



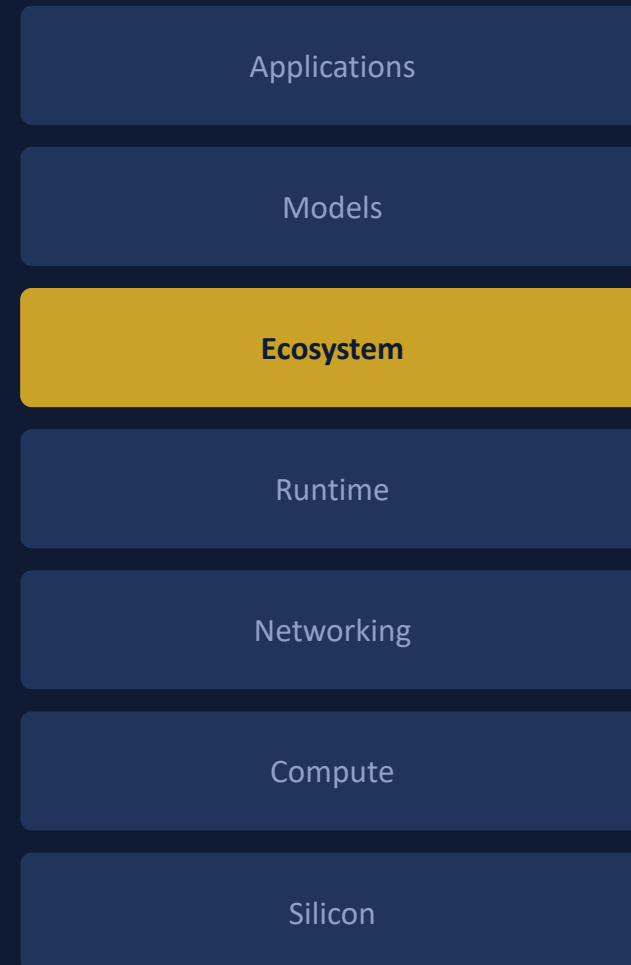
VIVIKTA ADVISORY · POINT OF VIEW

The Sovereignty Illusion

Why AI governance must expand beyond the model

A boardroom perspective on ecosystem concentration, strategic autonomy, and the layers of AI sovereignty that owning a model alone cannot secure.

Vendor-neutral · Thought-leadership edition · 2026



THE OPEN-WEIGHT / ECOSYSTEM LAYER

The governance question has moved down the stack

FIRST-GENERATION GOVERNANCE

“Who owns the model?”

Focused on model risk — accuracy, bias, explainability, and reliance on a single external API.



NEXT-GENERATION GOVERNANCE

“Who owns the layers the model needs to exist?”

Focused on ecosystem risk — compute, runtime, distribution and developer platforms converging in few hands.



The thesis. As AI providers integrate from silicon to compute to software to model distribution, organizations risk exchanging one dependency for another. Dependency rarely arrives as a single decision — it accumulates, invisibly, across layers.

WHY NOW

The trigger: a compute leader reaching into the model-distribution layer

Reports of NVIDIA's interest in Hugging Face are strategically significant — not as a single deal, but as a signal. Hugging Face is no longer just a model repository; it has become the primary distribution and collaboration layer for the global open-weight ecosystem. Influence there extends a compute provider's reach across a much larger portion of the AI value chain.

This is why sovereign-AI, healthcare and public-sector programs increasingly center on open-weight models rather than proprietary APIs.

