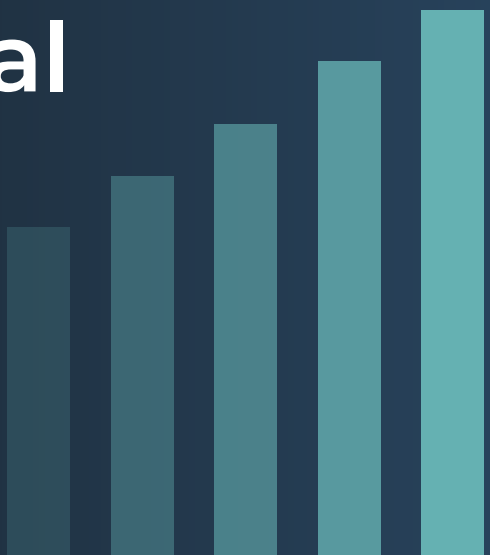
DigiRen

Challenges to Scaling Technology Governance in the Australian Financial Services Industry



Australian Financial Services Institutions (FSIs) are operating in a moment of significant regulatory and technological convergence. Over the past five years, compliance regulations specific to the use of hyperscale Cloud, Data, and Artificial Intelligence (AI) have rapidly matured, with standards and expectations emerging from APRA, the ACCC, OAIC, and international counterparts. These mandates reflect growing concern about systemic risk, operational resilience, and ethical use of advanced technologies.

> Overly burdensome, ambiguous, or premature regulations throttle experimentation, deter investment, and put Australian businesses at a disadvantage."
>
> *Bran Black, CEO of the Business Council of Australia - BCA* [1]

At the same time, FSIs are accelerating their adoption of hyperscale platforms, expanding from isolated migrations to enterprise-wide transformation efforts. According to recent Gartner studies, over 80% of financial firms have active multi-cloud strategies[2], and nearly 70% are piloting or scaling AI use cases[3]. Hyperscale services are now foundational to core banking, fraud analytics, and digital engagement.

This transformation has introduced a new category of compliance risk. As adoption scales, so too does the burden of ensuring secure, compliant, and consistent operation across increasingly complex delivery ecosystems. This paper explores three critical execution challenges FSIs must address to scale governance effectively:

- Aligning governance across disparate operating models
- Ensuring controls are implemented in practice
- Managing the volume of compliance data generated by modern techniques

Before addressing these areas, it is worth acknowledging three common failure points in governance implementation:

- A one-size-fits-all control model that fails across diverse use cases
- Static compliance blueprints that quickly become outdated
- Real-time attestation systems that overwhelm teams with undifferentiated compliance data

Aligning Governance Across Disparate Operating Models

Governance often falters when multiple operating models coexist without integration. FSIs today typically manage separate structures for Cloud, Data, and AI, each with unique vocabularies, workflows, and tooling. When governance frameworks fail to bridge these domains, policy fragmentation and inconsistent control adoption result.

A more sustainable approach begins with applying a common governance framework across technology domains. Secure-by-design, policy-as-code, and real-time attestation should apply universally—even if specific implementations differ. Moreover, governance must be embedded in Agile and Product delivery methods to ensure compliance is part of sprint planning and "definition of done."

Governance mechanisms must also be designed for ease of use. Controls that disrupt workflows or require excessive context-switching will be bypassed. Usability, automation, and transparency are essential for adoption.
Finally, alignment between funding flows and compliance accountabilities is critical. Cost and compliance are deeply linked, and teams tasked with enforcing controls must have access to the resources needed to do so.

Reflection Points:

- Are **Cloud**, **Data**, and **AI** teams operating under a unified control framework?
- Is compliance embedded in Agile delivery practices?
- Are controls optimised for user experience?
- Are funding and accountability aligned for compliance outcomes?

Ensuring Controls Are Implemented in Practice

Defining a control is not the same as implementing it. Real governance effectiveness depends on embedding controls into everyday delivery. Three critical enablers make this possible:

1 **Standardised Metadata:** Governance begins with consistent metadata across Cloud, Data, and AI resources. Without it, policy enforcement and reporting become fractured. Enforcing metadata at provisioning time enables risk classification, automated tagging, and workload-specific control application.

