AI and Digital-Infrastructure PPPs: Sovereignty, Power, Cybersecurity and Service Evolution

A Contract and Financing Framework for Data Centres, Government Cloud and AI Compute

Authored by Chennakeshav Adya, Independent Researcher

September 2026

Abstract

Governments increasingly require data centres, sovereign or community cloud, high-performance computing and artificial-intelligence capacity to deliver public services and economic infrastructure. Public-private partnerships can mobilise specialist design, capital and operating capability, yet conventional long-term infrastructure contracts fit poorly with rapid changes in accelerators, cooling, model architectures, cybersecurity threats, software, data policy and electricity systems. This paper develops a contract and financing framework for AI and digital-infrastructure PPPs. It separates durable site, power, connectivity and facility layers from faster-refresh compute and service layers; converts sovereignty into testable controls over data, jurisdiction, access, keys, portability and operations; integrates grid capacity, energy sourcing, water, cooling, carbon and resilience; and establishes cybersecurity, AI-assurance, supply-chain, incident, audit and exit obligations. It also addresses demand aggregation, anchor tenancy, capacity allocation, performance metrics, benchmarking, technology refresh, obsolescence, residual value, lender rights and fiscal exposure. Five figures and five tables provide an infrastructure stack, sovereignty control map, power-and-capacity scenario, cyber-resilience dashboard and evolution certificate. Eight frequently asked questions and forty primary or authoritative references support practical application. Numerical values and scores are illustrative analytical scenarios. Project conclusions require verified technical, energy, water, connectivity, cybersecurity, privacy, AI, legal, financial, fiscal, procurement, environmental and market evidence and advice.

JEL Classification: H54, H57, L32, L86, O33

Keywords: artificial intelligence, data centres, digital infrastructure, public-private partnerships, data sovereignty, cybersecurity, electricity, cloud services

1. Define the public digital outcome

The contracting authority and delivery partners should state the services, users, resilience, sovereignty and economic objectives. The required output is a digital-infrastructure outcome charter. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [1][2].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that procurement can buy technology capacity without a durable public-service result. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

2. Map the infrastructure stack

The contracting authority and delivery partners should separate land, grid, generation, cooling, connectivity, facility, compute, cloud, data and AI services. The required output is a layer-and-interface map. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [1][3].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that one bundled contract can hide mismatched asset lives and accountabilities. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

3. Choose the partnership perimeter

The contracting authority and delivery partners should decide which layers should be public, private, regulated, competed or retained. The required output is a delivery-model comparison. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [4][5].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that private finance can be applied where risk transfer and contestability are weak. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

4. Define sovereignty operationally

The contracting authority and delivery partners should translate policy into controls over location, jurisdiction, access, keys, operations, portability and continuity. The required output is a sovereignty control schedule. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [6][7].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that sovereignty can remain a slogan that fails under subpoena, outage or supplier exit. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

5. Classify data and workloads

The contracting authority and delivery partners should segment public, sensitive, critical, personal, classified and open workloads. The required output is a workload-placement matrix. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [8][9].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that all workloads can inherit the cost and rigidity of the highest classification. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

6. Establish legal jurisdiction

The contracting authority and delivery partners should map governing law, regulatory reach, cross-border transfer and lawful-access exposure. The required output is a jurisdiction memorandum. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [6][10].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that contractual location can diverge from legal control over providers and data. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

7. Control identity and privileged access

The contracting authority and delivery partners should apply least privilege, strong authentication, segregation, logging and emergency access. The required output is an access-control architecture. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [11][12].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that administrators or suppliers can bypass nominal data protections. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

8. Govern encryption and keys

The contracting authority and delivery partners should set encryption, key custody, rotation, recovery and sovereign-control requirements. The required output is a cryptographic control plan. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [11][13].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that data can remain exposed through provider-controlled keys or weak recovery. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