API MODELS

Let you consume AI

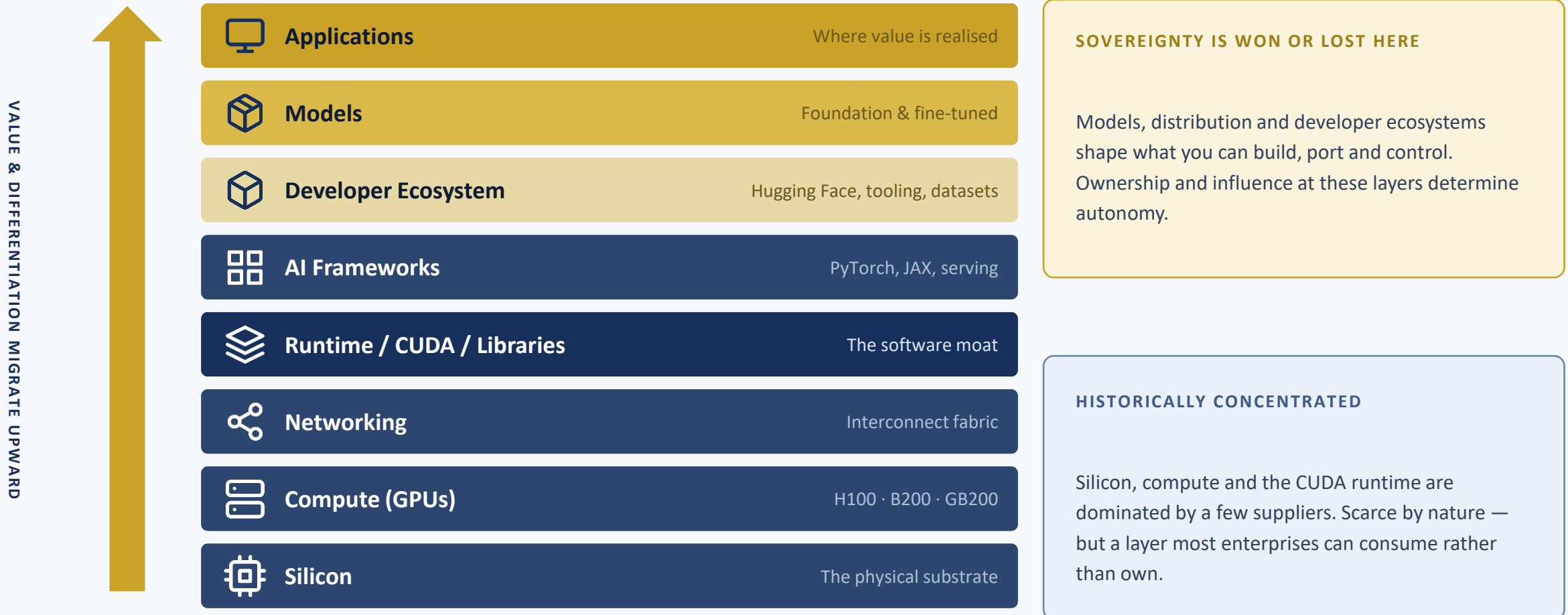
Fast to adopt · controlled elsewhere · pricing, access and lifecycle outside your hands.

OPEN-WEIGHT MODELS

Let you own & operationalize AI

Deployable in-country · fine-tunable on local data · survivable if a supplier changes course.

Eight layers — and where strategic value is migrating



MARKET STRUCTURE

From distinct roles to vertically integrated AI ecosystems

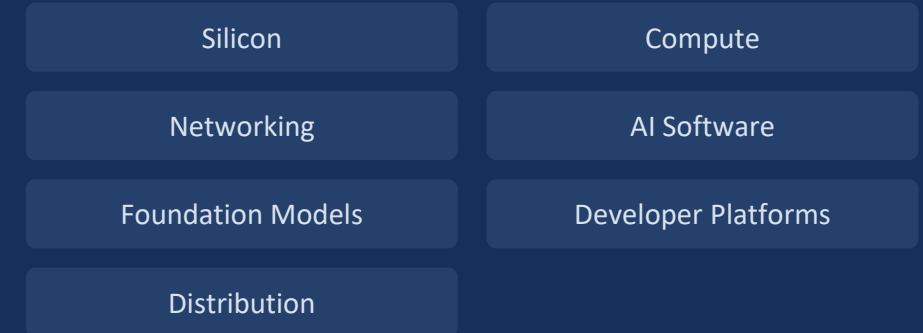
Yesterday, the layers of the stack were built and owned by different players. Today those boundaries are dissolving as providers extend across the chain.

