



State of AI Governance

2026 - THE UNITED KINGDOM
PERSPECTIVE

Where Operational Governance Meets
Reconstruction Challenge

Research conducted by



A Closer Look
at the UK

Strong Operational
Governance, Uneven
Evidence Continuity

Governance Has
Moved Into the
Workflow

The Record Breaks
as Communications
Move

Investigations
Expose the Cost of
Fragmentation

Modernization Must
Balance Regulatory
Agility and Assurance

UK Organisations Are
Prioritising Connected
Compliance

The UK Movement:
From Operational
Controls to True
Defensibility

About This Research

Research conducted by



A Closer Look at UK

When we published our report, *State of AI Governance 2026: The Policy-to-Proof Gap in AI-Assisted Communications*, organisations are moving beyond simply drafting AI policies to proving what actually happens when AI is used in official workplace communications and decision-making.

Our global research showed that compliance and risk teams are setting clear rules, assigning accountability, and maintaining strict human oversight. At the same time, we are seeing rapid investments in technical tools to track, store, link, and reconstruct AI activity across the enterprise.

Looking specifically at the United Kingdom, we see a clear pattern emerge. UK businesses are relatively advanced in embedding AI governance into daily operational routines. Practices like human reviews, staff training, prompt and output logging, regular audits, and standard monitoring are already widespread among compliance-minded organisations using AI.

AI adoption keeps growing. Out of 100 UK organisations we surveyed, 82 use AI in regulated communications or key decision-making workflows. Nearly one-third of all surveyed UK companies plan to expand AI across their entire business. As AI use scales, a critical new challenge takes shape.

Having strong policies does not automatically create a connected audit record. When AI-assisted work crosses multiple apps, systems, and teams, data gets scattered and hard to piece together during an investigation. This creates a vital benchmark for Compliance, Risk, and Legal leaders.

After setting up foundational AI governance, UK organisations are now focusing on making those actions easier to track, reconstruct, and defend when regulators come asking.

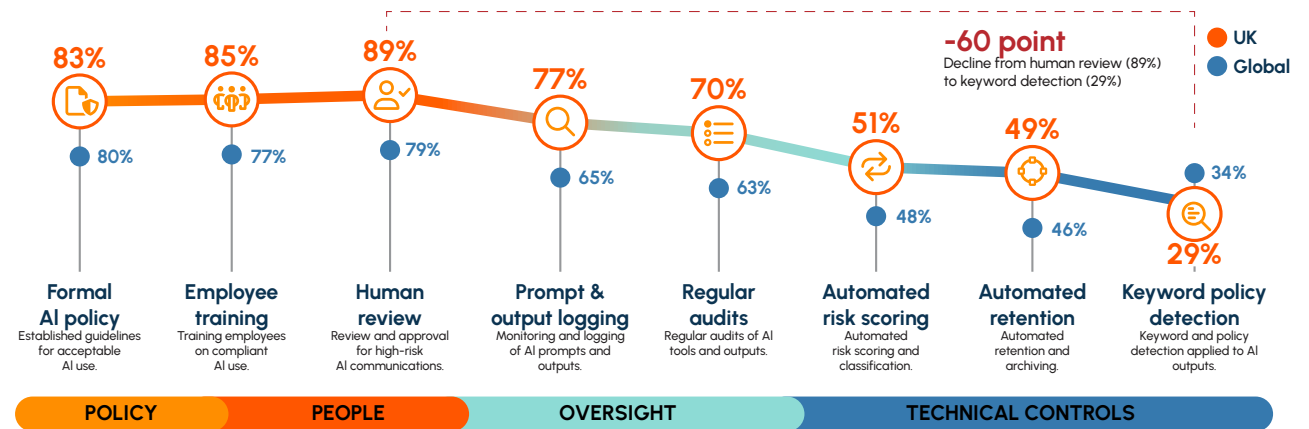
For our complete global benchmark and six-signal framework, explore *State of AI Governance 2026: The Policy-to-Proof Gap in AI-Assisted Communications*.

[DOWNLOAD REPORT](#)

Strong Operational Governance, Uneven Evidence Continuity

The clearest pattern in the UK appears when we compare different governance controls. While policies, employee training, and human reviews are common, UK companies also show impressive adoption of technical controls. Prompt and output logging, automated retention, automated risk scoring, and regular audits are already core components of many compliance programmes.