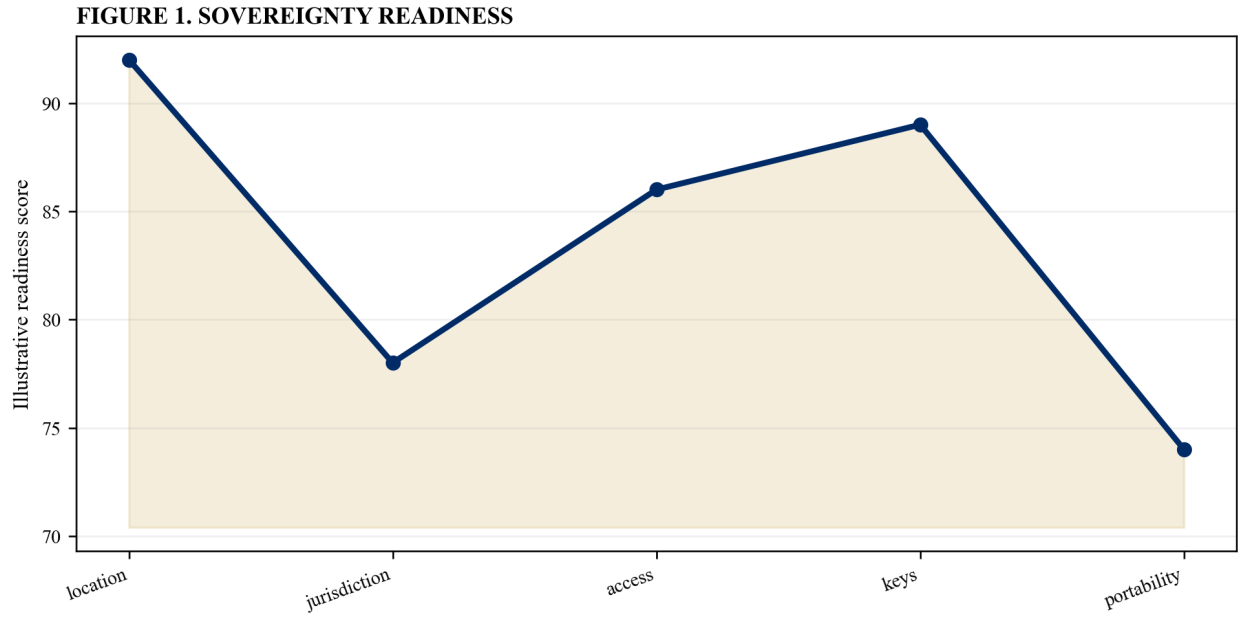
Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

Table 1. Sovereignty control map

Control	Evidence	Failure test
data location	verified architecture	cross-border failover
legal authority	jurisdiction analysis	lawful-access request
key custody	HSM and roles	provider compromise
portability	tested export	supplier exit

Illustrative analytical structure; verified technical and contractual evidence govern.

Figure 1. Sovereignty readiness



Illustrative analytical scenario; verified project evidence should replace values.

9. Secure power before procurement

The contracting authority and delivery partners should verify grid capacity, connection dates, redundancy, quality and expansion rights. The required output is a power-readiness certificate. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [3][14].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that compute delivery can fail because contracted electricity is unavailable. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

10. Design the energy portfolio

The contracting authority and delivery partners should compare grid, renewables, storage, firm generation, PPAs and backup. The required output is an energy-supply strategy. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [14][15].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that a single nominal source can create reliability, price or carbon concentration. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

11. Model electricity demand

The contracting authority and delivery partners should forecast IT load, PUE, utilisation, growth, model mix and efficiency. The required output is a power-demand model. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [3][16].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that fixed forecasts can underbuild connections or strand expensive capacity. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

12. Govern grid interaction

The contracting authority and delivery partners should set curtailment, demand response, ramping, export and emergency priorities. The required output is a grid-services protocol. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [14][17].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that large flexible loads can destabilise the system or miss value from flexibility. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

13. Design cooling for evolving density

The contracting authority and delivery partners should test air, liquid and immersion cooling across rack-density scenarios. The required output is a cooling evolution plan. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [18][19].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that facilities can become incompatible with future accelerators. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

