# GCC Space-Security JVs: Sovereign Control without Fragmented Architecture

*A Transaction Framework for Technology Access, Operational Accountability and Regional Scale*

**Authored by Chennakeshav Adya**

Independent Researcher

September 2026

---

## Abstract

*Gulf governments and national champions can use joint ventures to combine sovereign control with foreign space technology, specialist talent and global operating experience. The transaction can also divide one mission across separate ownership, licensing, data, command, spectrum and cybersecurity regimes. A legal majority or reserved-matters list does not by itself create operational sovereignty. Control depends on whether the venture can make authorised decisions, operate critical services, access necessary technology, respond to incidents and continue after a supplier or shareholder disruption.*

*This paper develops an evidence-led transaction framework for GCC space-security joint ventures. It defines sovereign control as a set of decision, access, continuity and accountability capabilities. It then maps those capabilities to the system architecture, operating model, technology licence, export-control perimeter, regulatory permissions, data governance, cybersecurity design, financing, shareholder agreement and exit provisions. The framework is designed for satellite communications, Earth observation, ground infrastructure, hosted payloads, non-terrestrial networks and hybrid government-commercial services.*

*The analysis draws on the UAE space regulatory framework and National Space Strategy, Saudi space and non-terrestrial-network regulation, national cybersecurity controls, Qatar spectrum licensing, International Telecommunication Union filing processes, NIST guidance for hybrid satellite networks, CCSDS security architecture, United Nations space treaties and United States export-control guidance. These sources identify relevant obligations and design constraints. They do not establish that one governance structure is suitable for every jurisdiction, mission or technology.*

*A wholly hypothetical venture illustrates the method. A GCC national investor and an international space-technology company propose a USD 240 million regional platform. The national investor holds 51 percent and the technology partner holds 49 percent. Management assumes USD 120 million of initial equity, USD 70 million of asset financing and USD 50 million of milestone-linked customer prepayments and grants. The proposed structure uses a controlled technology-access schedule, an independent mission-assurance function, mirrored operational capability, a USD 20 million continuity reserve and staged release of economics against verified capability transfer. These figures are management assumptions, not observed transaction terms or market forecasts.*

*The central conclusion is that sovereign control and integrated architecture can reinforce each other when governance follows the mission's critical paths. The venture should allocate authority at the same level as technical dependency, preserve a single system design authority, test continuity without either shareholder and connect economic rights to measurable transfer and service outcomes. The resulting structure can support national objectives while preserving the interoperability, safety and commercial discipline required for regional scale.*

**JEL Classification:** G34, L14, L63, L96, O32, O38, P45

**Keywords:** space security, GCC joint ventures, sovereign control, technology transfer, satellite architecture, cybersecurity, M&A, export controls, operational resilience, spectrum licensing

## Introduction

Space-security ventures combine strategic infrastructure, specialised technology, public obligations and commercial capital. A GCC sponsor may seek national control over command, data, service availability, regulatory relationships and critical skills. A foreign partner may contribute spacecraft technology, payloads, software, ground systems, intellectual property, engineering methods and access to global suppliers. The joint venture must integrate these contributions into one service that can be licensed, financed, operated and defended.

The transaction often begins with ownership percentages and board rights. Operational reality begins elsewhere. It sits in cryptographic keys, source access, engineering authority, export licences, ground-station control, spectrum rights, vendor contracts, incident response, mission assurance and the ability to restore service. If those elements remain outside the venture, a majority shareholder can possess formal control while depending on a minority partner for every consequential action.

Fragmentation creates the opposite risk. A sponsor can insist on separate national systems, duplicated interfaces and multiple approval paths until the architecture becomes expensive and difficult to operate. The desired outcome is an integrated technical system with explicit sovereign-control points. This paper presents a transaction method for reaching that outcome.

## 1 Define the sovereign-control objective

The parties should define which national outcomes the venture must deliver. These may include assured service availability, control of sensitive data, national command authority, domestic incident response, local engineering capacity, supply-chain resilience, economic participation and compliance with international obligations. Each outcome should be expressed as a capability that can be evidenced.

Ownership is one capability among several. A 51 percent holding can support appointment rights and economic control. It does not prove access to source code, command credentials or replacement suppliers. A golden share can protect defined national decisions. It does not operate a ground segment during an incident. The sovereign-control statement should therefore identify the decision, asset, data, technology, people and continuity rights that matter.

The statement should also define limits. Export-controlled technology, third-party intellectual property and safety responsibilities may constrain access. Those limits should be known before valuation and commitment. A credible structure states what national control means in practice and which dependencies remain external.

## 2 Classify the mission and service perimeter

The venture should map the services it will provide and the missions they support. Satellite communications, Earth observation, positioning augmentation, hosted payloads, space-domain awareness and non-terrestrial connectivity can create different security, licensing and customer requirements. A mixed platform may carry both commercial and government services with different access and assurance levels.

The service perimeter should connect customer obligations to space, ground, network, cloud, data and support components. It should identify which legal entity owns each component, which party operates it, where it is located and which regulator or authorisation applies. The map should include third-party

ground stations, launch services, cloud regions, identity platforms, terrestrial carriers and specialist software.

