Sovereign Space Communications JVs: Control, Encryption and Data Residency

A Transaction and Governance Framework for Strategic Service Continuity

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Sovereign space communications joint ventures combine strategic infrastructure with commercial capital, technology and operating expertise. Their value depends on a chain of rights and capabilities that spans spectrum filings, national licences, satellites, gateways, terrestrial backhaul, encryption, cryptographic key custody, network operations, customer contracts and crisis-period service obligations. A joint venture can own valuable assets and still fail its public purpose when a foreign shareholder controls software updates, mission commands, security logs, customer metadata, gateway routing or the practical ability to restore service.

This paper develops a transaction and governance framework for governments, sovereign investors, satellite operators, infrastructure funds and strategic partners considering such ventures. It separates economic ownership from operational control, security authority and continuity responsibility. It proposes a reserved-powers matrix, a key-custody architecture, a data-location and access ledger, an independently testable service-continuity plan and a capacity-allocation mechanism for normal and crisis conditions. It also integrates foreign-investment review, export controls, spectrum coordination, cyber assurance and change-of-control consent into valuation and transaction structure.

The framework draws on the International Telecommunication Union satellite coordination process, the European Union Secure Connectivity Programme, United Kingdom space-security and investment-screening guidance, United States government satellite-communications procurement evidence, current post-quantum cryptography standards and UAE data-protection law. These sources show that sovereign connectivity is governed through several independent systems. ITU filings coordinate spectrum and orbital use through national administrations. Domestic licences determine lawful operation and market access. Security authorities define accreditation, classified-information and incident requirements. Data-protection rules govern personal-data processing and cross-border transfers. Investment-screening and export-control regimes can constrain ownership, technology access and closing.

A wholly hypothetical venture is used to demonstrate the method. A state sponsor and an international operator fund a multi-orbit capacity platform with secure gateways and national network operations. The venture has USD 185 million of annual contracted revenue at stabilisation, including USD 80 million of sovereign availability payments. The illustrative model converts that revenue into USD 44 million of distributable cash after network operations, security operations, gateway costs, lifecycle reserves and tax. A hypothetical enterprise-value bridge produces USD 520 million before contingent consideration. The model assigns no value to unapproved spectrum, untested encryption, non-transferable licences, unsupported data-localisation claims or crisis capacity that cannot be exercised and verified.

The central conclusion is that a sovereign communications venture should be structured as a controlled service system rather than a conventional shared-equity company. The state needs enforceable authority over defined sovereign functions. The operator needs sufficient commercial discretion to run a competitive network. Each control right should connect to a technical mechanism, named decision maker, measurable

service obligation and remedy. Transaction value should follow accepted capability, funded demand, transferable rights and collected cash. Strategic access should be valued separately and only when continuity can be demonstrated through technical tests, legal rights and funded operating arrangements.

JEL Classification: G24, G32, G34, L51, L63, L96, O32, O33

Keywords: sovereign satellite communications, space communications joint venture, encryption sovereignty, data residency, key custody, spectrum rights, ground segment, foreign investment review, service continuity, space M&A

Introduction

The board decision is whether a proposed joint venture can deliver sovereign communications through disruption while earning an acceptable return on invested capital. The answer cannot be derived from share ownership alone. A shareholder may hold a majority interest while depending on another party for mission software, encryption modules, gateway access, specialist engineers, supply-chain support or priority capacity. Effective control therefore sits across legal documents, technical architecture, operating permissions, information access and crisis procedures.

The diligence perimeter should follow the end-to-end service. It begins with lawful spectrum and orbital use, continues through space and ground assets, and ends with delivery into an authorised user network. Every dependency should have an owner, an operating record, a replacement route and a documented consequence of failure. The same map should support valuation, transaction agreements, security accreditation and the post-close operating model.

Public sources establish useful reference points. The ITU records frequency assignments after national administrations complete applicable coordination and notification procedures. The European Union Secure Connectivity Programme uses a public-private structure with explicit governance, service-continuity and security-accreditation principles. UK investment-screening guidance identifies satellite communications links and operational-control facilities as sensitive activities. NIST has finalised three post-quantum cryptography standards, creating a practical migration reference for long-lived infrastructure. UAE data-protection legislation requires proportionate security measures and regulates cross-border transfers of personal data.

These sources do not produce one universal joint-venture model. National-security law, procurement rules, telecoms licensing, data protection and export controls vary by jurisdiction and service. The proposed framework is therefore a decision system. It identifies the questions, evidence and allocation mechanisms that boards can adapt with local legal, technical, tax and security advice.

1 Define the sovereign service before the company

The transaction should begin with a service statement that identifies authorised users, geographic coverage, traffic classes, minimum performance, continuity levels and crisis powers. A broad objective such as national connectivity is insufficient. The venture may serve government ministries, defence users, emergency services, critical-infrastructure operators, enterprises and retail customers through different networks and security domains. Each service class needs a defined route from terminal to satellite, gateway, terrestrial network and recipient.

The statement should distinguish availability from usable service. A satellite can be operational while a user lacks a compatible terminal, authorised frequency, cryptographic credential or domestic gateway. Capacity can exist while contractual priority belongs to another customer. A service can be technically available while a foreign support restriction prevents fault recovery. The minimum test is whether a named user can send and receive protected traffic under specified normal and degraded conditions.

The service definition becomes the reference for procurement, capital release and valuation. It allows the board to identify which assets are necessary, which can be shared, and which functions require sovereign control. It also prevents a venture from accumulating technology that does not improve an accepted service outcome. Every material investment should retire a service risk or expand a funded service.

2 Separate four forms of control

Four forms of control should be recorded separately. Corporate control concerns voting rights, board appointment, budgets, financing and distributions. Operational control concerns network configuration, capacity scheduling, mission commands, software deployment and incident response. Security control concerns accreditation, cryptographic policy, key custody, privileged access, classified information and audit. Continuity control concerns the ability to sustain or restore service when a partner, supplier, gateway or jurisdiction becomes unavailable.

These controls can sit with different parties. A state shareholder may hold reserved rights over sovereign capacity and security policy. An operator may manage commercial scheduling and routine network operations. An independent security authority may accredit the system and investigate incidents. A continuity operator may retain a tested capability to run specified functions from a national facility. The allocation should reflect competence as well as policy.

The joint-venture agreement should reference the technical controls that make each legal right effective. A veto over software changes has limited value when the state cannot inspect code, reproduce a build or prevent an unauthorised deployment. A right to crisis capacity has limited value without a scheduling interface, credential, terminal inventory and exercised operating procedure. Legal drafting and systems engineering should therefore proceed from one control matrix.

3 Establish the transaction perimeter

The perimeter should identify the assets, contracts, rights, people and obligations that transfer or become available at closing. The asset map should cover spacecraft interests, hosted payloads, gateway equipment, ground sites, terrestrial backhaul, network-management systems, security operations, user terminals, software, source code, intellectual property, spectrum filings, national licences, customer contracts, supplier agreements, insurance and programme records.

Shared assets require specific treatment. A global operator may use common satellites, network software and operations centres for several markets. The venture may receive service rights rather than ownership. Diligence should test capacity priority, term, renewal, price reset, termination, change of control, insolvency, force majeure and step-in rights. It should also identify which rights are enforceable against operating subsidiaries and critical suppliers.

