

AI Solutions: Preparing for AI Assurance



The challenge

Artificial Intelligence (AI) is becoming embedded in products, services, and business processes across many organizations. While AI enhances productivity and competitiveness, it also introduces new risks. As AI adoption grows, stakeholders increasingly expect organizations to demonstrate that AI systems are governed responsibly and supported by effective controls.

KPMG's assurance readiness assessment helps organizations assess whether the governance, controls, documentation, and evidence needed to support future AI assurance are in place. Action taken now can help an organization reduce risk, build stakeholder confidence and prepare for future assurance requirements.



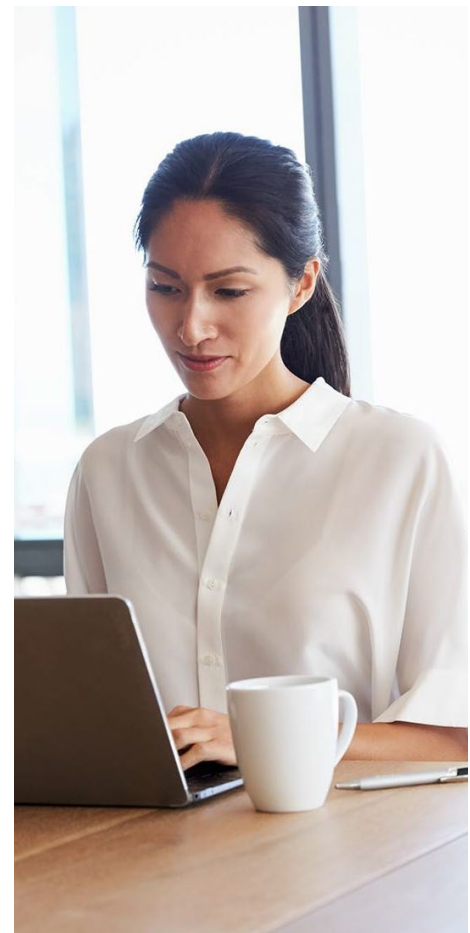
Governance and Entity-Level Controls

As AI becomes increasingly integrated into various business processes, establishing strong governance policies and procedures over its development/acquisition, deployment, and operation is essential. Assurance can exhibit management's commitment to strong governance through these policies and procedures and entity-level controls, supporting proactive identification and mitigation of potential risks associated with the responsible deployment of AI.



Regulatory Requirements

Current regulations over technology may be applicable to AI. Additionally, regulations governing the use of AI are emerging in multiple jurisdictions. Specific industries, such as those handling personally identifiable information in their AI systems, will have additional requirements. Assurance provides an efficient way to meet compliance requirements with current (and future) regulations, as well as client contractual requirements and expectations.





Trust

AI presents risks around bias, fairness, and unintended outcomes, potentially impacting reputation and brand. Assurance can help to build trust by demonstrating a clear focus on explainability, accountability, and transparency to promote confidence in AI-driven decisions.



Human-in-the-Loop (HITL)

The nature of AI and level of reliance in the business processes may require HITL involvement incorporated into the process. Assurance can demonstrate effective management of AI-related risks through HITL.



General IT Controls (GITCs)

Incremental risks may be introduced by using AI, and new or updates to existing GITCs at the application, database, and operating system level will likely need assurance to user entities. Additionally, a service organization may use AI in the execution of GITCs to provide information to the control operator or to carry out control activities.



Process Changes

The way data is initiated, authorized, processed, recorded, and reported may change because of AI adoption. User entities will expect assurance over these new processes as they evolve.



Cybersecurity risks

Cybersecurity risks may change upon adoption of AI. These risks encompass multiple aspects of an entity's operations, including cyber-related fraud, changes impacting internal controls, and overall integrity of data used in AI. User entities will want to understand how AI is interacting with service organizations' systems and environment, and how the service organization identifies risks and implement controls.

KPMG recommends



Assurance readiness assessment

can help entities prepare to deliver assurance to their customers and user entities. It provides observations and recommendations on related controls through an assessment against the relevant criteria identified by management.



As entities integrate AI into their ecosystems, they may need to provide assurance over AI-enabled systems by demonstrating trusted AI governance, compliance, and effective controls across business processes and the technology environment.

The potential benefits of KPMG Ready for Assurance service

A readiness assessment provides observations and recommendations that help organizations identify and address risks and control gaps before commencing an assurance engagement. Examining the entities' commitment to AI governance, risk, and controls can meet their compliance needs while simultaneously enhancing trust in the relationship with user entities.

Additionally, you may also want to undertake further analysis to identify gaps in your reporting and/or to benchmark against your peers. These activities can help support your organization's long-term strategy and may include:

- Industry and peer benchmarking* to contextualize progress
- Gap assessments* to identify areas for improvement



Potential benefits to the entity

1. Receive practical observations and recommendations to help identify and address risks and control gaps earlier in the process and before providing the actual assurance reporting to their user entities.
2. Receives pre-assurance feedback on use of AI related criteria such as data quality and lineage, bias and fairness, explainability, performance and calibration thresholds, drift monitoring, privacy and security, change and version control.
3. Prepares entities to deliver assurance to user entities by improving transparency over AI system governance and supporting user entities' compliance with third-party risk requirements.



Potential benefits to the user entities

1. Gain greater confidence in the governance of third-party AI systems by identifying and managing associated risks while strengthening internal controls.
2. Provides an opportunity to assess and enhance operational controls and processes.
3. Supports AI transformation efforts by providing clarity of the processes and controls over data integrity and whether they are aligned with the objective of the AI solution.

KPMG professionals' capabilities and expertise in AI governance, business processes, and controls can provide entities with essential insights during their AI Transformation journey.

Contact us



Neil Morris
Global Head of Assurance and Assurance Methodology
E: neil.morris@kpmg.co.za



John Razos
Global Head of IT Audit
E: jrazos@kpmg.com



Oliver Geier
EMA Coordinating Assurance Partner
E: ogeier@kpmg.com



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

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 on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit kpmg.com/governance.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document, "we", "KPMG", "us" and "our" refers to the KPMG global organization, to KPMG International Limited ("KPMG International"), and/or to one or more of the member firms of KPMG International, each of which is a separate legal entity.

Document Classification: KPMG Confidential