Operationalizing AI Sovereignty in Morocco: Architecture, Governance, and Capability Assurance within the Digital Morocco 2030 Framework

Asmae Lamgari,

Master's Degree in Big Data, Cloud Infrastrucutre and AI Systems Engineering
National Higher School for Computer Science and Systems Analysis (ENSIAS)
Rabat, Morocco

e-mail: asmaelamgarim@gmail.com

Abstract - This brief sets out a concrete framework for **AI sovereignty** in Morocco, defining it as **full lifecycle control**—spanning **data**, **models**, **infrastructure**, and **governance**—under national jurisdiction. Anchored in the **Digital Morocco 2030** strategy and **OECD AI Capability Indicators**, it assesses current readiness via active initiatives (the **AI & Data Center of Excellence**, education and e-government pilots, and ethical AI commitments) while identifying risks from foreign-controlled models (compromised **provenance**, cultural bias, vendor lock-in). It proposes a **sovereign AI stack**: provenance-tracked datasets; controlled training/adaptation; a **national model registry**; localized evaluation and **adversarial testing**; a **sovereign API gateway**; secure inference backends; and continuous monitoring with codified **incident response**. Governance is operationalized through a multi-stakeholder **Capability Review Board**, measurable **capability thresholds** enforced in **CI/CD**, and **tiered transparency**. A phased **roadmap** details quick wins, procurement integration, and strategic partnerships, aligning sovereignty with Morocco's **data**, **cloud**, and **cybersecurity** strategies to produce systems that are **verifiable**, **contextually aligned**, and **strategically autonomous**.

***Keywords*:** AI sovereignty; Digital Morocco 2030; OECD AI Capability Indicators; data sovereignty; model governance.

***Main Reference Reports*:** *OECD – AI Policy Observatory: AI Capability Indicators* (June 2025); *Digital Morocco 2030 – Strategic Roadmap* (Ministère de la Transition Numérique, Sept. 2024); *Protocol for Data & AI Center of Excellence in Casablanca–Settat* (Government of Morocco & Onepoint, July 2025); *CNSS and ANCFCC Data Breach Reports* (TechXplore & CybelAngel, April–June 2025)

1 Definition & Scope: What AI Sovereignty Means for Morocco

AI sovereignty is Morocco's capacity to design, adapt, deploy, and govern AI systems—from dataset creation to live inference—in ways that serve national priorities, reflect linguistic and cultural contexts, and remain under national institutional control. It entails full lifecycle ownership with transparent checkpoints and verifiable authority over decisions.

Unlike generic adoption dependent on opaque, foreign-controlled models, sovereignty positions Morocco as **architect, operator, and regulator** of its AI ecosystem, with the ability to inspect, modify, or roll back any system when required.

This approach is **controlled interoperability**, not isolation. Participation in the **Current AI** global initiative for ethical and inclusive AI reflects Morocco's intent to engage internationally while safeguarding national policies. Grounded in **Digital Morocco 2030** and aligned with **OECD AI Capability Indicators**, sovereignty becomes an urgent priority to

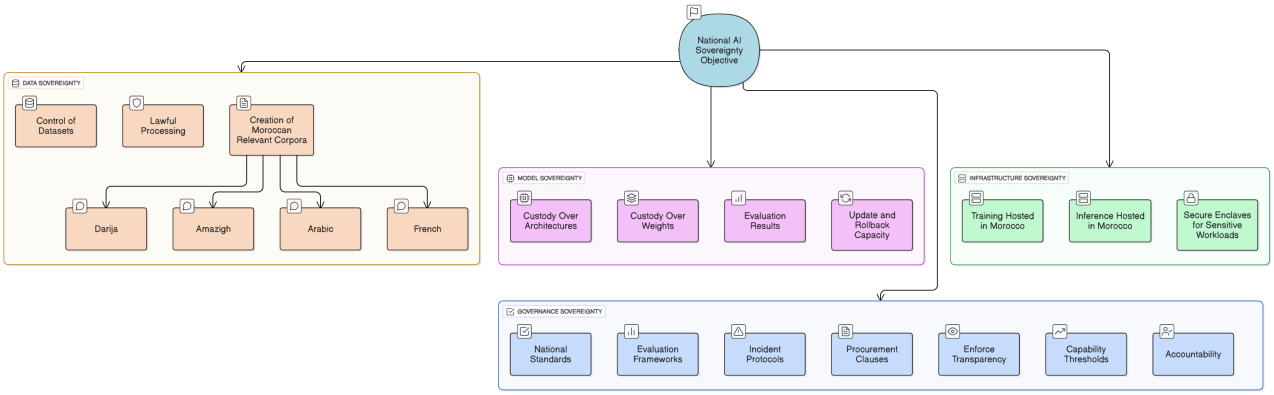

Figure 1: Four pillars of AI sovereignty for Morocco, aligned with the National AI Sovereignty Objective.

ensure control over model provenance, capability, and operational trust.

Recent initiatives illustrate this shift: the planned **government AI model** for service simplification and citizen feedback; the **Center of Excellence for Data & AI** with Onepoint to develop sovereign models; and the **energy sector's AI integration** that improved wind energy efficiency by 40%. These show sovereignty as an active agenda, not a distant goal.

AI sovereignty spans four interdependent domains:

1. **Data Sovereignty** – Custody of datasets, lawful processing, and creation of Moroccan-relevant corpora in Darija, Amazigh, Arabic, and French.
2. **Model Sovereignty** – Control over architectures, weights, evaluation results, and update/rollback mechanisms.
3. **Infrastructure Sovereignty** – Training and inference hosted on Moroccan infrastructure, including secure enclaves for sensitive workloads.
4. **Governance Sovereignty** – National standards, evaluation frameworks, incident protocols, and procurement clauses enforcing transparency, capability thresholds, and accountability.

Together, these pillars ensure Moroccan AI systems serve national objectives in capability, ethics and governance while connecting to the global ecosystem.

