THE SOVEREIGN STACK

TOOLKIT

Sovereignty Maturity Index Assessment
+ 90-Day Implementation Roadmap

From the book

OWN YOUR AI

The Sovereign Stack Playbook for Nations and Enterprises

Prem Naraindas & Vinod Bijlani

ABOUT THIS TOOLKIT

Assess. Plan. Deploy.

This toolkit extracts the two core assessment and execution frameworks from **Own Your AI: The Sovereign Stack Playbook for Nations and Enterprises**. They work as standalone tools - use them right now to assess your organisation's AI sovereignty posture and plan your first 90 days of implementation.

Tool 1: Sovereignty Maturity Index

A six-dimension weighted scoring framework (0-100) that gives you an honest assessment of where you stand today. Score yourself across Data, Compute, Model, Application, Governance, and Security sovereignty. Most organisations score below 50.

Tool 2: 90-Day Sovereignty Roadmap

A structured three-phase execution plan from assessment to pilot deployment. Includes separate tracks for government and enterprise leaders, plus the Sovereignty Certificate checklist that proves your independence to regulators and stakeholders.

How Scoring Works

The SMI expands the Three Pillars of sovereignty (Data, Compute, Model) into six measurable dimensions. The first three correspond directly to the pillars. The remaining three - Application, Governance, and Security - capture the operational capabilities required to make the pillars effective in practice.

A sovereign model on sovereign infrastructure means little without sovereign applications, governance frameworks, and security posture to protect it. Each dimension is scored on a 0-100 scale using the five-level rubric on the following pages. Your composite SMI is the weighted average across all six dimensions.

$$SMI = (Data \times 0.25) + (Compute \times 0.20) + (Model \times 0.20) + (Application \times 0.15) + (Governance \times 0.10) + (Security \times 0.10)$$

0-20	21-40	41-60	61-80	81-100
Dependent	Compliance	Strategic	Advanced	Autonomous

Benchmark: Accenture's global research found most organisations score below 50.
Regulated sectors lead - Aerospace & Defence (67), Government & Public Sector (64), Health (60).

Dimension 1: Data Sovereignty

Control over data residency, data flows, and data governance.

25%

Where does your training data physically reside? Who has legal access under which jurisdictions? What percentage crosses international borders?

0-20	No formal data residency policies; data flows unmonitored
21-40	Basic residency compliance; limited visibility into cross-border flows
41-60	Comprehensive data mapping; classification system in place
61-80	Full data residency control for sensitive workloads; dual-zone architecture
81-100	Complete data sovereignty with automated enforcement and real-time monitoring

YOUR SCORE: _____ / 100

Dimension 2: Compute Sovereignty

Control over AI training and inference infrastructure.

20%

Who owns the physical infrastructure? What is your GPU supply chain dependency? Can you operate if disconnected from foreign providers?

0-20	Complete dependency on foreign hyperscalers
21-40	Hyperscaler with domestic region; no hardware ownership
41-60	Hybrid architecture; domestic inference with foreign training
61-80	Domestic training capability; strategic hardware reserves
81-100	Full domestic compute stack with supply chain resilience

YOUR SCORE: _____ / 100

Dimension 3: Model Sovereignty

Control over AI model selection, training, and deployment.

20%

Can you audit your model's training data? Do you control model updates? What happens if your provider revokes access?

0-20	API-only access to proprietary models
21-40	Licensed models with LoRA adapters
41-60	Open-weight models with full parameter fine-tuning
61-80	Continued pre-training on sovereign data; model provenance documentation
81-100	Ground-up model training with transparent datasets

YOUR SCORE: _____ / 100

Dimension 4: Application Sovereignty

Control over the application layer between models and users.

15%

Where do inference calls execute? Do your RAG pipelines store vectors domestically? Are telemetry and logging sovereign?

0-20	SaaS applications with data leaving jurisdiction	
21-40	Data residency compliance but foreign orchestration	
41-60	Domestic inference with controlled data flows	
61-80	Full application stack sovereignty; agentic AI under control	
81-100	Air-gapped capability for critical workloads	

YOUR SCORE: ____ / 100

Dimension 5: Governance & Compliance

Maturity of AI governance frameworks and regulatory compliance.

10%

Do you have a dedicated AI governance framework? How do you map to EU AI Act? Is auditability built into architecture?

