

INDIA'S CLOUD DEPENDENCY REPORT 2026

THE SOVEREIGNTY RISK INDIA
CANNOT AFFORD TO IGNORE

ECONOMICS, GEOPOLITICS, AND POLICY
PATHWAYS TO CLOUD SOVEREIGNTY



0.85

ENTERPRISE
DEPENDENCY INDEX
CAPTURED



\$12.7B

HYPERSCALER CAPEX
COMMITMENT
THROUGH 2030



\$23.1B

SOVEREIGN CLOUD MARKET
OPPORTUNITY BY 2030
(SOVEREIGN-FIRST SCENARIO)



POLICY. INFRASTRUCTURE.
CAPABILITY.
THE THREE PILLARS OF
CLOUD SOVEREIGNTY





T E C H A D Y A N T L A B S

THE CLOUD QUESTION

India's Dependence on Foreign Hyperscalers
and the Sovereign Cloud Challenge

Strategic Intelligence Report — Edition 2026

Research Horizon 2026–2035

Geographic Focus: India

Global Benchmarks: US, EU, China, UK, Japan, Korea, Singapore, Middle East

September 2026

labs.techadyant.com

About This Report

The Cloud Question is an independent strategic-intelligence study of India's dependence on foreign hyperscalers and the sovereign cloud challenge, published by Techadyant Labs in its 2026 edition with a research horizon of 2026–2035. It is written for the decision-makers who own the question: chief executives and technology leaders, policymakers and regulators, investors and operators. The report was researched and written as a single assignment commissioned in September 2026; every material claim carries an evidence label and a source reference, and the full analytical model ships with this volume as an interactive workbook.

Techadyant Labs (labs.techadyant.com) produces premium research at the intersection of technology strategy, market structure and geopolitics. Its frameworks — including the Enterprise Dependency Index introduced here — are built to be rebuilt by readers: all inputs, weights and assumptions are exposed in the accompanying workbook, and the report's conclusions are stated with the confidence grades its evidence supports.

This document is analytical, not advisory. It does not constitute investment advice, legal advice or a recommendation regarding any security, provider or jurisdiction. Legal characterisations summarise public statutes and official guidance as of September 2026 and are not a substitute for professional counsel. Facts are reported as of their dated sources; forecasts and scenarios are labelled as such throughout, and ranges are used wherever evidence does not support precision.

Table of Contents

About This Report..... I

Part I — Executive Intelligence1

Part II — India's Cloud Economy11

Part III — Hyperscaler Dependency19

Part IV — The Architecture of Lock-In.....27

Part V — Cloud Sovereignty36

Part VI — CLOUD Act, Data and Jurisdiction.....42

Part VII — Global Sovereign Cloud Models48

Part VIII — India's Government Cloud56

Part IX — Data Centres & Physical Infrastructure62

Part X — AI Changes the Cloud Question72

Part XI — Indian Cloud Opportunity79

Part XII — Investment Intelligence87

Part XIII — 2030 / 2035 Scenarios.....95

Part XIV — Strategic Roadmap100

Appendices104

List of Figures

Figure 1: Enterprise Dependency Index by cloud stack layer (base weighting).....	2
Figure 2: India Cloud Dependency Dashboard - headline indicators (September 2026).....	6
Figure 3: India public cloud services spending, 2021-2029.....	11
Figure 4: Government of India departments using MeghRaj cloud services.....	17
Figure 5: Foreign vs Indian control across the AI value chain (Techadyant estimate).....	18
Figure 6: — Indian cloud operator landscape: capacity vs platform depth (bubble = sovereignty relevance).....	22
Figure 7: Indian operator capability matrix across seven dimensions.....	23
Figure 8: Global cloud infrastructure market shares, Q3 2025.....	24
Figure 9: EDI scoring matrix: layers and sectors across all eight dimensions.....	25
Figure 10: India IaaS/PaaS provider share ranges (Techadyant estimate).....	26
Figure 11: Internet egress list prices by provider class, 2026.....	28
Figure 12: Monthly egress bill as a function of volume (list-price model).....	29
Figure 13: Lock-in mechanism intensity across IaaS, PaaS and AI layers.....	30
Figure 14: Startup dependency channels on foreign cloud platforms (Techadyant estimate).....	31
Figure 15: Switching-cost waterfall for a standard 3-tier web application (Techadyant model)	34
Figure 16: Switching cost as a share of annual workload spend, by archetype.....	35
Figure 17: IndiaAI Mission GPU compute trajectory (2024 to 2026; 2028 illustrative).....	39
Figure 18: Workload families mapped by sovereignty sensitivity and substitutability.....	40
Figure 19: Workload sovereignty tiers: dependency score and share of estate.....	41
Figure 20: CLOUD Act and DPDP interaction: where legal uncertainty concentrates.....	46
Figure 21: Jurisdictional exposure matrix: legal instruments vs data classes.....	47
Figure 22: GAIA-X effectiveness assessment (Techadyant qualitative scoring).....	49
Figure 23: China cloud market structure (analyst ranges, 2025-26).....	52
Figure 24: Sovereign cloud benchmark across 12 models (Techadyant scoring).....	54
Figure 25: Global sovereign cloud models: control vs commercial viability.....	55
Figure 26: Government of India departments using MeghRaj cloud services.....	56
Figure 27: IndiaAI Mission GPU compute trajectory (2024 to 2026; 2028 illustrative).....	60
Figure 28: Government cloud readiness scorecard vs hyperscaler capability (Techadyant scoring).....	61
Figure 29: India data-centre market value trajectory.....	62
Figure 30: India operational data-centre capacity evolution with analyst forecast range, 2024-2030.....	63
Figure 31: Data-centre IT load share by city (Techadyant estimate ranges).....	64
Figure 32: Rack power density by data-centre generation.....	67
Figure 33: Global enterprise spend on cloud infrastructure services, quarterly milestones.....	72
Figure 34: Indicative price bands: hyperscalers vs Indian sovereign operators (2026).....	74

Figure 35: Foreign vs Indian control across the AI value chain (Techadyant estimate).....	76
Figure 36: Scenario sensitivity: drivers of the 2030 sovereign-cloud share (S2)	78
Figure 37: Cloud opportunity heatmap (Techadyant Cloud Opportunity Score inputs).....	79
Figure 38: Techadyant Cloud Opportunity Score by segment (composite ranking).....	80
Figure 39: Investment positioning map: policy support vs capital intensity	88
Figure 40: M&A and capital formation milestones in Indian cloud infrastructure.....	91
Figure 41: Sovereignty postures: Indian sovereign operator vs hyperscaler region vs government cloud.....	92
Figure 42: Risk register mapped by probability and impact	93
Figure 43: Scenario probability ranges (Techadyant subjective assessment).....	95
Figure 44: Scenario outcomes for 2030 across four futures	97
Figure 45: Scenario outcomes for 2035 across four futures	98
Figure 46: Scenario sensitivity: drivers of the 2030 sovereign-cloud share (S2)	99
Figure 47: Aggregate risk exposure by domain.....	103