2 Current State & Risks

Morocco has entered the AI sovereignty debate with **clear strategic intent** and **early institutional actions**, yet the technical and governance layers for full lifecycle control remain incomplete. Strong progress exists in data creation, talent, and pilots, but without unified governance, infrastructure, and evaluation frameworks, sovereignty is not enforced from design to deployment.

2.1 Where Morocco Stands Today

Training data. Efforts such as DODa (a 100,000–entry Moroccan dialect dictionary) and DarijaBERT show active progress in Darija and Amazigh NLP[1] [2]. However, resources remain scattered and domain-limited. A Seq2Seq

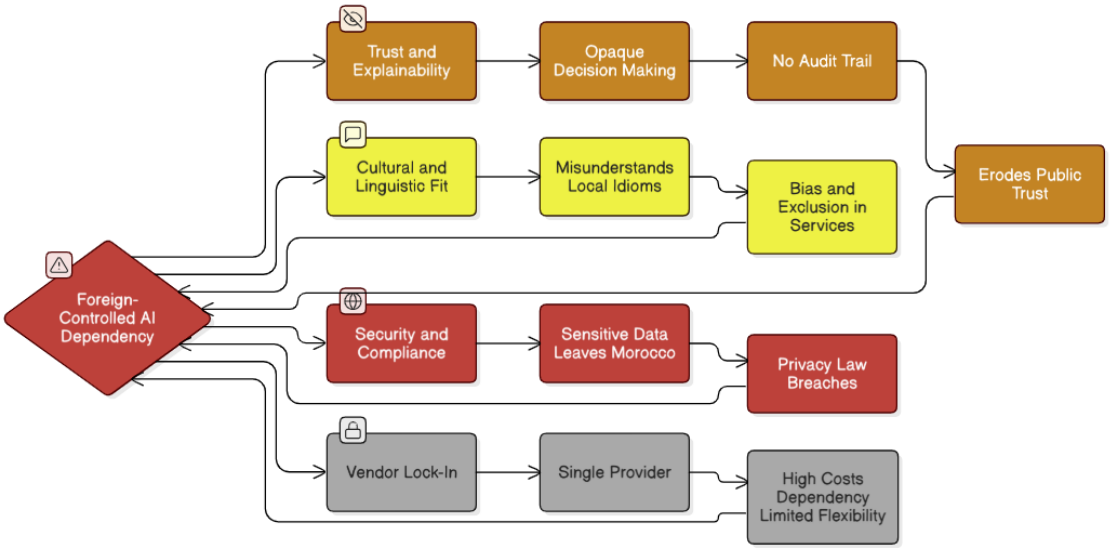

Figure 2: Risk map of foreign-controlled AI dependency.

chatbot trained on Draa-Tafilalet tourism data achieved 94% accuracy, yet its narrow scope highlights the absence of a centralized, multi-domain corpus capable of scaling across ministries.[3]

Model weights and architectures. The Center of Excellence for Data & AI (with Onepoint) is building infrastructure and talent pipelines for sovereign model development[4] [5][6]. Yet Morocco lacks the compute power, secure environments, and governance mechanisms required to sustain innovations comparable to the surgical AI developed by Moroccan researcher **Sara Ben Hmido** at Amsterdam UMC, which predicts postoperative complications during live colorectal surgeries. The strategic goal is to make Morocco a place where such systems can be conceived, trained, validated, and governed end-to-end within its own ecosystem.[7]

Inference pipelines. Citizen-facing portals like Rokhas.ma and Chikaya.ma already integrate AI pilots, and a government complaint-handling model was announced in July 2025. However, the absence of a sovereign API gateway leaves these deployments siloed, with no centralized logging, auditing, or policy enforcement.

Evaluation and safety processes. Morocco participates in **Current AI**, and healthcare adoption is advancing—45% of hospitals use AI for scheduling, 30% for diagnostics [8] [9]. Yet there is still no national evaluation suite tied to the **OECD AI Capability Indicators**, nor protocols for red-teaming or incident disclosure. This leaves pilots vulnerable to undetected failures, bias, or misalignment.

2.2 Risks of Relying on Opaque, Foreign-Controlled AI

Foreign-developed AI systems can deliver advanced capabilities, but over-reliance in critical services introduces risks that go beyond performance. These risks affect trust, cultural fit, data security, and long-term autonomy.

Trust and explainability. If the decision process is opaque, users cannot verify reasoning. Even when a government chatbot answers correctly, its black-box nature erodes oversight and civic trust.

Cultural and linguistic fit. Generic multilingual models fail with Darija and Amazigh, meaning off-the-shelf solutions in education risk misunderstanding local idioms and reinforcing inequity.

Security and compliance. Foreign inference APIs risk exporting sensitive citizen data, undermining privacy and localization rules, especially without signed models or secure sovereign execution.

Vendor lock-in. Dependence on a single provider's AI API exposes government services to high costs, limited flexibility, and strategic vulnerability if contracts shift or prices rise.

These vulnerabilities show that sovereignty requires more than local pilots—it demands transparent governance, culturally aligned models, secure infrastructure, and diversified control over critical technology.

Sectoral Gaps with Urgent Sovereignty Needs

AI is already entering Morocco's justice, health, education, and administration. Without sovereign control over data, models, and deployment, adoption risks widening gaps in trust, accountability, and performance.

Justice. Court assistants must justify reasoning and citations. Judges cannot reliably verify legal logic unless on-premise, explainable models are available—otherwise accountability gaps emerge.

Health. The surgical complication predictor shows clinical promise. Yet scaling such tools requires consent governance, bias checks, and reliable audit trails to ensure patient safety.

Education and language access. Ignoring Darija and Amazigh in education technology risks excluding large student populations. Sovereign datasets and evaluations are needed for fair inclusion. [10]

Public administration. Services like Rokhas and Chikaya reach thousands daily. In the absence of a sovereign API gateway, deployments remain fragmented, weakly monitored, and difficult to govern.