AI Governance Is Moving Into Operational Controls



This trend is crucial. UK organisations are embedding governance directly into daily workflows, going well beyond high-level policy statements.

Company policies define which AI tools employees may use, training ensures sensitive data stays protected, and human review workflows verify risky outputs before send-off. Technical controls add necessary defensibility: logging captures inputs and outputs, retention keeps records accessible, risk scoring flags anomalies, and audits confirm safety rules work in practice over time.

The UK cohort also leads the global average in combining these mechanisms. **Thirty-seven percent have established a complete technical foundation—policy, prompt/output logging, and automated retention—compared to 29% globally.** That is significant progress. Now, compliance leaders must answer a deeper question: as these controls spread across workflows, can we reliably link all generated records if we need to reconstruct an event?

A Closer Look
at the UK

Strong Operational
Governance, Uneven
Evidence Continuity

Governance Has
Moved Into the
Workflow

The Record Breaks
as Communications
Move

Investigations
Expose the Cost of
Fragmentation

Modernization Must
Balance Regulatory
Agility and Assurance

UK Organisations Are
Prioritising Connected
Compliance

The UK Movement:
From Operational
Controls to True
Defensibility

About This Research

Research conducted by



Governance Has Moved Into the Workflow

For many compliance and risk teams, the primary concern is whether different governance layers stay connected. Consider a scenario we see every day: an employee uses an approved AI tool to draft an official message. The prompt and output are logged, a human reviewer edits the draft, an automated tool checks for risks, and the final text is sent via email and archived. Every individual control functioned as designed. But if that communication is challenged six months later:

- Can your teams swiftly retrieve the original AI activity?
- Can you demonstrate exactly what the reviewer saw and approved?
- Can you pinpoint what changed between the initial AI output and the final outbound message?
- Can you seamlessly connect review histories with the final sent record?
- Can you accomplish this without requiring multiple teams to manually reconstruct the sequence from siloed systems?

This is where operational governance becomes an evidence-tracking imperative. The UK regulatory approach makes this urgent: rather than imposing a single overarching AI law, the UK regulates AI based on context and application. Existing standards across data privacy, financial conduct, consumer protection, and sector rules all govern AI activities.

In financial services, for example, the Financial Conduct Authority (FCA) has made clear it will not create standalone AI rules. Instead, firms are expected to apply established governance, risk management, and outcome standards to AI. The FCA's objective is to foster safe, responsible, and accountable AI adoption.

The Information Commissioner's Office is also updating its rules on automated decisions under the Data (Use and Access) Act 2025, with a broader code of practice for AI currently in development.

For Compliance, Risk, and Legal leaders, the core takeaway is clear: **while AI fundamentally changes how work gets done, you remain fully accountable for proving that your oversight and decision-making controls operate effectively in practice.**

The Record Breaks as Communications Move

Compliance officers have long managed communication risks across platforms, but AI adds new layers of operational complexity. An employee might start with an AI prompt, edit the text in an email draft, discuss modifications in Microsoft Teams, resolve details on a video call, and complete the conversation via a mobile messaging app.

Even if the final email is properly archived, the critical decision sequence leading up to it sits fragmented across multiple environments. UK respondents identify personal messaging apps as their primary surveillance blind spot, followed by third-party communications and unrecorded phone calls. Comparing channel usage against surveillance coverage reveals the true scope of exposure.

Off-Channel Use Is Not Always Matched by Surveillance Coverage



Surveillance coverage frequently fails when business conversations move to unmonitored channels. Among the 33 UK respondents reporting employee use of personal messaging apps, nearly three-quarters acknowledge partial or zero monitoring coverage. Among the 41 reporting work-related calls on personal phones, nearly six in ten face the same gap.

