Evidence-based assurance over AI systems

How Internal Audit assesses whether AI systems and controls work as intended

AI failures and misuse can create operational, financial, compliance and liability risks, and undermine trust. Internal Audit tests whether AI systems work as intended and whether governance and controls address these risks.

Six areas for evidence-based AI assurance

AI use, value and governance

Challenge: Shadow AI, unclear accountability and changing staff roles.

Relevant question: Does the organisation know which AI systems it uses, who owns them and whether they deliver value?

Potential Internal Audit project: AI strategy, inventory and governance review. Compare inventory with use. Assess value, ownership, risk classification, oversight, AI literacy and IP/know-how protection.

AI performance, oversight and resilience

Challenge: Variable outputs, model drift and limited explainability.

Relevant questions: Do AI systems work as intended, with a workable fallback? Can users understand, challenge and override their outputs?

Potential Internal Audit project: AI lifecycle and resilience review. Review design, validation and transparency. Test outputs against agreed criteria. Use logged cases to test human intervention. Assess monitoring, incident response, fallback, remediation and retirement.

Regulation and responsible use

Challenge: Overlapping requirements across jurisdictions and sectors.

Relevant question: Can the organisation demonstrate that its AI use meets applicable AI, data and digital requirements?

Potential Internal Audit project: AI regulatory compliance review. Trace AI, data and digital obligations to controls and evidence. Assess cross-border applicability and responses to regulatory change.

Security and agentic AI

Challenge: Prompt attacks and unauthorised autonomous actions.

Relevant question: Do access controls and guardrails restrict AI systems and agents to authorised use and actions?

Potential Internal Audit project: AI security and agent controls review. Test permissions and guardrails. Review autonomous action logs and escalation arrangements.

Data quality and protection

Challenge: Unreliable data, unlawful use and loss of sensitive information.

Relevant question: Is AI data traceable, fit for purpose, lawfully used and adequately protected?

Potential Internal Audit project: AI data governance review. Test provenance, quality and lawful use. Assess privacy, security and data sovereignty controls.

Third parties and dependencies

Challenge: Supplier dependencies and model updates.

Relevant question: Does the organisation understand and control the AI risks it inherits from suppliers?

Potential Internal Audit project: AI third-party risk review. Assess due diligence, contracts, dependencies and risks from supplier and model updates.

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG helps Internal Audit deliver evidence-based AI assurance

KPMG's Trusted AI framework sets out principles for responsible AI. Our methodology translates these principles into a practical assurance approach, supported by RegRadar™ and the Trusted AI Risk & Control Matrix. This helps Internal Audit assess AI risks, controls and applicable AI, data protection and digital resilience requirements.

KPMG support	Application in Internal Audit
AI audit planning and work programmes	Translate AI risks into audit scope, assessment criteria and tailored audit procedures, using the Trusted AI Risk & Control Matrix.
Test of Design and Test of Effectiveness	Assess whether AI controls address the identified risks and test whether they operate as intended, using documented evidence.
Specialist AI and governance testing	Support testing of model validation, AI outputs and human oversight. Assess technical controls, including agent permissions and guardrails.
Regulatory compliance testing	Use RegRadar™ to identify applicable requirements and regulatory changes. Trace obligations to controls and test the supporting evidence.
AI assurance and reporting	Draw evidence-based conclusions on AI governance, controls and outcomes. Report findings and follow up on agreed remediation actions.



© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Trusted AI framework

Sustainability

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

Fairness

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

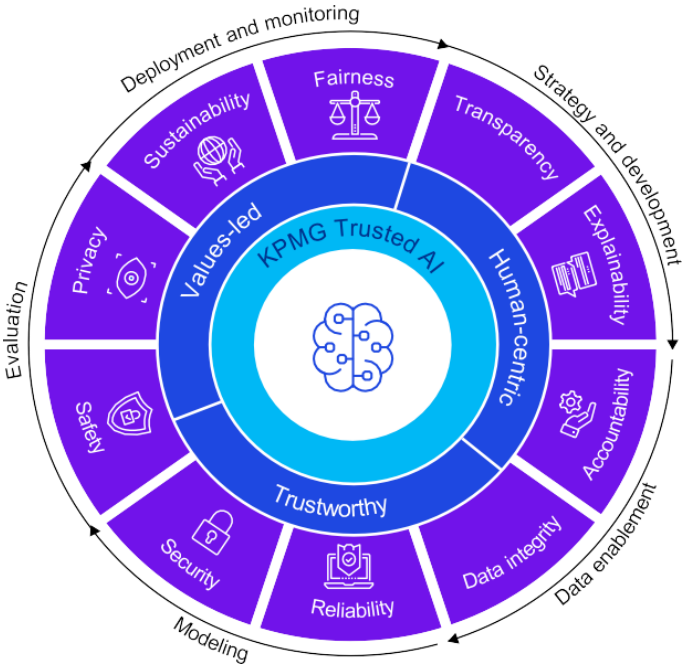
Transparency

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

Explainability

AI systems should be developed and delivered in a way that explains how and why the system reached a conclusion.

Ten pillars for responsible AI across the lifecycle



Accountability

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

Safety

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

Security

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

Reliability

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

Data integrity

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

Privacy

AI systems should protect personal data and privacy by design and comply with applicable privacy and data protection requirements.

Contact us



Huck Chuah
Partner, Internal Audit Services
T: +31 20 656 4501
E: Chuah.Huck@kpmg.nl



Marc van Meel
Responsible AI Lead
T: +31 20 426 2564
E: VanMeel.Marc@kpmg.nl



Stefan Zuijderwijk
Senior Manager, AI in Internal Audit
T: +31 70 338 2130
E: Zuijderwijk.Stefan@kpmg.nl

Generative AI was used to support the draft and final version of this whitepaper.
All AI outputs have been validated and reviewed by the authors, and a human-in-the-loop approach was continuously applied

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.