Transferability is a valuation gate. A licence, filing, government contract or technology agreement may require consent. Export controls can restrict technical data, source code, hardware or support personnel. Security approval may depend on ownership, citizenship, facilities or information barriers. Any item that cannot transfer at closing should be excluded from the base value or addressed through a binding condition, replacement route or contingent payment.

4 Build the spectrum and orbital-rights ledger

Satellite communications depend on coordinated use of radio-frequency spectrum and associated orbital resources. ITU procedures operate through national administrations, while domestic authorities license operators, gateways, terminals and services. A venture should not describe spectrum as an owned asset. The diligence record should identify each filing, assignment, coordination status, responsible administration, bringing-into-use requirement, deployment milestone, national authorisation and renewal date.

The ledger should connect rights to the planned network configuration. It should record frequency bands, orbital characteristics, service direction, geographic coverage, earth stations, power limits and coordination obligations. It should identify harmful-interference exposure, unresolved coordination, priority status and dependencies on a parent operator's filings. A proposed change in satellite, beam, gateway or ownership may require regulatory action.

The economic model should include the time and cost required to secure, maintain and coordinate rights. It should also test a delayed or constrained case. Capacity that cannot lawfully be used in the target market is not commercial capacity. A contractual representation about spectrum should be supported by a filing and licence schedule, regulatory opinions where appropriate, and a post-close compliance owner.

5 Map national licences and market access

Domestic licensing can include satellite-service authorisations, landing rights, gateway licences, telecoms licences, equipment approvals, lawful-interception obligations, emergency-service duties and customer restrictions. The required approvals depend on the jurisdiction, service and architecture. The venture should maintain a country-by-country legal-operability matrix rather than rely on a global operator's general market presence.

Each market entry should have an accountable licence holder and operating entity. The model should record whether the venture, a shareholder, a distributor or a customer holds the relevant permission. It should identify fees, local presence, ownership limits, data-handling conditions, reporting, renewal and enforcement risk. Contracts should allocate responsibility when a licence is delayed, suspended or narrowed.

The board should connect revenue recognition to regulatory readiness. A sales pipeline in an unlicensed market is a strategic option. It becomes forecast revenue only after the service, customer, permission and delivery path are verified. The transaction should avoid paying full value for market-access claims that depend on future approvals or non-binding relationships.

6 Design reserved sovereign powers

Reserved powers should be narrow, explicit and exercisable. They may cover changes to sovereign service levels, encryption policy, key custody, gateway location, foreign privileged access, security-critical suppliers, transfer of sensitive assets, crisis capacity, classified information, material incidents and changes of control. Routine commercial decisions should remain with management within an approved operating plan.

The matrix should identify the decision threshold, evidence required, approving body, response time and deadlock route. Some matters may require state-shareholder consent. Others may require approval by a security committee, regulator or independent authority. Emergency powers should identify who can act first, how long the action remains valid and how commercial consequences are reviewed.

Reserved powers impose value and cost. They can protect the sovereign purpose and make government demand bankable. They can also slow procurement, constrain financing and create minority-protection issues. The shareholder agreement should therefore pair powers with process disciplines, objective triggers and information rights. Lenders and investors should understand which actions can affect revenue, costs, distributions and asset use.

7 Allocate board and committee authority

The board should have directors with commercial, technical, security, regulatory and finance competence. Appointment rights should reflect contribution and risk without creating an unworkable bloc. An independent chair or director can support decisions involving related-party services, transfer pricing,

security incidents and capacity conflicts. Directors should receive sufficient cleared information to discharge their duties.

Specialised committees can reduce the risk that sensitive matters are decided through general governance. A security and resilience committee can oversee accreditation, key management, privileged access, continuity testing and incidents. A commercial committee can review pricing, customer concentration and related-party capacity. An audit and risk committee can reconcile service records, revenue, capital, compliance and assurance findings.

Committee authority should remain integrated with the board. Reports should state decisions, exceptions, owners and deadlines. Matters that affect both security and economics should reach both relevant committees. A technical waiver, for example, may increase service risk, insurance cost, customer liability and lifecycle capital. The decision record should preserve those connections.

8 Create sovereign key custody

Encryption sovereignty requires control over the cryptographic lifecycle, including generation, distribution, storage, use, rotation, revocation, recovery and destruction of keys. It does not require the venture to invent proprietary algorithms. The objective is to ensure that authorised national personnel and systems can control protected sovereign traffic without an unapproved external party exercising unilateral access.

The architecture should separate traffic encryption, command and control, identity, software signing and administrative credentials. Hardware security modules, split knowledge, dual control and offline recovery can reduce single-person and single-system risk. Key-management facilities should have defined physical, personnel, logical and procedural controls. Audit logs should be protected from alteration and available to the authorised security authority.

Long-lived space and ground assets require cryptographic agility. NIST's FIPS 203, 204 and 205 provide standardised post-quantum mechanisms for key establishment and signatures. A migration plan should identify where algorithms are implemented, which components can be upgraded, how hybrid modes are tested, and what happens when a spacecraft cannot receive a new cryptographic stack. Procurement contracts should require an inventory, supported algorithms, update rights and evidence of interoperability.

9 Protect telemetry tracking and command

Telemetry, tracking and command functions determine whether an operator can observe, configure and direct the space system. Compromise can affect service, safety and customer trust. The venture should identify every command path, control station, privileged role, authentication method, approval rule, software dependency and emergency procedure. It should separate commercial network management from spacecraft command authority where the risk case requires it.

Command operations should follow least privilege, strong identity, dual authorisation for critical actions, authenticated command loads, protected telemetry and independent monitoring. Remote support should be time-limited, approved, logged and technically constrained. Emergency access should be tested without creating a permanent bypass. The state should know which functions can be performed from national facilities and which require a foreign operations centre.

Transaction diligence should test practical control through a witnessed operating exercise. Documents and screenshots are weaker evidence than a controlled demonstration of credential issuance, command approval, configuration change, log review, failover and recovery. Any function that cannot be demonstrated should enter the remediation plan and valuation adjustment.

10 Define the data map before data residency

Data residency discussions often fail because the parties use the word data for different records. The venture should classify customer payload data, traffic content, metadata, network telemetry, spacecraft telemetry, security logs, identity records, billing data, support records, software repositories, cryptographic material, regulatory reports and backups. Each class has different confidentiality, operational and legal significance.

The data map should record collection point, controller, processor, purpose, legal basis, storage location, processing location, transit route, recipients, retention, deletion, encryption, key custodian and audit access. It should include cloud services, content-delivery networks, monitoring tools, ticketing systems and subcontractors. A national gateway does not create national data residency when management or backup systems replicate records elsewhere.

The map should distinguish policy preference from legal requirement. Personal-data transfer rules do not automatically require all operational data to remain in one country. National-security contracts may impose stricter requirements. Local counsel and the competent authorities should confirm the applicable rules. The technical design should implement the approved policy through routing, tenancy, access and monitoring controls.