0-20	No AI-specific governance	
21-40	Extended IT governance to AI	
41-60	Dedicated AI governance framework	
61-80	Comprehensive NIST AI RMF implementation	
81-100	Governance-as-code with automated compliance	

YOUR SCORE: ____ / 100

Dimension 6: Security & Resilience

Cybersecurity posture and operational resilience for AI systems.

10%

What is your recovery time if a provider terminates access? Do you have adversarial testing? Are supply chain risks monitored?

0-20	Standard IT security only	
21-40	AI-specific threat awareness	
41-60	Regular adversarial testing; supply chain visibility	
61-80	Comprehensive red-teaming; multi-provider resilience	
81-100	Zero-trust AI architecture with proven failover capability	

YOUR SCORE: ____ / 100

SMI Calculation Worksheet

Dimension	Your Score	Weight	Weighted Score
Data Sovereignty		× 0.25	
Compute Sovereignty		× 0.20	
Model Sovereignty		× 0.20	
Application Sovereignty		× 0.15	
Governance & Compliance		× 0.10	
Security & Resilience		× 0.10	
TOTAL SMI SCORE			

Quick Self-Assessment

This rapid assessment approximates your full SMI level. For a detailed score, use the six-dimension rubric on the preceding pages. Score your organisation 1-5 on each statement (1 = strongly disagree, 5 = strongly agree):

#	Statement	Score
1	We know exactly where all AI training data is physically stored.	
2	We could operate our critical AI systems if our primary cloud provider terminated access.	
3	We own (not license) the weights of models used for sensitive applications.	
4	Our AI applications can function offline or with alternative model providers.	
5	We have documented AI governance policies that are actively enforced.	
6	We regularly test our AI systems against adversarial threats and supply chain disruption.	
	TOTAL (max 30)	

Scoring

6-12	**Fully Dependent**	Significant gaps across all dimensions
13-18	**Compliance-Driven**	Basic controls, strategic gaps remain
19-24	**Strategically Sovereign**	Meaningful sovereignty, room to improve
25-30	**Fully Autonomous**	Comprehensive sovereignty

> ***Worked example:*** *A mid-sized European retailer scored Q1=4, Q2=2, Q3=1, Q4=2, Q5=3, Q6=2. Total: 14 (Compliance-Driven). Their data residency was strong (GDPR compliance), but they had no model ownership and could not operate if their cloud provider terminated access. Their sovereignty strategy focused on compute and model gaps, not data.*

SECTION 2

90-Day Sovereignty Roadmap

This roadmap synthesises infrastructure decisions, model selection, application architecture, governance frameworks, and regional context into an actionable execution plan.

CRITICAL PATH WARNING: Hardware Lead Times

Physical GPU procurement (H100s, MI300X, Gaudi 3) often requires 12-20 weeks - exceeding this 90-day roadmap. Assume the pilot will run on interim infrastructure: sovereign cloud capacity, available on-premises resources, or pre-positioned hardware. Begin hardware procurement in Week 1-2 alongside stakeholder alignment.



FOUNDATION — DAYS 1-30

Week 1-2: Stakeholder Alignment - Secure executive sponsorship. Form the Sovereignty Working Group (IT, data governance, legal, compliance, security, business units, finance). Present the business case for sovereignty.

Week 2-3: SMI Assessment - Score your organisation across all six dimensions using the rubric above. Conduct current-state architecture review. Map all AI workloads, data flows, and provider dependencies.

Week 3-4: Gap Analysis & Quick Wins - Identify highest-priority gaps. Execute quick wins: telemetry audit (check what data leaves your network), data classification, policy documentation. Define target sovereignty level.

ARCHITECTURE — DAYS 31-60

Week 5-6: Reference Architecture - Evaluate the five reference architectures. Select based on requirements, not convenience. Specify the dual-zone architecture: public zone vs. sovereign zone with security gateway.

Week 7: Vendor Evaluation - Assess sovereign cloud offerings. Evaluate open-weight models for your use case. Negotiate sovereignty terms with existing providers.

Week 7-8: Governance & Pilot Scoping - Design governance framework mapping to applicable regulations (EU AI Act, local requirements). Select pilot workload with clear success criteria and rollback procedures.

DEPLOYMENT — DAYS 61-90

Week 9-10: Infrastructure & Application - Stand up sovereign infrastructure per architecture specs. Deploy selected model(s) with zero external dependencies at runtime. Test data flows. Security hardening.