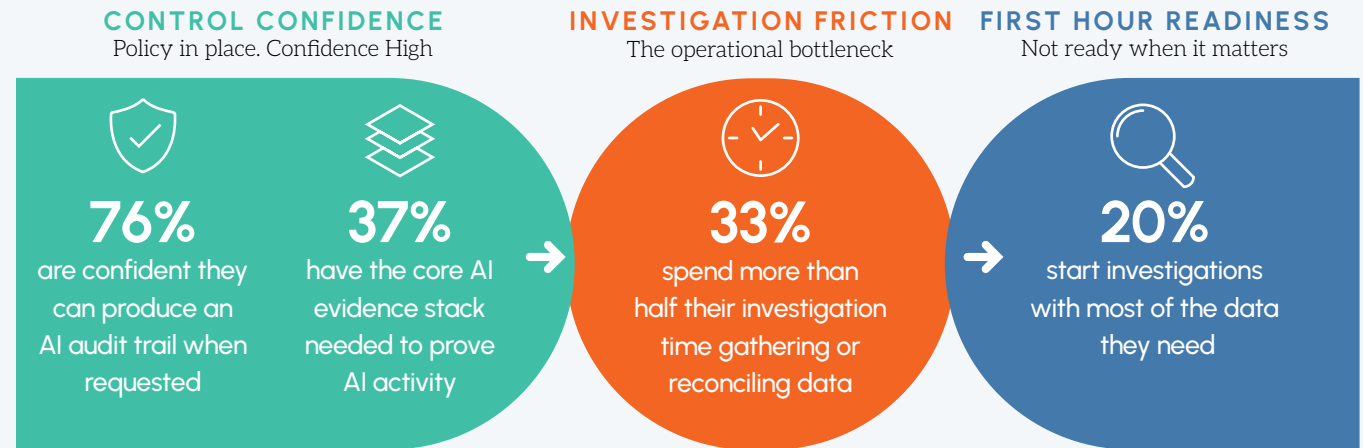
This creates a severe evidence gap for AI governance. An AI draft may originate within a secured corporate environment, but the surrounding contextual discussions easily drift off-channel. Key context gets pasted into chat apps, approvals occur on unrecorded calls, third parties share critical inputs elsewhere, or customer responses shift the conversation off-grid.

Retrieving the final outbound email is helpful, but reconstructing the initial AI prompts, human interventions, informal discussions, and underlying approvals is essential to defend what actually occurred. AI governance confronts a familiar compliance reality: **the audit trail breaks whenever interactions cross disparate applications.** Today, defensibility starts long before a final message is transmitted.

Investigations Expose the Cost of Fragmentation

Most corporate compliance teams can eventually locate scattered records, but the real test is how long it takes to assemble fragmented data into a cohesive, defensible narrative. This is where the UK survey data provides crucial insights into investigation readiness. While UK firms demonstrate robust AI controls and express strong confidence in producing audit trails, formal inquiries reveal significant operational friction in gathering data before meaningful analysis can even begin.

Stronger Controls Have Not Eliminated the Reconstruction Gap



This disconnect is striking: UK companies report higher control adoption rates than global peers, yet their initial investigation posture looks virtually identical. Only 20% can launch an investigation with the majority of required data immediately accessible. Meanwhile, a full third devote over half of their investigation lifecycle to manually collecting and reconciling data. Furthermore, **40% identify cross-platform record correlation as their single greatest bottleneck caused by data fragmentation.**

A Closer Look at the UK

Strong Operational
Governance, Uneven
Evidence Continuity

Governance Has
Moved Into the
Workflow

The Record Breaks
as Communications
Move

Investigations
Expose the Cost of
Fragmentation

Modernization Must
Balance Regulatory
Agility and Assurance

UK Organisations Are
Prioritising Connected
Compliance

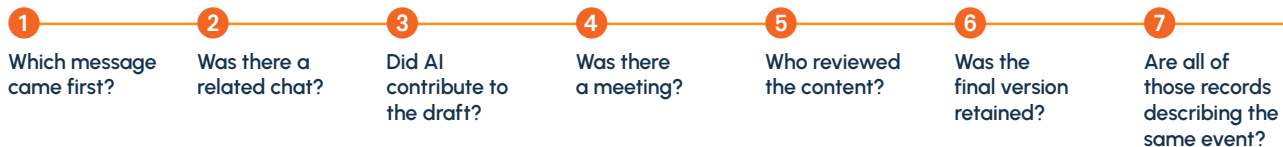
The UK Movement:
From Operational
Controls to True
Defensibility