Morocco has initiated key projects—the AI Center of Excellence, ethical AI commitments, and sovereign service pilots—but lacks the end-to-end control mechanisms for datasets, models, inference, and evaluation. Until these are established, dependency, opacity, and misalignment continue to pose structural risks.

3 Design Questions: Architecture & Infrastructure

For Morocco to achieve AI sovereignty, it needs a clear and enforceable systems architecture where every piece of data, every model update, and every inference request is auditable, secure, and kept under moroccan authority. This architecture must be modular, adopt **global interoperability standards** where they align with national priorities, and embed **OECD AI Capability Indicators** for instance, as measurable *policy gates* enforced automatically at each stage of the AI lifecycle.

3.1 Target Sovereign AI Stack – End-to-End Pipeline

The sovereign AI stack operates as a layered pipeline—from *data ingestion* to *training/adaptation*, *evaluation*, *deployment*, and *monitoring*—with explicit trust boundaries and cryptographic guarantees.

1. Data Layer The Data Layer forms the foundation of the sovereign AI stack, providing trusted pipelines for ingestion, governance, storage, and protection of datasets across all sectors and sources.

- **Ingestion & Curation:** Connectors to **government databases**, **open data portals**, IoT sensors in **energy** and **agriculture**, and crowdsourced language corpora, orchestrated via **Apache NiFi** or **Airbyte** with schema validation

and metadata enrichment.

- **Data Catalog & Governance:** Centralized catalog (**OpenMetadata**, **Apache Atlas**) with **W3C PROV** for provenance tracking.
- **Versioned Storage:** Immutable object storage (**MinIO** or S3-compatible) with **DVC** dataset versioning.
- **Security Controls:** PII masking, **differential privacy** at ingestion, and fine-grained access controls with **Apache Ranger** or **LakeFS**.

2. Model Training & Adaptation Layer This layer is responsible for creating, adapting, and tracking AI models within secure, sovereign environments, ensuring that each stage of training aligns with national governance and reproducibility standards.

- **Base Models:** Open-weight LLMs such as **LLaMA** or **Mistral**, as well as Moroccan-developed architectures, are trained on **sovereign compute** within **air-gapped environments** for sensitive workloads.
- **Fine-Tuning:** Domain-specific adaptation is achieved using **LoRA/QLoRA** techniques, orchestrated in **Kubeflow** or **MLflow** pipelines for efficiency and reproducibility.
- **Experiment Tracking:** Model development and tuning experiments are documented in self-hosted instances of **MLflow** or **Weights & Biases**, ensuring traceability of results.
- **ML-SBOM:** Every training output includes a digitally signed Machine Learning Software Bill of Materials, listing datasets, code, and dependencies, generated via **Sigstore Cosign**.

3. Model Registry The model registry serves as the authoritative repository for all AI models, maintaining their metadata, governance status, and deployment history while enforcing approval and rollback policies.

- **Core:** Central store (**MLflow Registry**, **KServe ModelMesh**) tagging models with **OECD domain mappings**, evaluation scores, deployment status, and license terms.
- **Approval Workflow: GitOps** promotion from staging to production contingent on capability thresholds and security review.
- **Rollback Policy:** Automatic rollback on monitoring alerts or red-team incident reports.

4. Evaluation & Safety Suite This is the quality gate of the sovereign AI stack, ensuring that every model meets domain-specific performance, safety, and fairness thresholds before it can advance to production deployment.

- **Capability Benchmarks:** Localized test sets for **Darija/Amazigh NLP**, **Moroccan legal reasoning**, **agricultural perception**, and **healthcare triage**.
- **Cognitive Domain Mapping:** Automated linking of benchmark scores to **OECD domains** with fixed cut-offs (e.g., $\geq 85\%$ accuracy in language tasks, $\leq 5\%$ hallucination rate).
- **Adversarial Testing:** Red-teaming with **Microsoft Counterfit** or **TextAttack** for jailbreaks, prompt injection, and bias.

- **Bias/Fairness Metrics:** Toolkits such as **Fairlearn** and **AIF360**.
- **Certification:** Auto-generated **Capability Impact Statement**; deployment blocked unless all domain thresholds are met.

5. Sovereign API Gateway The Sovereign API Gateway serves as the central control point for all AI inference requests, ensuring that only certified models are accessible and that every interaction is traceable, secure, and policy-compliant. It provides a unified interface for both internal and external consumers, integrating authentication, authorization, and routing logic based on capability scores and sector-specific rules.

Table 1: Sovereign API Gateway – Technical Overview

Function	**Details**
Core Functions	Single controlled entry point; Role-Based Access Control (Keycloak); request quotas; detailed logging; automated policy enforcement.
Protocol Support	OpenAI-compatible REST endpoints (`/v1/chat/completions`, `/v1/embeddings`) for external use; gRPC for internal service communication.
Security	Mutual TLS (mTLS) between gateway and backends; JWT tokens with embedded capability claims.
Policy Enforcement	Rejection of uncertified models; routing based on model capability scores and sector context.

6. Secure Inference Backends This layer ensures that all model executions are isolated, verifiable, and optimized for both security and performance, forming the last technical checkpoint before AI outputs reach end users.

- **Deployment:** All inference workloads are deployed on sovereign Kubernetes clusters using frameworks such as **vLLM**, **TGI**, or **KServe**, ensuring that the serving infrastructure remains under Moroccan jurisdictional control.
- **Isolation:** Sensitive workloads are executed within **Trusted Execution Environments** (**Intel SGX** or **AMD SEV**), providing hardware-level protection for data confidentiality during inference.
- **Output Provenance:** Every model output is embedded with **SynthID** watermarking and enriched with metadata tagging, enabling traceability and forensic verification when required.
- **Performance Tuning:** Through **dynamic batching** and low-precision optimizations such as **INT4/INT8 quantisation**, the system maintains high throughput while preserving acceptable accuracy levels.

