



State of AI Governance

2026 - THE AUSTRALIA
PERSPECTIVE

Where Strong Governance Meets
the Evidence Challenge

Research conducted by



A Closer Look
at Australia

Strong Governance,
Uneven Evidence
Readiness

Policy is Ahead
of Proof

Evidence Breaks
as Communications
Move

Investigations
Expose the Cost of
Fragmentation

Modernization Must
Balance Integration
and Governance
Assurance

Australian
Organisations
Are Prioritising
Connected Evidence

Australia Is Moving
From Governance
to Defensibility

Research conducted by



A Closer Look at Australia

When Arctera published the *State of AI Governance 2026: The Policy-to-Proof Gap in AI-Assisted Communications*, the global report showed a major change in how companies approach AI compliance and governance.

Organizations are moving well past basic questions about setting AI policies. Instead, compliance and risk leaders are confronting a much tougher operational reality: **can your team truly prove what transpired when employees used AI to draft official communications, executive decisions, or regulatory records?**

Our global benchmark reveals that while governance teams have made strong headway in writing guidelines, many are still scrambling to deploy the technical tooling required to capture, archive, and reconstruct AI-assisted workflows when auditors ask for proof.

When we examined the responses from Australian compliance professionals, a distinct and compelling story emerged.

Australian organisations have built an impressive foundation on human-centred governance—establishing clear policies, staff training, and executive oversight. Now, local compliance leaders are tackling their next crucial hurdle: embedding automated technical controls to capture verifiable evidence directly within everyday tools. They are actively upgrading cross-channel monitoring, streamlining internal investigations, and modernising compliance infrastructure without compromising strict privacy and data security mandates.

This offers an invaluable strategic roadmap for leadership: **Australia is leading the charge in converting corporate policy into rock-solid, audit-ready proof.** In this report, we dive into feedback from 50 Australian compliance and risk leaders to unpack how local practices compare against global benchmarks.

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

[DOWNLOAD REPORT](#)

Strong Governance, Uneven Evidence Readiness

The clearest trend in Australia shows up when you compare company policies directly with technical compliance safeguards.

While rules, training, and human reviews are widespread, organisations are still ramping up automated controls like risk classification, content filtering, and audit archiving.

Overview of Governance Controls and Technical Evidence Implementation

Formal AI usage policy



Human review / approval for high-risk AI communications



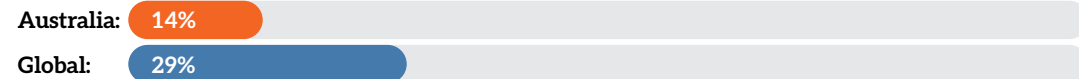
Employee training on compliant AI use



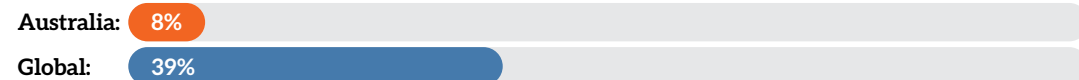
Formal AI usage policy



Human review / approval for high-risk AI communications



Employee training on compliant AI use



A Closer Look at Australia

Strong Governance, Uneven Evidence Readiness

Policy is Ahead of Proof

Evidence Breaks as Communications Move

Investigations Expose the Cost of Fragmentation

Modernization Must Balance Integration and Governance Assurance

Australian Organisations Are Prioritising Connected Evidence

Australia Is Moving From Governance to Defensibility

This contrast is telling. Australian organisations show strong intent to govern AI through active manager oversight and clear guidelines. The real operational test is what happens **after** those rules are established.

A written policy establishes compliant AI boundaries. Compliance training keeps confidential corporate data protected. A manager's review ensures an AI draft meets statutory and regulatory standards before release.

However, if a business decision is questioned months later, the company needs more than proof that a policy existed. It must show what the AI created, what the reviewer edited, which final version was approved, and where the record was stored. That is where Australia organisations differ globally.

Research conducted by



Policy is Ahead of Proof

For many compliance leaders, the first phase of AI governance felt familiar: set acceptable use rules, clarify who is responsible, train staff, and review high-risk work. Australian data reveals an initial emphasis on setting policies and manual checks. Now, the priority is verifying that employees follow these procedures in daily workflows.