About This Research

Research conducted by



This challenge stems from disconnected data architecture rather than inadequate policies or missing surveillance tools. When records are siloed across AI platforms, email archives, collaboration tools, monitoring systems, and legal discovery repositories, organisations waste precious hours attempting to reconstruct basic chronologies:



The global benchmark highlighted this disconnect between perceived confidence and true evidence continuity, and the UK findings strongly reinforce it. **Even sophisticated operational controls cannot eliminate the costly labour of rebuilding event timelines when underlying records remain disconnected.** This underscores why connecting compliance data upstream is vital for enterprise defensibility.

Modernisation Must Balance Regulatory Agility and Assurance

Eliminating data silos requires modern infrastructure, and UK compliance leaders are aggressively adapting. Forty-two percent of UK respondents report that their primary compliance platforms are mostly or fully cloud-based (SaaS)—compared to 36% globally—while another 35% operate hybrid environments. The most revealing divergence lies in what UK compliance leaders expect cloud modernisation to accomplish.

What Would Make SaaS More Compelling in the UK

Improved security and resilience

UK:

59%

Faster response to regulatory changes

UK:

50%

Easier integration across systems

UK:

45%

Improved scalability and performance

UK:

39%

Faster deployment of new capabilities

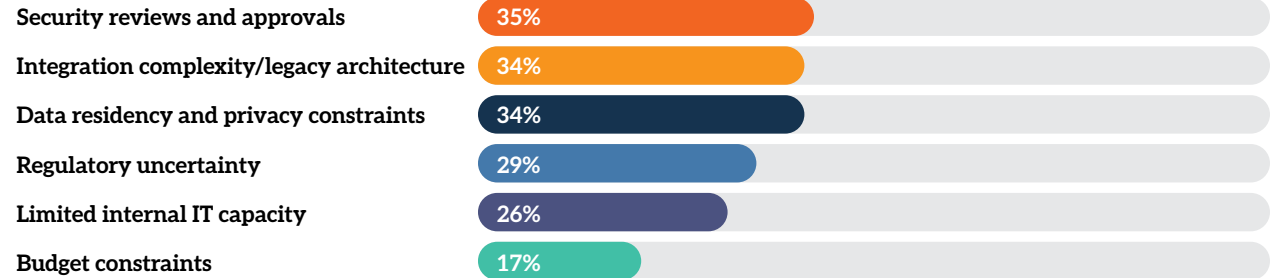
UK:

33%

The standout expectation for teams is regulatory agility. Half of UK respondents identify faster adaptation to regulatory shifts as a compelling reason to adopt cloud architecture—11 percentage points higher than the global baseline. This focus is directly aligned with the UK regulatory climate, where AI requirements evolve within existing oversight mechanisms. For instance, the FCA actively supports responsible innovation through initiatives like AI Live Testing and the Supercharged Sandbox, enabling financial firms to deploy AI tools within controlled environments while maturing their governance and risk controls.

However, compliance modernisation must continually satisfy stringent data governance and security standard mandates.