11 Control cross-border data access

Cross-border risk includes remote access as well as physical storage. A foreign engineer may access a nationally hosted system. A global security platform may export logs for analysis. A software supplier may receive diagnostic records. The contract and architecture should therefore govern access purpose, scope, location, identity, duration, approval, logging and onward transfer.

UAE Federal Decree-Law No. 45 of 2021 provides a relevant example. It requires appropriate technical and organisational security measures and regulates cross-border transfers of personal data. Articles 22 and 23 address transfers where adequate protection exists and circumstances where it does not. The venture should apply the law to verified data classes and processing roles with local advice.

Access controls should support operating reality. Permanent prohibitions can make fault resolution impossible. An approved support model can combine national first-line capability, controlled escalation, masked data, session recording, dual approval and post-session review. The venture should test the model during commissioning and continuity exercises.

12 Segment sovereign and commercial networks

Network segmentation can allow shared infrastructure while limiting spillover between sovereign and commercial services. The design should identify trust zones for spacecraft command, sovereign traffic, commercial traffic, network management, security monitoring, development, suppliers and user access. Interfaces should have explicit protocols, authentication, content validation, logging and failure behaviour.

Segmentation should extend beyond logical network rules. It can include separate cryptographic domains, credentials, ground equipment, operations teams, cloud tenants, software pipelines and incident procedures. The appropriate degree depends on threat, service criticality, cost and the ability to operate during disconnection. The board should approve any shared component that creates a common failure mode.

The financial model should show the cost of separation. Secure gateways, national operations, independent monitoring, personnel clearance, duplicate tooling and testing can be material. These costs support a sovereign availability payment or minimum commitment when they are required for the public service. They should not be hidden inside an assumed commercial margin.

13 Define security accreditation

Security accreditation is the formal basis on which an authorised body accepts residual risk for a defined system and use. The programme should identify the accreditation authority, scope, classification, assurance standards, evidence, testing, exceptions, review cycle and conditions of operation. Accreditation should cover the actual service architecture, including suppliers and operational processes.

The European Union Secure Connectivity Programme demonstrates the importance of separate security governance. Regulation 2023/588 establishes principles for security accreditation and assigns authority for governmental infrastructure and services. It also emphasises distribution of responsibilities, service continuity and risk mitigation. A bilateral or national venture can adapt those principles without copying the institutional form.

The transaction timetable should include accreditation dependencies. A service cannot be treated as accepted sovereign capacity before the authorised body approves its intended use. Deferred consideration, capital drawdown and government payments can be linked to defined accreditation milestones. Exceptions should have owners, expiry dates and funded remediation.

14 Test supply-chain sovereignty

Sovereignty can fail through a supplier even when the venture owns its main assets. Critical dependencies may include payload components, modems, user terminals, operating systems, network software, cloud services, ground antennas, launch interfaces, cryptographic hardware and specialist support. The venture should rank suppliers by substitutability, lead time, jurisdiction, access, update authority and operational consequence.

Contracts should provide appropriate rights to technical information, security evidence, vulnerability notification, maintenance, source materials, escrow, spares, training and transition support. A right without an executable replacement path has limited continuity value. The operating plan should identify inventories, alternative suppliers, qualification time and capital required to replace a critical component.

Supply-chain diligence should address software as well as hardware. The venture should maintain a software bill of materials, signed releases, reproducible or independently verifiable builds where practical, vulnerability management and controlled deployment. It should know which external services are contacted during operation and what occurs when they are unavailable.

15 Design crisis capacity and priority

Crisis capacity should be defined as a contractual and technical service rather than an aspiration. The venture should specify the triggering authority, eligible events, capacity quantity, geographic scope, user classes, activation time, duration, pre-emption rules, restoration, price and compensation. The architecture should reserve or create the required capacity under credible demand conditions.

Normal commercial utilisation can conflict with sovereign priority. Pre-emption may affect enterprise customers, roaming partners or other governments. The venture should identify which contracts permit interruption, what service credits or liabilities arise, and how customers are informed. The economic model should reserve the expected cost of exercising priority.

The capacity plan should be exercised. A tabletop review cannot prove terminal readiness, routing, credentials, staffing and partner coordination. The venture should run periodic end-to-end tests involving authorised users, gateways, operations centres and relevant suppliers. Findings should enter a funded remediation plan and board dashboard.

16 Engineer independent continuity

Continuity requires more than redundant satellites. Common dependencies can affect several routes at once. Examples include shared software, identity systems, gateway power, fibre backhaul, cloud control planes, key-management infrastructure, supplier support and a single operations team. The architecture should identify correlated failure and geopolitical interruption.

The venture should define a minimum sovereign service that can operate when the international partner or a foreign jurisdiction becomes unavailable. The minimum may be narrower than the normal service. It should identify capacity, coverage, terminals, national staff, cryptographic material, software, runbooks, spares and funding. The state should understand how long this mode can be sustained.

Step-in rights should be supported by technical and human capability. Escrowed code without build tools, documentation, credentials and trained personnel is inadequate. A backup gateway without spectrum authority, backhaul and current configuration is also inadequate. Continuity evidence should include exercised failover, measured recovery and resolution of findings.

17 Allocate capacity through transparent rules

The venture needs a capacity ledger that reconciles technical capacity, scheduled capacity, reserved sovereign capacity, commercial commitments, maintenance margin and degraded-mode capacity. It should state the unit of measure and avoid adding incompatible throughput, beam, time and coverage metrics. Availability should be measured at the service boundary experienced by the user.

Allocation rules should identify priority tiers, booking, overcommitment, congestion management, pre-emption, restoration and reporting. Related-party capacity should be priced and approved through a transparent process. The venture should prevent either shareholder from extracting value through undisclosed priority, transfer pricing or cross-subsidy.

Capacity becomes economically valuable when it has lawful coverage, an accessible terminal population, accepted quality and a paying customer. The base forecast should use contracted or strongly evidenced demand. Unused technical capacity can support an option case after incremental sales cost, terminal deployment, regulatory work and operating cost are included.

18 Build the revenue and cost model

Revenue can include sovereign availability payments, reserved capacity, usage, enterprise connectivity, roaming or wholesale access, managed security, terminals and integration. The model should separate funded minimum commitments from optional usage and market development. Government contract ceilings, framework agreements and non-binding demand should not be treated as contracted revenue.

Cost should include satellite or capacity payments, gateways, terrestrial backhaul, network operations, security operations, accreditation, licences, spectrum, terminals, customer support, insurance, personnel, cloud services, lifecycle replacement and incident readiness. Related-party services should have observable scope, pricing, performance and audit rights.

Cash conversion matters. Government acceptance, invoicing, dispute, tax and collection terms can differ from commercial customers. Lifecycle reserves may be needed before distributions. Debt service should be tested after operating and sovereign obligations, with correlated downside across utilisation, cost, availability and collection.

19 Value strategic access separately

Commercial cash-flow value and sovereign-access value answer different questions. Commercial value reflects expected distributable cash from enforceable services. Sovereign-access value reflects the benefit

of assured capability, resilience, national control or avoided disruption. Combining them into one unsupported premium reduces accountability.