Hybrid satellite networks can combine independently owned and operated segments into one service. NIST's profile treats varying trust levels and integration boundaries as core risk questions. The transaction should use the same approach. The perimeter is complete only when every critical service has an accountable operator, an authorised control path and a continuity route.

## 3 Separate ownership from operational control

Operational control should be decomposed into specific rights. These include authority to schedule missions, approve configurations, issue commands, manage cryptographic material, accept releases, suspend unsafe operations, declare incidents, notify regulators and restore services. The rights should be assigned to named functions rather than broad shareholder categories.

The board can reserve major policy and capital decisions. The mission-control function needs faster authority within approved boundaries. A joint approval for every operational change can delay response. Unilateral authority for the technology partner can weaken national accountability. The operating model should establish delegated authority, dual control for defined high-consequence actions and emergency procedures with retrospective review.

Evidence should include role descriptions, system permissions, approval matrices and exercise records. The venture should demonstrate that legal authority and technical access match. An officer cannot exercise a reserved right if the relevant platform permits only the other shareholder's employees to act.

## 4 Preserve one system design authority

An integrated architecture needs one accountable design authority. That function maintains the end-to-end baseline, approves interfaces, manages configuration, evaluates security and safety impact and resolves conflicts between shareholders or suppliers. It can sit within the venture while drawing specialists from both parties.

The design authority should own the system model and interface catalogue. Shareholders may retain component intellectual property. The venture still needs sufficient information to understand how components interact, test changes and diagnose failures. Black-box interfaces require performance, logging, security, support and exit obligations that make them governable.

Architecture boards should avoid parallel designs for national and commercial operations unless mission requirements justify separation. Segmentation can protect sensitive functions. Duplication without a defined control objective increases cost and failure points. Every separation should state the threat, authority or regulatory requirement it addresses.

## 5 Build the regulatory authority map

GCC space and telecommunications regulation is jurisdiction specific. In the UAE, the federal space framework requires permits for regulated space activities and identifies the UAE Space Agency as the federal regulator. Satellite services and spectrum also involve the Telecommunications and Digital Government Regulatory Authority. Saudi regulation involves the Communications, Space and Technology Commission, including non-terrestrial-network permissions, spectrum and cybersecurity obligations. Qatar's Communications Regulatory Authority manages spectrum and has issued public satellite telecommunications licences.

The venture should create an authority map for each jurisdiction in which it owns assets, operates facilities, uses spectrum, markets services, processes regulated data or supports public customers. The map

should identify licence holder, permit conditions, filing obligations, responsible manager, renewal date, change-of-control requirements and incident notification.

The map must distinguish current binding requirements from consultations, guidance and proposed rules. Saudi space-sector regulations were the subject of public consultation during 2026. Transaction documents should not treat a consultation text as enacted law. Qualified counsel should confirm the operative regime at signing and closing.

## 6 Align national authorisation with international responsibility

The Outer Space Treaty places responsibility on states for national space activities and requires authorisation and continuing supervision of non-governmental activities. It also connects registration with jurisdiction and control over a space object. A joint venture that spans ownership, launch, operation and service jurisdictions should identify which state performs each international role.

The parties should allocate responsibility for launch procurement, registration, supervision, liability support, harmful-interference management and treaty reporting. The commercial contracts should provide the information and cooperation needed by the relevant state authorities. Shareholder confidentiality cannot prevent a licensed operator from satisfying a lawful reporting obligation.

Continuing supervision is an operating requirement, not a closing item. The venture needs records, audit rights, change notifications and incident processes that remain effective throughout the mission. The board should receive a regulatory assurance report linked to the mission baseline and material changes.

## 7 Secure spectrum and orbital-resource rights

Spectrum and orbital resources can be central to service value. The International Telecommunication Union filing process operates through notifying administrations, and national regulators manage domestic authorisations. The venture should identify the filing sponsor, coordination status, milestones, national licence conditions and rights to use associated network filings.

Rights should be tested for transferability and dependency. A shareholder may control a filing or gateway licence that the venture expects to use. The agreement should state whether the right is assigned, licensed, sponsored or provided as a service; the circumstances in which it can be withdrawn; and the continuity path if the shareholder exits.

Technical and commercial teams should share one spectrum register. It should connect frequency bands, beams, coverage, gateways, terminals, customer services, interference obligations and renewal dates. A valuation should reflect the actual legal and coordination status rather than treating an application or partner commitment as an owned asset.

## 8 Define the technology-access perimeter

The technology-access schedule should identify each item the venture needs to design, integrate, operate, maintain, secure and replace the system. Items can include specifications, software, source code, development tools, cryptographic interfaces, test equipment, manufacturing data, supplier information, models, training and engineering support.

Access should be classified by purpose. Operational access permits routine use. Diagnostic access supports incident and failure analysis. Modification access enables change. Manufacturing access supports local production. Continuity access becomes available after a trigger. Each class may require different export permissions and protections.

