

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

AI Cybersecurity & Governance Assessment

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

8

assessment domains

120+

controls evaluated

2-8

weeks to board-ready clarity

NIST AI RMF

ISO/IEC 42001

POPIA

EU AI Act readiness

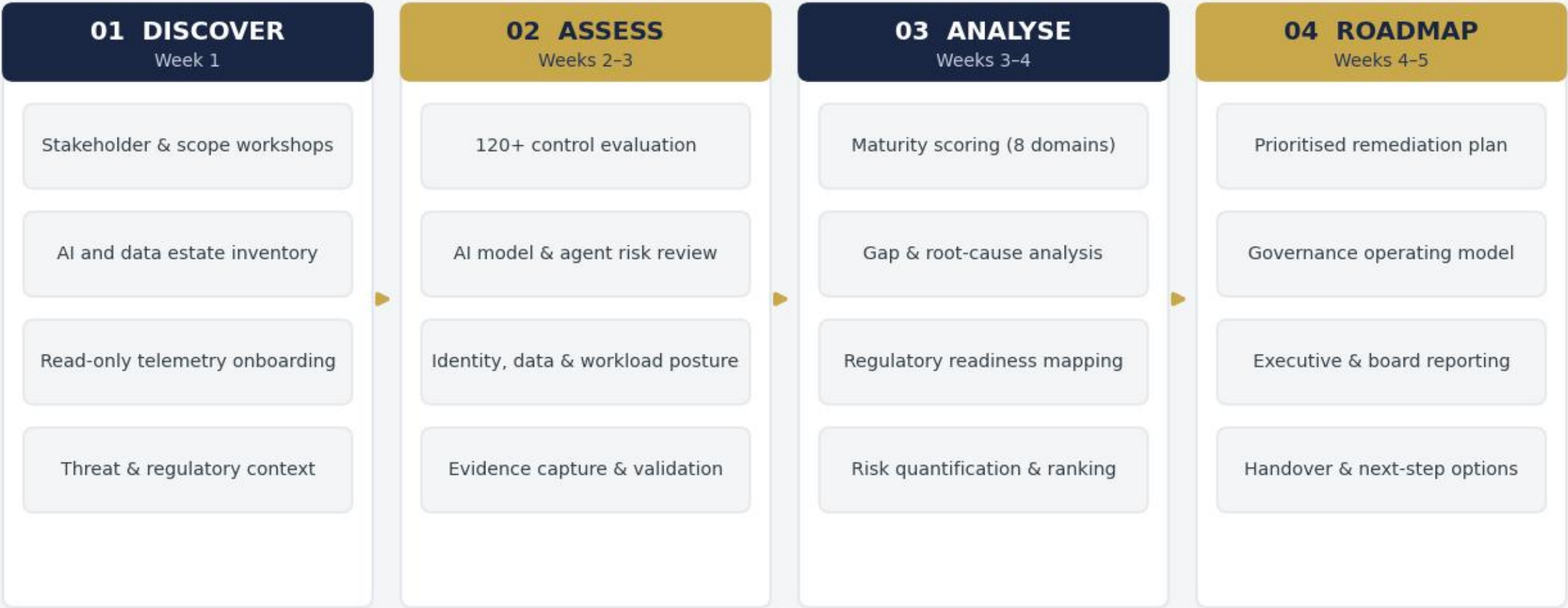
Microsoft Cloud Security Benchmark

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.

Four-Phase Assessment Methodology



Sample Deliverable — AI Risk Posture Dashboard

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

Choose the Depth That Matches Your Estate

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

AI Cybersecurity & Governance Assessment — Reference Architecture