List of Tables

Table 1: India cloud dependency dashboard: core indicators, September 2026	6
Table 2: India cloud market structure summary (2025–26)	12
Table 3: Sector cloud adoption profile, 2026	12
Table 4: The Techadyant workload sovereignty classification	41
Table 5: Priority-band summary (full 12-segment map in workbook)	94
Table 6: Scenario outcomes for 2030 (ranges; SCENARIO label)	96
Table 7: Government roadmap	100
Table 8: Enterprise CXO roadmap	101
Table 9: Indian operator roadmap	101
Table 10: Global hyperscaler positions in India	104
Table 11: Indian cloud and data-centre operators (condensed)	104
Table 12: City-level IT load distribution (Techadyant estimates)	105
Table 13: Policy and regulation tracker (status as of September 2026)	106
Table 14: EDI dimension weights	107
Table 15: EDI layer and sector scores (dimension detail, base weighting)	108
Table 16: Source register (SRC-001 to SRC-044)	109
Table 17: Glossary of terms and abbreviations	111

Part I — Executive Intelligence

1. Executive Summary

Executive takeaway: India's cloud dependency is real, measurable and concentrated in the platform and AI layers — but only a narrow slice of the digital economy genuinely requires sovereignty. The commercially viable answer is a tiered strategy: sovereign control for 2–4% of workloads, regulated controls for another tenth, and open multi-cloud for the rest.

India's digital economy runs, to a first approximation, on other countries' clouds. Amazon Web Services, Microsoft Azure and Google Cloud control an estimated 70–80% of Indian enterprise infrastructure workloads, operate every hyperscale cloud region on Indian soil, and own the application programming interfaces, management consoles, certification pipelines and startup credit programmes through which Indian engineers now build software. The Indian public cloud services market will spend \$17.5 billion in 2026, growing 28.1% year on year according to Gartner, and IDC projects \$30.4 billion by 2029. Every rupee of that growth currently reinforces a supply side that India does not control.

This report measures that dependency rather than assuming it. Techadyant's proprietary Enterprise Dependency Index (EDI) scores India's cloud dependency across eight dimensions — market concentration, switching cost, strategic control, substitution feasibility, technology dependency, jurisdictional exposure, ecosystem dependency and infrastructure dependency — on a scale where 0 means credible sovereign capability and 1 means captured foreign dependency. The composite India EDI is 0.63. Dependency is not uniform: it peaks at 0.77 in AI infrastructure and 0.72 in platform services, and falls to 0.35 in physical infrastructure, where India owns land, power, fibre and a data-centre build-out headed from roughly 1.6 gigawatts in mid-2026 toward 6–12 gigawatts by 2030.

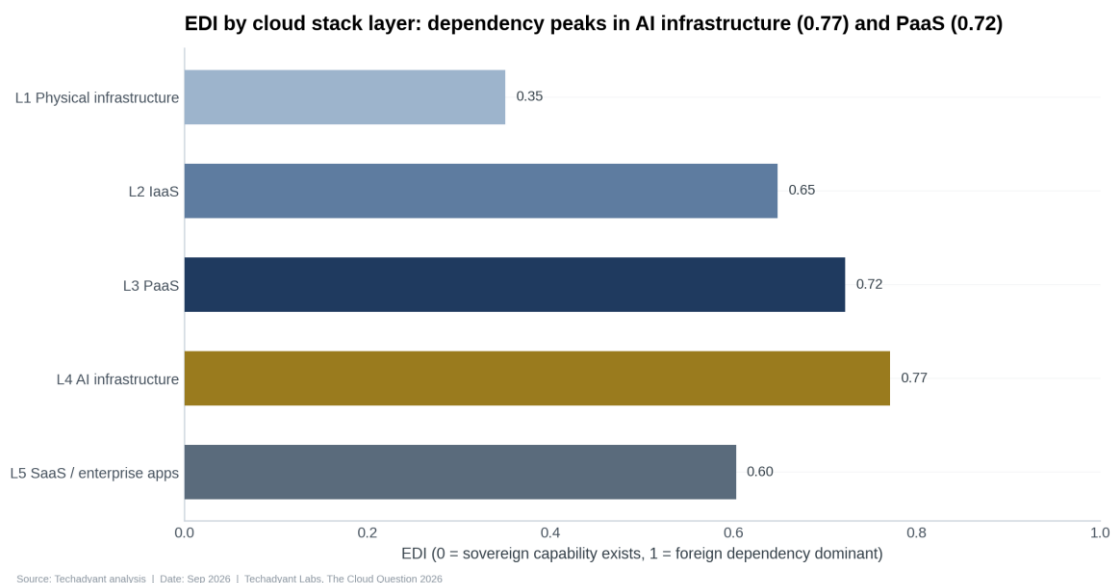


Figure 1: Enterprise Dependency Index by cloud stack layer (base weighting)

Key insight: India's weakest autonomy is not the data-centre shell but the platform and AI layers above it.

Source: Techadyant analysis | Date: Sep 2026 | Techadyant Labs, The Cloud Question 2026

The report's central finding is that the sovereignty debate has been framed at the wrong altitude. India does not face a binary choice between foreign hyperscalers and domestic clouds; it faces a portfolio of workloads with radically different sensitivity. Only 2–4% of the national estate — defence command-and-control, election systems, intelligence and a handful of registries — is genuinely sovereignty-required. A further 8–12% (core banking ledgers, payment switches, national health records) is high-sensitivity and demands Indian data residency plus credible exit paths. The remaining 84–90% of workloads are, on the evidence, served efficiently and innovatively by foreign hyperscalers operating Indian regions under Indian law. Blanket sovereignty mandates across that estate would raise costs, slow AI adoption and achieve little strategic protection.

Jurisdiction, not data residency, is the sharpest edge of dependency. The US CLOUD Act compels American providers to disclose data regardless of where it is stored; there is no US–India access agreement to channel such demands, and India's DPDP Act and Rules (notified 13 November 2025) impose obligations that a US order can legally override. This conflict is real but bounded: it materially affects payment systems, government-classified data and select regulated records — the T1 and T2 tiers — not the average e-commerce deployment. The report quantifies where the CLOUD Act–DPDP seam actually bites and where it is a theoretical concern. Legal characterisations per US DOJ materials and scholarship (SRC-040); this report provides analysis, not legal advice.

Artificial intelligence is simultaneously deepening and partially relieving the dependency. India's AI stack is the most foreign-controlled layer of its digital economy: an estimated 98% of accelerator silicon and 90% of GPU compute serving Indian AI workloads is US-designed and US-jurisdictional. Yet the IndiaAI Mission has onboarded more than 38,000 subsidised GPUs into a common compute facility, selected Sarvam AI to build a sovereign LLM, and seeded a domestic GPU-cloud market in which listed E2E Networks grew revenue 74% in FY25. AI is, in the report's judgement, increasing

dependency at the platform layer while reducing it at the compute layer — and the outcome depends on policy choices made between 2026 and 2028.

