Exit-Capable by Design

Vendor Concentration Is a Sovereignty Risk

SANJEET KUMAR

Enterprise Architecture & Technology Governance

Critical Infrastructure
Sovereign Digital Resilience
AI Governance

sanjeetkumar.com

Exit-Capable by Design: Vendor Concentration Is a Sovereignty Risk

Sanjeet Kumar — Enterprise Architecture & Technology Governance Leader *Critical Infrastructure ·Sovereign Digital Resilience ·AI Governance — July 2026. Views are the author's own.*

Two decades ago I sat adjacent to the debates of The Open Group's Jericho Forum — co-authoring papers with a founding member on "de-perimeterisation," the then-heretical idea that the network boundary was dissolving and security had to move to the data and the transaction. The industry eventually renamed that idea Zero Trust. I've carried one conviction from those rooms ever since: **the perimeter you should worry about is never only the network one.**

Today the perimeter quietly dissolving is *commercial*. Critical systems — registries, payment rails, government platforms — increasingly depend on a small number of hyperscale and specialist vendors, and that concentration is a sovereignty problem wearing a procurement badge. A jurisdiction whose system of record can only run, or only be understood, inside one supplier's ecosystem has ceded a measure of control no data-residency clause can recover. Foreign-access laws, licensing changes, product sunsets, acquisitions, sanctions regimes: any of these can reach your crown jewels through the vendor relationship, entirely legally, without a single packet crossing your firewall.

The architectural response I practice and advocate is **exit-capability as a design requirement** — resilience expressed as the permanent, tested ability to leave:

Decouple the record of authority from the platform of convenience. Authoritative data lives in open, documented formats; the vendor's value-add operates on top of it, never as the sole means of interpreting it. If your system of record is only legible through the vendor's software, the vendor owns your record in every way that matters.

Make the exit path a maintained artefact. An exit plan written at contract signing and never touched is theatre. Exit-capability means the migration path is documented, cost-estimated, and periodically exercised — treated like disaster recovery, because that's what it is: recovery from a *commercial* disaster.

Measure concentration deliberately. A technology heatmap that maps capabilities to platforms makes concentration visible and disciplinable: which critical functions share one vendor, one region, one licensing regime? Multi-year roadmaps and disciplined decommissioning then become the instruments that *reduce* the number — modular design, one retirement at a time. Simplification is not cost-cutting; it is de-risking with a budget line.

Extend the lens to AI immediately. Model dependencies are the fastest-forming concentration risk in the enterprise today. An organization whose workflows assume one proprietary model family — its behaviours, context formats, and pricing — is rebuilding the vendor lock-in of the 1990s at the cognition layer. The same disciplines apply: abstraction at the interface, portable context, and a tested answer to “what if we had to switch models in a quarter?”

None of this is anti-vendor. Great suppliers are leverage; the objective is a relationship where *both* parties know you could leave — which, not incidentally, is also when pricing and service are at their best. Sovereignty was never about isolation. It is about retaining the option to choose, at every layer: network, data, jurisdiction — and vendor.

De-perimeterisation taught us to stop trusting the network boundary. Its modern corollary: stop trusting the commercial one.