Consider a common scenario.

An employee uses an approved AI assistant to help prepare a regulated communication. A human reviews the draft. The wording changes. The final version moves into email and is retained.

On the surface, the process worked. But if that message is questioned six months later, can the company find the original AI draft? Can it show who reviewed it, separate the AI text from what was sent, and connect those steps without making teams search manually? This shows why written rules must connect directly with verifiable records.

The Australian regulatory conversation is moving in a similar direction.

The Australian Securities & Investments Commission (ASIC), Australia's financial regulator, warned financial services companies that their governance systems must keep up with AI adoption. They stressed that companies should not wait for new AI laws before fixing known risks.

The Australian Prudential Regulation Authority (APRA), the banking regulator, called for heightened corporate governance surrounding AI risk management in 2026. They noted that institutional oversight and regulatory assurance mechanisms were lagging behind rapid workplace deployment.

For legal and compliance teams, the takeaway is simple. It is not enough to set AI rules; **companies must be able to prove how those rules worked when tested.**

Evidence Breaks as Communications Move

Compliance leaders have dealt with a common problem for years: work conversations rarely stay in one place. An employee might start with an AI draft, move it into an email, discuss it on Microsoft Teams, jump on a video call, and finish the chat with a client on a mobile messaging app. A single business task can create records across five different apps, and Australian companies report major blind spots when tracking content across these handoffs.

Where Australian Respondents See Greater Communication Blind Spots

Consumer messaging apps on personal devices



Third-party / vendor communications



Video meetings with external participants



These gaps reveal how dynamic workflows actually operate: external vendors collaborate on key initiatives, clients demand mobile accessibility, third parties join executive calls, and AI content moves across boundaries effortlessly. Maintaining regulatory compliance demands both comprehensive oversight and unified monitoring across software platforms.

Australian respondents were also more likely to say that fragmented systems make it hard to link messages across mediums. Over half noted the difficulty of connecting records across email, chat, voice, and video.

In an investigation, this connection is vital. Finding one email is helpful, but showing that the email came after an AI draft, an internal chat, a video meeting, and a mobile message builds a complete picture. AI governance runs into a familiar issue: **the evidence trail often breaks when workers switch apps**. The main difference today is that the trail starts before the message is even written.

Investigations Expose the Cost of Fragmentation

Most organizations can eventually locate files, but the goal is to find stored records quickly and turn them into clear evidence during investigations. Australian teams report greater trouble piecing together messages across channels, spending significant time gathering data before they can even begin analysing it.

The Cost of Reconstructing the Record

Cross-channel reconstruction confidence



Spend more than half of investigation time gathering and reconciling data

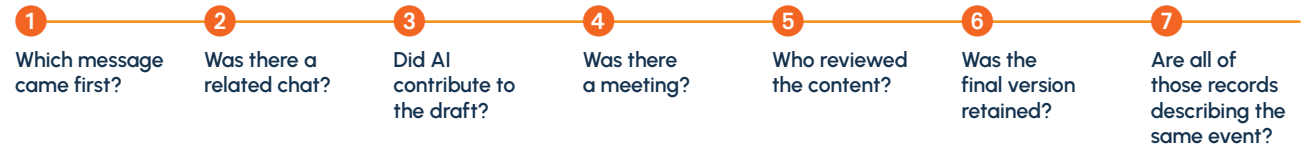


Respond to a multi-system regulatory inquiry within 48 hours



Understanding the specific stages of the investigation process where time is allocated helps identify opportunities for operational efficiency.

When records are spread across disconnected systems, the first task is often not assessing the conduct or understanding the risk. It is rebuilding the chronology.



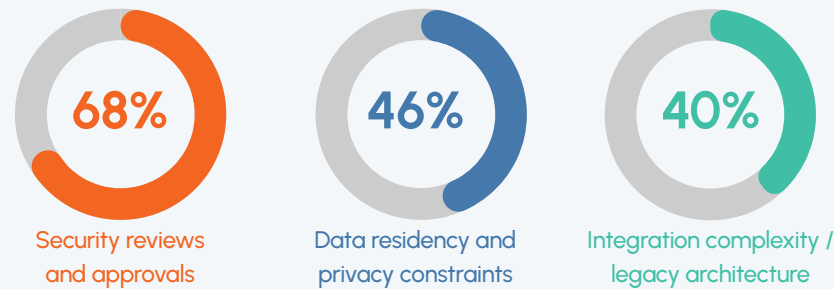
Piecing together events from multiple separate sources takes valuable time away from legal and compliance teams.