14. Control water risk

The contracting authority and delivery partners should measure source, consumption, treatment, discharge, scarcity and drought response. The required output is a water stewardship plan. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [20][21].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that cooling economics can transfer stress to local communities and utilities. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

15. Set environmental outcomes

The contracting authority and delivery partners should govern lifecycle emissions, energy attributes, refrigerants, equipment and construction. The required output is an environmental performance schedule. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [15][22].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that operational claims can omit embodied carbon and backup generation. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

16. Aggregate credible demand

The contracting authority and delivery partners should map government workloads, migration readiness, private tenants and ramp-up. The required output is an anchor-demand plan. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [1][23].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that a facility can reach completion before usable demand materialises. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

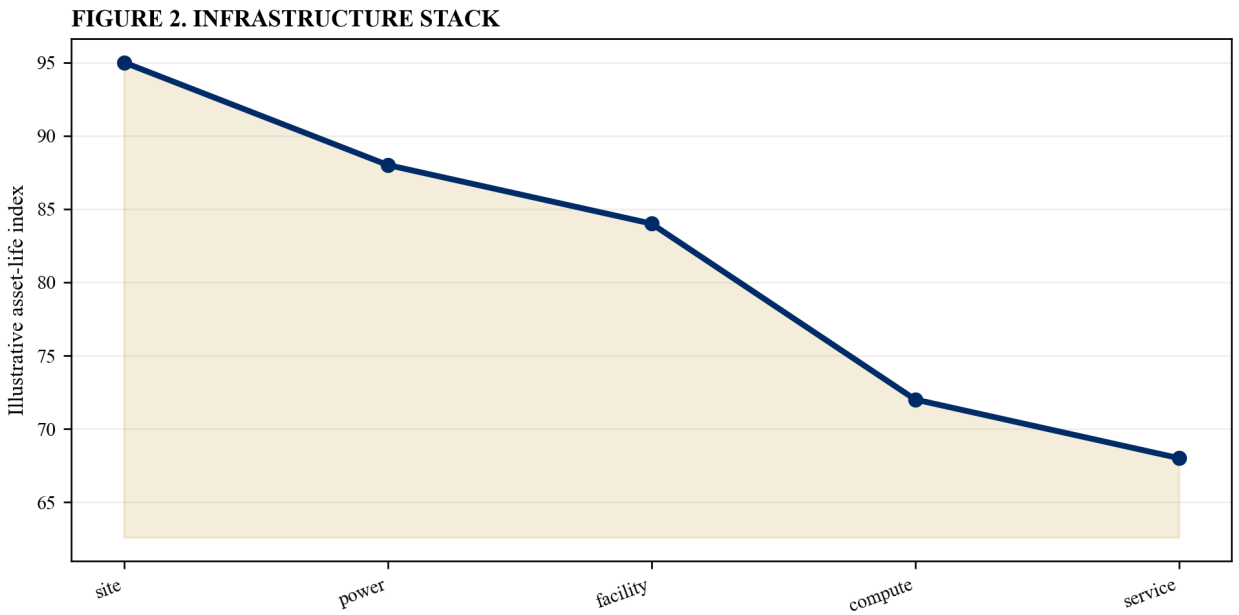
Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

Table 2. Digital-infrastructure stack

Layer	Typical life	Contract approach
land and shell	25+ years	long-term asset
power and cooling	10-25 years	capacity and refresh
compute	3-7 years	modular refresh
cloud and AI services	1-5 years	contestable service

Illustrative analytical structure; verified technical and contractual evidence govern.

Figure 2. Infrastructure stack



Illustrative analytical scenario; verified project evidence should replace values.