The schedule should record owner, control classification, authorised users, territory, end use, sublicensing, storage, audit and termination treatment. A broad promise to transfer technology is too imprecise for valuation or enforcement. The venture should measure delivered capability against an itemised baseline.

## 9 Treat export control as an architecture input

United States controls can apply to defence articles, technical data, defence services, dual-use spacecraft, software and technology. DDTC guidance identifies Technical Assistance Agreements and Manufacturing License Agreements as relevant authorisation paths for certain foreign support and manufacture. Bureau of Industry and Security rules address exports, reexports and releases of controlled technology to foreign persons.

The parties should obtain jurisdiction and classification analyses before assuming that technology can enter the venture. The proposed ownership, employees, subcontractors, cloud environment, support model, countries and end users can affect the required permissions. An approval for one activity or programme should not be treated as authority for a different transfer.

Architecture decisions can reduce exposure. The system may separate controlled modules, use documented interfaces, retain support in an authorised environment or develop independent national components. These choices should preserve mission integrity and avoid a collection of opaque gateways. Export counsel, engineers and transaction teams should evaluate the same design.

## 10 Design the intellectual-property stack

The intellectual-property structure should distinguish background technology, venture-funded developments, local adaptations, mission data, operational know-how and independently developed improvements. Each category needs ownership, licence scope, access, protection, enforcement and exit treatment.

Background technology can remain with the contributing shareholder while the venture receives a durable field-of-use licence. Venture-funded development may be owned by the venture or allocated with cross-licences. The decision should reflect who funds development, who bears liability, who needs future use and what export rules permit.

Continuity rights deserve separate treatment. Escrowed source code without build tools, documentation, keys or trained staff can have limited value. A complete continuity package should be verified periodically and released on objective triggers such as insolvency, support failure, prohibited withdrawal or persistent service breach, subject to applicable authorisations.

## 11 Govern data by function and consequence

Space ventures can generate command data, telemetry, payload data, derived products, customer information, security logs, engineering records and regulatory reports. The data schedule should identify owner, controller, location, access, classification, retention, permitted use and export or disclosure restrictions.

Sovereign-control objectives may require national storage or access for selected data. The architecture should implement those requirements through segmentation, encryption, key control, logging and approved support paths. Copying every dataset into an isolated national environment can weaken consistency and increase attack surface. The venture should preserve a governed authoritative record for each data class.

Derived models and analytics require attention. A foreign partner may use operational data to improve a global product. The national shareholder may require local value and protection of sensitive patterns. The agreement should define training, aggregation, anonymisation, model ownership and prohibited use.

## 12 Establish cryptographic and identity control

Cryptographic authority often provides the most direct expression of operational control. The venture should define who generates, stores, rotates, revokes and recovers keys for command, payload, ground and customer systems. Dual control can protect high-consequence actions. National custody can support sovereign requirements when the operating model can still meet availability and support needs.

Identity governance should cover shareholder staff, venture employees, suppliers, service accounts and emergency access. Role assignments should follow mission function. Access should be time bound, reviewed and logged. Remote support should use approved paths that can be suspended without disabling the service.

The venture should test continuity after loss of a shareholder identity service or support team. Mirrored national capability can include resilient identity, break-glass procedures and trained operators. The objective is verified independence for defined critical actions rather than permanent duplication of every administrative tool.

## 13 Build cybersecurity into the joint operating model

National cybersecurity controls, NIST hybrid-network guidance and CCSDS security architecture provide complementary perspectives. The venture should translate them into one control baseline covering governance, asset management, access, configuration, monitoring, incident response, recovery, supply chain and assurance.

The control baseline should identify the accountable entity for each shared service. A shareholder-operated ground system should not sit outside the venture's risk model. The service agreement should define control evidence, incidents, audit rights, remediation and continuity. Material exceptions should be visible to the board and relevant authorities.

Security operations need a joint escalation model. The venture should define who can isolate a component, suspend a link, revoke access, preserve evidence, notify customers and contact national authorities. Exercises should include disagreement between shareholders and loss of one party's support.

## 14 Protect mission assurance and safety independence

Mission assurance should have authority independent of delivery and commercial pressure. It should review architecture, changes, supplier evidence, test results, anomalies and readiness. The head of mission assurance should have a direct route to the board or a board committee for unresolved high-consequence risks.

The function should maintain acceptance criteria and evidence. Shareholder nominations can provide expertise, but the venture should avoid a veto that allows one supplier to accept its own unresolved risk. Independent technical advisers can support defined reviews when export and confidentiality rules permit.

Safety and security decisions should use a common change process. A security patch can affect mission stability. A continuity workaround can weaken access control. The design authority and mission-assurance function should evaluate the combined consequence and record the accepted residual risk.

## 15 Create a sovereign capability-transfer plan

Capability transfer should be designed as an operating programme. It can cover mission operations, systems engineering, cybersecurity, supplier management, regulatory reporting, data exploitation, product development and commercial delivery. Each capability needs a target proficiency, evidence method, accountable mentor and deadline.