The board should first value commercial cash flows using an evidence-linked forecast. It should then state any strategic-access value through a separate decision record. The record should identify the service, alternative, consequence, probability, funding source and period. It should exclude benefits that are already paid through availability revenue or embedded in cash flows.

Strategic value should follow tested rights and capability. A board may reasonably fund resilience before it produces normal commercial return. The decision should show the public-purpose output and the conditions under which further capital is released. This approach supports transparent allocation between commercial shareholders and the state.

20 Structure consideration around evidence

Cash at completion should reflect transferable assets, effective rights, funded contracts and accepted capability. Deferred consideration can address approvals, accreditation, migration, crisis-capacity tests, customer retention and collected cash. Seller rollover can align longer-term performance when governance and future funding are clear.

Conditions precedent should cover material licences, foreign-investment approvals, security agreements, spectrum consents, key contracts and financing. Covenants should preserve operations and information security between signing and closing. Termination and long-stop provisions should address delays outside either party's control.

Representations should be supported by schedules and evidence. Important topics include rights ownership, licences, filings, security incidents, software, encryption, data handling, export controls, customer commitments, supplier dependencies and government disclosures. Indemnities and escrow should address identified exposures. Transaction insurance should not substitute for diligence or specific remedies.

21 Address foreign-investment review

Space communications can fall within mandatory or voluntary investment-screening regimes. UK guidance under the National Security and Investment Act identifies satellite communications links, secure facilities and space-infrastructure operational-control facilities within the sensitive sector description. United States CFIUS jurisdiction can include control and certain non-controlling foreign investments involving sensitive technology, infrastructure or data.

The deal team should identify relevant entities, activities, investors, rights and jurisdictions before agreeing control terms. Review can consider access to technology, facilities, information, supply chains, government customers and operational capability. A minority investment may still raise issues when it grants board, information or technical rights.

The transaction model should include timing, remedies and a fallback structure. Possible mitigations include ring-fenced operations, national directors, security officers, access restrictions, proxy arrangements, data controls and government agreements. Their cost and operating effect should be reflected in value and financing.

22 Integrate export controls and technical assistance

Space hardware, software, encryption and technical data may be controlled for export or transfer. Restrictions can apply to nationality, destination, end use, re-export and technical assistance. The venture should classify relevant items and identify licence requirements with specialist counsel. Commercial timetables should not assume unrestricted movement of engineers or technology.

The operating model should define what information each party can access and where work can be performed. Product modularity, controlled interfaces and local capability may reduce unnecessary transfer while preserving service. Contracts should allocate responsibility for licences, record keeping, changes in law and denial risk.

Export-control restrictions can affect integration, maintenance and continuity. A state may invest in an asset that cannot be repaired locally. Diligence should identify this dependency and the time, cost and permission required to replace it. The valuation should deduct unfunded localisation and contingency capital.

23 Protect related-party economics

Joint ventures often buy capacity, technology and services from their shareholders. These arrangements can accelerate deployment, but they can also shift value through transfer pricing, bundled costs, priority rights and renewal terms. Each material related-party agreement should have a clear scope, price mechanism, service level, audit right, benchmarking process and termination route.

The board should distinguish shareholder contribution from ongoing commercial supply. Technology or spectrum access represented as equity value should not be charged again without explanation. Shared services should be allocated through observable drivers. Capitalised development should produce identifiable and usable outputs.

Independent review is important when a shareholder controls both the supplier and the venture approval process. The audit and risk committee should receive reconciled service, cost and market evidence. Disputes should not threaten operational continuity while the economic issue is resolved.

24 Finance the venture to the next accepted service gate

The capital plan should connect sources and uses to technical, regulatory, commercial and security gates. Equity is suited to development, approval and integration risk. Government milestone or availability payments can fund public-purpose requirements. Debt becomes more supportable when contracts, acceptance, cash collection and replacement obligations are understood.

The model should include contingency and liquidity through a delayed case. Accreditation, spectrum coordination, launch, gateway construction and customer integration can move together. A single schedule slip can defer revenue while engineering, security and financing costs continue. The board should approve a minimum cash floor and pre-agreed actions.

Distributions should follow reserve and service obligations. The venture may need lifecycle, security, incident, insurance and debt-service reserves. A distribution lock-up can apply when availability, accreditation, liquidity or covenant thresholds are breached. The state should avoid extracting cash that weakens the service it intends to protect.

25 Design lender protections without impairing sovereignty

Lenders require security, information and remedies. Sovereign services can limit enforcement over critical assets, licences, encryption and government contracts. The financing structure should identify bankable cash flows and permitted collateral at the start rather than discover restrictions after credit approval.

Direct agreements can establish cure, step-in and continuity procedures with key customers and suppliers. Step-in should respect security accreditation, ownership limits and operational competence. Lenders may receive economic protection through accounts, reserves, assignment of receivables and share pledges while sensitive operational powers remain restricted.

The downside model should test revenue reduction, pre-emption, service failure, regulatory delay and lifecycle capital. Debt size should follow cash that remains available after the venture meets sovereign obligations. Refinancing assumptions should be excluded from minimum liquidity.

26 Establish service acceptance and payment evidence

Acceptance should be defined for each service class. Measures can include geographic coverage, throughput, latency, availability, restoration, security controls, gateway delivery and user-terminal interoperability. The test method, data source, observation period, exceptions and approving authority should be agreed before service starts.

The operating record should connect performance to invoice and payment. It should show ordered capacity, delivered service, exclusions, deductions, accepted invoice and bank receipt. This chain supports revenue recognition, contract management, financing and transaction value. It also reduces dispute over related-party or government payments.

The venture should preserve raw and processed evidence with controlled access and retention. Metrics should be independently reproducible. Any manual adjustment should have a reason, approver and audit trail. Boards should receive exceptions and trends rather than only aggregate availability.

27 Create an incident and disclosure protocol

Space communications incidents can involve cyber compromise, interference, service outage, data exposure, command anomaly, supplier failure or physical damage. The protocol should define severity, response authority, evidence preservation, customer notification, regulator notification, shareholder reporting and public communication. It should address classified and commercially sensitive information.

The venture should establish one operational picture while respecting information compartments. Technical responders need sufficient evidence to contain and recover. The state needs timely awareness of sovereign-service impact. Commercial customers need contractual notification. Directors need information to oversee risk and disclosure.

Exercises should test decision speed and cross-border coordination. The lessons should update architecture, contracts, runbooks, training and reserves. Repeated findings should affect supplier status, management incentives and capital allocation.

28 Build the partner-selection matrix

Partner selection should assess more than technology and price. Relevant dimensions include spectrum and market access, network performance, security assurance, cryptographic agility, data-control fit, supply-chain transparency, exportability, local capability, government-customer record, financial capacity, continuity alignment and willingness to accept transparent governance.

The scoring model should identify threshold failures. A partner with excellent capacity may be unsuitable when the proposed architecture cannot meet national key-custody or access requirements. A local partner may improve market access while lacking operations capability. The preferred structure may combine an operator, state sponsor, security integrator and domestic network company with clearly separated roles.

Scores should be supported by evidence and verified through diligence. Management should identify the next proof required and the consequence of failure. The matrix should be refreshed before final commitment because ownership, regulation, sanctions, supplier status and technology can change.