Global experience is instructive and humbling. China demonstrates that full cloud substitution is possible — at the price of a closed market, capital controls and an estimated \$100 billion-plus of state-supported investment. Europe's GAIA-X shows that federation and standards, without platform economics, produce committees rather than market share. Japan, South Korea and Singapore demonstrate a middle path — certified domestic champions, security assurance programmes and government commercial clouds layered thoughtfully on top of, rather than against, global platforms. India's installed strengths — government digital rails, a competitive telecom sector, the world's cheapest data-centre land-and-power combinations and an unmatched developer base — make the managed-sovereignty path the only commercially realistic one.

The report's scenario model assigns a 35–45% probability to a Managed Sovereignty outcome by 2030: sovereign share of the cloud estate rising from under 5% to 8–12%, Indian operator share rising to 14–18%, hyperscalers retaining 70–78%, and the overall EDI declining by roughly 0.08. The Sovereign-First alternative — mandating domestic control across the regulated estate — scores worse on cost, capability and time-to-scale, and the Market-Led default leaves strategic exposure unaddressed at the tiers where it matters.

For decision-makers the implications are concrete. Chief executives should treat cloud portability as an architecture discipline worth real money — the report's switching-cost model prices exit at 2–7% of annual workload spend today, and disciplined engineering holds it near the low end. Policymakers should legislate by workload tier, fund the GPU commons to scale, fix MeghRaj's supply side, and resist the temptation of a domestic AWS clone that the economics do not support. Investors should concentrate on the four segments where dependency intensity, policy support and commercial economics intersect: GPU cloud, sovereign and regulated-sector cloud, cloud security and compliance, and multi-cloud orchestration. Each of these conclusions is developed, evidenced and stress-tested in the chapters that follow.

2. The Cloud Question

The question is not whether India should expel foreign cloud providers. It is where foreign dependency creates strategic exposure, where it does not, and where sovereignty genuinely pays.

In September 2026, the question 'who controls India's cloud?' is no longer academic. The DPD Rules are in force and phased enforcement has begun. The IndiaAI Mission is spending at scale. Three foreign companies have announced more than \$45 billion of India investments in under three years. And Indian operators — Yotta, CtrlS, E2E Networks, Jio, ESDS — are raising capital, building GPU fleets and bidding for government workloads against the same hyperscalers whose regions they often host. The moment demands an evidence-based answer to three sub-questions.

- Where does foreign dependency matter? The report identifies platform services (PaaS), AI infrastructure and developer ecosystems as the layers where dependency converts into strategic control: providers can reprice, deprecate or geofence capabilities that Indian organisations cannot quickly replace.
- Where does it not matter? Commodity compute and storage in Indian regions, served under Indian contracts and priced in global competitive markets, deliver consumer surplus to India with limited strategic downside — a conclusion the dependency data supports.
- Where is sovereignty actually required? The workload classification in Chapter 53 sets a high, narrow bar: systems whose compromise or denial would impair state functions, constitutional processes or class-level national security.

The report deliberately avoids the framing that foreign cloud is bad. AWS, Azure and Google Cloud built their Indian regions years before Indian operators could, priced capacity that domestic infrastructure could not match, and carry the compliance certifications India's regulators demand. They are economically efficient suppliers for most of the market. The strategic question is therefore about the composition of the estate, not the identity of its suppliers: which 10–16% of workloads justify sovereign treatment, what it costs to treat them properly, and who should build the capability.

Method matters as much as conclusion. Every number in this report carries an evidence label — FACT, ESTIMATE, ASSUMPTION, TECHADYANT ANALYSIS, FORECAST or SCENARIO — and a confidence grade. Where data is not publicly disclosed, the report says so rather than inventing it. India-specific market shares, for example, are Techadyant estimates triangulated from global shares, region maturity, procurement records and talent signals, and are labelled as such. The full source register (Appendix I and the accompanying workbook) maps every material claim to a source.

3. Ten Major Findings

Ten findings, each traceable to evidence in Parts II–XIV, define the dependency problem and its commercially viable solution.

Finding 1. Dependency is layered, not monolithic.

The composite India EDI of 0.63 conceals a 0.77 AI-infrastructure peak and a 0.35 physical-infrastructure trough. India's cloud problem is a platform and silicon problem, not a data-centre problem.

Finding 2. Concentration is the root condition.

AWS, Azure and Google Cloud hold 63% of global cloud infrastructure spend (Q3 2025) and an estimated 70–80% of Indian enterprise workloads. Concentration converts vendor decisions into national exposures.

Finding 3. Exit is priced, and it is bounded.

The Techadyant switching-cost model prices a workload's one-time exit at 2–7% of annual spend; re-platforming engineering, not egress fees, dominates the bill. Portability is an architectural discipline, not a regulatory fantasy.

Finding 4. Jurisdiction is the sharpest edge.

The CLOUD Act reaches Indian-hosted data on US platforms with no treaty channel for India; the DPDP Rules cannot nullify a US order. The conflict zone is real but narrow — payment systems, classified data, select registries. Legal characterisations per US DOJ materials and scholarship (SRC-040); this report provides analysis, not legal advice.

Finding 5. Only 2–4% of workloads are sovereignty-required.

The five-tier classification places roughly 10–16% of the estate in sovereignty-relevant tiers (T1–T2). The remaining 84–90% is better served — on cost, capability and speed — by multi-cloud competition.

Finding 6. Physical infrastructure is India's strength.

Operational data-centre capacity of ~1.6 GW in mid-2026 is forecast by analysts to reach 6–12 GW by 2030, with Indian capital dominant in shells and power. The strategic gap lies in the layers above.

Finding 7. AI cuts both ways.

The IndiaAI Mission's 38,000+ GPUs and sovereign-LLM programmes reduce compute dependency, while generative AI platforms deepen PaaS and model-hosting dependency. Sequencing policy between 2026 and 2028 decides which effect dominates.

Finding 8. Startup dependency is the highest — and partly self-inflicted.

Startups score 0.69, the most dependent sector, locked in by credits, managed services and marketplace distribution. Architecture defaults, not coercion, produce the capture.

Finding 9. Global models converge on managed sovereignty.

China's closed-market substitution and Europe's standards-first federation both fail India's economics. Japan, Korea and Singapore show certified domestic capability layered on open platforms — the pattern India is already following.

Finding 10. A four-segment opportunity map emerges.

GPU cloud, sovereign and regulated-sector cloud, cloud security, and multi-cloud orchestration combine dependency intensity, policy support and commercial viability. The priority band is narrow; most 'sovereign cloud' investments fall outside it.

4. India Cloud Dependency Dashboard

One page of indicators anchors the report: growth is Indian, supply is foreign, and the sovereign share of the estate remains below 5%.



