# DIGITAL ATMANIRBHARTA

## Why cloud sovereignty will define the next decade of Indian enterprise strategy

## Executive summary

**The future of Indian enterprise won't be written in margins of efficiency but in margins of control.**

- Control over data
- Control over infrastructure
- Control over legal jurisdiction

**The pillars of Digital Atmanirbharta**

In the past year alone, Indian businesses have watched unsettling headlines roll in. Tariff wars that disrupted global tech supply chains. Sanctions that forced major cloud service providers to halt services due to foreign policy pressures. Export restrictions on GPUs stalling AI development. All this while they were told their cloud was 'secure.' It's a reminder of why India must strengthen its Swadeshi cloud capabilities.

What became clear? **Compliance doesn't equal control.** A data residency clause means little if the control plane lives in another country. Encryption is moot if foreign courts can demand access to your data. And contracts won't help if your provider's operations are bound by laws that supersede your own.

This isn't a debate about technology, it's a call for strategic clarity. This paper outlines why **sovereign cloud is no longer optional,** shows where current models fall short, and helps leaders ask the right questions to stay protected, prepared, and in control.

# 1. When your cloud crosses borders: The legal minefield no one talks about

Most enterprises assume their data is safe as long as it resides in India. But here's the catch: **where data is stored isn't the same as where it's controlled.**

Consider this: if your CSP is headquartered in another country, it's subject to that nation's laws, even if your data never leaves Indian soil. If a foreign court subpoenas your data or mandates service suspension, you may have no legal recourse, even if you're fully compliant under Indian law.

This is not fiction. It has happened and continues to happen. And it leaves Indian enterprises exposed to **digital disruption without warning.**

This legal asymmetry isn't just a theoretical risk -it's an operational one. From BFSI to manufacturing, contracts are being revisited in boardrooms across the country, asking: **What happens if our provider becomes a liability, not an enabler?**

# 2. The silent risk in your cloud contracts

*What your legal team signed could become your biggest digital liability.*

When was the last time you, or your board, reviewed the fine print of your cloud service agreements?

For most enterprises, cloud contracts are viewed as operational rather than strategic. They're signed, filed, and forgotten. But within these clauses lie the roots of future disruption. Seemingly standard terms around "jurisdiction," "termination," and "force majeure" can grant your provider the unilateral power to suspend access to critical workloads - sometimes without recourse.

Take a typical situation: a cloud provider governed by a foreign nation's laws is asked to comply with an external sanction. Even if your business operates entirely within Indian borders, your data, access, or services could be impacted overnight - not due to a breach, but due to geopolitics.

This is not a paranoid scenario; it's a **boardroom blind spot**. Cloud service contracts drafted years ago under the assumption of global harmony are now misaligned with today's fractured, sanction-heavy world.
And yet, few CIOs have made these agreements a risk category. It's time they did. Because compliance does not prevent disruption - **contractual clarity does**.

## Decision lens

**What should CXOs be asking?**

01 Is our cloud contract governed by Indian law or foreign jurisdiction?

02 Do we retain operational control if services are suspended due to sanctions?

03 Who owns the encryption keys and who can be compelled to surrender them?

04 Can we enforce our SLAs in Indian courts if service is disrupted?

05 What's our exit strategy and how fast can we migrate workloads if needed to sovereign CSPs?

# 3. Rethinking cloud decisions through the lens of sovereignty

*Not all data is equal and neither should be its treatment.*

One-size-fits-all cloud strategies are convenient, but they're also increasingly risky.

The modern organisations handles data that ranges from public-facing assets to highly confidential operational intelligence. Yet, many organisations fail to tier their workloads based on sovereignty risk, treating a product catalog the same as financial ledgers or PII-rich AI training data.

The real problem? **Data classification hasn't caught up with deployment speed.** In the rush to modernise, enterprises often prioritise scale, speed, or cost and overlook the sovereignty implications of where their most critical workloads reside.

This oversight becomes acute during disruptions: A compliance audit, a government request, or even a service blackout caused by overseas intervention. That's when enterprises realise they've handed over the keys to systems they assumed they controlled.

It's time cloud selection became a board-level decision, not a procurement checklist.

## Decision lens

**Are you in control of what matters the most?**

01 Have we classified our workloads by sovereignty sensitivity?

02 Which applications are "compliance-critical", and where do they run today?

03 Does our CSP have the legal right to deny access due to foreign laws?

04 Is our metadata managed within Indian jurisdiction?

05 Do we conduct regular reviews of where our critical workloads sit—and why?

# 4. When AI meets sovereignty: why it gets even more critical?

*Your future models are only as free as the infrastructure they depend on.*

Artificial Intelligence isn't just another workload. It's the new digital backbone of enterprise decision-making. From fraud detection and patient diagnostics to LLM-driven service automation, AI models are rapidly becoming central to competitive advantage.