Week 10-12: Validation & Certificate - Network traffic analysis to verify no unauthorised data flows. User acceptance testing. Performance baseline. Resilience testing. Issue the Sovereignty Certificate.

Week 12: Lessons & Scale - Post-implementation review. Re-score your SMI. Update business case with actual costs and demonstrated benefits. Define 12-month expansion roadmap.

Adapting the Roadmap: Government vs. Enterprise

The core 90-day framework adapts to your context. Government and enterprise tracks differ in constraints, stakeholders, and success criteria.

Phase	Government Leaders	Enterprise Leaders
Days 1-30	• Secure ministerial/cabinet-level sponsorship • Establish inter-agency working group with clear mandate • Map to national AI strategy and digital transformation objectives • Identify pilot with clear public benefit • Initiate parallel procurement workstream	• Secure C-suite sponsorship (CEO, CTO, CISO alignment critical) • Quantify regulatory exposure and compliance gaps • Map customer sovereignty requirements • Identify pilot with clear revenue or cost impact
Days 31-60	• Draft sovereign AI policy framework • Evaluate domestic provider ecosystem • Engage with regulatory sandbox if applicable • Plan public communication strategy	• Negotiate sovereign terms with existing vendors • Evaluate sovereign cloud offerings • Build financial model for full deployment • Develop customer communication strategy
Days 61-90	• Deploy pilot with appropriate security controls • Conduct sovereignty validation (network analysis, data residency proof) • Issue Sovereignty Certificate signed by appropriate authority • Document lessons for national playbook • Present to cabinet/ministry with expansion plan	• Deploy pilot with customer visibility • Measure impact on customer acquisition/retention • Issue Sovereignty Certificate (use for partner assurance) • Document compliance posture improvements • Present business case for scale investment

The Sovereignty Certificate

The culminating deliverable of the 90-day roadmap. A formal attestation report proving that zero packets left the sovereign zone during pilot operation - documented proof of sovereignty for stakeholders, regulators, and auditors.

#	Requirement	Description	Done
1	**Network traffic analysis logs**	Demonstrating no unauthorised external connections	☐
2	**Data residency verification**	Confirming all data remained within sovereign jurisdiction	☐
3	**Model provenance documentation**	Showing audit trail for all AI components	☐
4	**Compliance mapping**	To applicable regulatory frameworks (EU AI Act, local requirements)	☐
5	**CISO sign-off**	Or equivalent security authority	☐

SOVEREIGNTY CERTIFICATE SIGN-OFF

Organisation: _____

Pilot Workload: _____

Pilot Duration: _____ to _____ SMI Score (Before): _____ SMI Score (After): _____

Signed (CISO / Security Authority): _____ Date: _____

Key Takeaways

1. **Assess Before You Build.** The SMI provides your starting coordinates. Without honest assessment, you will build solutions to problems you do not have while ignoring vulnerabilities you do.
2. **Foundation First.** Days 1-30 stakeholder alignment and gap analysis prevent months of backtracking later. Resist the temptation to start building immediately.
3. **Quick Wins Build Momentum.** Early, visible improvements - telemetry audits, data classification, policy documentation - demonstrate progress while longer-term work proceeds.
4. **Architecture Determines Destiny.** The reference architecture you select in Days 31-60 constrains options for years. Choose based on requirements, not convenience.
5. **Pilots Prove Concepts.** Days 61-90 transform theory into practice. A working sovereign AI deployment is worth a thousand strategy documents.
6. **Sovereignty Is a Practice.** The 90-day roadmap gets you started, but sustainable sovereignty requires ongoing investment, vigilance, and adaptation.

Get the Full Playbook

This toolkit covers two frameworks from a 10-chapter, 45,000-word playbook. The full book includes deep technical guidance on dual-zone architectures, GPU economics, inference stack design, open-weight model licensing, agentic AI security, governance frameworks, and case studies from Saudi Arabia, Switzerland, India, Indonesia, and more.

OWN YOUR AI

The Sovereign Stack Playbook for Nations and Enterprises

Prem Naraindas & Vinod Bijlani

Available now on Amazon Kindle and in paperback

amazon.com/dp/B0GS7C6DN4

ownaistack.com

Copyright 2026 Prem Naraindas and Vinod Bijlani. All rights reserved.
This toolkit may be shared freely in its complete, unmodified form.