17. Allocate capacity transparently

The contracting authority and delivery partners should set reservation, priority, expansion, public emergency and unused-capacity rules. The required output is a capacity allocation policy. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [2][24].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that anchor demand can crowd out competition or leave public capacity idle. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

18. Choose commercial units

The contracting authority and delivery partners should compare space, power, compute, storage, workload and service-based charging. The required output is a tariff architecture. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [4][25].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that the payment unit can reward unused assets or obscure service economics. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

19. Define service performance

The contracting authority and delivery partners should measure availability, latency, recoverability, capacity, security and workload outcomes. The required output is a service-level framework. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [11][26].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that facility uptime can coexist with failed public applications. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

20. Design availability payments

The contracting authority and delivery partners should link payment and deductions to controllable, material service outcomes. The required output is a payment mechanism. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [4][27].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that weak deductions can socialise performance risk while harsh deductions impair bankability. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

21. Set compute-performance baselines

The contracting authority and delivery partners should define benchmark suites, workload classes, energy intensity and reproducibility. The required output is a compute benchmark protocol. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [28][29].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that vendor metrics can become incomparable as chips and software change. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

22. Govern AI service quality

The contracting authority and delivery partners should require testing, evaluation, monitoring, human oversight and traceability. The required output is an AI-assurance schedule. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [30][31].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that available compute can support unsafe, biased or unreliable public decisions. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

23. Apply secure-by-design requirements

The contracting authority and delivery partners should embed threat modelling, hardened defaults, vulnerability management and assurance. The required output is a secure-design baseline. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [12][32].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that security can be deferred to operations after architecture choices are locked. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

24. Segment the architecture

The contracting authority and delivery partners should separate tenants, networks, control planes, workloads and recovery environments. The required output is a zero-trust segmentation design. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [13][33].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that one compromise can propagate across public services and customers. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

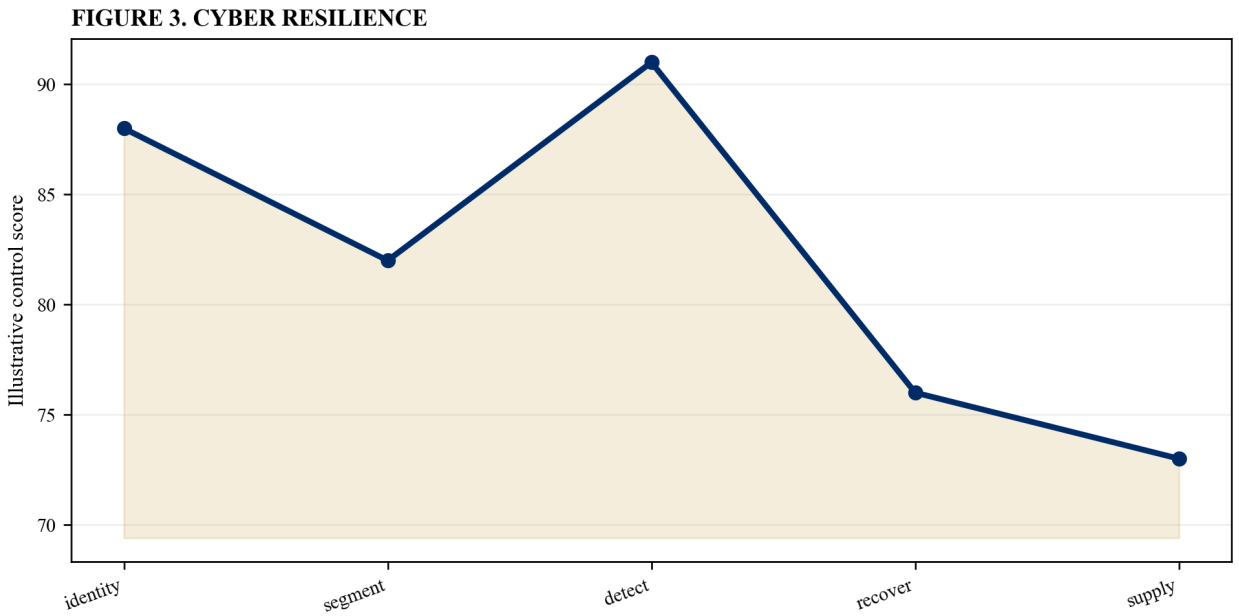
Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

Table 3. Cyber-resilience controls

Domain	Metric	Contract response
identity	privileged-access events	contain and investigate
segmentation	lateral movement test	remediate
recovery	verified recovery time	service deduction
supply chain	critical dependency status	replace or mitigate

Illustrative analytical structure; verified technical and contractual evidence govern.