But with this centrality comes a **new vulnerability.**

Training these models often involves massive compute (think GPUs), access to sensitive internal data, and integration with open-source or proprietary platforms. And if any of these dependencies are controlled by external jurisdictions, you've inadvertently exported your innovation pipeline.

Imagine:

- A GPU embargo halts your training mid-way.
- A foreign audit demands access to your training data.
- Your RLHF datasets can't be used because they reside outside sovereign bounds.

This isn't alarmism. It's already impacting enterprises building AI pipelines in strategic sectors.

If data is the new oil, then AI is the engine. And **you don't want to build that engine on someone else's chassis.**

The solution? Prioritise sovereign AI infrastructure that's locally hosted, jurisdictionally compliant, and built for scale. Cloud, data, compute, and governance - all on your terms.

## Decision lens

### Is your AI stack truly yours?

01 Is our AI infrastructure built on platforms governed by Indian law?

02 Where are our GPU and model training dependencies hosted?

03 Could sanctions or foreign audits disrupt our AI initiatives?

04 Are our model weights and training data fully controlled within Indian jurisdiction?

05 Do we have a sovereign fallback if external AI services become inaccessible?

# 5. Conclusion: Sovereign cloud is not a niche. It's the new mandate

The era of globalised cloud adoption - built on political stability and guaranteed access - is over. Today's reality demands a shift in mindset: from availability to assurance, from location to jurisdiction, and from cost to continuity.

India has already demonstrated digital sovereignty through platforms like Aadhaar, UPI, and ONDC - secure, inclusive, and autonomous systems built by India, for India. Yet, when it comes to cloud and compute, many Indian enterprises still depend on infrastructure legally and operationally controlled beyond our borders.

This creates a critical vulnerability: your customer data may sit in Mumbai, but the access layer could be governed from California or Dublin. Your IP might be yours, but your compute operations remain exposed to foreign policy risks outside your control.

Sovereign cloud is not about nationalism - it's about ensuring operational continuity, protecting AI and data infrastructure, and safeguarding your future from external forces.

Every transformation, AI, or cloud strategy discussion must now factor in a fourth variable: **control.** For sectors like BFSI, healthcare, and defence, the decisions made today will determine whether India's digital future is one of strength and resilience—or one of dependency. The choice is not just technical; it's strategic.

## Decision lens

**What should be your next step?**

01 Have we defined a sovereign cloud strategy at the board level?

02 Are we proactively reducing dependency on non-Indian legal entities?

03 Are our risk registers updated to include sovereignty disruption?

04 Is there a business continuity plan tied to jurisdictional risk?

05 Which workloads can be migrated to sovereign platforms in the next 6-12 months?

# Tata Communications Vayu Cloud

## Powering India's Digital Atmanirbharta with a Swadeshi cloud advantage

At Tata Communications, we see sovereignty not as a regulatory tick-box, but as the very foundation of resilience, trust, and long-term competitiveness.

Our Cloud brings this belief to life - resilient by design, sovereign by architecture, and aligned with national priorities that will shape our shared digital future. In doing so, it embodies the vision of a truly **Swadeshi cloud.**

**It is built on a Control-Comply-Continue framework:**

### Control

Every layer of the stack, from the control plane to operational processes, remains fully within Indian jurisdiction. Monitoring signals, metadata, and logs stay in-country. Physical access is restricted to authorised local personnel, with governance reinforced by full audit rights.

### Comply

MeitY-empanelled, STQC-audited, RBI-compliant, and aligned with PCI-DSS, HIPAA, GDPR, and ISO standards. Compliance is treated as a living discipline that adapts to evolving regulatory landscapes, not a one-time checklist.

### Continue

Designed for continuity without dependence on foreign-controlled infrastructure. Disaster recovery is anchored in-country, with failover-ready nodes across seismic zones to ensure uninterrupted operations - even amid sanctions, geopolitical instability, or cross-border disputes.

This is sovereignty by design - proving that the highest localisation and jurisdictional safeguards can be achieved without compromising performance, flexibility, or innovation.

It is the path to an independent, future-ready India
**Digital Atmanirbharta powered by your own Swadeshi cloud - Tata Communications Vayu.**

vayu | Cloud

**For more information, visit us at www.tatacommunications.com**

CONTACT