PhakamoTech

enabling & securing Africa's digital transformation

AI Cybersecurity & Governance Assessment

Know exactly where AI creates risk in your environment — and exactly what to do about it.

Copilots, custom agents and machine-learning workloads are already inside your environment — often adopted faster than your controls have adapted. Boards, regulators and auditors now expect evidence-backed answers: What AI is running? Who can reach it? What data does it touch? Are we ready for POPIA scrutiny and the EU AI Act? This fixed-scope, fixed-price assessment delivers those answers in weeks, not quarters.

What we assess

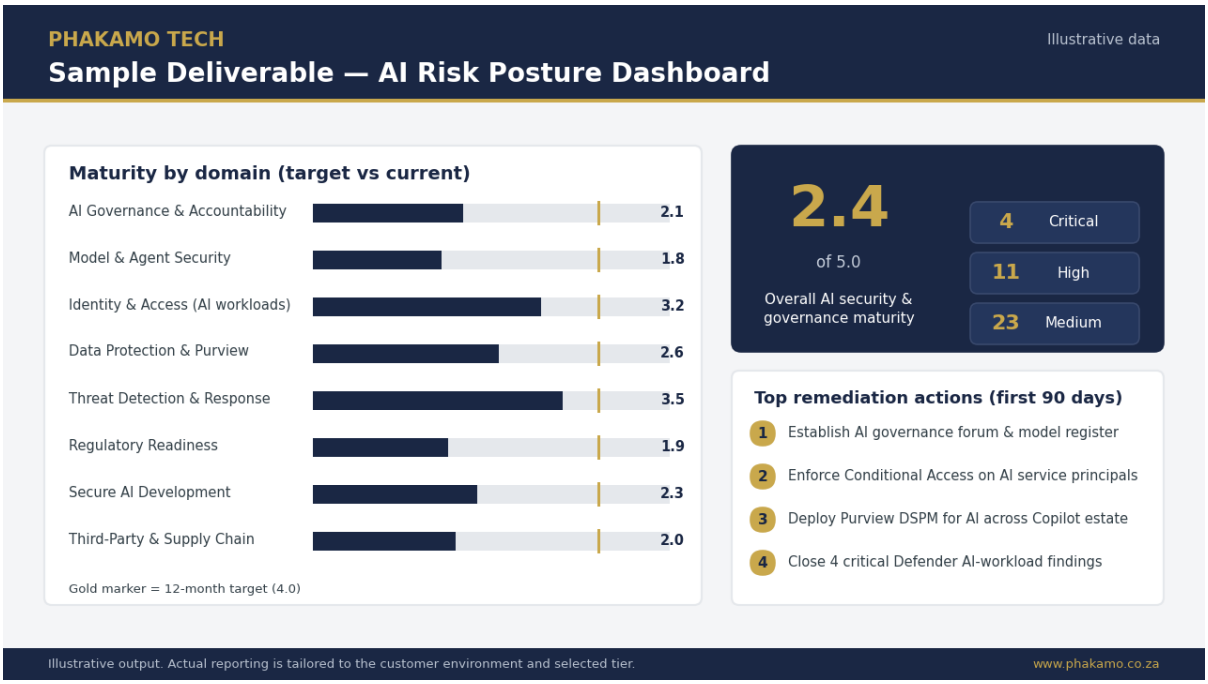
More than 120 controls across eight domains, evaluated read-only against your Microsoft estate — Entra ID, Defender, Purview, Azure and Microsoft 365 including Copilot and Azure AI workloads:

1. AI governance & accountability	5. Threat detection & response
2. Model & agent security	6. Regulatory readiness (POPIA · EU AI Act)
3. Identity & access for AI workloads	7. Secure AI development
4. Data protection & information governance	8. Third-party & supply-chain risk

Every finding is evidence-backed and mapped to NIST AI RMF, ISO/IEC 42001, CIS Controls and the Microsoft Cloud Security Benchmark.

What you receive

- A quantified maturity score across all eight domains, with a risk-ranked findings register.
- A regulatory readiness map giving your board and auditors a defensible position.
- A prioritised 90-day and 12-month remediation roadmap your team can execute.
- An executive report and briefing designed for board and audit-committee consumption.



Sample deliverable — AI risk posture dashboard (illustrative).

How it works

A four-phase, evidence-led methodology: Discover (scope, inventory, read-only onboarding), Assess (control evaluation and evidence capture), Analyse (maturity scoring, gap analysis, regulatory mapping) and Roadmap (prioritised plan, governance operating model, executive reporting). Access is read-only, least-privilege and time-boxed; nothing in your environment is changed without written approval, and all evidence is processed within the Azure South Africa North region.

Choose your tier

Tier	Duration	Best for
Essential	2 weeks	Single tenant needing a rapid, defensible baseline — 40 priority controls, executive briefing, 90-day quick-win plan.
Advanced	4 weeks	Organisations with production AI or active regulatory scrutiny — full 120+ control assessment, readiness map, 12-month roadmap. Our most selected tier.
Sovereign Enterprise	6–8 weeks	Multi-entity estates — governance operating model design, threat-led validation, board and regulator-ready pack, quarterly re-assessment option.

All tiers are fixed-scope and fixed-price. Find the assessment on Azure Marketplace and select Contact Me — we respond within one business day and offer a no-commitment scoping call within three, ending with a fixed written proposal.

Why Phakamo Tech

- A South African security engineering firm serving national departments, state-owned entities, municipalities and regulated enterprises.
- Deep engineering practice on Microsoft Entra, Defender, Purview and Azure AI foundations.
- Sovereign data handling by design — your evidence never leaves your jurisdiction.
- Level 1 B-BBEE contributor; public-sector references available on request.

Get started

Find the AI Cybersecurity & Governance Assessment on Azure Marketplace and select Contact Me, or reach us directly — we will recommend the right tier for your estate on a free scoping call.

Phakamo Holdings (Pty) Ltd trading as Phakamo Tech · Reg. 2010/009142/07

162 Tonetti Street, Growthpoint Business Park, Halfway House, 1685, South Africa · www.phakamo.co.za · support@phakamo.co.za

Contact: Lucas Ledwaba, Chief Executive Officer