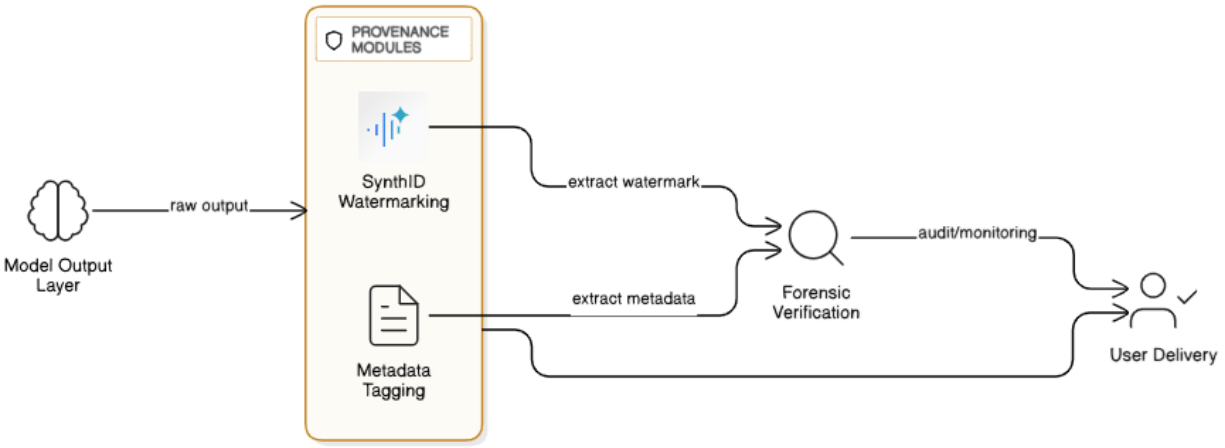

Figure 4: Provenance enforcement pipeline. Model outputs pass through SynthID watermarking and metadata tagging modules.

By combining controlled deployment, hardware-based isolation, verifiable output provenance, and tuned performance, the secure inference backend provides a foundation for trustworthy, efficient, and sovereign AI services.

7. Monitoring & Governance Layer This layer ensures that deployed AI systems remain compliant, performant, and aligned with national capability thresholds throughout their operational lifecycle.

- **Telemetry:** All inference activity is captured through centralized logging platforms such as **Elastic Stack** or **Grafana Loki**, recording prompts, outputs, latency, and model versions for complete traceability.
- **Drift Detection:** Models undergo scheduled re-evaluations, with automatic retraining or rollback triggered when performance or capability thresholds are breached.
- **Incident Response:** Operational anomalies generate alerts via **Prometheus Alertmanager**, with incidents recorded in a **national AI incident database** for oversight and accountability.
- **Annual Audit:** Each year, a public report consolidates capability scores, incident summaries, and remediation measures, ensuring transparency and sector-wide learning.

3.2 Embedding Capability Thresholds in the Stack

Each lifecycle stage applies specific checks:

- **Pre-training:** Dataset coverage and bias analysis against **OECD domains**.
- **Post-training:** Benchmark evaluation with strict pass/fail criteria.
- **Pre-deployment:** Red-team security testing and governance sign-off.
- **Post-deployment:** Continuous capability monitoring; automatic rollback or demotion on performance drop.

All controls are implemented *as code* in CI/CD pipelines to block circumvention.

3.3 Local Dataset Requirements for Contextual Fit

Domain	Dataset Requirements
Language	Speech/text corpora for Darija, Amazigh dialects, Modern Standard Arabic (MSA), and French; multi-accent Automatic Speech Recognition (ASR); code-switching examples.
Justice	Annotated Moroccan case law, statutes, and multilingual legal glossaries.
Health	De-identified medical records, medical imaging datasets, and Moroccan clinical terminology.
Agriculture	Satellite and UAV imagery, pest and disease datasets, and climate records.
Energy	Sensor data from wind and solar facilities, grid performance logs, and predictive maintenance datasets.

Table 2: Priority local datasets required for sovereign AI contextual alignment.

3.4 Interoperability Standards

Interoperability standards ensure Morocco's AI ecosystem integrates with global systems while preserving sovereign control over security, governance, and context:

- **APIs/Protocols:** REST/JSON, gRPC, OpenAI API schema.
- **Documentation:** Model and Data Cards compliant with **ISO/IEC 42001**.
- **Security Standards: ISO/IEC 27001**, **NIST SP 800-207** (Zero Trust).
- **Metadata: W3C PROV**, **OpenLineage**; **SPDX** for ML-SBOMs.
- **Evaluation: OECD AI Capability Indicators** mapped to global benchmarks.

The sovereign AI stack functions simultaneously as technical infrastructure and governance system, with **provenance controls**, **capability thresholds**, and **automated enforcement** ensuring systems remain secure, context-specific, and strategically aligned.

4 Governance & Trust

AI sovereignty requires more than infrastructure; it demands a **governance framework for verifiable trust**. Such a framework ensures that every dataset, model, and output is **proven in origin**, **certified before deployment**, **monitored continuously**, and **contained quickly if failures occur**, while balancing transparency with protection of security and intellectual property.

4.1 Provenance: Verifying Datasets, Models & Outputs

The April 2025 breach of Morocco's **social security fund (CNSS)** [11] and the June 2025 compromise of the **national land registry (ANCFCC)** showed the national risk of losing control over foundational data[12] [13]. In AI, compromised training sets or tampered models can propagate those risks into every dependent system.[14] [15]

To prevent this, provenance must be embedded across the lifecycle:

- **ML-SBOM:** Signed inventories for each model (datasets, preprocessing scripts, libraries, hyperparameters) using **Sigstore Cosign**.
- **Model & Data Cards:** Mandatory metadata on origin, intended use, licensing, and training context; no registration without them.
- **Signature Enforcement:** Inference services must reject models or datasets lacking cryptographic validation.
- **Output Provenance:** Watermarking with tools like **SynthID** for tamper-resistant tracing of generated content.

Together these measures establish a **verifiable chain of custody** from data collection to model output.