THEN — SPECIALISED ROLES

- **Chip makers** — built silicon
- **Cloud providers** — supplied compute
- **Model labs** — built models
- **Developers** — built applications

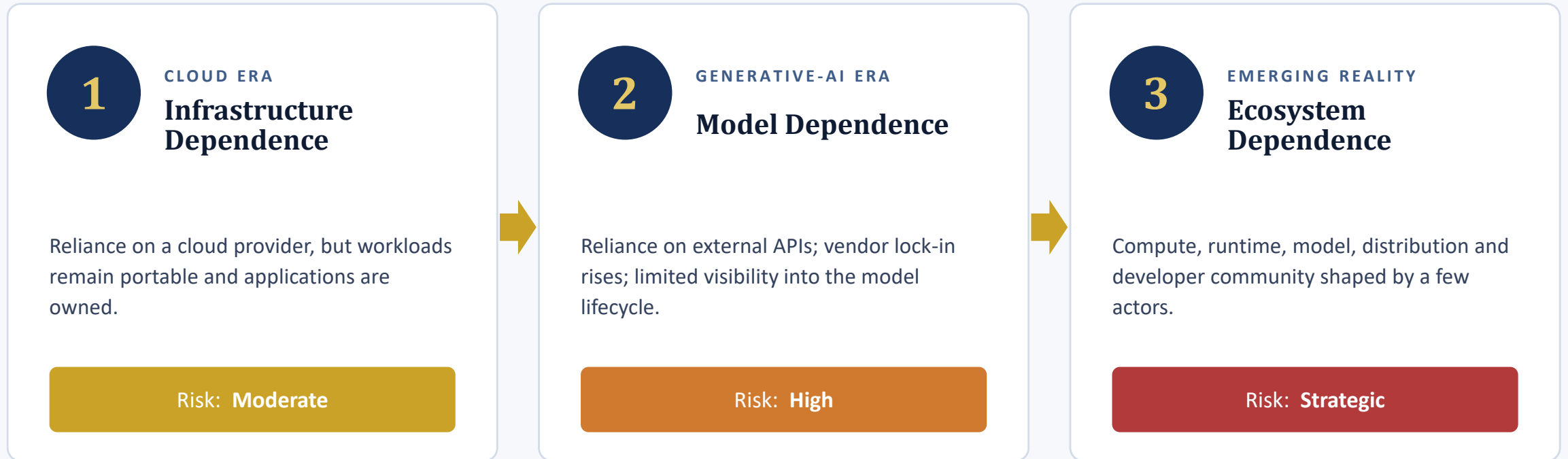


NOW — ONE ECOSYSTEM, MANY LAYERS



Board question. What happens to competition, pricing power and portability when a single ecosystem participates in every layer of the AI value chain?

Three phases — each raises switching costs and concentration



Each transition trades a portable dependency for a deeper, more entangled one — until exit is no longer a practical option.

THE CORE MISCONCEPTION

Owning the model is not the same as sovereignty

A common assumption: open-weight model = sovereignty. Necessary, but far from sufficient.

WHAT YOU MAY HAVE SECURED

- ✓ The model runs locally
- ✓ Data remains in-country
- ✓ Fine-tuning is performed in-house
- ✓ Weights are open and inspectable

WHAT MAY STILL BIND YOU

- ✗ Compute depends on one vendor
- ✗ Toolchains depend on one ecosystem
- ✗ Deployment depends on one runtime
- ✗ Discovery depends on one platform

True sovereignty requires ownership decisions across four — and arguably five — distinct layers.

HISTORICAL ANALOGIES

Every industrial transition creates powerful orchestrators

Concentration is not, in itself, the problem. The question is whether it creates dependency without substitutability.



Industrial Revolution

Specialised suppliers — Carnegie steel, Westinghouse, GE — powered whole industries. Winners owned differentiation, not every mill and mine.



Aviation Engines

Boeing and Airbus rely on a handful of engine makers (Rolls-Royce, P&W, GE). Sovereignty comes from design authority, integration and certification — not building engines.



Telecom Backbone

Carriers ran on a few backbone and equipment providers. Value accrued to services, reach and customer relationships above the shared infrastructure.