What Slows Compliance Modernisation in the UK



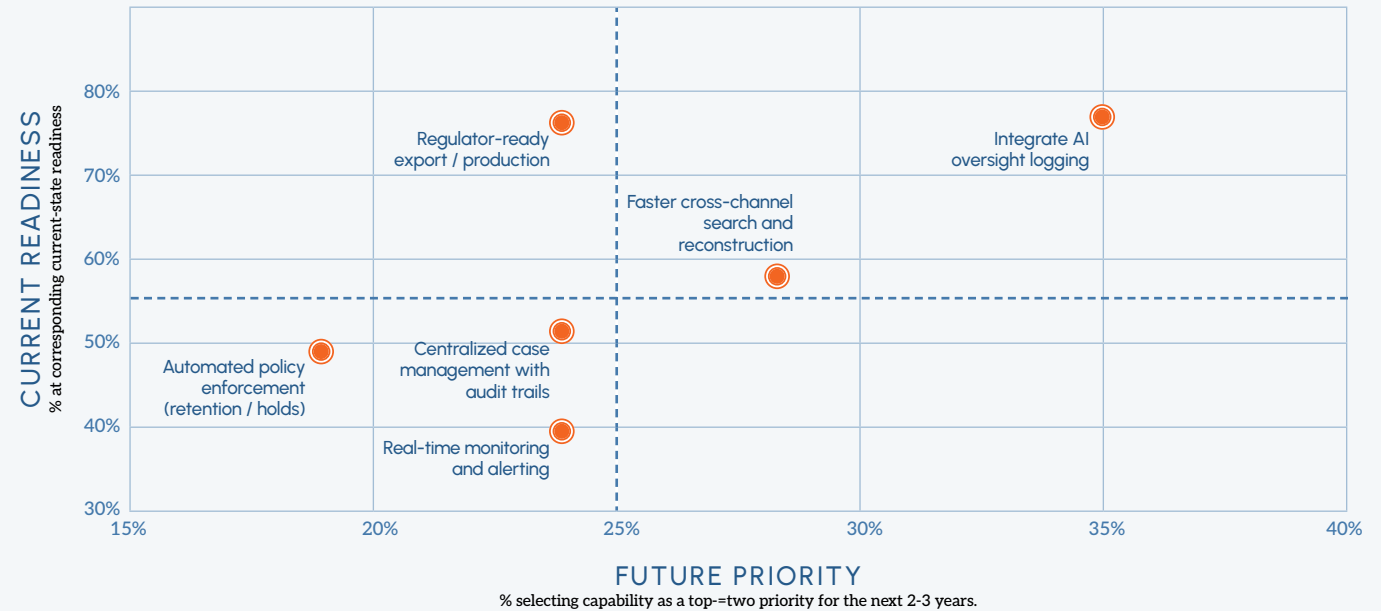
Noticeably, budget constraints rank far below operational, security, and governance considerations. UK risk leaders evaluate compliance technology upgrades by verifying that architectural changes will not compromise security, data privacy, existing platform integrations, or oversight controls, looking far beyond software costs alone.

This sets a demanding standard for compliance platforms. We require systems that dynamically adapt as employee tools, AI applications, and legal expectations evolve, while maintaining the unified connections necessary for automated retention, surveillance, internal investigations, and regulatory disclosures. Modernisation must simplify data correlation without introducing new security or compliance risks.

UK Organisations Are Prioritising Connected Compliance

Looking ahead over the next two to three years, UK compliance leaders are aligning their technology roadmaps to address these modern compliance challenges. Their top focus is integrating AI oversight logging, quickly followed by establishing unified visibility across email, chat, voice, and video channels.

UK Compliance Technology Priorities for the Next 2–3 Years



Cross-channel visibility stands out as a strategic imperative. UK respondents are 9 percentage points more likely than global peers to prioritise unified oversight across email, collaboration chat, voice, and video. Having invested in point governance solutions, compliance leaders are now focused on unifying their surveillance and archiving ecosystem to:

- Systematically capture high-risk AI interactions.
- Maintain continuous visibility as conversations migrate across platforms.
- Correlate data points and audit records across disparate channels.
- Streamline investigation workflows and narrative reconstruction.
- Produce regulator-ready disclosure packages without manual reconstruction.

A Closer Look at the UK

Strong Operational
Governance, Uneven
Evidence Continuity

Governance Has
Moved Into the
Workflow

The Record Breaks
as Communications
Move

Investigations
Expose the Cost of
Fragmentation

Modernization Must
Balance Regulatory
Agility and Assurance

UK Organisations Are
Prioritising Connected
Compliance

The UK Movement:
From Operational
Controls to True
Defensibility

About This Research

Research conducted by



This connects directly back to the broader *State of AI Governance 2026* benchmark framework. The global report positions comprehensive archives as foundational evidence, defining the complete Defensible AI Record—from prompts and context to human reviews, retention schedules, legal holds, and production workflows. The UK data proves that connected evidence models are essential as organisations mature from isolated controls into integrated governance environments.

For Compliance, Risk, and Legal officers, this research provides an essential framework for benchmarking organisational maturity, ensuring that existing operational controls yield complete, end-to-end audit trails.

The UK Movement: From Operational Controls to True Defensibility

The global *State of AI Governance 2026* study identified the Policy-to-Proof gap—the disconnect between defining AI policy and proving compliance—as a defining corporate risk, and the UK data demonstrates how leading firms are addressing this challenge.