4.2 Deployment Governance: Authority & Criteria

In high-impact domains such as **justice**, **health**, and **public administration**, deployment must follow an auditable, multi-stakeholder process:

- **Capability Review Board (CRB):** Comprising **ADD**, ministries, academia, civil society, and experts, acting as the final approval gate.
- **Approval Criteria:** Alignment with **OECD AI Capability Indicators**, sector thresholds (e.g., $\geq 85\%$ accuracy in language comprehension, $\leq 5\%$ hallucination), and fairness/robustness compliance.
- **Capability Impact Statement:** Auto-generated from evaluation pipelines, consolidating benchmark results, safety reports, and mitigations.

4.3 Evaluation & Certification Framework

Evaluation must be continuous, reproducible, and codified into CI/CD pipelines so that **deployment readiness is enforced as code**:

- **Localized Benchmarks:** Moroccan-context test suites for **Darija**, **Amazigh**, legal reasoning, agriculture, and healthcare.
- **Adversarial/Bias/Security Testing:** Red-teaming (**Microsoft Counterfit**, **TextAttack**) and fairness tools (**Fairlearn**, **AIF360**).
- **Certification Gates:** Hard pipeline blocks preventing promotion without passing benchmarks and governance approval.

4.4 Incident Response: Containment & Recovery

Given the speed of AI failures, incident response must be automated:

- **Detection:** Real-time anomaly monitoring (hallucinations, drift, abnormal reasoning, latency) integrated with sovereign SIEMs.

- **Tiered Response:**
  - *Severity 1 (High):* Rollback to last certified model; activate safe-mode inference.
  - *Severity 2 (Moderate):* Apply patches, update filters, or throttle endpoints.
- **Audit & Disclosure:** Immutable log storage and public postmortems within SLA, redacting exploitable details.

4.5 Transparency Without Compromising Security or IP

Structured openness builds trust without exposing critical assets:

- **Public Disclosures:** Model card summaries, evaluation results, sector capability scores.
- **Restricted Access:** Red-team logs and ML-SBOMs accessible only to oversight bodies.
- **Annual Sovereignty Report:** Public record of active models, certified capabilities, incidents, and remediation.
- **Legal Safeguards:** Rights to explanation and administrative review aligned with GDPR principles, without exposing proprietary data.

4.6 Red-Teaming: Sustaining Operational Trust

Adversarial testing should be recurring and contextual:

- **Routine Drills:** Simulations of jailbreaks, prompt injection, data exfiltration, and hallucination.
- **Sector-Specific Tests:** In justice, manipulated statutes; in health, adversarial symptom sets.
- **Closed-Loop Remediation:** Feeding results back into evaluation suites, retraining, and API gateway policies, ensuring a continuous cycle of *security* $\rightarrow$ *governance* $\rightarrow$ *resilience*.

Morocco's AI sovereignty depends on governance systems that make every AI asset **traceable**, **certified**, **accountable**, and **resilient**. Provenance controls, deployment authority, enforced evaluation, rapid incident response, structured transparency, and sustained red-teaming are the pillars of sovereign AI that is both **technically defensible** and **socially reliable**.

5 Comparative Lessons from Peer AI Ecosystem Initiatives

5.1 Egypt – Sectoral Pilots with Institutional Governance

Egypt's National AI Strategy shows the value of deploying AI in defined sectors—health, education, and agriculture—under the oversight of a permanent governance body. Regular use of OECD benchmarks provides a measurable framework for progress. Yet fragmented procurement and weak inter-ministerial data sharing have slowed implementation and limited impact. For Morocco, the lesson is clear: enforce cross-agency data governance rules and establish centralized procurement to sustain momentum.

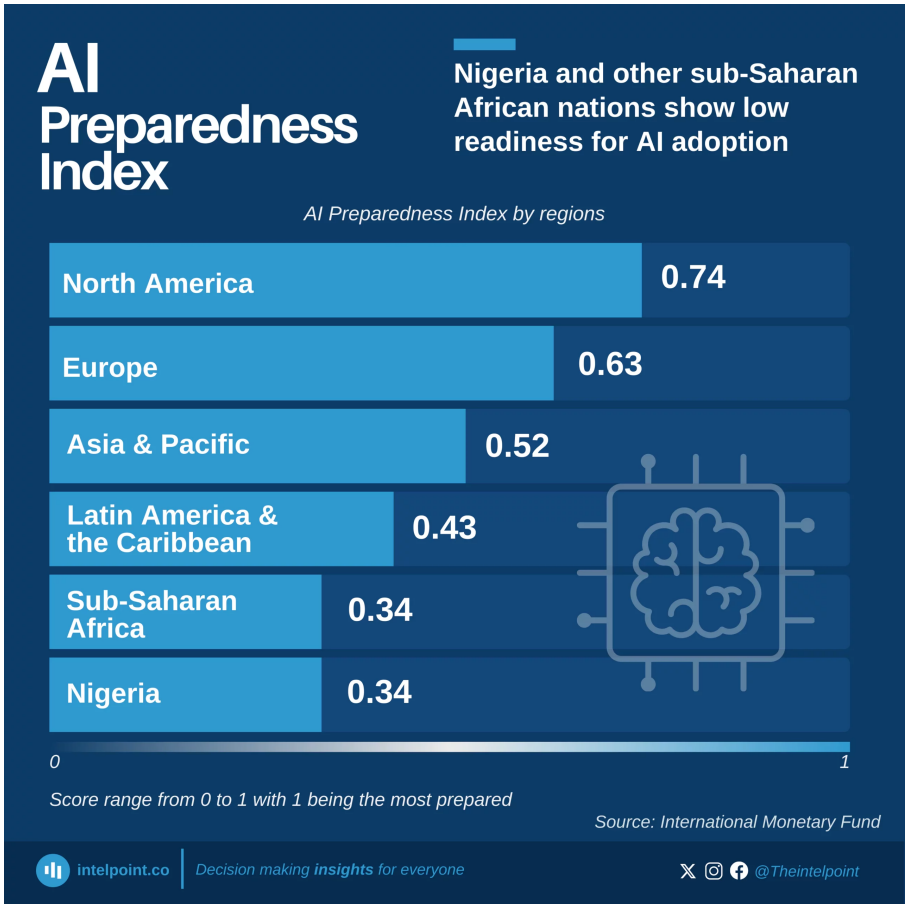

Figure 5: AI Preparedness Index by regions, showing significant gaps between North America/Europe and Sub-Saharan Africa. *Source: International Monetary Fund, via Intelpoint (2023).*

5.2 African Union – Regional Standards with Uneven Execution

The African Union's Continental AI Strategy seeks to harmonize regulation, pool infrastructure, and build shared datasets, especially for African languages. While this fosters interoperability and efficient resource use, uneven execution across member states has delayed collective outcomes. Morocco should engage in regional standard-setting to benefit from shared resources while retaining the ability to advance national priorities if regional timelines stall.