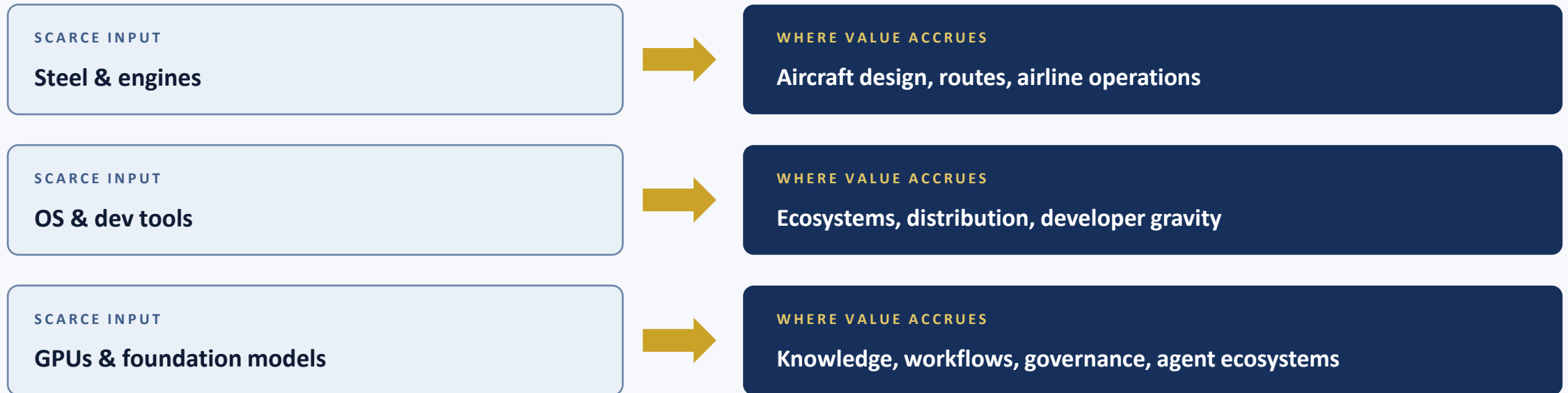
Microsoft → GitHub → OpenAI

OS, then developer community, then model layer. The advantage was never one asset — it was the connections between them.

THE PATTERN

Value migrates away from the scarce component

In every transformation, advantage moved from the scarce input toward the orchestration built on top of it. The question changes from “What do you own?” to “Where do you sit in the value chain?”



Implication. The future winners of AI need not own the chips. They will own the knowledge, governance and workflows those chips enable.