2 **Federated Compliance Blueprints:** Blueprint libraries accelerate compliant delivery but often become bottlenecks when centralised. A federated model—where platform teams define standards and delivery teams manage application—encourages agility while retaining control. Blueprints must be versioned, self-service, and extensible.

3 **Shift to Build-Time Controls:** Preventative controls applied during build-time are far more effective than reactive runtime detection. By embedding policy checks into CI/CD pipelines and infrastructure as code, non-compliant configurations are stopped before deployment. This "shift-left" approach is increasingly supported by major platform vendors.

Reflection Points:

- Do all domains use **consistent** metadata for classification and policy?
- Are compliance blueprints **maintained** collaboratively across teams?
- Are most controls **implemented** at build-time or post-deployment?

Managing Compliance Data Overload

As real-time control monitoring becomes the norm, FSIs are generating vast volumes of compliance data. According to HBR, 68 % of risk & compliance leaders cite 'too much data to digest' as a top barrier to continuous monitoring[4]. To manage this, three areas require focused investment:

1. **Apply Risk Context to Data:** Not all control failures carry equal risk. Findings must be contextualised by asset criticality, business function, and regulatory relevance. Risk-based prioritisation helps reduce alert fatigue and enables actionable oversight.

2. **Operational Readiness to Respond:** Teams receiving compliance alerts must be trained, resourced, and authorised to act. Many organisations detect issues effectively but lack pathways for timely resolution. Governance effectiveness depends on operational preparedness, not just tooling.

3. **Adopt AI for Compliance Remediation:** As data volumes grow, AI will be critical to summarise findings, suggest remediations, and eventually automate fixes. AI copilots are already emerging to translate policy failures into recommended code changes or configuration updates.

Reflection Points:

- Is compliance data **risk-ranked** and prioritised before it reaches users?
- Are teams **trained** and equipped to resolve findings quickly?
- Are **AI-assisted** compliance tools being piloted or deployed?

Conclusion: Scaling Governance for Strategic Advantage

Scaling governance is not just about regulatory compliance—it is foundational to enabling safe innovation at speed. In a federated, fast-moving FSI environment, execution matters more than policy design.

The most effective way to address this challenge is to assess current capabilities and develop an internal maturity model. A maturity model helps identify gaps, prioritise investments, and benchmark progress over time. Our team works with FSI clients to develop practical, risk-aligned maturity frameworks that support both compliance and transformation goals.

If these challenges resonate with your current state, we'd welcome a conversation on how to tailor a maturity model that supports your environment.

Let's make governance a capability — not just a compliance function.

Endnotes:

[1] Bran Black, CEO of the Business Council of Australia (BCA), "AI regulation must avoid 'strangling' innovation, says report," Accounting Times, June 3, 2025

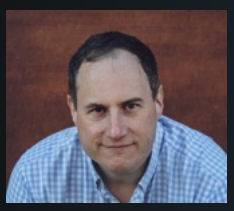
[2] 2024 Gartner CIO & Technology Executive Survey – Banking & Investment Services

[3] The Opportunity and Impact of Generative AI on Financial Services (Gartner Webinar)

[4] "Digitizing Risk and Compliance: How AI Can Help Manage a Growing Challenge" – HBR Analytic Services white-paper sponsored by PwC (Apr 2024)

Contact us with any questions or to start your journey toward scaling governance.

Author:



George Watts
Founder & Director
Digital Renewal Pty Ltd
george@digiren.com.au

Contributors:

Mark Ollerenshaw
General Manager
Digital Renewal Pty Ltd
mark.ollerenshaw@digiren.com.au

Anthony Hadfield
Consulting Director
Digital Renewal Pty Ltd
anthony.hadfield@digiren.com.au

Jessey Panesar
Consulting Director
Digital Renewal Pty Ltd
jessey.panesar@digiren.com.au

Simon Rolls
Senior Principal Consultant
Digital Renewal Pty Ltd
simon.rolls@digiren.com.au

DigiRen

DigiRen refers to Digital Renewal Pty Ltd, a 100% privately owned Australian company. Please see www.digiren.com.au to learn more about how we help organisations maximise value from their technology investments.