5.3 Kenya – Infrastructure-Led Growth with Application Gaps

Kenya's Konza Technopolis has built a solid physical foundation for AI through data centers, research hubs, and startup clusters. This has attracted investment and talent, but the lack of immediately deployable, high-value applications has left capacity underused. Morocco should ensure that its AI hub strategy links infrastructure development directly to certified applications in justice, health, and education, securing rapid utility and visible public impact.

5.4 Private-Sector Programs – Inclusion at the Cost of Control

Orange's African Language AI program promotes linguistic inclusion by fine-tuning large language models for African languages and making them accessible to institutions. While this accelerates availability, hosting, provenance, and update control remain in corporate hands, creating dependency and limiting sovereignty. Morocco should partner with private

actors for language model development, but keep sovereign hosting, governance, and update authority.

5.5 Key Takeaway for Morocco

The comparative evidence suggests Morocco must balance four imperatives: couple governance with sectoral applications, engage regionally without compromising autonomy, align infrastructure with operational use, and collaborate with private partners without ceding lifecycle control. This balance will prevent known pitfalls and ensure a resilient, context-specific AI ecosystem under moroccan control.

6 Operationalization & Implementation Framework

Transitioning from policy intent to functioning systems requires a staged plan with specific deliverables, governance checkpoints, and measurable outcomes—rooted in ongoing moroccan initiatives such as the AI & Data Center of Excellence.

6.1 Quick Wins (6–12 months)

- **AI & Data Center of Excellence (Casablanca-Settat)**
  Under the MoU with Onepoint, initial infrastructure deployment and team formation begin, with a target of 500 AI and data specialists by 2029 and large-scale training programs to support sovereign model development.
- **AI for Student Risk Detection Pilot**
  Operationalize the Ministry of Education's AI model (88% accuracy, recall, and precision) to identify at-risk students, creating a first reference case for educational AI under national governance.
- **AI Directorate & Regional Digital Hub**
  Establish the AI directorate and the UNDP-backed Arab-African digital hub to run pilots in AI-enabled public administration and blockchain-backed services.

6.2 Medium-Term Roadmap (12–24 months)

Phase 1 (Months 12–18)

- Activate domain-specific projects at the Center of Excellence (e.g., e-justice assistants, healthcare triage AI).
- Establish the **Capability Review Board**, model registry, and governance workflows.
- Introduce procurement clauses requiring SBOMs, model cards, and compliance with evaluation results.

Phase 2 (Months 18–24)

- Extend sovereign inference and evaluation pipelines across priority sectors.
- Launch the annual *AI Sovereignty Report* and enforce automated certification gates in CI/CD.
- Deploy the sovereign API gateway across major e-government platforms.

6.3 Embedding Sovereignty in Procurement

- **Mandatory Registry Entry** – All government AI projects must log models in the sovereign registry with full metadata, SBOM, and evaluation history.
- **Evaluation Thresholds as Pre-Qualification** – Bids must include proof of capability alignment and results from adversarial/fairness testing.
- **Governance Clauses** – Contracts must grant audit access, mandate incident reporting, and define rollback obligations.

6.4 Strategic Partnerships

- **Academic and Industrial Collaboration** – Work with UM6P's College of Computing to exploit supercomputing resources and incubators for model R&D.
- **Standards and Regulatory Engagement** – Coordinate with the UNDP digital hub, upcoming AI regulation agencies, and global governance bodies. [16]
- **Startup Sourcing** – Use platforms like GITEX Africa (Marrakesh) to identify AI startups for integration into sovereign initiatives.

6.5 Key Performance Indicators (KPIs)

KPI	Description
Center of Excellence Staffing	AI professionals onboarded vs. 500 by 2029 target
Pilot Deployment Count	Number of sovereign AI pilots per sector
Registry Coverage	% of government AI models registered with complete metadata
Certification Pass Rates	% of models meeting capability/evaluation criteria
API Gateway Traffic Share	% of inference routed through sovereign gateway
Incident Response Metrics	Average rollback time, incidents handled, remediation success
Annual Sovereignty Report Delivery	On-time public release each year

This roadmap links Morocco's strategic goals to concrete actions: rapid establishment of institutional capacity, operational pilots, governance embedded in procurement, strategic alliances with academia and industry, and KPIs that make sovereignty measurable in operational, technical, and governance terms.

7 Alignment & Integration

AI sovereignty in Morocco must rest on four interdependent pillars—data governance, cloud control, national cybersecurity, and the infrastructure and talent agenda of *Digital Morocco 2030*. The OECD AI Capability Indicators provide a common measurement framework, ensuring each pillar contributes to sovereignty in enforceable, quantifiable ways.[17]

7.1 Data Sovereignty

National datasets must remain under moroccan mandate and be structured for effective AI training and evaluation:

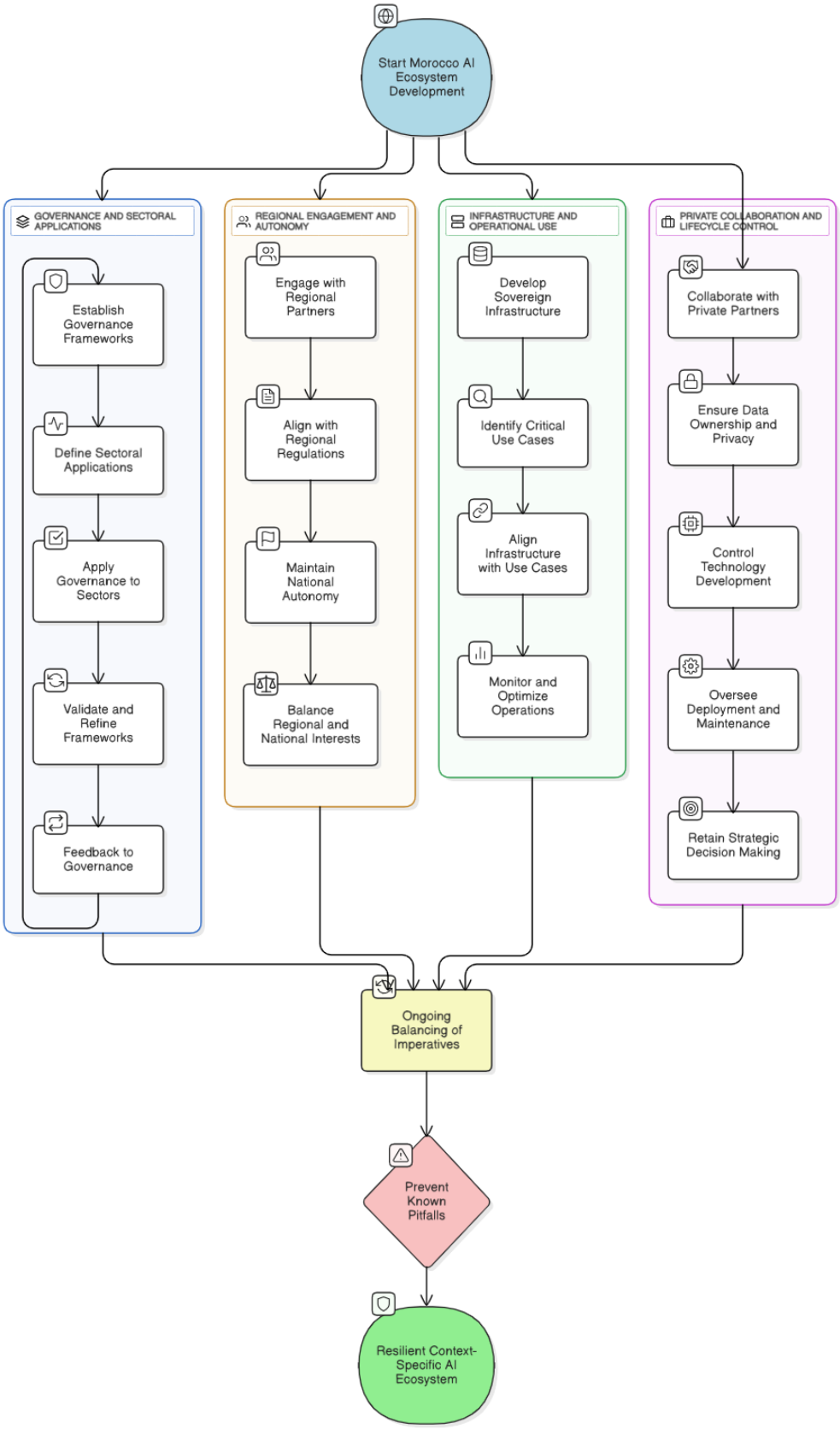

Figure 6: Proposed roadmap for Morocco's AI ecosystem development.

- **Controls & Tooling:** National data catalog (OpenMetadata/Apache Atlas) with W3C PROV lineage; default data residency; secure sharing templates; dataset versioning (DVC, LakeFS); privacy safeguards including PII minimization, k-anonymity, and differential privacy.
- **Policy Gates:** No dataset enters a pipeline without a complete data card (origin, consent, license, retention) and a validated risk score. Sensitive domains such as health and justice require elevated review and privacy impact assessments.

This guarantees that advanced Darija and Amazigh comprehension, along with other capability thresholds, are built on well-curated corpora.

7.2 Cloud Sovereignty

Model training and inference must run on infrastructure fully under moroccan supervision :

- **Controls & Tooling:** Sovereign or hybrid cloud regions; Kubernetes with runtime policy enforcement; TEEs (Intel SGX, AMD SEV) for sensitive inference; artifact signing (Sigstore); encrypted object storage (MinIO/S3-compatible); air-gapped enclaves for high-risk fine-tuning.
- **Policy Gates:** Only cryptographically signed artifacts deploy; only certified clusters (ISO/IEC 27001, Zero Trust) host high-impact workloads; all public workloads route through the sovereign API gateway.

These measures allow Morocco to enforce live service-level objectives and automatically demote models that fall below certified capability scores.

7.3 Cybersecurity Alignment

AI systems must remain defensible, observable, and recoverable under national cybersecurity standards :

- **Controls & Tooling:** ML-SBOM for every build; mTLS for all service communications; JWT with granular access claims; SIEM-integrated telemetry; adversarial testing playbooks (Counterfit, TextAttack); immutable logging; automated rollback and safe-mode failover.
- **Policy Gates:** No CI/CD promotion without adversarial and bias testing; Severity-1 incidents trigger immediate rollback and disclosure within SLA.

Capability degradation, such as accuracy loss under attack, is treated as a quantifiable risk, enabling rapid mitigation.

Digital Morocco 2030 – Infrastructure & Talent

Execution capacity depends on both robust infrastructure and skilled personnel :

- **Controls & Programs:** Data & AI Center of Excellence as the hub for registry, evaluation, and gateway; sovereign AI fellowships for engineers and auditors; procurement clauses mandating registry entry, capability scores, and incident reporting.[18]

- **Operating Model:** Capability Review Board (CRB) authorizes deployments; Platform Team manages registry and evaluation; Agency Teams fine-tune domain-specific models; Audit Cell stress-tests outputs for compliance and bias.