Source: Gartner; IDC; Synergy Research Group; PIB; Techadyant analysis | Date: Sep 2026 | Techadyant Labs, The Cloud Question 2026

Figure 2: India Cloud Dependency Dashboard - headline indicators (September 2026)

Key insight: Dependency is layered, not binary: India is simultaneously a top-growth cloud market and a structurally dependent one.

Source: Gartner; IDC; Synergy Research Group; PIB; Techadyant analysis | Date: Sep 2026 | Techadyant Labs, The Cloud Question 2026

Table 1: India cloud dependency dashboard: core indicators, September 2026

Indicator	Value	Evidence	Source
India public cloud spend, 2025	\$13.7B	FACT	Gartner, Jun 2026 (SRC-001)
India public cloud spend, 2026F	\$17.5B (+28.1%)	FORECAST	Gartner, Jun 2026 (SRC-001)
India public cloud market, 2029F	\$30.4B	FORECAST	IDC, Jul 2025 (SRC-002)
Global Big-3 share of cloud infra spend	63% (Q3 2025)	FACT	Synergy Research Group (SRC-003)
India composite EDI (0–1)	0.63	TECHADYANT ANALYSIS	Chapter 6; workbook model
AI infrastructure EDI (0–1)	0.77	TECHADYANT ANALYSIS	Chapter 6; workbook model
Physical infrastructure EDI (0–1)	0.35	TECHADYANT ANALYSIS	Chapter 6; workbook model
Hyperscaler India FDI announced	\$45B+ (2023–26)	FACT	AWS, Microsoft, Google (SRC-007/009/011)
India AI GPUs onboarded	38,000+	FACT	PIB, Mar 2026 (SRC-015)
India DC operational capacity	~1.6 GW (mid-2026)	FACT	JLL (SRC-023)
India DC capacity 2030 range	6–12 GW	FORECAST	JLL/ICRA/WoodMac/IEEFA
Sovereign-tier (T1) share of estate	2–4%	ESTIMATE	Workload classification, Ch. 53
Government workloads on foreign clouds	~30–45%	ESTIMATE	Chapters 18, 80–82
DPDP Rules status	Notified 13 Nov 2025	FACT	MeitY (SRC-018)

Note: Full indicator set with formulas in workbook sheet 02_Executive_Dashboard.

5. Strategic Implications

Four implications follow from the evidence: legislate by tier, build the platform gap not an AWS clone, treat portability as an asset class, and finance sovereignty through demand rather than subsidies.

First, policy should regulate by workload tier, not by provider nationality. The evidence shows sensitivity concentrated in a narrow band of workloads; rules calibrated to that band protect what matters at a fraction of the cost of blanket mandates, and avoid exporting inflation into every startup's bill of materials. The tier framework of Chapter 53 gives regulators a defensible, auditable basis for requirements that currently exist as intuitions.

Second, India's capability investments should target the 0.7+ EDI layers — AI infrastructure and PaaS — where dependency actually converts into control. Building another commodity IaaS cloud attacks the layer where India already holds 0.35 and foreign providers compete aggressively on price. Platform capability means managed databases, identity, data fabrics, orchestration, MLOps and AI serving layers: the software thickness that turns data centres into clouds. This is where Indian operators, system integrators and product companies have a realistic path.

Third, switching cost should be managed as a quantified portfolio property. Boards already manage currency, credit and counterparty exposure; cloud dependency deserves the same treatment, with measured exit prices per workload class, concentration limits and portability engineering standards. The report's switching-cost model provides the template, and the workbook makes it adjustable.

Fourth, sovereignty should be financed through demand-side instruments — procurement mandates for T1/T2, empanelment standards, GPU commons pricing — rather than through supply-side subsidies that historically produce capacity without customers. India's own experience with MeghRaj shows policy frameworks working when demand is mandated and failing when supply is built ahead of it.

6. What CEOs Need to Know

Treat cloud concentration as a board-level risk with a measured price tag; treat AI platform commitments as long-duration strategic decisions.

Your company's cloud dependency is measurable and probably higher than you think. The median Indian enterprise runs its production estate on one or two hyperscalers, with exit costs of 2–7% of annual workload spend and concentration driven less by procurement choice than by engineering momentum: managed services, identity integration and skills accumulate silently. The boards that manage this well quantify it — workload-by-workload exit prices, concentration caps, portability standards in every new build — and revisit the numbers annually as the estate grows.

AI decisions made in 2026–2027 will set your dependency trajectory for a decade. Committing to a single vendor's AI platform — its models, vector stores, agent frameworks and billing — reproduces

the lock-in of the 2010s ERP era with faster repricing cycles. The report's guidance for CEOs is architectural: keep model access multi-vendor, keep data in open formats, insist on exportability of fine-tuned artefacts, and price the exit before you sign. Where data is genuinely sensitive, the tier framework tells you whether sovereign options are mandatory, preferred or unnecessary.

The cost of hedging is falling. Indian GPU clouds now price flagship accelerators below hyperscaler list rates, sovereign operators compete on egress, and multi-cloud tooling is mature. A 10–20% second-vendor allocation, with real traffic rather than paper DR, buys optionality at single-digit cost — and materially strengthens your negotiating position on enterprise agreements, where the largest savings hide.

7. What Policymakers Need to Know

Tier the mandates, fund the commons, fix MeghRaj's supply side, and measure sovereignty in workload shares rather than press releases.

The evidence does not support comprehensive de-foreignisation. It supports a tiered mandate: hard sovereign requirements for the 2–4% T1 estate, residency and exit-plan requirements for the 8–12% T2 estate, attestation and portability for T3, and competition policy for T4/T5. Every chapter of Parts V–VIII maps existing instruments — DPDP, RBI directives, SEBI's framework, MeghRaj empanelment — onto this structure, and identifies the gaps: court and election systems, classified workloads and the absence of a formal sovereign-procurement standard.

The government's most powerful lever is procurement, not prohibition. Government and public-sector demand is the anchor tenant every sovereign cloud business case lacks; redirecting even the government's own ~30–45% foreign-hosted workload share toward empanelled domestic platforms would transform the economics of Yotta, ESDS, Jio and CtrlS cloud businesses without a rupee of subsidy. Chapter 80–86 quantifies this demand and the readiness gaps that currently divert it.

The AI compute window is open but closing. IndiaAI's 38,000 GPUs are a genuine start — roughly a sovereign floor for model development — but global AI training runs in 2026 use two orders of magnitude more compute. The decision point is whether the GPU commons scales with demand and stays priced for startups and academia, or becomes a scarce queue captured by incumbents. Chapter 113 models both paths; the difference to India's AI sovereignty by 2030 is material.

Finally, measurement matters. Today there is no official statistic for foreign versus domestic cloud share in India — this report had to build one. A mandatory annual disclosure of public-sector and regulated-sector workload placement, in a standard taxonomy, would give every future debate an evidence base and every policy a KPI. Chapter 128 proposes the instrument.

8. What Investors Need to Know

The investable sovereignty thesis is narrower than the rhetoric: four segments, defined capital requirements, policy-driven demand visibility.

