

Report: Africa AI Risk Index (AARI)

This report outlines the conceptual architecture, mathematical scoring system, and policy dimensions of the **Africa AI Dependency Risk Index**, a framework designed to assess and mitigate digital sovereignty exposure across African institutions and countries.

1. Executive Summary

As AI technologies become core infrastructure for public services, finance, education, and health, dependency on foreign-hosted model providers and cloud environments exposes African organizations to unique sovereign risks. These include regulatory misalignment, pricing shocks, vendor lock-in, data jurisdiction vulnerability, and sudden service withdrawal (e.g., due to geopolitical shifts or sanctions).

The **Africa AI Dependency Risk Index** acts as a diagnostic tool, providing structured assessments across 6 strategic pillars, aggregating them into a single score, and delivering actionable policy recommendation roadmaps.

2. Core Methodology & Aggregation

The index aggregates 34 variables across 6 weighted dimensions. Individual dimension scores are calculated as the weighted average of their component variables (each converted into a 0–100 risk rating).

Dimension Weight Allocation

The overall risk score is calculated using the following mathematical model:

Overall Risk = $\sum (D_i \times W_i)$

Dimension	Identifier	Weight (W_i)	Focus Area
Model Dependency	model_dependency	20%	API concentration, reliance on closed-weights models.

Cloud Dependency	cloud_dependency	18%	Foreign server reliance, egress lock-in, hybrid readiness.
Data Sovereignty	data_sovereignty	18%	Jurisdiction of storage, transfer rates, key management.
Local Model Availability	local_model_availability	16%	Domestic talent density, R&D funding, language adaptation.
Compute Access	compute_access	14%	Hardware supply chains, grid stability, local GPU setups.
Governance & Compliance	governance_compliance	14%	Policy existence, audit rates, incident runbooks.

Mathematical Design Principles

- 1. **Conservative Defaults:** Any missing, invalid, or corrupted assessment inputs degrade to the highest-risk value (e.g., defaulting to 100% foreign API reliance or nascent legal frameworks) rather than falsely indicating safety.
- 2. **Clamped Boundaries:** All variables and scores are strictly bounded to [0, 100] to prevent outlier metrics from skewing the aggregated index.
- 3. **Vendor Diversity Scaling:** Diversity is model-scored non-linearly:

$$R_{\text{vendor}} = \max(10, 100 - 18 \times (V - 1))$$

Where V is the vendor count. A single vendor yields 100% risk, while diversity benefits plateau at 6+ vendors (10% residual risk).

3. Pillar-by-Pillar Breakdown

1. Model Dependency (Weight: 20%)

Measures exposure to external proprietary models. High exposure limits long-term customization and risks abrupt API access suspension.

- **Variables:** Workload API percentage, active vendor diversity, open-source adoption share, proprietary weights share, local fine-tuning capability, and specialized custom-feature dependencies.

2. Cloud Dependency (Weight: 18%)

Examines vulnerability to global hyperscalers.

- **Variables:** Infrastructure hosting shares, multi-cloud active maturity, local cloud capacity, network egress fee levels, local data backups, and dynamic hybrid cloud orchestration.

3. Data Sovereignty (Weight: 18%)

Ensures localized control over digital assets and training corpora.

- **Variables:** Resident storage profile, legal frameworks, cross-border flows, KMS control (BYOK/HYOK), audit logging, and data sensitivity tiering.

4. Local Model Availability (Weight: 16%)

Evaluates the viability of domestic alternatives.

- **Variables:** Researchers per million, local model compatibility, R&D investments, indigenous language/dialect adaptations, university curricula, and industry-academic collaborations.

5. Compute Access (Weight: 14%)

Assesses the physical hardware tier.

- **Variables:** Local GPU availability, cost barriers, network backhaul fiber routing, energy grid stability (UPS/green PPAs), and hardware import lead times.

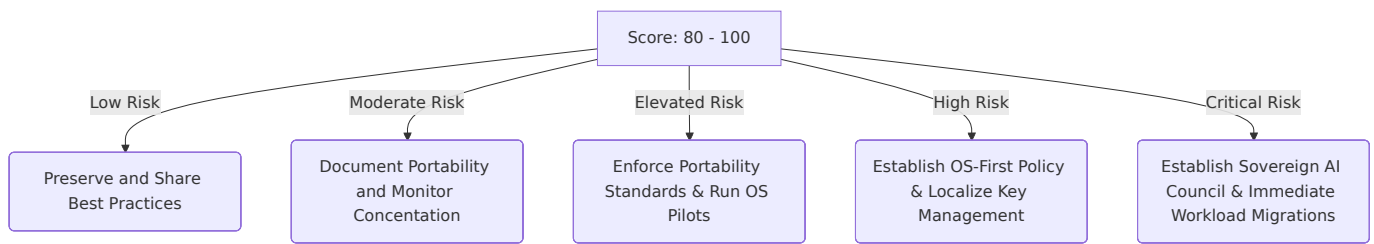
6. Governance & Compliance (Weight: 14%)

Tracks organizational maturity and risk protocols.

- **Variables:** Formal AI guidelines, bias/fairness audit frequencies, model failure incident response protocols, and alignment with national digital autonomy plans.

4. Risk Bands & Strategic Actions

Based on the aggregated score, organizations fall into five risk bands, triggering distinct policy playbooks:



- **Critical Risk (≥ 80):** Requires immediate transition of high-sensitivity workloads to local environments and the establishment of a Sovereign AI Council. Mandates "Hold Your Own Key" (HYOK) structures.
- **High Risk (60 – 79):** Triggers an "open-weights-first" procurement policy. Enforces localized data encryption keys and funds local academic-industry fellowships.
- **Elevated Risk (40 – 59):** Recommends standardized API layers to abstract vendor-specific logic, along with bi-annual compliance audits.
- **Moderate Risk (20 – 39):** Requires logging vendor concentration indexes to alert on creeping dependencies.
- **Low Risk (< 20):** Promotes sharing compliance frameworks as regional templates and maintaining long-term developer investments.