Training attendance is insufficient evidence. Operators should perform supervised tasks, respond to anomalies, execute recovery and make authorised decisions. Engineering teams should reproduce builds, analyse interfaces and approve changes within the authorised scope. Management should demonstrate that the venture can plan budgets, procure services and govern suppliers.

Economic rights can be linked to verified transfer. A portion of licence fees, milestone payments or shareholder distributions can depend on the venture reaching defined capability levels. The mechanism should respect export restrictions and avoid promising access that cannot lawfully be delivered.

## 16 Design localisation without forced fragmentation

Localisation can create jobs, supply resilience and national expertise. It can also produce uneconomic duplication if every component is localised without regard to scale or risk. The venture should rank activities by strategic consequence, learning value, market demand and feasibility.

High-priority activities may include mission operations, cybersecurity, data products, integration, selected ground infrastructure and supplier assurance. Global-scale component manufacture may remain with specialist suppliers until volume and capability support localisation. The roadmap should state the evidence required to move an activity into the venture.

Interfaces should remain standard and testable. Local components should enter through the same architecture, qualification and configuration process as foreign components. A national requirement should not create an undocumented parallel system that weakens reliability or regional interoperability.

## 17 Structure the board and reserved matters

The board should reflect economic ownership, sovereign obligations and independent technical judgement. A majority national shareholder may appoint more directors. The technology partner may require protection for background intellectual property and controlled technology. Independent directors can support mission assurance, audit and conflicts.

Reserved matters should focus on consequence. They can include mission scope, regulated activities, critical architecture, controlled-technology use, cybersecurity baseline, key custody, material outsourcing, data policy, capital structure, related-party contracts and exit. Routine operations should remain delegated under an approved plan.

Deadlock mechanisms should distinguish strategic disputes from urgent operations. Escalation to shareholders can suit capital and scope questions. Safety, security and service-continuity decisions need a defined interim authority. Arbitration cannot restore a failing mission in real time.

## 18 Control related-party services

The technology partner may supply hardware, software, engineering and support. The national shareholder may provide customers, facilities, licences or financing. These contributions should be documented as related-party arrangements with scope, price, service levels, evidence, audit and termination rights.

The venture should compare related-party pricing with alternative evidence where practicable. Unique technology may lack a direct comparator. Cost build-ups, benchmark components, volume tiers and performance deductions can still create discipline. The board should understand which margin sits inside the venture and which remains with shareholders.

Service failure should have operational remedies before financial remedies. The venture may need step-in rights, access to suppliers, temporary licences and continuity resources. A damages claim against a shareholder does not by itself restore service.

## 19 Build an integrated capital plan

The capital plan should connect mission milestones, regulatory permissions, procurement, launch, ground infrastructure, working capital and contingency. Equity is suited to development and risk absorption. Asset finance can support identifiable equipment with appropriate security and cash flow. Customer prepayments and grants may support contracted milestones when their conditions are understood.

The plan should show which costs sit in the venture and which remain with shareholders. An apparently asset-light venture can depend on shareholder-funded development or guarantees. Valuation and returns should include these economic contributions.

Liquidity should cover delay, remediation and shareholder disruption. A continuity reserve can fund replacement support, mirrored operations, legal authorisations and customer obligations. Its size should follow scenario analysis rather than a percentage convention.

## 20 Value the contribution package

The transaction should value cash, tangible assets, licences, spectrum access, technology rights, people, customer contracts, guarantees and continuing services separately. A headline equity percentage does not show whether contributions are economically balanced.

Technology value depends on access, duration, exclusivity, authorised use, support, performance and continuity. A licence limited to one programme or dependent on a shareholder service can be worth less than a transferable operating capability. Spectrum and regulatory rights should be valued according to their actual legal status and conditions.

The contribution model should avoid counting the same value twice. A customer relationship reflected in forecast cash flow should not also be added as an independent asset without reconciliation. Management assumptions should be sensitivity tested and approved with conflicts disclosed.

## 21 Translate dependency into economic mechanics

Material dependency should have a financial response. If the technology partner retains a critical capability, part of its economics can vest against transfer, service and continuity milestones. If the national shareholder controls customer access or licences, its contribution can be measured against executed contracts and maintained permissions.

Holdbacks, earn-ins, performance fees and distribution preferences can support alignment. They should use objective evidence and avoid incentives that compromise safety or security. A milestone should state who verifies it, which exceptions are allowed and what happens after delay.

The venture should also price residual dependency. The board may accept reliance on a unique supplier because the technology advantage exceeds the risk. That decision should be visible in valuation, reserve and exit planning.

## 22 Plan for shareholder distress and disengagement

The operating model should survive insolvency, sanctions, export denial, change of control, strategic withdrawal and persistent service failure. Each scenario can affect technology, people, licences, suppliers and customer confidence differently.

The agreement should define notification, cure, step-in, licence continuation, source release, employee transition, replacement procurement and funding. Some rights may be conditional on external authorisation. The transaction should identify these conditions before treating the rights as reliable.

