INNOVO NETWORKS · FREE SELF-ASSESSMENT

The GovernAI
Risk Snapshot Checklist

A 10-minute self-check for South African financial services firms — advisory practices, insurers, administrators, payments companies, fintechs and banks.

Why this matters: South Africa's first administrative POPIA fine was R5 million, issued in 2023, with fines of up to R10 million possible. Joint Standard 2 of 2024 has been in force since 1 June 2025 — documented risk management, continuous monitoring and incident response are now expected, not optional. Regulators internationally are moving toward explicit AI risk requirements next. Most firms have never formally checked where they stand.

How to use this: Tick every box that reflects your firm today. Each unticked box is a potential exposure point. Score yourself at the end.

1 AI USAGE VISIBILITY

☐ We know which AI tools (ChatGPT, Copilot, Gemini, etc.) our staff currently use for work. *— unknown usage = ungoverned risk*

☐ Someone has audited what client or company data has been entered into an AI tool in the last 6 months. *— most firms have never checked*

2 POLICY & OWNERSHIP

☐ We have a written, staff-acknowledged AI acceptable-use policy. *— verbal guidance isn't a policy*

☐ A named individual — not just “IT generally” — is accountable for AI governance at our firm. *— no owner = no accountability*

3 DATA & COMPLIANCE

☐ We are confident our current AI tool usage is fully POPIA-compliant. *— confidence without an audit is a guess*

☐ If a regulator asked to see our AI governance framework tomorrow, we could produce one. *— required under emerging AI risk expectations*

4 MONITORING & TECHNICAL CONTROLS

☐ We have technical monitoring in place for AI-related risks (data leakage, prompt injection, model drift). *— policy without monitoring is unenforced*

☐ AI tool usage is covered under our existing cyber incident response plan. *— often overlooked entirely*

5 VENDOR & OPERATIONAL ACCOUNTABILITY

☐ If our connectivity, phones and cyber security sit with different providers, we could say clearly who owns the fix when something breaks. *— fragmented vendors = slower resolution*

☐ We have a single, coherent view of our firm's cyber risk posture, not one fragmented across multiple suppliers' reporting. *— inconsistent reporting hides real exposure*

☐ We have reviewed our risk management practices against Joint Standard 2 of 2024 (documented risk management, continuous monitoring, incident response). *— in force since 1 June 2025*

☐ Our audit committee or board could read our ICT/AI governance spend and structure from one invoice, not contracts scattered across suppliers. *— unexplainable spend is a governance red flag*

SCORE YOURSELF

10-12 boxes ticked: Strong position. Worth validating with a full GovernAI Risk Snapshot to confirm and

document it formally.

6-9 boxes ticked: Partial governance. Meaningful gaps remain — exactly the kind that surface during an audit or regulatory review.

Below 6 boxes ticked: Significant exposure. Given where regulation is heading, this is worth prioritising now rather than after an incident.

Want the full version of this assessment — done with you, not by you?

As part of the Founding 100 offer, every FinanceIQ + GovernAI tier includes a complimentary GovernAI Risk Snapshot — a full assessment of your actual AI footprint and data flows, done by our team. Book a free 15-minute scoping call, no pitch deck.

Phone: 021 811 3333 · Email: [Your Email Address] · Web: innovonet.co.za