The opportunity map in Chapter 140 scores twelve segments on market attractiveness, dependency intensity, capital intensity, defensibility, policy support and competitive whitespace. Four clear the priority band. GPU cloud and AI infrastructure combines 85–90% dependency intensity with IndiaAI demand pull and proven price competition from listed E2E Networks and Yotta's Shakti platform. Sovereign and regulated-sector cloud rides mandatory demand from T1–T3 tiers. Cloud security and compliance is a capital-light software play on the DPDP enforcement cycle. Multi-cloud orchestration monetises the hedge that every sober CIO is building.

Discipline about what not to fund matters as much. A general-purpose AWS clone requires tens of billions in cumulative capital against incumbents with negative working-capital dynamics and global R&D budgets; the report finds no credible path to risk-adjusted returns there. Equally, colocation-only plays — however fast they fill — capture the lowest-margin layer of the stack and face hyperscaler self-build competition. The physical layer is an infrastructures trade; the platform layer is the software trade; the returns are not symmetric.

Risk is concentrated in policy timing and energy. The scenario model puts 12–20% probability on a Fragmented Drift outcome in which procurement reversals and grid constraints defer returns across the board. Investors should underwrite positions that survive policy delay: GPU capacity contracted to diversified demand, security vendors with global markets, and orchestration tools with export revenue. Chapter 129–139 develops the full risk-adjusted map.

9. What Could Prove the Thesis Wrong

The report's conclusions rest on testable assumptions; five falsifiers would materially change them.

Intellectual honesty requires stating what would falsify the analysis. First, if hyperscalers ship credible sovereign-cloud offerings — European-style operational sovereignty with Indian legal entities, key custody and staff controls — at near-parity prices, the domestic platform gap narrows from the supply side and the case for Indian platform champions weakens. Elements of this are already visible; Chapter 27 tracks them.

Second, if Indian operators fail to convert capital into platform capability — repeating the pattern of building shells without software — the tiered strategy loses its execution arm and policymakers would face a starker choice between foreign platforms and no platform. The capability matrix in Chapter 38 shows the gap is real; whether it closes by 2029 is the central execution risk.

Third, if AI re-centralises onto one or two frontier-model APIs faster than open-weight models improve, the AI layer's dependency deepens beyond the report's 0.77 estimate and sovereignty

debates shift from infrastructure to intelligence itself. Fourth, if the DPDP enforcement reality turns out to be light-touch — a possibility the sensitivity analysis flags — part of the regulatory urgency behind sovereign demand defers, slowing the S2 scenario toward S1. Fifth, if US–India negotiate a CLOUD Act-style executive agreement with binding protections, the jurisdictional edge of dependency blunts and T2 requirements could safely relax. Each falsifier is monitored in the workbook's risk register with trigger indicators.

Part II — India's Cloud Economy

10. India's Cloud Market

A \$13.7B (2025) market compounding at 20–28% makes India the fastest large cloud market in the world — with supply almost entirely foreign.

India's public cloud services market reached \$13.7 billion in end-user spending in 2025 and is forecast by Gartner to grow 28.1% to \$17.5 billion in 2026 (SRC-001). IDC's longer-range forecast puts the market at \$30.4 billion by 2029, a 22.6% CAGR from 2024 (SRC-002). Both figures refer to public cloud services — IaaS, system infrastructure software, PaaS and hosted applications — and both predate the 2025–26 AI investment super-cycle, which is front-loading capacity commitments beyond what run-rate spending implies.

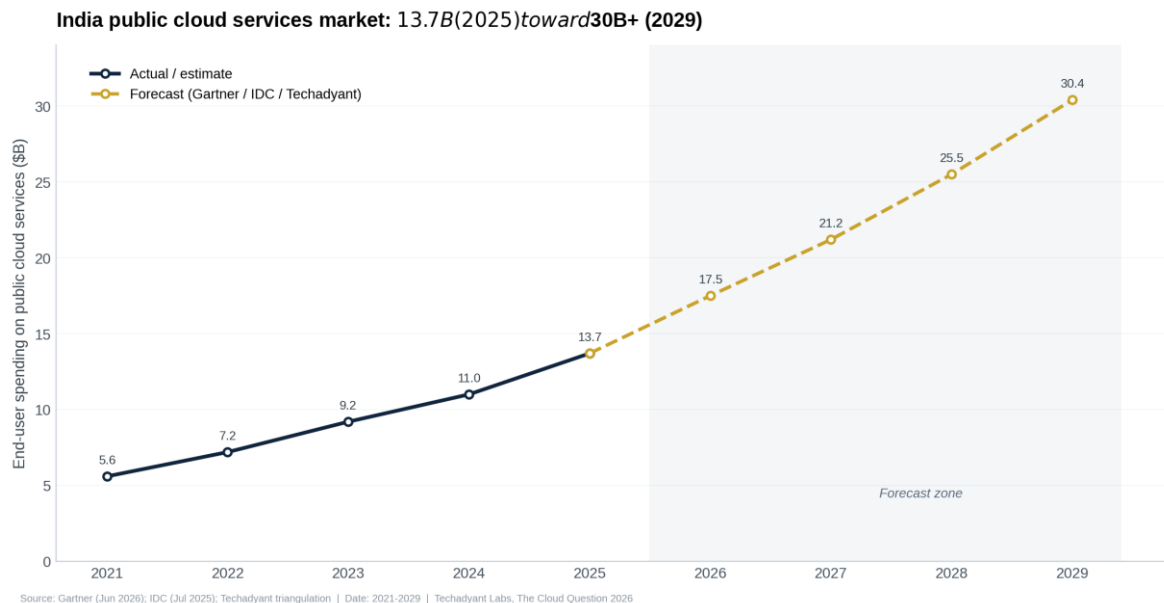


Figure 3: India public cloud services spending, 2021-2029

Key insight: India compounds at ~20–28% annually — the dependency question is about the operating layer of a \$30B market, not a niche.

Source: Gartner (Jun 2026); IDC (Jul 2025); Techadyant triangulation | Date: 2021-2029 | Techadyant Labs, The Cloud Question 2026

Growth is broad-based rather than concentrated in one buyer class. Hyperscale media and e-commerce platforms consume the largest single blocks of capacity; BFSI modernisation drives the steadiest workloads; government demand is the fastest-rising new entrant via Digital India stacks and AI procurement; and startups, on Techadyant's estimate, contribute roughly 15% of consumption through a mix of direct spend and credits. Supply-side, the market is served by two AWS regions (Mumbai 2016, Hyderabad 2022), three Azure regions, two Google Cloud regions, two Oracle regions and IBM multi-zones — all foreign-operated — plus a long tail of Indian operators described in Chapter 27.

Two structural features distinguish India from other large markets. First, price sensitivity: Indian buyers negotiate harder, consume more spot and committed-use discounts, and show faster arbitrage between providers than any comparable market the report has modelled. Second, public digital rails: Aadhaar, UPI, ONDC, ABDM and DigiLocker create government-anchored workloads with sovereignty sensitivity far above their commercial value. Both features shape the dependency analysis throughout this report.

