PHAKAMO TECH

AI Cybersecurity & Governance Assessment

Service Overview

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

PT-AZMP-AICGA-BROC-2026-001

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

PHAKAMO TECH

AI Cybersecurity & Governance Assessment

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

8	120+	2–8
assessment domains	controls evaluated	weeks to board-ready clarity

NIST AI RMF · ISO/IEC 42001 · POPIA · EU AI Act readiness · Microsoft Cloud Security Benchmark · Zero Trust

Built for regulated and public-sector environments

Delivered by a South African security engineering team on Microsoft Entra, Defender, Purview and Azure AI foundations — with sovereign data-handling by design: your evidence never leaves your jurisdiction.

PHAKAMO TECH

Four-Phase Assessment Methodology

Evidence-led · Framework-mapped · Board-ready

01 DISCOVER
Week 1

- Stakeholder & scope workshops
- AI and data estate inventory
- Read-only telemetry onboarding
- Threat & regulatory context

02 ASSESS
Weeks 2–3

- 120+ control evaluation
- AI model & agent risk review
- Identity, data & workload posture
- Evidence capture & validation

03 ANALYSE
Weeks 3–4

- Maturity scoring (8 domains)
- Gap & root-cause analysis
- Regulatory readiness mapping
- Risk quantification & ranking

04 ROADMAP
Weeks 4–5

- Prioritised remediation plan
- Governance operating model
- Executive & board reporting
- Handover & next-step options

Every finding is traceable to evidence, mapped to a control framework, and paired with a remediation action.

PHAKAMO TECH

Sample Deliverable — AI Risk Posture Dashboard

Illustrative data

Maturity by domain (target vs current)

Gold marker = 12-month target (4.0)

2.4

of 5.0

Overall AI security & governance maturity

4	Critical
11	High
23	Medium

Top remediation actions (first 90 days)

1. Establish AI governance forum & model register
2. Enforce Conditional Access on AI service principals
3. Deploy Purview DSPM for AI across Copilot estate
4. Close 4 critical Defender AI-workload findings

PHAKAMO TECH

Choose the Depth That Matches Your Estate

Three fixed-scope tiers

MOST SELECTED

ESSENTIAL

2 weeks · fixed scope

- Single Microsoft tenant
- AI & Copilot exposure snapshot
- 40-control rapid evaluation
- Executive findings briefing
- 90-day quick-win plan

ADVANCED

4 weeks · fixed scope

- Full 120+ control assessment
- AI model & agent inventory
- POPIA / EU AI Act readiness map
- Technical + executive reports
- 12-month remediation roadmap

SOVEREIGN ENTERPRISE

6–8 weeks · fixed scope

- Multi-tenant / multi-entity scope
- Governance operating model design
- Board pack & regulator-ready pack
- Threat-led validation workshops
- Quarterly re-assessment option

All tiers are fixed-scope and fixed-price, delivered remotely or on-site within South Africa.

www.phakamo.co.za

PHAKAMO TECH

PT-AZMP-AICGA-ARCH-2026-001

AI Cybersecurity & Governance Assessment — Reference Architecture

CUSTOMER ESTATE

Microsoft Entra ID
Identities, apps, service principals

Azure & M365 Workloads
Subscriptions, Copilot, data services

AI Workloads
Azure OpenAI, ML, custom agents

Data Estate
Purview-governed data sources

Read-only telemetry →

PHAKAMO ASSESSMENT FABRIC (AZURE)

Secure Collection Layer
Entra app registration · read-only Graph, ARM and Defender APIs · customer-consented scopes

Analysis & Scoring Engine
Control mapping to NIST AI RMF, ISO/IEC 42001, CIS, MCSB · AI-assisted evidence analysis

Governance Workbench
POPIA / EU AI Act readiness · model inventory · risk register · maturity scoring

Reporting Layer
Executive report · technical findings · remediation roadmap · board pack

Findings & artefacts →

CUSTOMER OUTCOMES

AI Risk Posture Report
Quantified maturity across 8 domains

Regulatory Readiness Map
POPIA · EU AI Act · sector mandates

Prioritised Roadmap
90-day / 12-month remediation plan

Governance Operating Model
Policies, RACI and board reporting