Exercises should test a credible disengagement scenario. The venture should demonstrate which services continue immediately, which degrade and how long replacement takes. The output informs liquidity, insurance, customer commitments and valuation.

## 23 Design exit without dismantling the mission

Exit provisions should preserve service, regulatory compliance and system integrity. A shareholder sale may trigger change-of-control review, export reauthorisation, licence consent and customer approval. The permitted-buyer test should therefore address nationality, capability, security and regulatory eligibility.

Put and call rights need a valuation method that recognises dependency. A technology partner should not receive full going-concern value after withdrawing essential support without an agreed adjustment. The national shareholder should not obtain background technology beyond the authorised continuity scope without compensation and approval.

Transition services should be detailed before exit. The agreement should identify duration, pricing, staffing, access, data transfer, security and dispute resolution. The venture's architecture and records should make separation executable.

## 24 Use a transaction data room built around decisions

The data room should connect corporate documents to technical and regulatory evidence. Core materials include ownership, permits, spectrum rights, filings, architecture, interfaces, technology classifications, licences, source-access evidence, cybersecurity controls, supplier contracts, customer obligations, capital plans and capability-transfer records.

Each material claim should identify source, owner, date, limitation and decision use. A licence application is not an issued licence. A memorandum of understanding is not a customer contract. A training plan is not operational capability. The diligence team should preserve those distinctions.

Access controls should protect classified, export-controlled and commercially sensitive material. Review protocols can use clean teams, controlled environments, summaries and specialist advisers. Restricted access should be recorded as a diligence limitation, with a completion condition where material.

## 25 Hypothetical GCC joint venture

A GCC national investment company and an international space-technology supplier propose a regional space-security platform. Management assumes USD 240 million of total programme funding. Initial sources are USD 120 million of equity, USD 70 million of asset financing and USD 50 million of customer prepayments and grants. The national investor owns 51 percent and the technology partner owns 49 percent.

The venture will operate a hybrid service using hosted payload capacity, national ground infrastructure and the technology partner's mission software. It will serve government and commercial customers. The shareholder agreement gives the national investor board majority and reserved rights over mission scope, regulated services, key custody, sensitive data and material outsourcing. The technology partner retains background intellectual property and supplies defined engineering services.

Diligence identifies four dependencies. The venture cannot reproduce one mission-software build, a foreign shareholder controls a global identity tenant, two specialist suppliers contract only with the technology partner and continuity rights have not been tested. Management allocates a USD 20 million continuity reserve and makes USD 16 million of technology-partner economics conditional on verified remediation and capability transfer. These amounts are wholly hypothetical.

## 26 Interpret the hypothetical economics

The capital stack should be tested against milestones. Asset financing is assumed to fund eligible ground and payload equipment after acceptance. Customer prepayments and grants are assumed to release against contracted evidence. Equity covers development, integration, working capital and contingency. Actual availability and terms would require lender, customer and grant documentation.

The continuity reserve is not presented as a probability-weighted loss estimate. It represents management's stated budget for mirrored identity, source and build verification, supplier novation, local operator qualification and incident exercises. The reserve remains within the venture until defined evidence gates are met.

The conditional economics align the technology partner with delivery of authorised access and capability. Release occurs in four hypothetical tranches: reproducible build, independent national operations, supplier continuity and tested disengagement. The mechanism should be adapted to actual export permissions and tax, accounting and legal advice.

## 27 Build the first 180-day programme

The first thirty days should establish governance, system authority, regulatory ownership and the dependency baseline. The venture should reconcile access rights, service obligations, permits, filings and critical suppliers. It should approve the control baseline and incident authority.

Days thirty-one to ninety should focus on executable capability. Teams should reproduce permitted builds, operate supervised missions, exercise incident response, establish national key custody and complete supplier novation or step-in arrangements. Funding should follow verified milestones.

Days ninety-one to one hundred eighty should test independence and scale. The venture should run a shareholder-disruption exercise, confirm regional licence plans, test recovery, approve the next architecture baseline and update the valuation and risk register. Unresolved dependencies should retain funding and board attention.

## 28 Set the board decision agenda

Before approving the transaction, the board should receive a control map showing each critical decision, technical access and accountable role. It should see the end-to-end architecture, regulatory authority map, export-control analysis, technology-access schedule, capital plan and continuity scenarios.

The board should identify accepted dependencies. It should understand which capabilities remain with shareholders, why the dependency is acceptable, how it is monitored and what happens after failure. The decision record should separate legal rights from tested operating capability.

Approval conditions should be specific. They can require permits, export authorisations, source verification, key custody, supplier agreements, customer contracts, funded reserves and exercises. The final decision should connect national outcomes to operational evidence and transaction economics.

## Conclusion

Sovereign control in a GCC space-security joint venture is a system of capabilities. It combines lawful authority, technical access, accountable operations, data and key governance, national expertise, supplier continuity and the ability to act during disruption. Ownership and reserved matters support that system when they align with the mission's critical paths.

Integrated architecture remains essential. A venture can protect national interests through clear control points, segmentation and evidence without creating parallel systems for every shareholder concern. One

system design authority, standard interfaces and common configuration control preserve mission integrity and regional scale.