Figure 3. Cyber resilience



Illustrative analytical scenario; verified project evidence should replace values.

25. Control technology supply chains

The contracting authority and delivery partners should trace critical chips, firmware, software, dependencies, vendors and maintenance. The required output is a supply-chain risk register. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [34][35].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that hidden dependencies can create backdoors, sanctions exposure or unsupported assets. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

26. Prepare for cyber incidents

The contracting authority and delivery partners should define detection, containment, reporting, evidence, recovery and public command. The required output is a joint incident-response plan. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [11][36].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that unclear authority can delay containment and service restoration. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

27. Test operational resilience

The contracting authority and delivery partners should run failover, backup, cyber, grid, cooling, fire and regional-disaster exercises. The required output is a resilience-test programme. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [11][37].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that paper redundancy can fail during a correlated event. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

28. Govern AI model and data incidents

The contracting authority and delivery partners should set escalation for drift, misuse, leakage, harmful output and model compromise. The required output is an AI incident protocol. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [30][38].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that facility operations can remain normal while AI services cause public harm. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

29. Create the technology-refresh mechanism

The contracting authority and delivery partners should set review cycles, triggers, standards, testing, competition and approvals. The required output is an evolution schedule. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [5][28].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that a long concession can freeze obsolete compute or permit uncontrolled scope creep. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

30. Separate refresh capital

The contracting authority and delivery partners should allocate lifecycle capex for facility, network, compute, software and security layers. The required output is a refresh-capex waterfall. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [4][18].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that short-life equipment replacement can be unfunded within long-life debt. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

31. Manage obsolescence and residual value

The contracting authority and delivery partners should define useful life, redeployment, resale, impairment, recycling and handback. The required output is an asset-evolution model. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [22][39].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that optimistic residual values can inflate financeability and end-of-term value. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

32. Preserve interoperability

The contracting authority and delivery partners should require open interfaces, data formats, identity federation and workload portability. The required output is an interoperability architecture. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [7][40].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that proprietary integration can make competitive replacement impracticable. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

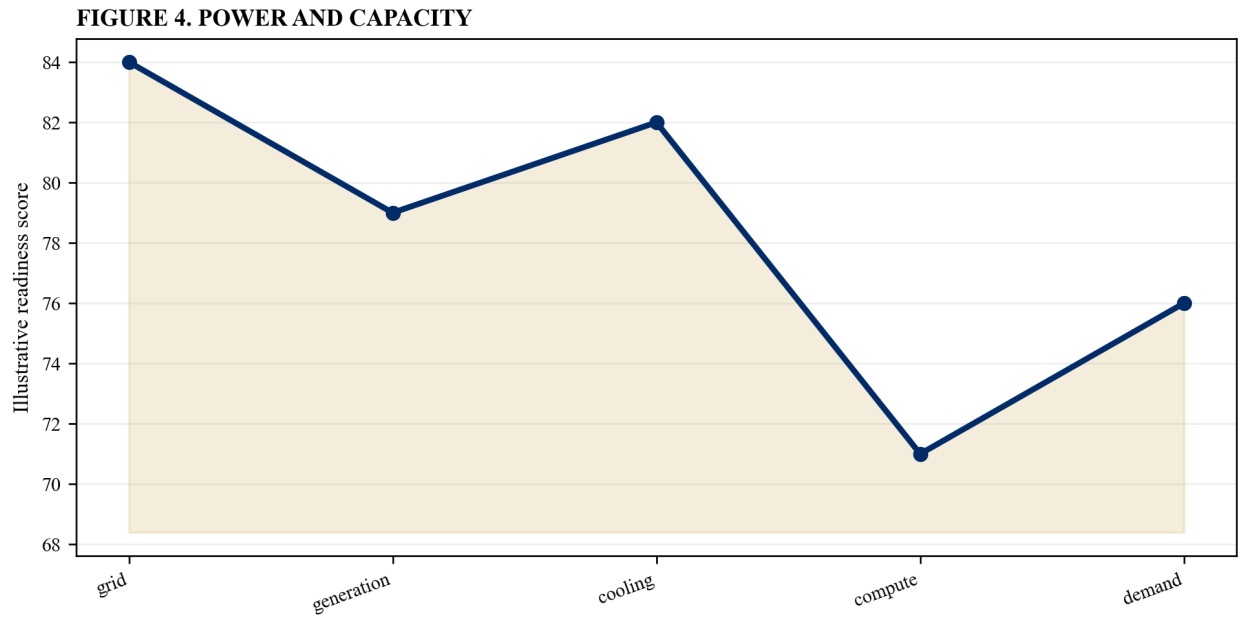
Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

