# AI adoption held back by trust and governance concerns, says Forrester



Many organisations are accelerating their adoption of artificial intelligence to drive innovation and gain a competitive edge. But a new study by Forrester Consulting, commissioned by security automation firm Tines, finds that serious barriers continue to slow progress and expose businesses to risk.

Surveying over 400 IT leaders across North America and Europe, the research highlights that while AI’s potential is widely recognised, challenges around governance, security, trust and organisational alignment are limiting its effective scale.

Governance and security emerge as the leading concerns. Thirty-eight per cent of respondents said these challenges are the primary blockers to broader AI adoption. Traditional governance frameworks were not designed to manage AI’s complexity and shifting regulatory demands, leaving businesses vulnerable to compliance failures, data loss and security breaches. This is further compounded by fears of reputational damage and operational disruption.

Trust and transparency are also key hurdles. Forty per cent of IT leaders reported that employee scepticism around AI-generated outcomes was holding back adoption. Siloed projects and fragmented tools reduce transparency and confidence, undermining investment in AI initiatives. Without explainable, consistent results, AI risks stagnation.

Organisational dynamics present another barrier. Despite 86 per cent of IT leaders believing their teams are well positioned to lead AI efforts, many said they are underestimated by other departments. Over a third said IT’s role is seen as reactive rather than innovative. Nearly half cited poor alignment between IT and the wider business as a major obstacle to unified AI strategies.

The report points to orchestration — the integration of systems, tools and teams — as central to overcoming these barriers. By linking fragmented efforts, orchestration can provide secure, transparent and compliant workflows. Almost three-quarters of respondents stressed the need for end-to-end visibility across AI systems, and nearly half said they wanted partners offering centralised orchestration to reduce silos and build trust.

To succeed, the study recommends that IT teams increase visibility into AI initiatives, align across departments and adopt low-code or no-code tools to scale more efficiently. Articulating AI outcomes in terms of return on investment and operational efficiency is key to winning executive support and funding.

The focus on governance reflects growing academic concern around the risks of autonomous and agentic AI systems. Researchers have identified novel threat vectors stemming from AI’s cognitive functions, persistent memory and tool integration — all of which outstrip the capacity of traditional security models. New governance frameworks designed specifically for AI are needed to address these threats and prevent systems from becoming liabilities.

In the public sector, existing compliance models are often too siloed and episodic to oversee AI responsibly. Researchers argue for adaptive institutional designs that combine governance, operational visibility and continuous auditing.

At a global level, proposals for hardware-based guarantees and cryptographically enforced governance are emerging to manage AI’s geopolitical risks, underlining the need for multi-layered international approaches. Today’s fragmented governance landscape — where risk, compliance and ethics are handled in isolation — adds to the difficulty of scaling AI responsibly. Unified frameworks are now being developed to integrate regulatory requirements, risk management and actionable controls into agile systems that can evolve alongside new regulations.

The Forrester study presents a cautiously optimistic outlook. With the right tools, alignment and oversight, IT teams can lead scalable, secure and trusted AI efforts. This not only strengthens the UK and international position in responsible AI but also fosters innovation in a sustainable and secure way.

Created by [Amplify](https://www.hbmadvisory.com/amplify): AI-augmented, human-curated content.

## Bibliography

1. <https://www.ciodive.com/spons/forrester-study-shows-why-it-is-key-to-building-trust-and-scaling-ai/759657/> - Please view link - unable to able to access data
2. <https://www.itprotoday.com/it-security/forrester-study-shows-pivotal-role-ai-orchestration> - A Forrester Consulting study, commissioned by Tines, reveals that IT teams are crucial in scaling AI but often face organizational barriers. The study highlights that governance and security concerns, budget constraints, and siloed initiatives hinder AI adoption. Orchestration, which connects people, processes, and tools, is identified as essential to overcome these challenges. While 86% of IT leaders believe they are uniquely positioned to orchestrate AI, many organizations have yet to fully recognize IT's strategic role. The study emphasizes the need for IT to lead AI orchestration to drive secure, scalable innovation.
3. <https://www.prnewswire.com/news-releases/it-leaders-hold-the-key-to-scaling-ai-responsibly-according-to-new-tines-study-302549212.html> - A Forrester Consulting study, commissioned by Tines, surveyed 417 IT leaders and practitioners from North America and Europe to explore challenges in scaling AI. The study found that security and governance concerns (38%), budget constraints (35%), inability to prove ROI (34%), and fragmented ownership across departments (33%) are the most cited barriers. The research underscores the need for strategic planning, ethical governance, and workforce readiness to ensure successful AI implementation.
4. <https://arxiv.org/abs/2504.19956> - This paper introduces a comprehensive threat model tailored for generative AI agents, focusing on how their autonomy, persistent memory access, complex reasoning, and tool integration create novel risks. It identifies nine primary threats across five key domains: cognitive architecture vulnerabilities, temporal persistence threats, operational execution vulnerabilities, trust boundary violations, and governance circumvention. The research presents two complementary frameworks: ATFAA (Advanced Threat Framework for Autonomous AI Agents) and SHIELD, proposing practical mitigation strategies designed to reduce enterprise exposure. The study argues that generative AI agents require a new lens for security to prevent turning a powerful tool into a serious enterprise liability.
5. <https://arxiv.org/abs/2506.04836> - This paper examines the challenges posed by agentic AI systems to traditional public sector oversight mechanisms, which rely on siloed compliance units and episodic approvals. It identifies five governance dimensions essential for responsible agent deployment: cross-departmental implementation, comprehensive evaluation, enhanced security protocols, operational visibility, and systematic auditing. Through a mixed-methods approach, the study finds that agent oversight intensifies existing governance challenges, including continuous oversight, deeper integration of governance and operational capabilities, and interdepartmental coordination. The authors propose approaches to adapt institutional structures and design agent oversight compatible with public sector constraints.
6. <https://arxiv.org/abs/2506.15100> - This report examines how flexible hardware-enabled guarantees (flexHEGs) could address international security challenges through comprehensive governance frameworks. It analyzes four critical international security applications: limiting proliferation to address malicious use, implementing safety norms to prevent loss of control, managing risks from military AI systems, and supporting strategic stability through balance-of-power mechanisms while respecting national sovereignty. The report explores two primary governance models: verification-based agreements that enable transparent compliance monitoring, and ruleset-based agreements that automatically enforce international rules through cryptographically-signed updates. Through game-theoretic analysis, it demonstrates that comprehensive flexHEG agreements could remain stable under reasonable assumptions about state preferences and catastrophic risks.
7. <https://arxiv.org/abs/2503.05937> - The rapid adoption of AI systems presents enterprises with a dual challenge: accelerating innovation while ensuring responsible governance. Current AI governance approaches suffer from fragmentation, with risk management frameworks focusing on isolated domains, regulations varying across jurisdictions despite conceptual alignment, and high-level standards lacking concrete implementation guidance. This fragmentation increases governance costs and creates a false dichotomy between innovation and responsibility. The authors propose the Unified Control Framework (UCF), a comprehensive governance approach that integrates risk management and regulatory compliance through a unified set of controls. The UCF consists of three key components: a comprehensive risk taxonomy synthesizing organizational and societal risks, structured policy requirements derived from regulations, and a set of 42 controls that simultaneously address multiple risk scenarios and compliance requirements. The study validates the UCF by mapping it to the Colorado AI Act, demonstrating how the approach enables efficient, adaptable governance that scales across regulations while providing concrete implementation guidance.