THE FRAMEWORK

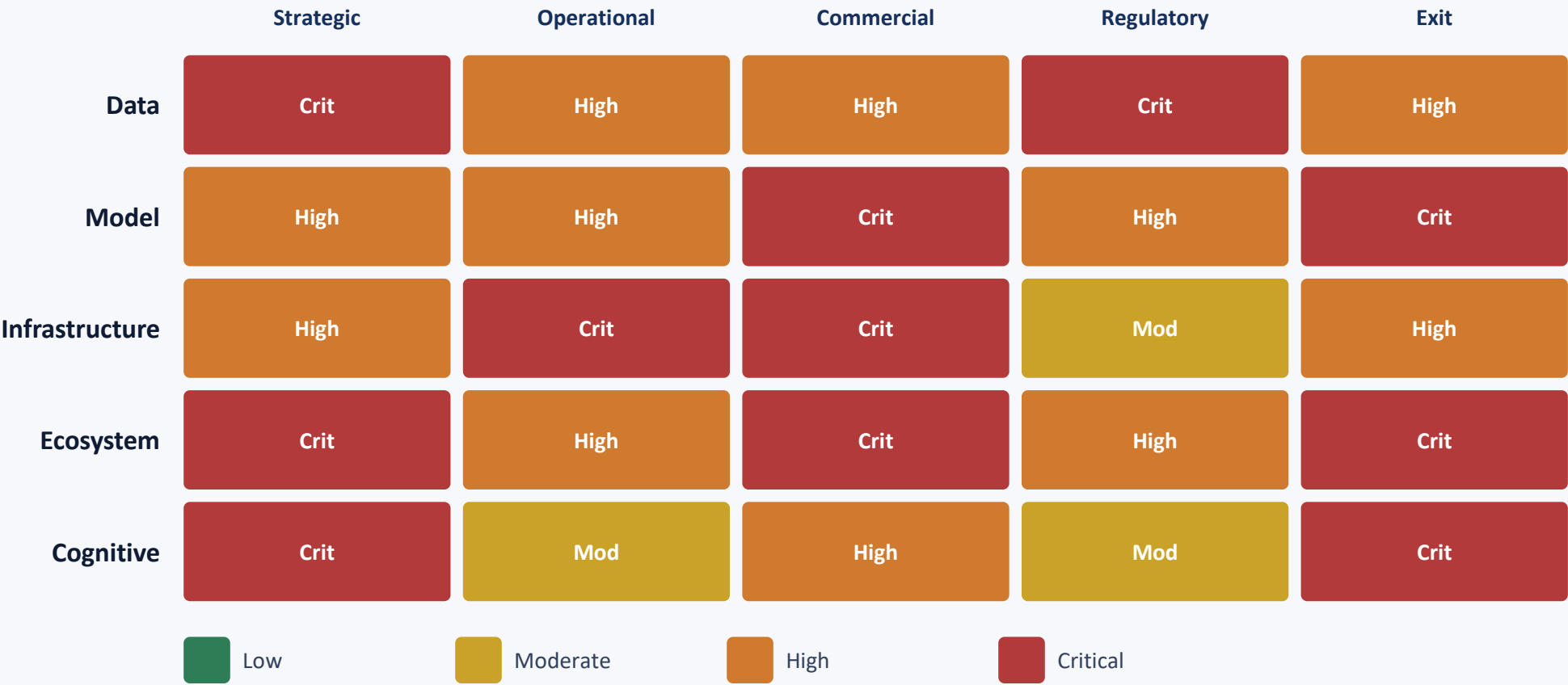
Five layers of AI sovereignty

Sovereignty is a stack of decisions, not a single one. The upper layers are least discussed — and increasingly the most strategic.

	Data Sovereignty	Who owns the data, where it lives, who governs access.	Very High
	Model Sovereignty	Can the model be operated, modified and survive supplier disruption.	High
	Infrastructure Sovereignty	Can compute be substituted; is inference portable.	High
	Ecosystem Sovereignty	Who controls standards, distribution and developer communities.	Strategic
	Cognitive Sovereignty	Do you build your own knowledge assets — or only consume intelligence produced elsewhere.	Defining