29 Define exit and change of control

Exit should preserve service continuity and national-security protections. The documents should address permitted transferees, state consent, first-offer or first-refusal rights, valuation, deadlock, default, sanctions, insolvency and regulatory prohibition. A sale of a shareholder or critical supplier may need to be treated as an indirect change of control.

The venture should maintain an executable separation plan. It should identify ownership and portability of data, keys, software, licences, equipment, customer records and staff. Transition services should have scope, term, price and security conditions. The state should know how sovereign service continues during a dispute or exit.

Exit value should reflect these constraints. A buyer pool may be limited by investment screening, accreditation and technology restrictions. A partner contribution may have value only while the partner remains. The valuation should distinguish transferable enterprise value from relationship-dependent value.

30 Implement a 180 day transaction programme

The first thirty days should define the service, control perimeter, regulatory map, data classes, security authority and workplan. The parties should appoint accountable commercial, technical, legal, security and finance leads. The initial red-flag review should identify any condition that could make the proposed structure unlawful or operationally ineffective.

Days thirty to ninety should complete detailed diligence, architecture, financial modelling and term negotiation. The parties should test key custody, privileged access, command paths, data routing, capacity priority and continuity. Regulatory engagement should proceed in parallel. The value model should be updated as evidence matures.

Days ninety to one hundred and eighty should finalise transaction documents, financing, approvals, implementation plans and acceptance tests. The board should approve unresolved risks, funding and remedies. Closing should occur only when minimum lawful operability, governance and continuity conditions are met or are covered by enforceable and funded conditions.

31 Board decision framework

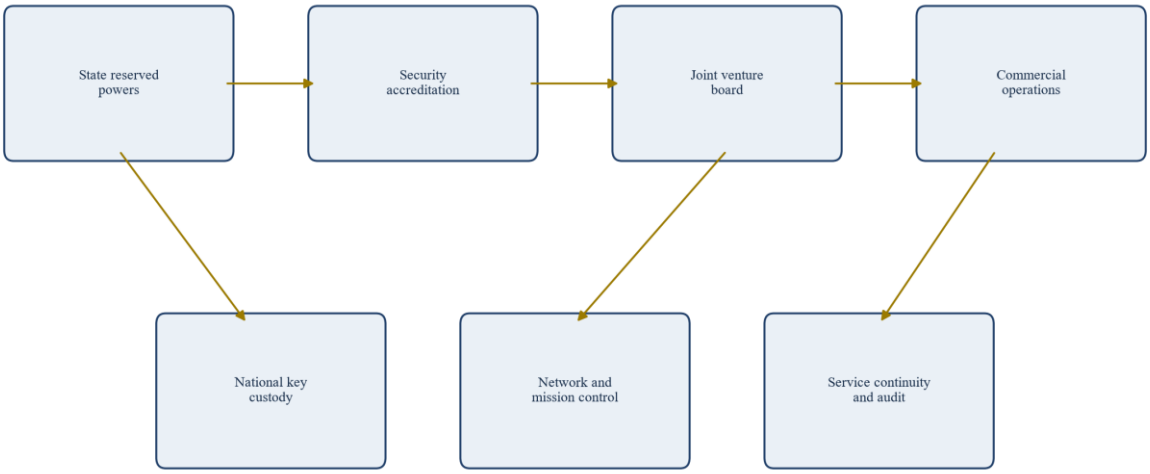
The board should approve the venture only when the sovereign service is defined, rights are effective, control is technically enforceable, data and encryption arrangements are approved, continuity is tested to the required stage, funding is sufficient and value reflects residual risk. Each positive conclusion should point to evidence, not presentation language.

The decision paper should show the central case, correlated downside, required capital, service consequences and executable responses. It should identify which assumptions are hypothetical management inputs and which are supported by contracts, licences, tests or receipts. It should also state where legal or security approval remains outstanding.

Approval should create a controlled programme rather than a static investment. Management should report progress through the same gates used in underwriting. Capital, consideration, distributions and strategic-access value should move only when the relevant evidence is accepted.

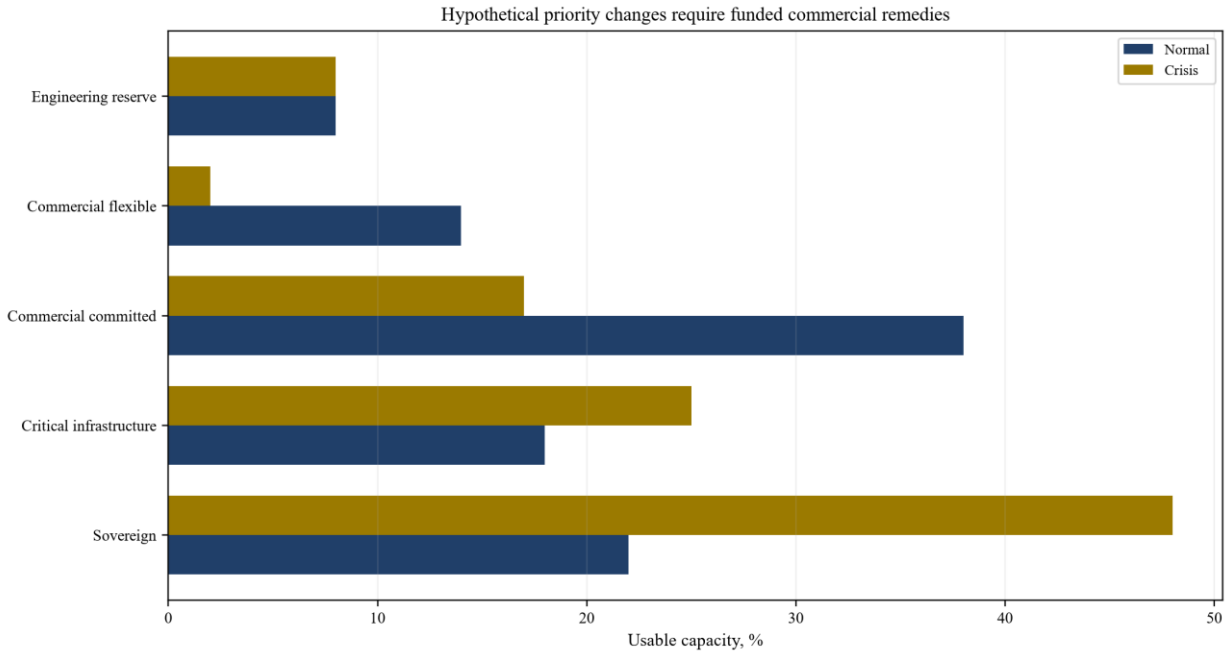
Figure 1. Sovereign-control architecture