Table 4. Illustrative capacity model

Driver	Base case	Stress case
IT load MW	80	120
PUE	1.30	1.45
utilisation	72%	90%
refresh interval years	5	3

Illustrative analytical structure; verified technical and contractual evidence govern.

Figure 4. Power and capacity



Illustrative analytical scenario; verified project evidence should replace values.

33. Design exit and migration

The contracting authority and delivery partners should set data export, transition assistance, deletion, key transfer and continuity. The required output is an exit-and-portability plan. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [6][40].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that supplier failure or expiry can trap critical public workloads. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

34. Protect competition over time

The contracting authority and delivery partners should use modular lots, benchmarking, reopeners and contestable service layers. The required output is a competition roadmap. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [2][24].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that one provider can convert infrastructure control into enduring service monopoly. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

35. Structure lender rights

The contracting authority and delivery partners should align security, step-in, cure and enforcement with cyber and sovereignty controls. The required output is a digital-infrastructure direct agreement. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [4][27].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that lender remedies can conflict with data, security or public-continuity duties. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

36. Model fiscal exposure

The contracting authority and delivery partners should measure availability payments, guarantees, power support, termination and refresh obligations. The required output is a fiscal-risk statement. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [4][5].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that off-balance-sheet presentation can obscure long-term public commitments. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

37. Control change and benchmarking

The contracting authority and delivery partners should set evidence, market tests, cost review, gain sharing and dispute processes. The required output is a change-control mechanism. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [5][25].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that necessary evolution can become recurring bilateral renegotiation. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

38. Retain audit and observability

The contracting authority and delivery partners should preserve telemetry, configurations, access, model, incident and decision records. The required output is an evidence-retention architecture. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [11][30].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that the authority can lose the evidence needed to govern opaque services. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

39. Plan handback or renewal

The contracting authority and delivery partners should define asset condition, software rights, data, skills, licences and transition readiness. The required output is a digital handback plan. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [4][39].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that physical assets can transfer without operable systems or institutional capability. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

40. Issue the digital-infrastructure certificate

The contracting authority and delivery partners should reconcile sovereignty, power, capacity, cyber, AI, finance, evolution and exit controls. The required output is an auditable readiness certificate. Record the accountable owner, applicable rule, source evidence, acceptance criterion, approval, exception and review date [1][11].

Test the conclusion across public outcomes, sovereignty, competition, power, connectivity, facility resilience, cybersecurity, privacy, AI trustworthiness, financeability, fiscal affordability and service continuity. Preserve secure evidence from design through exit.

The principal risk is that approval can rest on disconnected technical and commercial reviews. Quantify the effect on capacity, availability, latency, energy, water, emissions, security, public payments, user outcomes, lifecycle cost and recovery. Compare the proposed approach with modular, public, private and competitively refreshed alternatives.