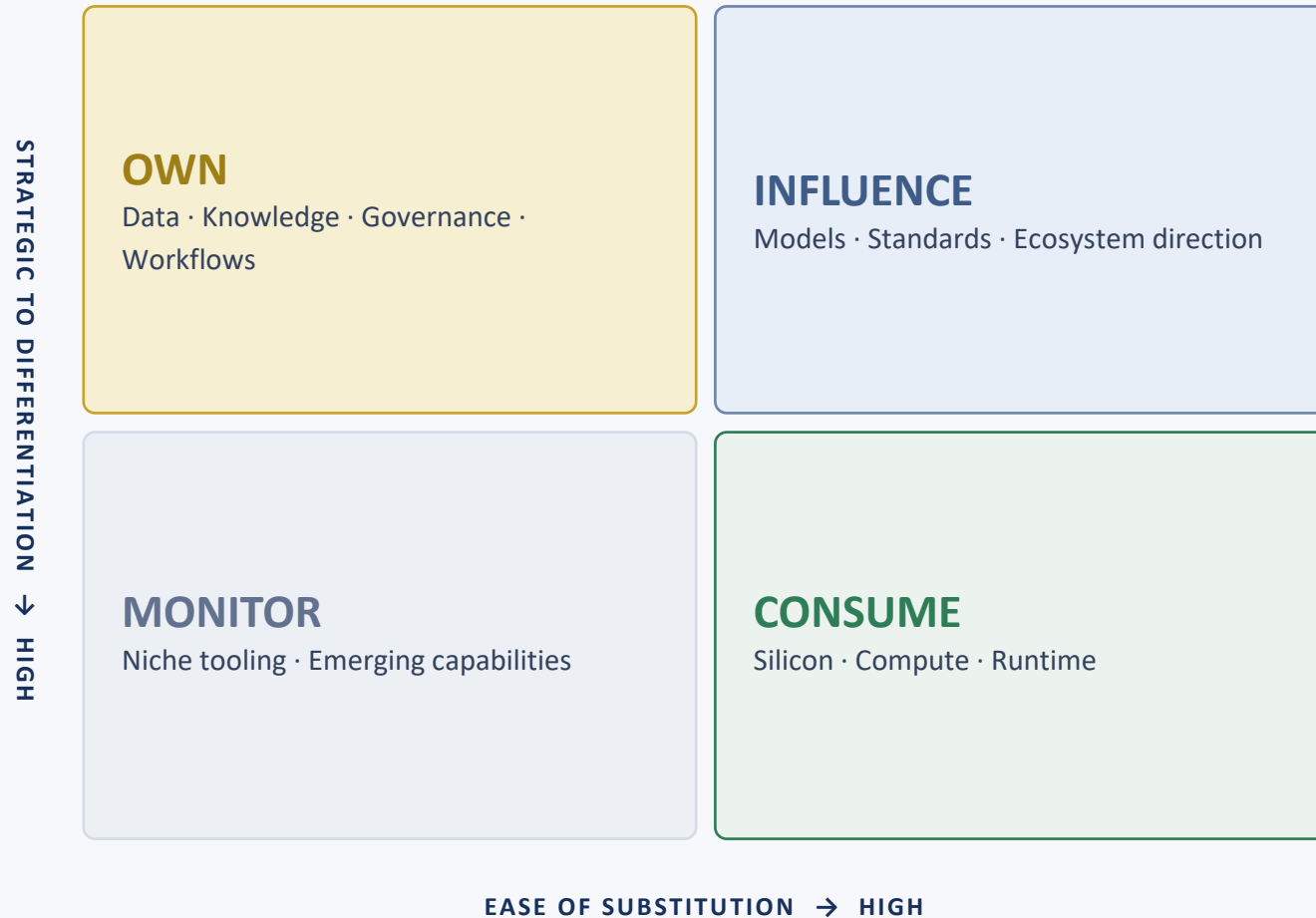
CONCENTRATION RISK HEATMAP

Where exposure concentrates across the stack



Illustrative — organizations should score their own posture. The strategic and exit columns are where invisible dependency accumulates fastest.

Deciding what to own, influence, or consume



READ IT THIS WAY

The more strategic and the harder to replace, the stronger the case to own it.

The more substitutable, the safer to consume as a service — even at scale.

Read AI concentration through familiar risk categories

Not a technology topic — a governance one. The board already knows how to reason about concentration in cyber, supply chains and counterparties.



Strategic

Dependence on a single ecosystem across many layers.



Operational

Disruption to compute availability or service continuity.



Commercial

Pricing power shifts decisively to the provider.



Regulatory

Jurisdictional or export restrictions constrain access.



Innovation

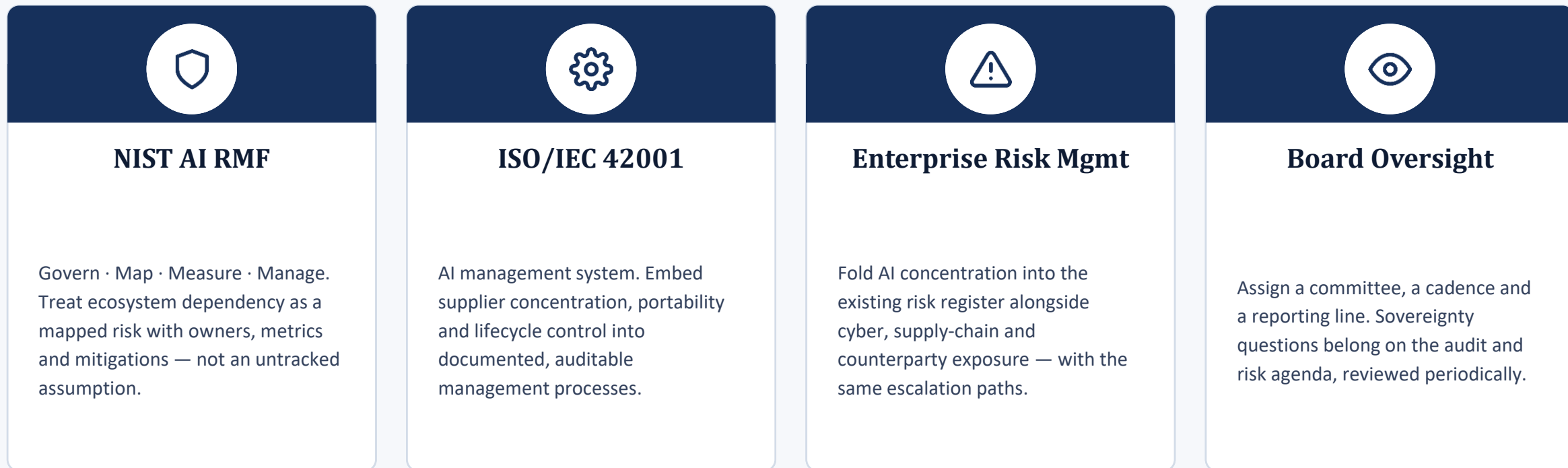
The organization becomes a consumer, not a creator.