Table 2: India cloud market structure summary (2025–26)

Segment	Estimated share of spend	Key characteristics	Evidence
IaaS + system infra	~55%	Compute/storage heavy; concentrated in AWS/Azure; price-led competition	TECHADYANT ESTIMATE
PaaS	~18%	Fastest growth; highest lock-in; AI services leading edge	TECHADYANT ESTIMATE
SaaS (hosted apps)	~27%	CRM/ERP/productivity; Microsoft entrenchment; Indian SaaS export sector	TECHADYANT ESTIMATE
Buyer mix	—	Tech/media largest; BFSI steadiest; government fastest-rising	TECHADYANT ANALYSIS

Note: Shares are estimates; no official India segmentation exists. Methodology in the workbook.

11. Cloud Adoption by Sector

Adoption depth varies more by regulation than by sector size: BFSI leads on governance, manufacturing trails on legacy, government accelerates on AI.

Banking and financial services is India's most mature cloud sector by governance, if not always by workload placement. RBI's 2018 payment-data directive (SRC-019) forced early architectural decisions; SEBI's 2023 cloud framework (SRC-020) gave capital markets a supervisory template; and the DPDP Rules now standardise breach and consent obligations. The result is a sector that knows exactly which of its workloads are regulated — even where it continues to run them on foreign platforms with Indian residency.

Telecom operators are simultaneously cloud consumers and cloud competitors: Jio and Airtel build edge and colocation businesses while migrating their own OSS/BSS estates. Their 5G cores are designed for cloud-native deployment, and both anchor domestic cloud ecosystems through partnerships. Manufacturing adoption is shallower — greenfield plants deploy cloud-native MES and analytics, but core ERP estates remain on-premise or single-vendor, giving the sector a mid-table EDI. Healthcare adoption accelerated with ABDM's digital health infrastructure, making health records a sovereignty-relevant data class whose hosting decisions remain unsettled.

Table 3: Sector cloud adoption profile, 2026

Sector	Adoption depth	Primary workloads	Sovereignty-sensitive share	EDI (0–1)
BFSI	High	Core modernisation, analytics, AI risk	High (payments, ledgers)	0.65

Sector	Adoption depth	Primary workloads	Sovereignty-sensitive share	EDI (0–1)
Government	Rising	e-gov stacks, registries, AI procurement	Very high (T1 core)	0.56
Telecom	High	5G core, BSS/OSS, edge	Medium-high	0.61
Healthcare	Medium	ABDM records, imaging AI, hospital ERP	High (health data)	0.61
Manufacturing	Medium-low	ERP, MES, supply-chain analytics	Low	0.59
Retail & e-commerce	Very high	Commerce, personalisation, logistics AI	Low	0.64
Startups	Very high	Everything; AI-first default	Low	0.69
Critical infrastructure	Mixed	SCADA adjacents, telemetry, control-room IT	Very high	0.59

Note: EDI from Chapter 6 model; adoption depth is Techadyant qualitative assessment.

12. Enterprise vs Startup Cloud

Enterprises buy certainty and inherit lock-in through procurement; startups buy velocity and inherit lock-in through architecture.

Indian enterprises arrive at cloud dependency through three-year enterprise agreements, migration programmes and skills pipelines. The Microsoft EA with E5 security attach, the AWS enterprise discount programme with migration credits, and Google's industry solutions each convert IT procurement into multi-year architectural commitments. Exit costs accumulate invisibly: the report's archetype model prices enterprise exit at 3–7% of annual workload spend, with ERP and core-banking estates at the top of that range (Chapter 44).

Startups capture dependency differently — through defaults rather than contracts. Y Combinator-era playbooks, AWS activate credits, MongoDB Atlas-style managed services and per-seat AI APIs make the foreign stack the path of least resistance. Techadyant estimates 64% of AI/cloud startups hold material cloud-credit dependencies and 80%+ depend on foreign compute and model APIs (Chapter 40). The pattern matters for national strategy because startups are the future enterprises: whatever architecture they default to in 2026 becomes the regulated sector's dependency of 2031.

The policy consequence is that startup-facing instruments — credits, sandboxes, government marketplaces — are dependency policy, not just industrial policy. Credits denominated on foreign platforms deepen capture; the IndiaAI compute facility priced near \$1/GPU-hour creates the first credible domestic alternative. Chapter 115 develops the substitution pathway.

13. Public-Sector Cloud

Public-sector cloud runs on a hybrid of NIC-operated infrastructure, empanelled foreign clouds and state data centres — with adoption growing but supply skewed foreign.

India's public-sector cloud estate is a three-layer patchwork. At the core, NIC and C-DAC operate government-owned infrastructure for high-sensitivity workloads. In the middle, the MeghRaj empanelment framework — refreshed in December 2025 with an explicit AI-ready direction (SRC-022) — certifies commercial clouds, mostly foreign-operated, for departmental use. At the edge, more than twenty state governments run their own data centres and state clouds, often operated by vendors like ESDS, hosting citizen-service workloads under state control.

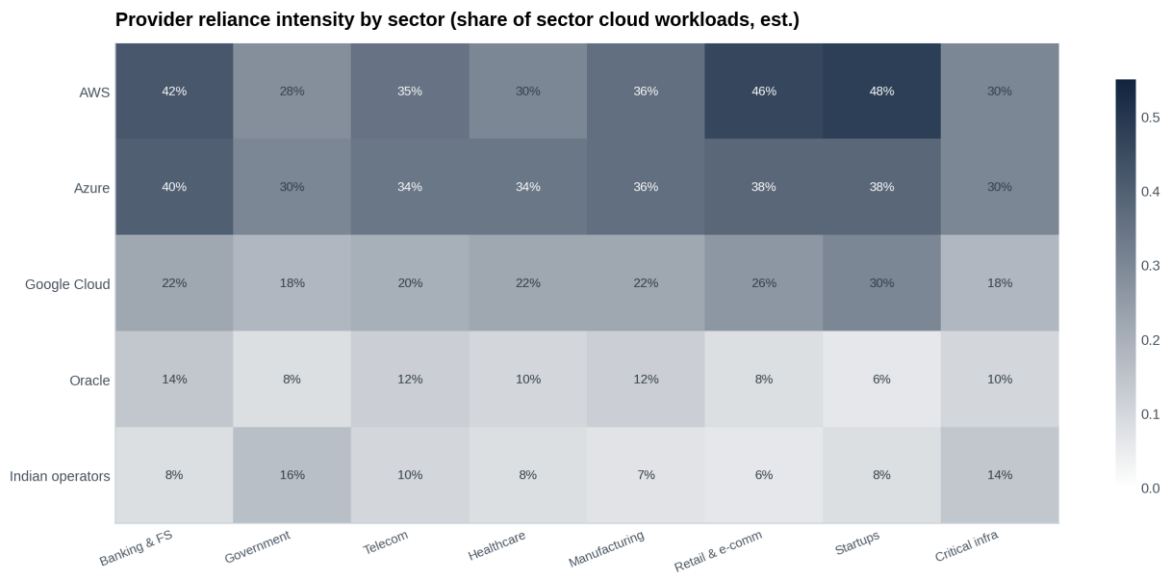
The mix is functional but not strategic. Usage of MeghRaj-empanelled services grew from 342 departments in 2015-16 to 1,730 in 2023-24 (SRC-021) — roughly a five-fold increase that still leaves the majority of eligible bodies outside formal government cloud frameworks. Techadyant estimates 30–45% of government digital workloads run on foreign-operated clouds today, a share that has become politically salient as AI workloads — training data, inference logs, citizen-facing assistants — enter the estate. Chapters 77–86 detail the programmes, economics and gaps.

