

Deploying AI without governance isn't agility. **It's uncontained enterprise risk.**

An auditable 25-point framework to assess model risk, prevent bias, and ensure POPIA & NDPA compliance.



Model Inventory & Risk Classification

Catalog all active machine learning models, third-party APIs, and shadow AI usage across business units with multi-tier risk categorisation.



Data Sovereignty & Lineage

Ensure customer prompt data and RAG embeddings comply with national data residency, PII anonymization, and cross-border statutory rules.



Algorithmic Bias & Drift Control

Implement continuous statistical baselines, fairness audits, and automated explainability (SHAP/LIME) to satisfy supervisory audits.

The future of enterprise AI isn't unmonitored adoption — **It's Auditable, Responsible AI.**

[REQUEST REVIEW](#)yips.org.za • info@yips.org.za • +27 76 099 5773

The 5 Governance Control Pillars **every African Risk Officer must verify.**

Evaluating enterprise AI readiness across technical, legal, and operational dimensions.

01

Inventory & Discovery

- Centralized Model Register
- Multi-Tier Risk Classification
- Business Impact Analysis (BIA)
- Shadow AI Discovery & CASB
- Approved-Use Policy Enacted

02

Privacy & Sovereignty

- POPIA / NDPA Consent Mapping
- Automated PII Redaction
- Sovereign In-Country Hosting
- Cross-Border Transfer Assessment
- Right to Erasure / Vector Purge

03

Bias & Drift Monitoring

- Historical Bias & Parity Audits
- Automated Feature Drift Alarms
- Explainability (XAI) Standards
- Adversarial Stress Testing
- Champion/Challenger Staging

04

Security & Oversight

- Prompt Injection Defenses
- Role-Based RAG Filtering
- Zero-Trust Model Endpoints
- Human-in-the-Loop Thresholds
- Immutable Audit Logging (5-Yr)

Achieve full compliance certification — **Benchmark against ISO/IEC 42001.**

BOOK AUDITyips.org.za • info@yips.org.za • +27 76 099 5773

From Diagnostic Baseline to **Certified Continuous Assurance.**

A structured engagement delivering a prioritized 30-day remediation roadmap and board pack.

Maturity Benchmark Matrix

Score 0 – 10 (Ad-Hoc): Immediate moratorium on high-stakes pilots. Commission gap audit.

Score 11 – 18 (Developing): Standardize inventory; deploy Azure AI Content Safety guardrails.

Score 19 – 23 (Managed): Finalize ISO 42001 remediation; automate continuous drift monitoring.

Score 24 – 25 (Optimized): Full board assurance; continuous automated regulatory reporting.

What You Receive in the Review

- 1. Executive AI Risk Dashboard:** Board-level scorecard highlighting critical exposures and liabilities.
- 2. Technical Remediation Punch-List:** Step-by-step engineering tasks ordered by severity and effort.
- 3. ISO 42001 & POPIA Mapping:** Audit evidence register ready for supervisory inspection.
- 4. 30-Day Action Roadmap:** Clear milestones with assigned technical and governance owners.

Empower your enterprise with certified AI governance — **Schedule your review today.**

SCHEDULE REVIEW

yips.org.za • info@yips.org.za • +27 76 099 5773