The transaction should make dependency visible. Technology rights, export permissions, licences, people, customer access and continuing services should be valued separately and linked to objective milestones. The result is a joint venture that can serve national objectives, attract capital and operate as one accountable platform.

## Appendix A Sovereign-control test

The control test asks five questions. Can the venture make the required decision? Can authorised personnel execute it through the system? Can the venture access the necessary technology and data? Can it continue after a shareholder disruption? Can it evidence the action to its board, customers and regulators?

Each answer should identify the right, platform permission, accountable role, dependency and test result. A contractual right without access is incomplete. Access without authority is unsafe. Authority and access without continuity can fail during the event that matters most.

The test should be repeated after material changes in ownership, architecture, suppliers, regulation and export permissions.

## Appendix B Architecture principles

The architecture should preserve one authoritative baseline, explicit trust boundaries, least-privilege access, resilient identity, governed cryptographic control, observable interfaces, recoverable services and tested supplier continuity. Segmentation should address a defined risk or regulatory requirement.

Interfaces should specify functionality, performance, security, logging, versioning and support. Proprietary components can remain protected while providing enough evidence for integration and assurance. Material changes should enter one configuration process.

The design authority should maintain the relationship between mission requirements, technical components, licences, control evidence and customer obligations.

## Appendix C Joint venture data room

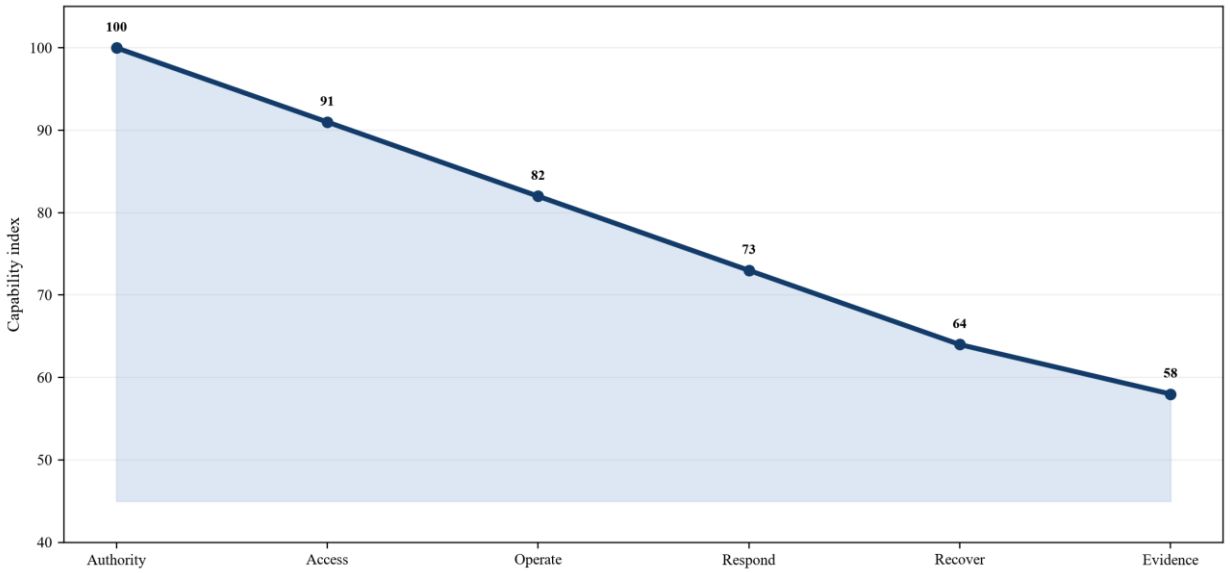
The data room can contain constitutional documents, shareholder arrangements, regulatory permissions, spectrum and orbital records, export classifications, licences, architecture, interface specifications, asset and supplier registers, cybersecurity evidence, mission-assurance records, customer contracts, financial models and capability-transfer plans.

Restricted material should use a defined review protocol. The diligence report should record information that could not be examined and the resulting decision limitation. Material gaps should become conditions, holdbacks or funded actions.

The final data room should support continuing supervision after closing. Records needed for permits, incidents, audits and customer assurance should move into controlled operational repositories.