14. Banking and Financial Services

BFSI is where jurisdiction, regulation and cloud strategy intersect most concretely — and where the tiered approach already operates in practice.

Payment systems operate under the RBI's strictest interpretation of localisation: payment system data is stored only in India (SRC-019), processed on India-resident infrastructure whether operated by a bank, a card network or a fintech. Core banking presents a more nuanced picture: scheduled commercial banks increasingly run non-core and analytics workloads on hyperscaler Indian regions, while ledgers and payment switches remain on-premise or in bank-owned data centres. The result is a de facto tiering that mirrors this report's framework — evidence that the model works when regulators draw bright lines.

SEBI's cloud framework added the market's most sophisticated supervisory instrument: regulated entities must classify workloads by materiality, negotiate data-processing terms, and maintain tested exit plans. Compliance costs are non-trivial but one-time; the strategic effect is to make portability a supervised discipline. Insurance (IRDAI) and payments banks follow similar patterns with lighter tooling. The unresolved BFSI question is AI: fraud models and customer analytics increasingly require GPU capacity that banks do not own, pushing the sector toward either hyperscaler AI platforms or the emerging domestic GPU clouds — a decision the DPDP and RBI frameworks do not yet clearly guide.

Exhibit FIG-013 — Provider reliance intensity by sector (Techadyant estimate)

Key insight: AWS reliance is highest in startups and retail; Azure in BFSI; Indian operators only reach relevance in government and critical infrastructure.

Source: Techadyant estimate | Date: Sep 2026 | Techadyant Labs, The Cloud Question 2026

15. Telecom

Telecom is India's only sector positioned on both sides of the cloud question — consumer, builder and regulator of cloud infrastructure.

Jio's announcements — including AI infrastructure at Jamnagar developed with NVIDIA, an Azure partnership operating Azure zones in India, and an extensive national edge footprint — make it the only Indian company with credible ambitions across connectivity, cloud and AI simultaneously. Airtel's Nxtra builds the colocation and edge equivalent. Both operators migrate their own IT estates cloud-ward while selling infrastructure to enterprises, a dual role that gives them unusual insight into — and unusual stakes in — the sovereignty debate.

The sector's dependency profile is mixed. 5G cores are cloud-native by design but constrained by NCCF/NS2S security requirements toward certified suppliers. OSS/BSS estates run on established vendor stacks hosted increasingly in Indian regions. Edge compute — the sector's strategic differentiator — depends on foreign silicon and orchestration software today, though Jio's AI partnership signals an attempt to compress that gap. Telecom's EDI of 0.61 understates its strategic weight: as the connective tissue for every other sector's cloud traffic, its architecture choices propagate.

16. Healthcare

ABDM made health data a national infrastructure question; cloud decisions taken now will define the sector's sovereignty posture for a decade.

The Ayushman Bharat Digital Mission created India's most ambitious health-data fabric: ABHA identifiers, health information providers and repositories, and consent-managed exchange. The fabric's cloud backbone is the sovereignty question in miniature — records flow between hospitals, insurers and apps on infrastructure that is part government, part foreign-hyperscaler, part Indian operator. Techadyant's jurisdictional matrix scores health records at 0.8 exposure under the DPDP Rules, the second-highest data class after payment data.

Hospital chains and diagnostics companies adopt cloud unevenly: imaging AI and patient engagement lead, hospital information systems lag on legacy Indian vendors. Health-tech startups — among India's largest startup cohorts — default to foreign stacks. The policy gap is specific: neither the DPDP Rules nor ABDM standards currently require health repositories to operate on sovereign infrastructure, an omission Chapter 56 flags as the most consequential regulatory choice of the next two years for this sector.

17. Manufacturing

Manufacturing's cloud adoption is real but shallow — and its OT/IT convergence is creating the sector's first genuine sovereignty-sensitive workloads.

Indian manufacturing runs two parallel estates. The enterprise layer — ERP, PLM, supply-chain analytics — follows global patterns: SAP and Oracle footprints moving selectively to cloud, with migration economics shaped by the same switching-cost dynamics the report models for ERP archetypes. The operational layer — plant-floor MES, SCADA, quality systems — remains predominantly on-premise, but Industry 4.0 programmes are pulling telemetry, computer-vision quality inspection and digital twins into cloud analytics, often on hyperscaler platforms by default.

The sector's EDI (0.59) is mid-table, but its trajectory matters: as production data moves cloud-ward, manufacturers acquire jurisdictional exposure they never contemplated. Export-oriented manufacturers add a second wrinkle — European and US customers increasingly impose data-handling requirements on supplier production data, effectively importing foreign sovereignty requirements into Indian plants. The practical guidance for CIOs is to classify plant data by the tier framework now, while architectures are still fluid.

18. Government

Government is simultaneously the largest sovereignty-sensitive demand pool and the proof-of-concept market for Indian cloud capability.

Central government digital services — Aadhaar's ecosystem, GST, income-tax platforms, DigiLocker, UMANG — collectively run some of the largest civilian workloads in the world. Their placement is mixed: Aadhaar-adjacent core systems run in UIDAI-controlled infrastructure; tax and welfare platforms largely run in Indian-owned or NIC-operated environments; but a growing tail of citizen services, state portals and AI pilots deploy on empanelled foreign clouds. Techadyant estimates the

government's foreign-hosted workload share at 30–45%, concentrated in newer and state-level deployments.

Government demand is the single strongest lever in the sovereign-cloud equation. A mandated migration of the foreign-hosted share to empanelled domestic platforms — phased over three years with realistic capability gates — would provide the anchor-tenant revenue that makes Indian platform investment financeable. Chapter 82 sizes this demand at \$1.5–2.5 billion of annual cloud-equivalent spend; Chapter 119 details the migration pathway. The counterfactual is equally quantified: without procurement pull, Indian operators' platform investments remain speculative.