The global benchmark measured overall investigation readiness. **The Australian data proves that readiness depends heavily on how well teams can connect records across different software platforms.** That is why linking records matters long before an investigation starts.

Modernization Must Balance Integration and Governance Assurance

Upgrading technology offers a seamless way to integrate governance systems, but Australian data shows why compliance leaders move deliberately. The main priorities are not just about platform features; they are about guaranteeing that new tools meet strict statutory frameworks for regulated data.

What Slows Compliance Modernisation in Australia



These concerns are reasonable. Compliance tools hold sensitive messages, internal investigation notes, employee files, customer data, and legal records. Moving or connecting these records brings up important questions beyond basic software features:

- Where will the data reside?
- Who can access it?
- How does a new platform connect to existing archives and business systems?
- What happens if a service provider fails?
- Can the company maintain strong safeguards while updating its software architecture?

Those considerations are increasingly part of the Australian regulatory environment as well.

Australian privacy regulators are highlighting these exact points. Guidance from the Privacy Commissioner stresses security reviews, risk management, transparency, and human oversight for AI tools. New privacy laws taking effect on **10 December 2026** will require companies to clearly explain how automated systems make decisions about individuals.

For leaders planning the next stage of compliance technology, the benchmark suggests a more nuanced question than whether to modernize.

Organisations are focusing on connecting their evidence trails while keeping security, privacy, and governance standards strong.

Australian Organisations Are Prioritising Connected Evidence

The top goals selected by respondents for the next two to three years bring the picture into focus.

Their main priorities include **connected AI activity logs, faster search across multiple channels, and a unified view across email, chat, voice, and video.**

These choices show that companies do not just want more rules—they want to make existing rules easier to manage and prove. Since Australian businesses have already invested in human oversight (policies, training, and reviews), their next investments focus on technical infrastructure:

**Capture the AI activity
that matters.**

**Keep the evidence
connected as
work moves.**

**Make the record easier
to reconstruct when
questions arise.**

For risk and compliance leaders evaluating their own programmes, this provides a clear standard for readiness.

The goal for companies is the ability to track high-risk AI tasks from start to finish and produce clear proof without relying on manual exports, screenshots, or memory.

A Closer Look
at Australia

Strong Governance,
Uneven Evidence
Readiness

Policy is Ahead
of Proof

Evidence Breaks
as Communications
Move

Investigations
Expose the Cost of
Fragmentation

Modernization Must
Balance Integration
and Governance
Assurance

Australian
Organisations
Are Prioritising
Connected Evidence

Australia Is Moving
From Governance
to Defensibility

Research conducted by



Australia Is Moving From Governance to Defensibility

The global benchmark highlighted the gap between setting AI policies and proving compliance. Australian survey data shows how local businesses are navigating this shift. Surveyed organisations are strong in human governance—policies, training, reviews, and accountability.

However, challenges appear when gathering proof: automated technical controls are less common, messages move into hard-to-monitor channels, separate systems make tracking difficult, and technology updates must navigate strict privacy and security rules.

For Australian business leaders, this provides a clear takeaway. Improving AI governance means backing up policies with reliable technical proof. When AI-assisted work is questioned, the strongest organisations will be able to show what happened instantly—connecting company policies directly with clear, complete records.

About This Research

This Australia Perspective is derived from Arctera's *State of AI Governance 2026: The Policy-to-Proof Gap in AI-Assisted Communications*, an independent quantitative benchmark conducted by Hanover Research.

The Australia analysis includes responses from 50 compliance, legal, risk, and IT decision-makers within the global study. Results serve as directional indicators for the surveyed group rather than exact measurements of all Australian businesses.

The global report provides the complete research methodology, six-signal governance framework, proof-readiness analysis, and 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 organizations 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