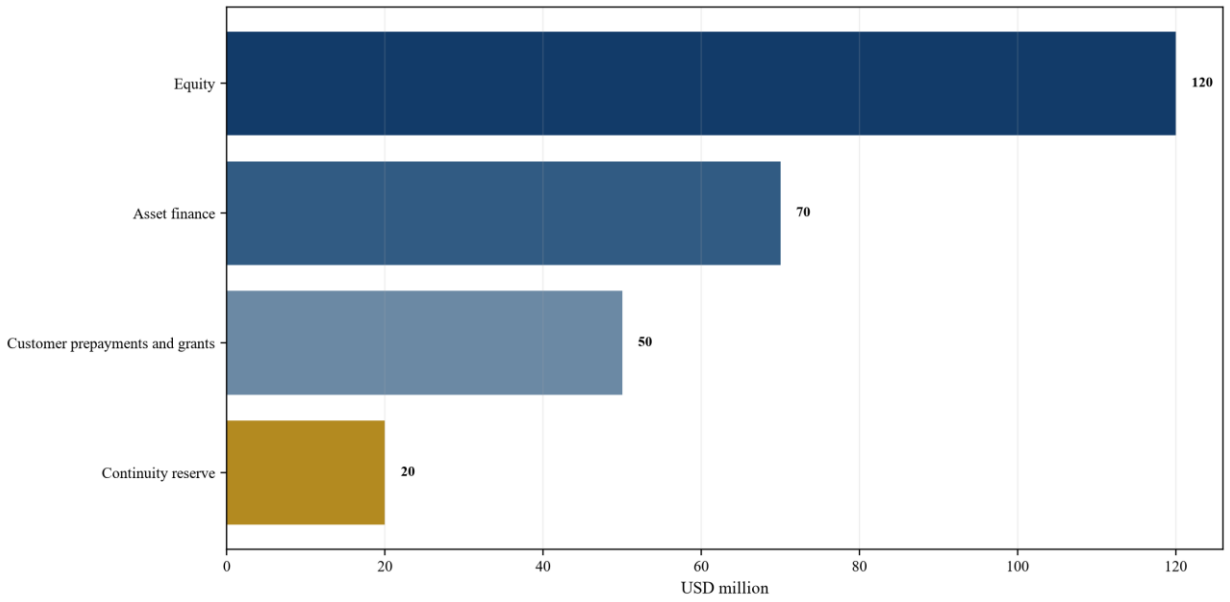
# Appendix D Decision figures and tables

**Figure 1. Sovereign-control capability chain**



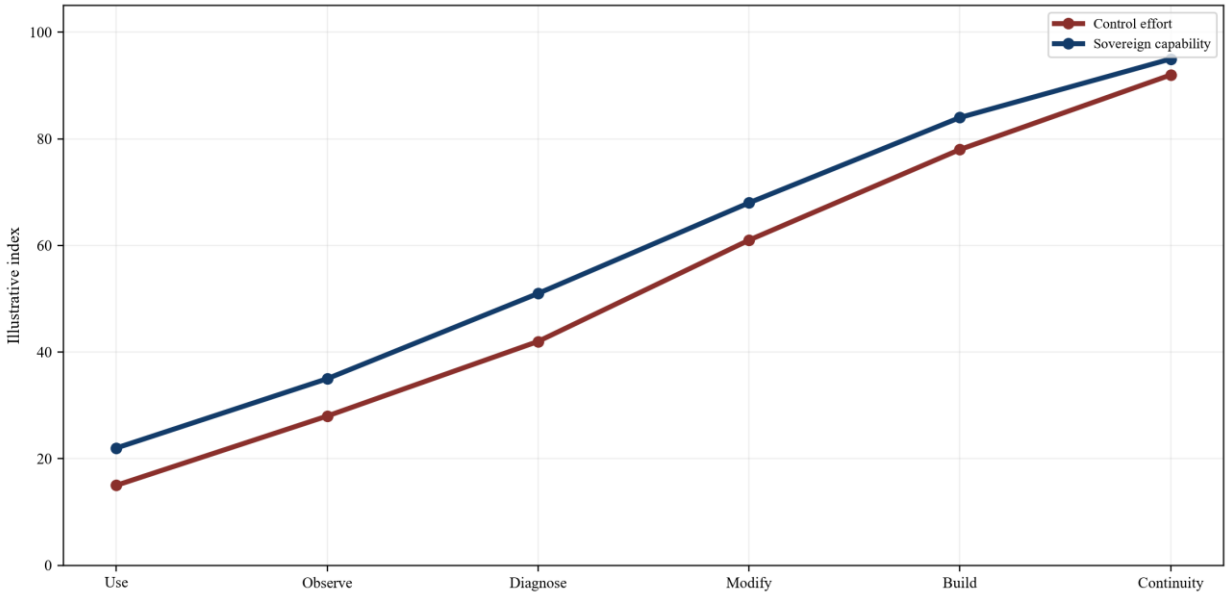

*Proposed progression from legal authority to tested continuity and accountable evidence.*