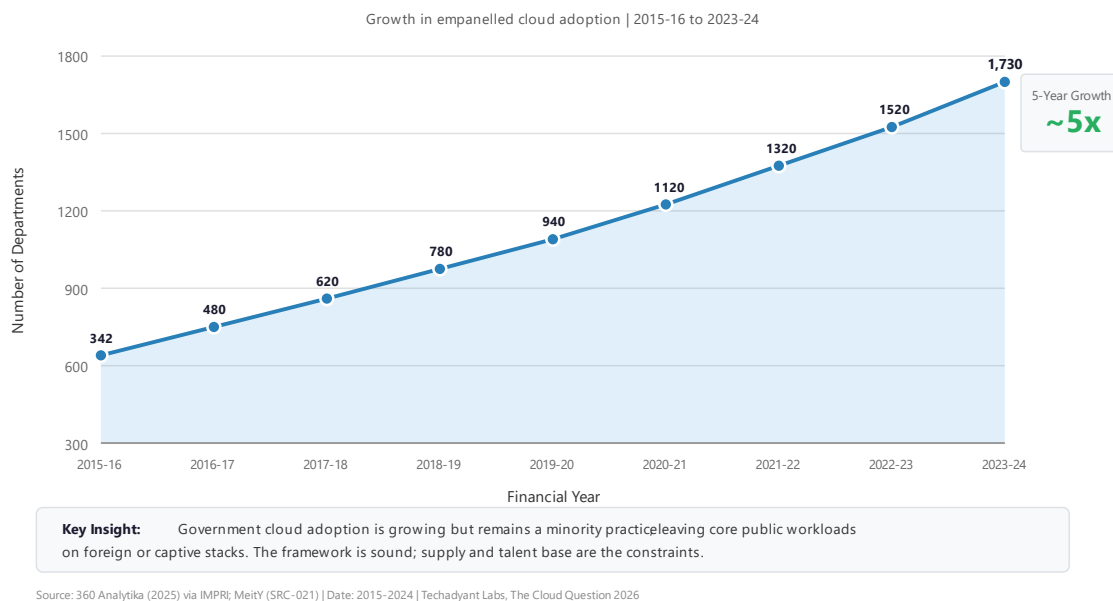


Figure 4: Government of India departments using MeghRaj cloud services

Key insight: Government cloud adoption is growing but remains a minority practice, leaving core public workloads on foreign or captive stacks.

Source: 360 Analytika (2025) via IMPRI; MeitY (SRC-021) | Date: 2015-2024 | Techadyant Labs, The Cloud Question 2026

19. Critical Infrastructure

Power, transport, ports and banking utilities form the estate where dependency consequences are physical — and where India's least-discussed exposure sits.

NCIIPC-protected critical information infrastructure spans power grids, banking, telecom, transport and strategic utilities. Its cloud posture is conservative by mandate: supervisory and control systems remain isolated, while adjacent IT — forecasting, asset management, customer systems — has moved cloud-ward. The dependency question for this estate is less about ordinary breach risk than about availability under coercion: could a foreign provider's decision, sanction exposure or jurisdictional conflict disable a grid operator's analytics or a port community system at a critical moment? The report scores critical infrastructure's strategic-control exposure at 0.70, the highest of any sector's single EDI dimension.

The practical exposure is narrower than the rhetoric suggests but not empty. Port community systems, toll collection, railway passenger systems and grid telemetry platforms all run significant workloads on infrastructure whose ultimate operational control is foreign. The report's recommendation — T2 treatment for CII-adjacent IT, with documented sovereign fallbacks — formalises what NCIIPC guidance implies but does not yet mandate.

20. AI and Cloud

AI is the largest single driver of cloud demand growth in India — and the layer where dependency questions have moved from theoretical to budgeted.

AI workloads now anchor most new hyperscaler capacity commitments in India: Microsoft's \$17.5 billion pledge, Google's \$15 billion Visakhapatnam hub and AWS's Maharashtra expansion are all justified primarily by AI demand (SRC-007/009/011). On the demand side, the IndiaAI Mission's compute facility, sovereign-LLM selections and sectoral AI missions create a public AI workload class that did not exist in 2023. AI has effectively fused the cloud and industrial-policy agendas.

The dependency structure of AI is steeper than cloud's: control concentrates in accelerator silicon (98% foreign on Techadyant's estimate), GPU cloud (90%), foundation-model APIs (74%+) and AI platforms (88%). India's counterweights are the GPU commons, sovereign model programmes and a deep applications layer. Whether AI nets out as dependency-deepening or capability-building depends on decisions — compute pricing, model procurement, data governance — detailed in Part X. The headline judgement: AI increases India's cloud dependency in 2026–2028 and can reduce it by 2030–2035, with policy sequencing as the swing factor.

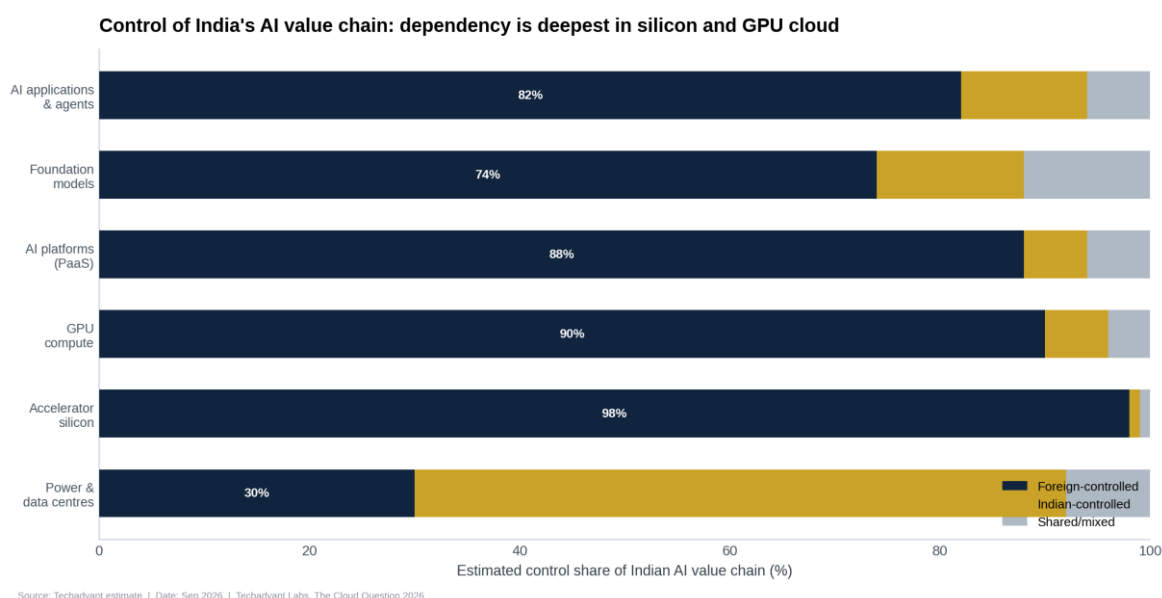


Figure 5: Foreign vs Indian control across the AI value chain (Techadyant estimate)

Key insight: India owns the electrons; it rents the intelligence stack above them - the inverse of its power-sector position.

Source: Techadyant estimate | Date: Sep 2026 | Techadyant Labs, The Cloud Question 2026