk approved vendors.

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
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**