Targeted investment and training close capability gaps, including explainability in justice-sector AI.

7.4 OECD Indicators as the Assurance Backbone

The OECD AI Capability Indicators serve as Morocco's operational scorecard. Each model's Capability Impact Statement details scores against sector thresholds, with CI/CD gates blocking promotion until requirements are met. During deployment, dashboards track scores and trigger rollback or safe-mode fallback on degradation. Capability passports preserve provenance, scores, incidents, and fixes, feeding into the Annual AI Sovereignty Report that guides investment.

7.5 Integration in Practice – The Closed Loop

Figure 7: AI Sovereignty Operationalized: The Closed Loop.

through the closed-loop cycle AI sovereignty becomes measurable and enforceable. From data entry to certification, monitoring, and annual review, each stage is linked in a continuous process that ensures accountability, resilience, and alignment with national priorities.

Conclusion

This brief sets out an enforceable vision for AI sovereignty in Morocco, underpinned by full lifecycle control over data, models, infrastructure, and governance. A sovereign AI stack with verifiable capability thresholds and continuous monitoring, backed by institutional governance, turns strategic intent into operational reality. Comparative lessons highlight the need to tie infrastructure to high-value applications, embed governance across the lifecycle, and protect autonomy while engaging regionally and globally.

Aligning sovereignty with Morocco's digital pillars—data governance, cloud control, cybersecurity, and talent—ensures technical progress serves national priorities. The OECD AI Capability Indicators provide the measurement backbone, translating policy into quantifiable performance metrics.

The next section turns to **Data Sovereignty**, the foundation of this framework, outlining how Morocco can secure jurisdictional control, apply rigorous governance, and build culturally and linguistically representative corpora in Darija, Amazigh, Arabic, and French—establishing the trustworthy base for all subsequent stages of the AI lifecycle.

References

[1] Y. Mourchid, A. Lakhouaja, and A. El Mahdaouy, "Doda: A comprehensive moroccan darija–english–arabic lexical dataset," *arXiv preprint arXiv:2405.13016*, 2024. [Online]. Available: https://arxiv.org/abs/2405.13016.

[2] SI2M Lab, *Darijabert – moroccan dialect bert model*, Hugging Face Model Card, 2024. [Online]. Available: https://huggingface.co/SI2M-Lab/DarijaBERT.

[3] Y. Chahidi, M. El Adnani, and H. Ezzikouri, "A tourism chatbot for morocco using seq2seq with lstm and attention mechanism," *arXiv preprint arXiv:2501.00049*, 2025. [Online]. Available: https://arxiv.org/abs/2501.00049.

[4] "Onepoint to open ai centre of excellence in morocco." Middle East AI News, July 22, 2025. (Jul. 2025), [Online]. Available: https://www.middleeastainews.com/....

[5] "Morocco partners with onepoint to create ai center of excellence in casablanca-settat region." Yabiladi, July 23, 2025. (Jul. 2025), [Online]. Available: https://en.yabiladi.com/articles/....

[6] "Morocco forges strategic alliance with onepoint to establish landmark data & ai hub." TechAfrica News, July 23, 2025. (Jul. 2025), [Online]. Available: https://techafricanews.com/....

[7] "Moroccan researcher pioneers ai-powered surgical risk assessment tool." Walaw Press, December 22, 2024. (Dec. 2024), [Online]. Available: https://sport.walaw.press/....

[8] C. Idaomar, D. Idaomar, M. Hannaoui, and K. Chafik, "Applications of artificial intelligence in morocco's healthcare sector: A springboard to medical excellence," *Journal of Computer and Communications*, vol. 12, pp. 63–77, Sep. 2024. DOI: 10.4236/jcc.2024.129004.

[9] O. Omari Haraké, "Artificial intelligence in healthcare in morocco: Potential, ethical challenges, and responsibility framework," *PM World Journal*, vol. XIV, no. V, May 2025. [Online]. Available: https://www.pmworldlibrary.net/wp-content/uploads/2025/05/pmwj152-May2025-Omari-Harake-Artificial-Intelligence-in-Healthcare-in-Morocco.pdf.

[10] I. Elbouknify, I. Berrada, L. Mekouar, *et al.* "Ai-based identification and support of at-risk students: A case study of the moroccan education system." (Apr. 2025), [Online]. Available: https://arxiv.org/abs/2504.07160.

[11] C. Cimpanu. "Morocco investigates breach after hackers claim theft of millions of records." The Record. (Apr. 2025), [Online]. Available: https://therecord.media/morocco-investigates-breach-hackers-algeria.

[12] Associated Press. "Morocco investigates alleged hack of social security fund." AP News. (Apr. 2025), [Online]. Available: https://apnews.com/article/753ce01484ceb8d1ec02459910285235.

[13] Resecurity. "Cybercriminals attacked national social security fund of morocco: Millions of digital identities at risk of data breach." Resecurity Blog. (Apr. 2025), [Online]. Available: https://www.resecurity.com/blog/article/cybercriminals-attacked-national-social-security-fund-of-morocco-millions-of-digital-identities-at-risk-of-data-breach.

[14] CybelAngel. "A cnss breach update: Broader implications for morocco's digital sovereignty." CybelAngel. (Jun. 2025), [Online]. Available: https://cybelangel.com/a-cnss-breach-update/.

[15] Yabiladi. "Morocco: Jabaroot leak targeted notaries' tawtik platform, not the ancfcc land registry." Yabiladi. (Jun. 2025), [Online]. Available: https://en.yabiladi.com/articles/details/168060/morocco-jabaroot-leak-notaries-land.html.

[16] UNDP – Arab States. "Undp and morocco partner to accelerate digital transformation for sustainable development in the arab states region and africa." UNDP, July 5, 2025. (Jul. 2025).

[17] "France's onepoint to launch ai centre of excellence in morocco, create 500 jobs by 2029." AI Africa (via iAfrica.com). (Jul. 2025).

[18] "Strategic agreement with the moroccan government." Groupe Onepoint, July 22, 2025. (Jul. 2025).