Legal authority must connect to technical control and continuity



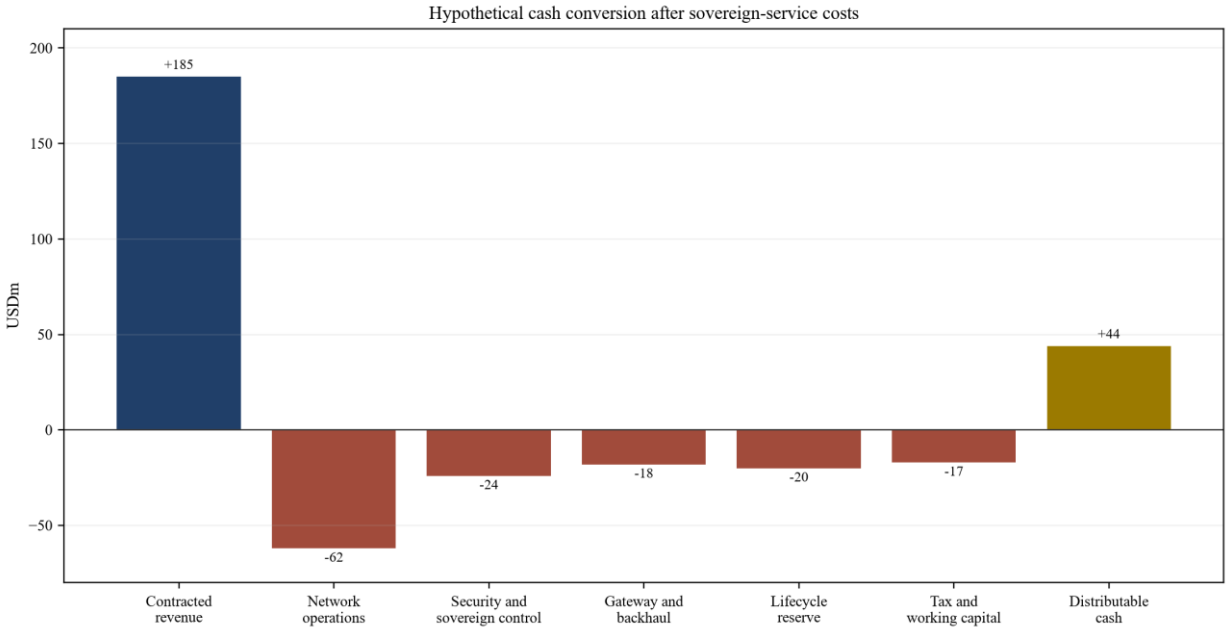
Proposed allocation of powers; local law and security authority determine the final design.

Figure 2. Hypothetical capacity allocation in normal and crisis conditions



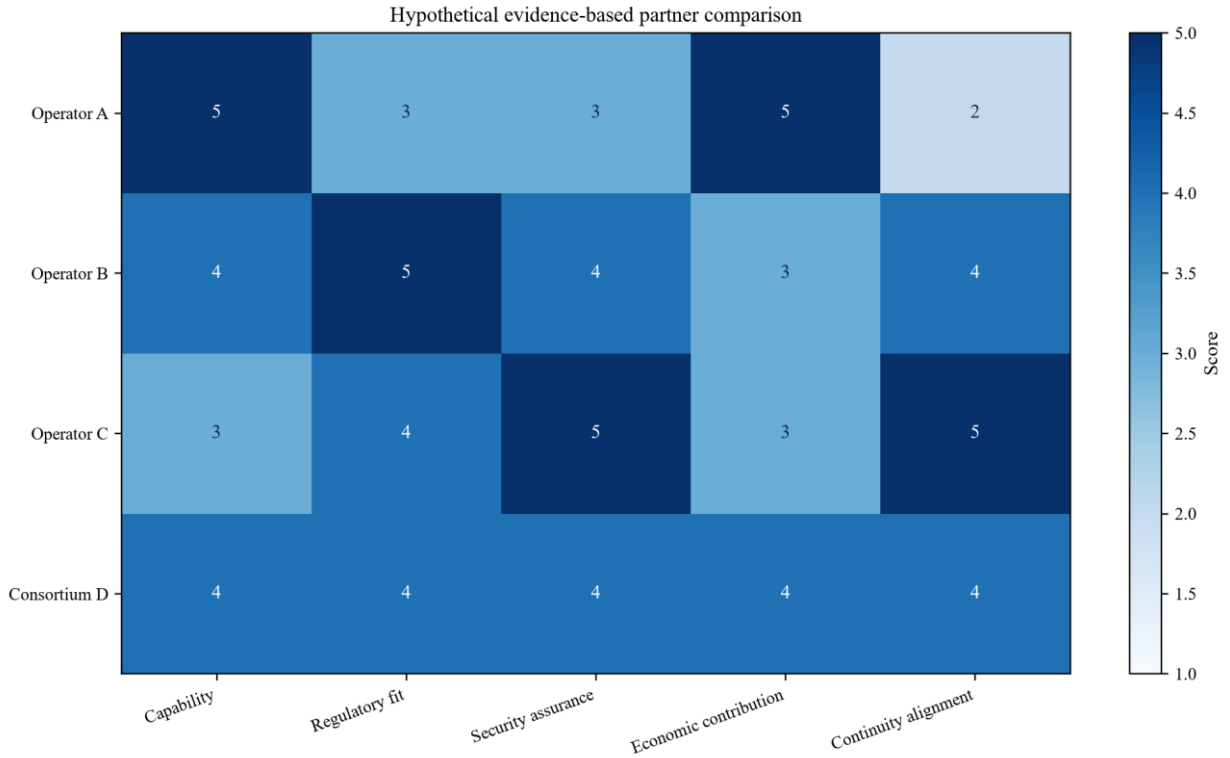
Illustrative percentage of usable capacity; no operator or government programme is represented.

Figure 3. Hypothetical annual cash bridge at stabilisation



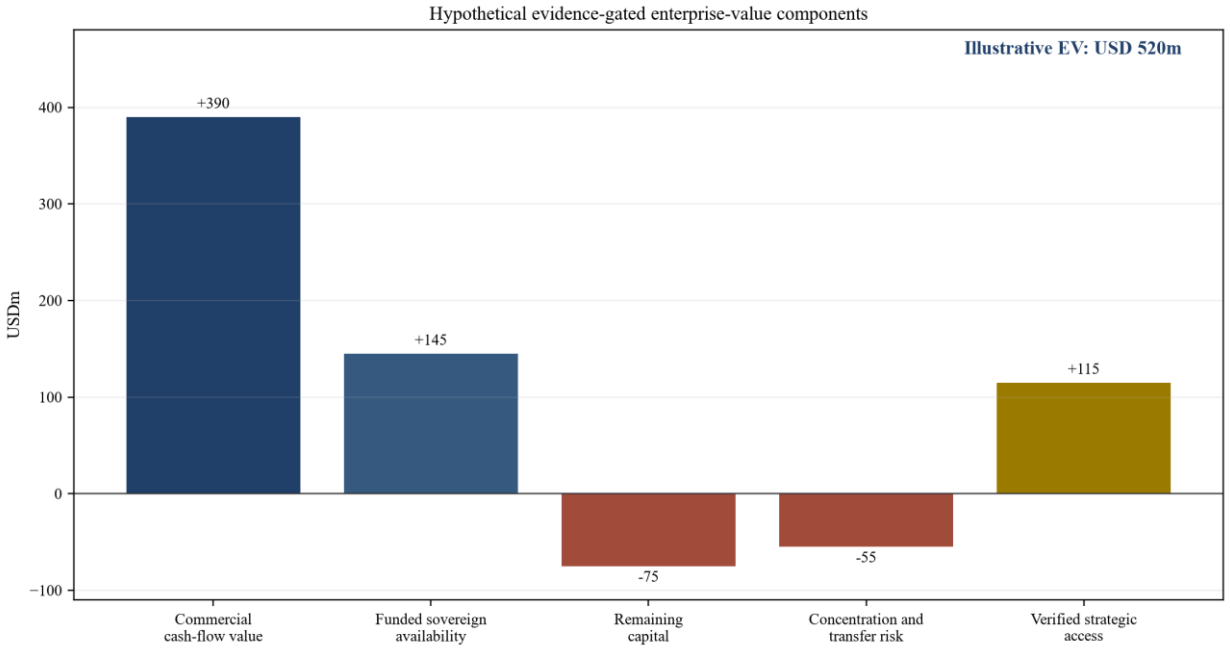
Illustrative USD millions; all figures are management assumptions used only to demonstrate the framework.