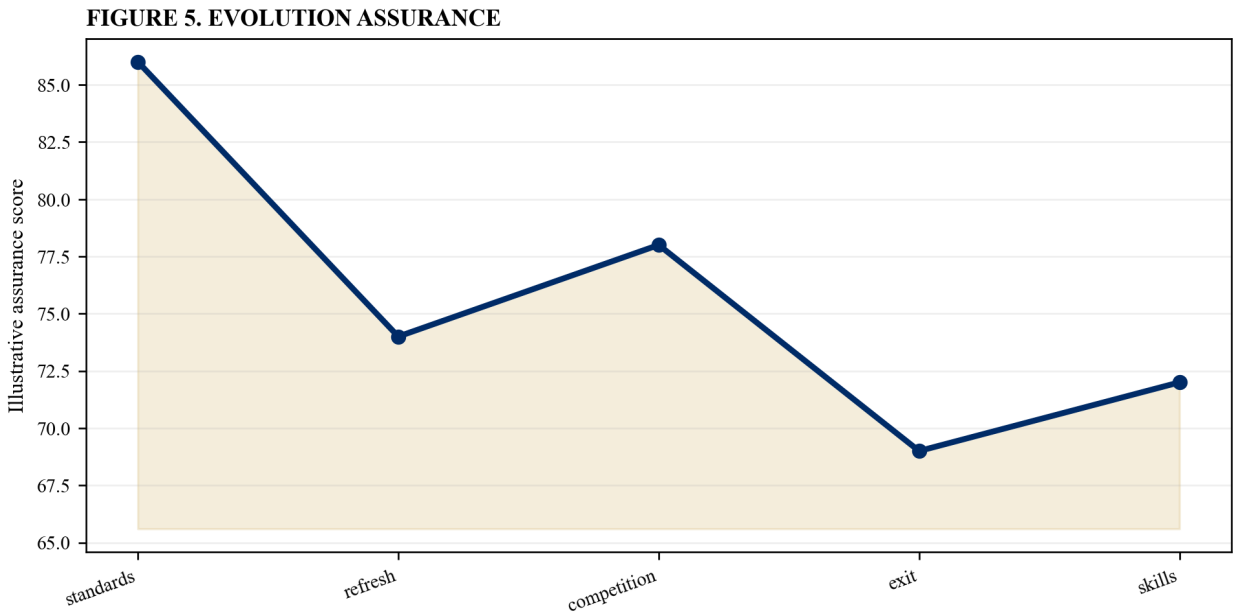
Translate the conclusion into technical schedules, payment metrics, security controls, change rules, financing conditions, monitoring and exit obligations. Refresh it after material technology, threat, energy, demand, regulatory or supplier change.

Table 5. Digital-infrastructure certificate

Decision	Evidence	Owner
sovereignty	control schedule	data authority
power	connection and portfolio	energy lead
security	assurance and tests	security authority
evolution	refresh and exit	contract authority

Illustrative analytical structure; verified technical and contractual evidence govern.

Figure 5. Evolution assurance



Illustrative analytical scenario; verified project evidence should replace values.

References

[1] World Bank Group, Building Data Infrastructure for AI Readiness, https://www.worldbank.org/en/results/2026/05/06/data-infrastructure-for-ai

[2] World Bank, Digital Development and Data Centre PPPs, https://www.worldbank.org/en/programs/quality-infrastructure-investment-partnership/digital-development

[3] IEA, Energy and AI, https://www.iea.org/reports/energy-and-ai

[4] World Bank PPP Resource Center, PPP Reference Guide Version 3, https://ppp.worldbank.org/sites/default/files/2024-08/PPP%20Reference%20Guide%20Version%203.pdf

[5] World Bank PPP Resource Center, Guidance on PPP Contractual Provisions, https://ppp.worldbank.org/sites/default/files/2024-07/Guidance_%20PPP_Contractual_Provisions_EN_2017.pdf

[6] European Union, General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[7] European Commission, European Data Strategy, https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[8] NIST, Privacy Framework, https://www.nist.gov/privacy-framework