UK companies lead in implementing practical oversight controls. Human reviews and staff training are standard, prompt and output logging are widely deployed, regular audits are embedded into operations, and core technical configurations (policy + logging + automated retention) exceed global adoption rates.

The remaining milestone for enterprise risk management is evidence continuity. Conversations continue to shift onto unmonitored channels, data remains fragmented across business systems, linking activity across formats remains complex, and compliance teams still spend critical hours manually stitching together audit trails during inquiries.

Modernisation initiatives are gaining momentum as UK leaders demand greater regulatory agility, data security, system resilience, and cross-channel connectivity. For executive leadership, the strategic mandate is clear: **the next era of AI governance centers on connecting existing control data into a fully defensible, unified record of compliance.**

This requires maintaining visibility into AI usage, capturing high-value interactions, preserving conversational context across platforms, linking human review approvals directly to outbound messages, automating retention policy enforcement, and continuously testing investigation readiness before formal inquiries occur. When an AI-assisted communication is scrutinised, leading organisations can defend the complete operational record with clarity and speed.

Set the policy. Capture the evidence. Govern the record. Read our complete *State of AI Governance 2026: The Policy-to-Proof Gap in AI-Assisted Communications benchmark*.

[DOWNLOAD REPORT](#)

A Closer Look
at the UK

Strong Operational
Governance, Uneven
Evidence Continuity

Governance Has
Moved Into the
Workflow

The Record Breaks
as Communications
Move

Investigations
Expose the Cost of
Fragmentation

Modernization Must
Balance Regulatory
Agility and Assurance

UK Organisations Are
Prioritising Connected
Compliance

The UK Movement:
From Operational
Controls to True
Defensibility

About This Research

Research conducted by

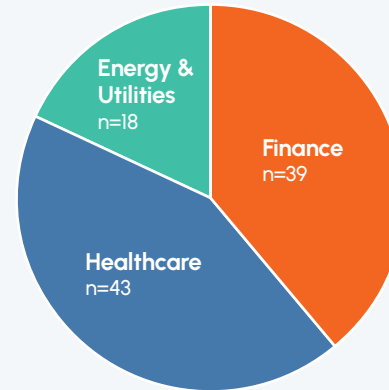


About This Research

This UK Perspective report is drawn from Arctera's *State of AI Governance 2026* benchmark research, independently conducted by Hanover Research.

The UK analysis reflects insights from **100 qualified Compliance, Legal, Risk, Regulatory, and IT decision-makers** participating in the global research.

The UK cohort includes respondents from:



AI-SPECIFIC FINDINGS

82 UK respondents actively using AI in regulated communications or decision-making workflows

EUROPEAN MARKET EXPOSURE

100 Respondents report their organisations serve European markets

All UK respondents confirmed their organisations serve European markets. This indicates business presence rather than specific legal applicability, which depends on individual operations.

These findings provide valuable directional insights for our UK compliance cohort rather than absolute statistics for all UK enterprises. Sample sizes vary across survey modules, subgroup data should be evaluated accordingly, and reported figures are subject to standard rounding.

Our comprehensive global report delivers the full research methodology, six-signal governance framework, proof-readiness evaluation matrix, and complete Defensible AI Record model.

Read the full *State of AI Governance 2026* benchmark:

[DOWNLOAD REPORT](#)



About Arctera

Arctera, a business unit of Cloud Software Group, is a leading global provider of compliance and governance solutions that enable firms to unleash game-changing technologies into their organisations while minimizing risk. Created in 2024 from Veritas Technologies, Arctera helps the biggest companies in the world monitor and control exactly how their information is being accessed, used and shared. The Arctera™ Unified Platform is able to capture data from over 130+ different content sources, and more than 280 AI policies help firms streamline compliance and adapt to evolving regulations.

Copyright © 2026 Arctera. All rights reserved. Arctera and the Arctera Logo are trademarks or registered trademarks of Arctera or its affiliates in the U.S. Other names may be trademarks of their respective owners.



Learn more at arctera.com

Connect with us on [LinkedIn](#)

Contact: press@arctera.com