Figure 4. Hypothetical partner-ranking matrix



Illustrative scores from one to five; threshold security or regulatory failures override aggregate score.

Figure 5. Hypothetical transaction-value bridge



Illustrative USD millions; strategic access is included only after legal and technical verification.

Table 1. Sovereign-control allocation

Control domain	State or security authority	Venture management	International operator	Minimum evidence
Sovereign service	Define users, priority and minimum continuity	Deliver and report	Supply contracted capability	Accepted service specification
Spectrum and licences	Approve national permissions	Maintain compliance ledger	Support filings and coordination	Effective authorisations
Cryptographic policy	Approve policy and custodians	Operate controlled processes	Provide interoperable technology	Key ceremony and audit
Network operations	Set sovereign constraints	Schedule and operate	Provide capacity and support	Operating demonstration
Incidents	Receive and direct sovereign response	Contain, recover and notify	Cooperate under agreed protocol	Exercised response plan
Crisis capacity	Trigger authorised priority	Execute allocation	Honour pre-emption and restoration	End-to-end exercise

Proposed allocation; final authority depends on applicable law, contract and security accreditation.

Table 2. Data and access ledger

Data class	Typical purpose	Required decision	Principal control	Evidence
Customer payload	User communications	Routing, storage and authorised access	Encryption and traffic separation	Packet-path test
Traffic metadata	Operations and billing	Retention and lawful access	Restricted analytics and deletion	Processing register
Spacecraft telemetry	Safety and maintenance	Access and exportability	Segregated operations and logging	Role test
Security logs	Detection and investigation	Location, recipients and integrity	Protected collection and dual access	Log reconciliation

Data class	Typical purpose	Required decision	Principal control	Evidence
Identity records	Authentication	Controller, processor and transfer	Strong identity and minimisation	Access review
Cryptographic material	Protected services	Custody, backup and recovery	Hardware security modules and dual control	Witnessed key ceremony

Proposed minimum fields for deciding residency, access and retention.

Table 3. Hypothetical stabilised revenue and cash

Item	USDm	Evidence gate	Principal downside
Sovereign availability revenue	80	Funded minimum commitment and accepted service	Budget or acceptance delay
Critical-infrastructure capacity	45	Executed contracts and connected terminals	Concentration and churn
Enterprise and wholesale capacity	50	Committed service orders	Price and utilisation
Managed security and terminals	10	Accepted deliverables	Integration delay
Total contracted revenue	185	Reconciled contract ledger	Combined schedule risk
Distributable cash	44	Accepted invoices and reserves funded	Cost and collection stress

Illustrative USD millions; every amount is a management assumption and describes no existing venture.

Table 4. Hypothetical sources and uses

Source or use	USDm	Purpose or condition
State sponsor equity	170	Sovereign facilities, control and initial liquidity
Operator contribution	130	Capacity rights, technology and cash contribution
Infrastructure investor equity	90	Growth and independent capital
Limited-recourse debt	160	Drawn after contracts, permits and acceptance gates
Total sources	550	Fully funded illustrative plan
Capacity and space-segment rights	190	Contracted multi-year access
National gateways and backhaul	105	Permitted and commissioned facilities
Security, key custody and operations	80	Accredited sovereign operating capability
Terminals and customer integration	65	Accepted user access
Fees, reserves and liquidity	110	Completion, lifecycle and downside protection
Total uses	550	Illustrative funding requirement

Illustrative USD millions; financing terms and tax consequences require separate advice.

Table 5. Partner threshold and scoring framework

Dimension	Threshold question	Scored evidence	Failure response
Regulatory fit	Can the structure lawfully operate and close?	Licence record and authority engagement	Restructure or stop
Security assurance	Can sovereign controls be accredited?	Architecture, tests and cleared capability	Remediate before commitment
Continuity	Can minimum service survive partner unavailability?	Exercised national operating mode	Fund localisation or stop
Capability	Does the partner deliver accepted performance?	In-service record and reference tests	Limit scope or stage value
Economics	Are contributions and related-party terms transparent?	Benchmarks, cash and audited services	Reprice and add controls
Alignment	Are crisis, investment and exit incentives workable?	Binding governance and funding terms	Renegotiate structure

Proposed investment-committee screen; a threshold failure is not cured by a high aggregate score.

Table 6. Hypothetical consideration structure

Consideration	USDm	Release condition	Protection
Cash at completion	335	Transferable assets, effective rights and funded contracts	Warranties, escrow and conditions
Accreditation milestone	45	Authorised sovereign service	Independent acceptance
National continuity milestone	40	Exercised minimum service without foreign control plane	Defined test and remediation
Customer-retention milestone	35	Contribution retained after migration	Revenue and margin threshold
Collected-cash milestone	25	Reconciled third-party receipts	Set-off and clawback
Seller rollover	40	Continuing equity and funding alignment	Governance and dilution terms

Illustrative USD millions linked to observable outcomes.

Table 7. Board approval gates

Gate	Decision question	Minimum evidence	If evidence fails
Service	Is the sovereign output defined and funded?	Service specification and customer authority	Redefine scope
Rights	Can the network lawfully operate?	Spectrum, licences and approvals	Condition or stop
Control	Are reserved powers technically enforceable?	Control matrix and demonstrations	Redesign governance
Security	Can the system be accredited and keys controlled?	Architecture, test and authority record	Stage capital

Gate	Decision question	Minimum evidence	If evidence fails
Continuity	Can minimum service survive partner loss?	Exercised failover and funded remediation	Localise or resize
Economics	Does cash cover operations, reserves and financing?	Evidence-linked model and downside	Reprice or restructure
Transaction	Does consideration follow transferable value?	Value bridge and contingent terms	Defer payment

Proposed decision sequence and evidence standard.

Frequently asked questions

Q: Does majority state ownership establish sovereign control? A: Majority ownership establishes corporate rights only to the extent provided by law and the venture documents. Sovereign control also requires enforceable authority over security policy, cryptographic keys, privileged access, mission or network operations, crisis capacity, data handling and continuity. Each right should connect to a technical mechanism and exercised procedure.