[9] NIST, Data Classification Practices, https://csrc.nist.gov/publications

[10] OECD, Guidelines on the Protection of Privacy and Transborder Data Flows, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

[11] NIST, Cybersecurity Framework 2.0, https://www.nist.gov/cyberframework

[12] CISA, Secure by Design, https://www.cisa.gov/securebydesign

[13] NIST, Zero Trust Architecture SP 800-207, https://csrc.nist.gov/pubs/sp/800/207/final

[14] IEA, Energy Supply for AI, https://www.iea.org/reports/energy-and-ai/energy-supply-for-ai

[15] GHG Protocol, Corporate Standard, https://ghgprotocol.org/corporate-standard

[16] IEA, Energy Demand from AI, https://www.iea.org/reports/energy-and-ai/energy-demand-from-ai

[17] IEA, Electricity Grids and Secure Energy Transitions, https://www.iea.org/reports/electricity-grids-and-secure-energy-transitions

[18] ASHRAE, Data Center Resources, https://www.ashrae.org/technical-resources/bookstore/datacom-series

[19] U.S. Department of Energy, Data Center Energy Efficiency, https://www.energy.gov/eere/buildings/data-centers-and-servers

[20] World Bank, Water Resources Management, https://www.worldbank.org/en/topic/waterresourcesmanagement

[21] UNEP, Freshwater Strategy, https://www.unep.org/explore-topics/water

[22] International Telecommunication Union, Circular Economy for ICT Equipment, https://www.itu.int/en/ITU-T/climatechange/Pages/default.aspx

[23] World Bank, Cloud and Data Infrastructure Market Development, https://www.worldbank.org/en/results/2026/05/06/data-infrastructure-for-ai

[24] OECD, Competition in the Digital Economy, https://www.oecd.org/competition/digital-economy-innovation-and-competition.htm

[25] World Bank PPP Resource Center, Managing PPP Contracts, https://ppp.worldbank.org/managing-ppp-contracts

[26] ISO, ISO/IEC 20000 IT Service Management, https://www.iso.org/isoiec-20000-it-service-management.html

[27] World Bank PPP Resource Center, Performance and Payment Mechanisms, https://ppp.worldbank.org/structuring-ppp-contract

[28] MLCommons, AI Benchmarking, https://mlcommons.org/benchmarks/

[29] NIST, AI Measurement and Evaluation, https://airc.nist.gov/

[30] NIST, AI Risk Management Framework, https://www.nist.gov/itl/ai-risk-management-framework

[31] NIST, AI RMF Playbook, https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook

[32] NIST, Secure Software Development Framework SP 800-218, https://csrc.nist.gov/pubs/sp/800/218/final

[33] NIST, Security and Privacy Controls SP 800-53 Rev. 5, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[34] NIST, Cybersecurity Supply Chain Risk Management SP 800-161 Rev. 1, https://csrc.nist.gov/pubs/sp/800/161/r1/final

[35] European Union Agency for Cybersecurity, NIS2 Security Measures Guidance, https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

[36] CISA, Cybersecurity Incident and Vulnerability Response Playbooks, https://www.cisa.gov/news-events/news/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

[37] NIST, Risk Management Framework SP 800-37 Rev. 2, https://csrc.nist.gov/pubs/sp/800/37/r2/final

[38] NIST, Trustworthy AI in Critical Infrastructure Profile Concept Note, https://www.nist.gov/system/files/documents/2026/04/08/Draft%20Concept%20Note_%20Development%20of%20the%20NIST%20AI%20RMF%20Trustworthy%20Use%20of%20AI%20in%20Critical%20Infrastructure%20Profile.pdf

[39] Basel Convention, Technical Guidelines on E-waste, https://www.basel.int/Implementation/TechnicalMatters/DevelopmentofTechnicalGuidelines/TechnicalGuidelines/tabid/8025/Default.aspx

[40] European Commission, European Interoperability Framework, https://commission.europa.eu/publications/european-interoperability-framework_en

About the Author

Authored by Chennakeshav Adya, Independent Researcher

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds; bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.