KPMG | servicenow

Technology enabled AI performance

A practical approach to AI governance, risk, and controls

When it comes to artificial intelligence (AI) applications, notably the use of generative AI (GenAI), security and regulatory compliance is quickly becoming a top priority. Today's chief technology officers, chief information officers, and chief information security officers face heightened scrutiny as regulatory demand on the GRC function increases. This represents a significant shift in how AI technology is governed, driving towards a future where AI is implemented and used in a responsible, ethical, and efficient way.

A new dimension of risks, created in part by GenAI hallucinations, prompt injections, biased data sets, and other newly emerging and evolving threats, creates even more burden on those responsible for managing and mitigating risk across the enterprise. The balance of embracing the innovation enabled by GenAI with the risks it introduces will quickly become a high priority for enterprise risk programs.

How can organizations safely and quickly adopt and innovate with AI while adhering to complex and evolving regulatory requirements and security concerns? An overarching AI strategy becomes critical. This strategy must govern how the AI applications are used to produce safe and reliable outcomes, and the data fed into and generated out of large language models (LLMs). Furthermore, adherence to regulatory requirements can foster a spirit of trustworthiness among stakeholders. The absence of their trust can lead to a culture of skepticism and risk avoidance. Creating a proper governance model puts the guardrails in place for employees, customers, and investors to feel more confident in your AI program.

A human-centered approach to AI governance

AI is a tool for humans. As such, organizations must consider both the technology components as well as the "human in the loop" when creating their AI governance model. It is not enough for AI to be secure. AI technology, and its users, must be bound by controls that allow for it to be trusted by all stakeholders who may be impacted by its use.

KPMG Trusted AI is a human-centric approach to governing AI. It is based on ethical practices that inspire a commitment to trustworthiness, help ensure data practices uphold the highest ethical standards, and reinforce the need to comply with privacy, data protection regulations and confidentiality requirements.

Our approach to trusted AI rests on ten ethical pillars across the AI lifecycle.

Fairness

Designing AI solutions that actively work to reduce or eliminate bias against individuals, communities, and groups

Reliability

Helping ensure AI solutions consistently operate in line with their intended purpose, scope, and desired precision level

Transparency

Making pertinent information accessible to stakeholders clear, facilitating a thorough understanding of the functions and performance of AI solutions

Security

Implementing robust and resilient practices to safeguard AI solutions against bad actors, misinformation, or adverse events

Explainability

Providing answers to the "how and why" of the conclusions drawn from AI solutions

Safety

Building AI solutions that prevent harm to people, businesses, and property

Accountability

Incorporating human oversight and responsibility across the AI lifecycle to manage risk and help ensure compliance with applicable laws and regulations

Privacy

Designing AI solutions to comply with privacy and data protection laws and regulations

Data integrity

Making sure the data used, aligns with applicable laws and regular checks for accuracy, completeness, appropriateness, and quality

Sustainability

Designing AI solutions in an energy-efficient way to reduce carbon emissions and support a clean environment.

A tech-enabled approach to AI governance

The KPMG Trusted AI framework can be combined with the native capabilities of the ServiceNow platform to support governance, risk, and compliance management of AI applications. KPMG embeds the ten pillars of Trusted AI into detailed risk and control objectives in the ServiceNow Integrated Risk Management (IRM) suite to help organizations adopt AI safely and ethically. This approach helps clients focus on building a robust controls library with regular updates and automated indicators as AI management solutions evolve and differ across businesses.

Using ServiceNow to enable the KPMG Trusted AI framework creates an interactive and cohesive workspace to manage AI integrated risk management components, CMDB and asset inventory classes, AI use case profiles, and other core capabilities of the ServiceNow platform.

Mapping all AI governance requirements to ServiceNow's suite of solutions enables clients to manage their AI model inventory, model governance, risk-tracking, workflow automation, auditability, transparency, and traceability systematically.

1. **CMDB and Asset Management**
   Takes charge of model inventory management, model certification process, and model governance role management, the applications they serve, their respective lifecycles and operational costs.

2. **IRM/GRC Suite**
   Manages risk and issue tracking, and workflow automation.

3. **App Engine**
   Powers a centralized workspace, an integration hub, reporting, flow, process designer, new CI and Asset classes, new reports and metrics, and other features tailored to the enterprise.

By combining a digitized Trusted AI framework with out-of-the-box features of ServiceNow, clients are able to simplify, streamline, and automate various aspects of their AI governance, enabling quicker decision making and increasing confidence that regulatory and internal compliance requirements are met. With effective risk management guardrails in place, Information Technology, Risk, and Security leaders can demonstrate that AI is being applied responsibly and ethically, helping to earn the trust of their regulators, investors, employees, third parties and customers.

Contact us

Are you looking to achieve a lower risk profile and create a compliant environment for your AI? Talk to one of our specialists today about how KPMG Trusted AI and ServiceNow can help. Learn more at: read.kpmg.us/servicenow

Bryan McGowan
T: 314-458-8898
E: bmcgowan@kpmg.com

P. Michael Lutz
T: 415-963-5158
E: mikelutz@kpmg.com

Prasanna Govindankutty
T: 212-954-2737
E: pkgovindankutty@kpmg.com

Sean Barrins
T: 206-913-6747
E: sbarrins@kpmg.com

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

Learn about us: **kpmg.com**