Exit

Cost and complexity of switching ecosystems.

Mapping sovereignty to frameworks the board already trusts



The point is not new bureaucracy. It is routing an emerging exposure through governance machinery the organization already operates.

Compute was the scarce asset. Increasingly, it is not.



Proprietary data



Institutional knowledge



Domain expertise



Governance frameworks



Talent



Local context

A country — or company — that owns its data but rents compute can still be sovereign. One that owns compute but not its data, knowledge and models is not.

MATURITY MODEL

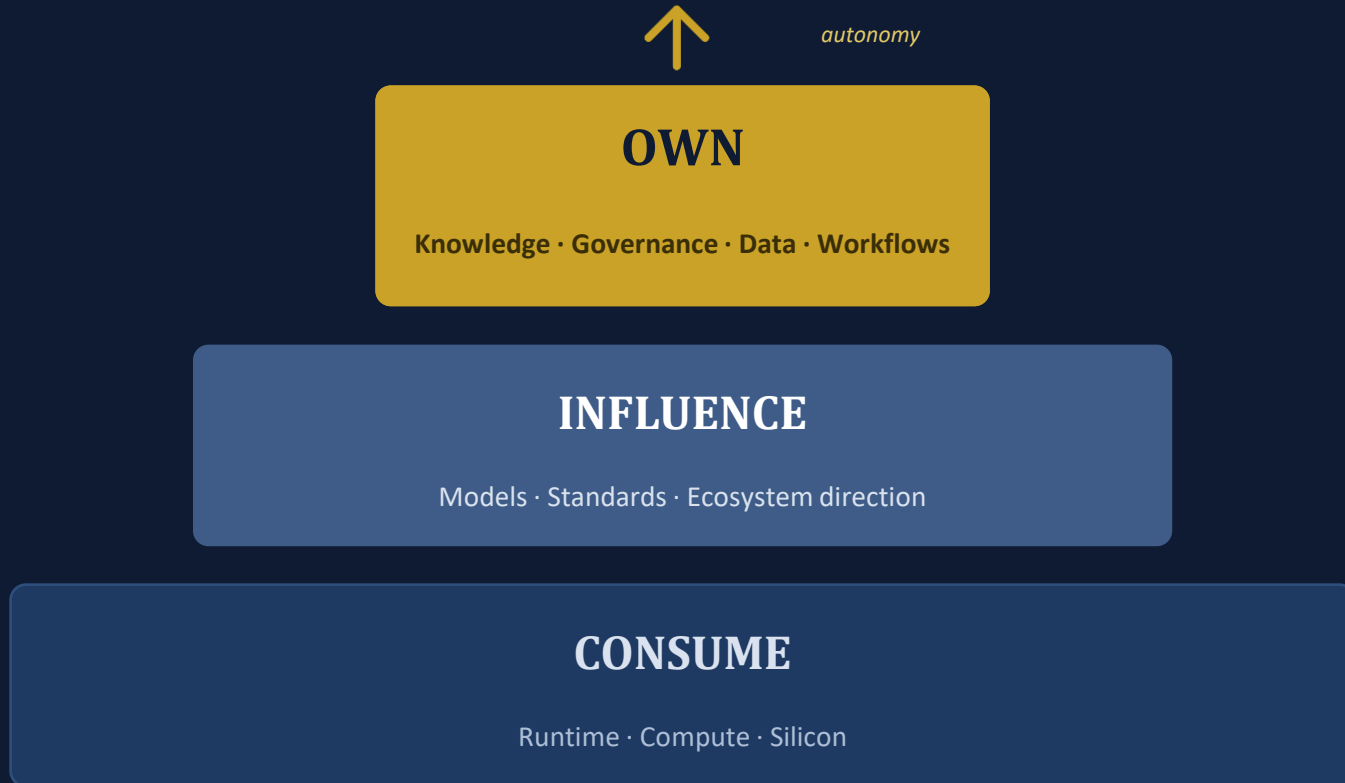
From API consumer to strategic AI autonomy



