



The AI Confidence Gap

Can your organisation
prove its AI can be trusted?



Can your organisation prove its AI can be trusted?

Artificial intelligence is rapidly moving from experimentation to enterprise-wide adoption.

From customer service and software development to finance, HR and risk management, businesses are embedding AI into core business processes at an unprecedented pace.

As AI adoption accelerates, boards and executive teams are increasingly asking a simple question:

How do we know our AI systems are operating as intended, and how can we demonstrate that confidence to stakeholders?

We are seeing a clear dividing line opening between organisations: those that can evidence their AI is working as intended, and those that cannot. A recent survey by KPMG Board Leadership Centre highlights that 45% of Business Leaders had Trust as their biggest concern¹. In our view, this is not just a governance issue; it is increasingly a value issue. When employees, customers and other stakeholders do not trust AI systems, adoption slows, decisions are second-guessed, and manual workarounds emerge.

As a result, organisations often fail to realise the productivity, efficiency and insight benefits that underpinned their AI investment in the first place. Trust is therefore becoming a critical enabler of AI value, not simply a compliance consideration.

This is where AI assurance has an important role. It provides an independent, evidence-based assessment of whether an organisation's AI governance and controls are appropriately designed, and operating as intended.

By helping businesses demonstrate how AI is governed, controlled and monitored, assurance can strengthen stakeholder confidence and support responsible adoption at scale.

45% of Business Leaders had Trust as their biggest concern

¹ [The AI oversight challenge: Insights from our board member survey](#)

AI Governance is becoming a board-level topic



Recent discussions with clients across sectors reveal a common trend: AI is now appearing regularly on board and audit committee agendas, with 81% of UK CEOs saying AI is a top investment priority for their organisation and 87% anticipating that 10% or more of their budgets will be spent on AI.²

Boards see the opportunity. Their focus is on capturing it responsibly.

Many businesses see significant opportunities to improve efficiency, enhance customer experiences and unlock new insights through AI. The KPMG 2025 UK CEO Outlook also indicates that organisations are preparing for AI's workforce impact: 71% of UK CEOs are redesigning roles and career paths to reflect AI collaboration, while 52% are engaging external AI experts to help their workforce embrace AI.

However, boards recognise that increased adoption brings a responsibility to ensure these technologies are deployed responsibly and effectively.

Just as cybersecurity risk evolved from an IT issue to a boardroom priority, AI is following a similar trajectory.

Organisations that can demonstrate robust oversight of their AI systems are likely to be better positioned to build trust with customers, regulators, employees and investors.



87%
of UK CEOs
anticipate that 10%
or more of their
budgets will be
spent on AI.²

² KPMG 2025 CEO Outlook – UK

Practical steps organisations can take today

01



Establish clear AI accountability

Define the individuals who own AI risks within the organisation and ensure accountability is clearly assigned. Governance structures should include oversight from relevant business, technology, risk and compliance stakeholders. Importantly, organisations should ensure humans remain in the lead, with AI augmenting rather than replacing human judgement, accountability and decision-making.

02



Maintain an AI inventory

In our work with clients we have found that many organisations are surprised by the number of AI-enabled tools already in use across the business. Maintaining an inventory of AI systems helps provide visibility and supports effective risk management. This should also extend to AI use within the supply chain, particularly where third-party tools or services support critical business processes.

Organisations should then ask: Who is accountable for each AI system? If an AI agent takes an action, who is ultimately responsible for that outcome? And where one agent relies on multiple interconnected agents, where does accountability sit? Establishing clear human ownership over AI-enabled processes is critical to ensuring effective governance and maintaining trust.

03



Implement risk-based assessments

Not all AI systems present the same level of risk. A customer-facing decision-making model may require significantly greater scrutiny than an internal productivity tool.

Organisations should assess AI systems proportionately based on their intended use and potential impact.

04



Document controls and decision-making

Strong documentation remains fundamental. Organisations should be able to demonstrate how AI systems are selected, implemented, monitored and governed throughout their lifecycle.

05



Monitor performance and outcomes

AI validation and assurance is not a one-time exercise. Ongoing monitoring helps organisations understand whether systems continue to perform as expected and whether emerging risks require attention.

Why AI Assurance matters

Most organisations already recognise the importance of assurance in areas such as financial reporting, ESG, cybersecurity and operational controls.

Assurance frameworks have become widely adopted because they provide confidence that systems and processes are appropriately governed and controlled.

AI introduces a new set of risks and also increases the likelihood that existing risks crystallise, for example, cyber threat. As a result, traditional control frameworks alone may not provide sufficient confidence.

Unlike established software, Generative AI is dynamic and, by design, will not produce the same output every time. Outcomes can vary depending on context, prompts and underlying training data.