Q: Should all data remain inside the sponsoring state? A: The answer depends on data class, applicable law, national-security policy, customer contract and operating need. The venture should map content, metadata, telemetry, logs, identity records, software and backups separately. It should then approve storage, processing, access, transit, retention and transfer for each class with local legal and security advice.

Q: What is the minimum evidence for encryption sovereignty? A: Minimum evidence includes an approved cryptographic policy, controlled key generation and custody, hardware and software inventory, authorised personnel, dual-control procedures, audit logs, recovery capability, tested interoperability and an upgrade path. A contractual statement that traffic is encrypted does not prove sovereign key control.

Q: How should crisis capacity be priced? A: Pricing should reflect reserved technical capacity, readiness, terminals, secure operations, exercise cost, commercial pre-emption, restoration obligations and lifecycle capital. A funded availability payment can support these costs. Usage charges can cover activated service. The contract should state triggers, duration, measurement and compensation.

Q: Can a foreign operator retain routine network control? A: It can retain defined routine authority when the arrangement complies with local law and approved security architecture. The state should retain or supervise specified sovereign functions and maintain an exercised continuity route. Privileged access, software deployment, incident response and crisis allocation should follow explicit controls.

Q: How should a board value strategic access? A: Commercial cash flows should be valued first. Strategic access should be stated separately with the service, alternative, consequence, probability, funding source and evidence. It should be recognised only when rights, technical capability, operating readiness and continuity are verified and when the benefit is not already captured in availability revenue.

Q: What should be linked to deferred consideration? A: Suitable milestones include regulatory approval, security accreditation, national key custody, service acceptance, continuity exercises, customer migration, retained contribution and collected cash. Each milestone needs an objective test, independent evidence, deadline, dispute process and treatment of partial performance.

Q: What should directors monitor after closing? A: Directors should monitor effective licences, spectrum coordination, accepted availability, capacity allocation, key-management exceptions, privileged access, incidents, continuity tests, supplier concentration, lifecycle capital, related-party performance, customer retention, liquidity, debt-service coverage and cash collection against the approved transaction case.

References

[1] International Telecommunication Union, Satellite regulation and coordination. https://www.itu.int/en/mediacentre/backgrounders/Pages/Regulation-of-Satellite-Systems.aspx

[2] International Telecommunication Union, Radio Regulations. https://www.itu.int/pub/R-REG-RR

[3] International Telecommunication Union, Frequently Asked Questions on ITU Satellite Filings, March 2025. https://www.itu.int/en/ITU-R/Documents/FAQs%20on%20ITU%20satellite%20Fillings-March%202025.pdf

[4] International Telecommunication Union, e-Submission of Satellite Network Filings. https://www.itu.int/ITU-R/go/space-e-submission/en

[5] International Telecommunication Union, Space Services Department. https://www.itu.int/ITU-R/go/space/en

[6] European Union, Regulation (EU) 2023/588 establishing the Union Secure Connectivity Programme. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R0588

[7] European Commission, IRIS2 concession contract awarded to the SpaceRISE consortium, 7 November 2024. https://digital-strategy.ec.europa.eu/en/news/iris2-european-commission-awards-concession-contract-spacerise-consortium

[8] European Space Agency, ESA to support the development of the EU secure communication satellites system, 16 December 2024. https://www.esa.int/Newsroom/Press_Releases/ESA_to_support_the_development_of_EU_s_secure_communication_satellites_system

[9] United Kingdom Space Agency, Cyber Security Toolkit for space assets, 2021. https://www.gov.uk/government/publications/cyber-security-toolkit

[10] United Kingdom Government, Cyber resilience in space, 2025. https://www.gov.uk/government/publications/unlocking-space-govbridge-resources/cyber-resilience-in-space--2

[11] United Kingdom Government, Secure by Design: Cultivating a Culture of Information Security, 2025. https://www.gov.uk/government/publications/unlocking-space-security-awareness-resources/secure-by-design-cultivating-a-culture-of-information-security

[12] United Kingdom National Cyber Security Centre, Cyber Assessment Framework, Principle B4 System Security. https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-b/principle-b4-system-security

[13] United Kingdom National Cyber Security Centre, Secure by Default. https://www.ncsc.gov.uk/information/secure-default

[14] United Kingdom Government, National Security and Investment Act guidance on notifiable acquisitions in Satellite and Space Technology. https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions/national-security-and-investment-act-guidance-on-notifiable-acquisitions

[15] United Kingdom Government, UK Space Strategy, 2026. https://www.gov.uk/government/publications/uk-space-strategy/uk-space-strategy

[16] United States Department of the Treasury, Committee on Foreign Investment in the United States. https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius

[17] United States Government Accountability Office, DOD Satellite Communications: Reporting on Progress Needed to Provide Insight on New Approach, GAO-25-107034, 2025. https://www.gao.gov/products/gao-25-107034

[18] United States Government Accountability Office, Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed, GAO-02-781. https://www.gao.gov/products/gao-02-781

[19] United States Government Accountability Office, Telecommunications: Competition, Capacity, and Costs in the Fixed Satellite Services Industry, GAO-11-777. https://www.gao.gov/products/gao-11-777

[20] United States National Institute of Standards and Technology, FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, 2024. https://csrc.nist.gov/pubs/fips/203/final

[21] United States National Institute of Standards and Technology, FIPS 204, Module-Lattice-Based Digital Signature Standard, 2024. https://csrc.nist.gov/pubs/fips/204/final

[22] United States National Institute of Standards and Technology, FIPS 205, Stateless Hash-Based Digital Signature Standard, 2024. https://csrc.nist.gov/pubs/fips/205/final

[23] United States National Institute of Standards and Technology, Zero Trust Architecture, SP 800-207, 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

[24] United States National Institute of Standards and Technology, Cybersecurity Framework 2.0, 2024. https://www.nist.gov/cyberframework

[25] United Arab Emirates, Federal Decree-Law No. 45 of 2021 Concerning the Protection of Personal Data. https://www.uaelegislation.gov.ae/en/legislations/1972/download

[26] Dubai International Financial Centre, Data Protection Law No. 5 of 2020. https://www.difc.com/business/laws-and-regulations/legal-database/data-protection-law-difc-law-no-5-2020

[27] Consultative Committee for Space Data Systems, Security Working Group publications. https://public.ccsds.org/Publications/Security.aspx

[28] European Union Agency for Cybersecurity, Space threat landscape. https://www.enisa.europa.eu/publications/enisa-space-threat-landscape

[29] United States Federal Communications Commission, Space Bureau. https://www.fcc.gov/space

[30] United States Office of Space Commerce, Licensing of private remote-sensing space systems. https://space.commerce.gov/regulations/commercial-remote-sensing-regulatory-affairs/licensing/

[31] United States Department of Justice and Federal Trade Commission, Merger Guidelines, 2023. https://www.justice.gov/atr/2023-merger-guidelines

[32] European Commission, EU merger control. https://competition-policy.ec.europa.eu/mergers_en

[33] IFRS Foundation, IFRS 3 Business Combinations. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/

[34] IFRS Foundation, IFRS 13 Fair Value Measurement. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-13-fair-value-measurement/

About the Author

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.

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.