DEPENDENCY → DECREASES AS MATURITY RISES

THE SIGNATURE EXHIBIT

Own · Influence · Consume



THE PRINCIPLE

The goal of AI sovereignty is not to own every layer.

It is to understand which layers must be owned, which must be influenced, and which can safely be consumed.

Six questions that surface hidden dependency

The objective is not independence from every provider — that is unrealistic. It is preventing dependency from accumulating invisibly across layers.

1

What dependencies exist across data, model, compute, runtime and distribution today?

2

Which of those dependencies are acceptable — and which create strategic exposure?

3

Where is switching realistically possible, and at what cost and time?

4

What portability and multi-sourcing options are in place for each critical layer?

5

Which knowledge and governance assets are genuinely ours and cannot be taken away?

6

If our primary AI provider disappeared tomorrow, what capability would remain under our control?

A fuller 20-question set appears in the appendix.

The Sovereignty Paradox

The organizations most worried about owning infrastructure may be focused on the wrong layer. In every major transformation, value migrated away from the scarce component toward the orchestration built on top of it.

The future winners of AI will not necessarily own the chips. They will own the knowledge, governance, workflows and institutional intelligence those chips enable.

That single question often reveals the true level of AI sovereignty.



THE ONE QUESTION

If our primary AI provider disappeared tomorrow, what capability would remain under our control?

APPENDIX

Board discussion & strategic implications

Twenty board questions · investment, procurement, regulatory and exit implications

Twenty questions for the board

STRATEGY	PROCUREMENT	REGULATORY	EXIT & RESILIENCE
1 Where does strategic dependence migrate as the stack consolidates? 2 Which layers are core to our differentiation? 3 Are we becoming a creator or a consumer of intelligence? 4 What is our multi-year AI autonomy ambition? 5 Who on the board owns this topic?	6 Are contracts structured for portability and exit? 7 Do we avoid single-vendor lock-in on critical layers? 8 Are open-weight options evaluated for each use case? 9 Do we control our fine-tuning data and pipelines? 10 Are pricing and access terms resilient to change?	11 What jurisdictional or export risks affect our stack? 12 Are data residency and governance requirements met? 13 Do we map to NIST AI RMF and ISO/IEC 42001? 14 Is AI concentration on the risk register? 15 Can we evidence oversight to regulators?	16 What is our AI exit strategy per layer? 17 How fast could we switch a critical provider? 18 Which knowledge assets survive a supplier loss? 19 Do we run portability tests or drills? 20 What remains ours if the ecosystem shifts?

What this means for the operating agenda



Investment

Direct capital toward durable assets — data estates, evaluation frameworks, governance and talent — over one-off compute or model bets.



Procurement

Write portability, multi-sourcing and exit terms into every critical contract. Treat open-weight options as a first-class evaluation path.



Regulatory

Map the stack to NIST AI RMF and ISO/IEC 42001; track jurisdictional and export exposure; keep evidence of oversight current.



Exit strategy

Define, per layer, how quickly a provider could be replaced and what would survive the switch. Rehearse it before you need it.



A Point of View on AI Sovereignty

Vendor-neutral · Prepared for boards, CIOs, risk committees, regulators and sovereign-AI programs

This document is a strategic perspective for discussion. It does not constitute an endorsement of, or position against, any named provider.

LET'S CONTINUE THE CONVERSATION

Bring the sovereignty lens to your board



Vivikta Advisory & Creatives

Viivek Mahendrra

Advisory · Governance · Enterprise Architecture Advisory · AI Led Transformation



vivek@vivikta.net



www.vivikta.net

Request the full deck at www.vivikta.net