Organisations must consider questions such as:

- Is the AI performing consistently within acceptable risk tolerances?
- Are appropriate controls in place over training data and model management?
- Can decisions be explained and justified where necessary?
- Are governance structures keeping pace with AI deployment?
- Are regulatory and ethical considerations being appropriately addressed?

These questions are also no longer confined to technology teams. As AI becomes embedded across organisations, boards are taking a more active role in overseeing its strategic value, risks and wider impacts. At the same time, standards and regulation, including ISO/IEC 42001 and the EU AI Act, are

raising expectations around documented governance, accountability and control. Investors, customers and other stakeholders are also seeking greater evidence that businesses can demonstrate how material AI risks are being managed, rather than relying on statements of intent alone.³

Recent AI testing incidents, involving advanced models gaining unintended access to external systems⁴, highlight the importance of effective governance, containment controls and ongoing monitoring. As AI systems become more capable and autonomous, organisations will need not only to maintain

these safeguards, but also to demonstrate that they are operating effectively. Independent assurance can provide one credible way of supporting that confidence as AI risks and governance expectations continue to evolve.

³ AI Governance Principles for Boards.

⁴ BBC News, [OpenAI says its AI went rogue and launched 'unprecedented' cyber-attack](#).

The emergence of AI assurance

As expectations increase, organisations will likely turn to more formal and structured assurance approaches.

This reflects the growing role AI plays both within organisations and in the services they provide to customers. We've seen an increase in organisations using AI to support elements of their control environment, such as software development, monitoring and testing activities whilst at the same time, embedding AI capabilities directly into customer-facing products and services. In both cases, stakeholders need confidence that AI is operating as intended and that appropriate controls are in place. Without that confidence, organisations may struggle to realise the full value of their AI investments.

Employees may be reluctant to rely on AI outputs, customers may question AI-enabled services, and the expected productivity and efficiency gains may never fully materialise.

AI assurance can involve a range of approaches depending on what an organisation wants confidence over, who needs that confidence, and how the AI system or related claims will be used. This may include governance and risk assessments, assurance readiness reviews, controls assurance, specialist testing of systems or models, and assurance over defined AI-related disclosures or claims.

Service Organisation assurance (resulting in a formal opinion) can be a particularly effective route, where an organisation wants to provide this structured assurance to external stakeholders. Established frameworks such as SOC 1 and SOC 2 can be extended with AI-specific considerations, including areas such as:

- Transparency and explainability
- Data integrity and governance
- Fairness and ethical use
- Accountability across the AI lifecycle

These areas align to broader trusted AI principles, which also encompass considerations such as privacy, security, reliability and safety.

KPMG's SOC 1 and 2 approaches extend traditional assurance principles by incorporating these AI specific considerations, leveraging the KPMG Trusted AI framework⁵ to provide a more comprehensive view of AI governance and control.

This approach enables organisations to:

- Provide independent, evidence-based assurance over their AI environment.
- Respond to evolving regulatory and stakeholder expectations.
- Demonstrate, in a structured and credible way, how AI systems are governed, controlled and monitored.
- Build confidence among customers, regulators, boards and other stakeholders that AI governance and controls are robust and operating as intended.

⁵ KPMG's Trusted AI framework has been systematically mapped against the EU AI Act and ISO/IEC 42001.

Looking ahead

- > AI is not a temporary trend; it is a core capability that will continue to reshape organisations.
- > The key question is no longer whether AI will be used, but **how confidently can it be deployed, and how credibly can that confidence be demonstrated?**



AI assurance should not be viewed as a barrier to innovation. Rather, it can serve as an enabler to move more quickly providing the confidence that innovation is supported by appropriate governance, oversight and accountability.

In the evolving AI landscape, capability alone will not be enough. Organisations that

invest early in governance, controls and assurance will be better positioned to demonstrate that their AI is operating as intended and to:

- Scale AI with confidence
- Earn and maintain stakeholder trust
- Unlock sustainable value and performance gains

KPMG brings together deep expertise across assurance, technology, risk, cyber, data, regulatory matters and sector specialisms.

Wherever organisations are on their AI journey, KPMG can help address the confidence gap and determine the right approach.



Contact us



Thomas Collins

Partner, Controls Assurance
KPMG in the UK
thomas.collins@kpmg.co.uk



Daria Yudina

Director, ESG Assurance
KPMG in the UK
daria.yudina@kpmg.co.uk

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



kpmg.com/uk

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 endeavour 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.

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

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

CREATE. | CRT168005 | September 2026



As organisations accelerate AI adoption, building trust and confidence has never been more important.

Visit our hub, [Building Confidence in Your AI Assurance Journey](#), for the latest insights, practical guidance and resources to help you navigate AI risk, governance and assurance.