**Figure 2. Hypothetical joint-venture funding structure**



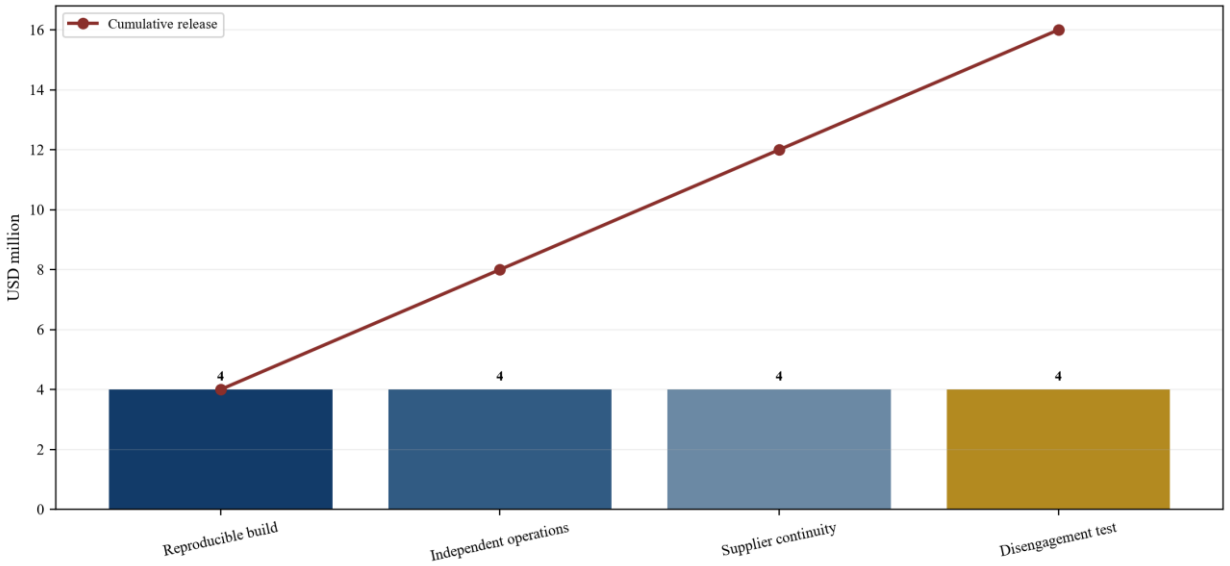

*Wholly hypothetical management assumptions; USD million.*

**Figure 3. Proposed technology-access ladder**



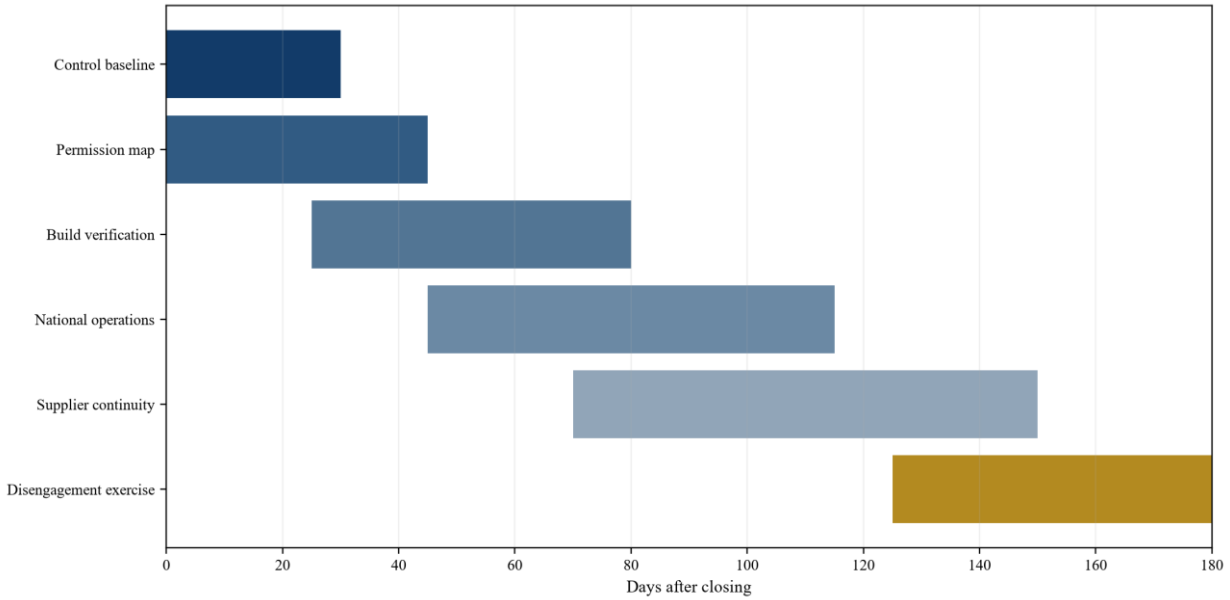

*Access should progress only where purpose, permission and controls support it.*

**Figure 4. Hypothetical economic release against capability**




*Wholly hypothetical technology-partner economics; USD million.*

## Figure 5. Illustrative 180-day capability programme




*Proposed sequence subject to regulatory and export authorisations.*

## Table 1. Sovereign-control evidence map

| Control area | Required capability | Evidence | Failure implication |
|---|---|---|---|
| Mission authority | Approve and suspend defined operations | Delegation, permissions and exercise records | Formal right cannot be executed |
| Technology access | Diagnose and maintain critical services | Itemised access schedule and verified tools | Persistent shareholder dependency |
| Data and keys | Govern sensitive data and cryptographic authority | Custody, logs and recovery tests | Loss of confidentiality or command control |
| Continuity | Operate after shareholder disruption | Mirrored capability and disengagement exercise | Service interruption and weak bargaining position |
| Accountability | Evidence actions to authorities and customers | Controlled records and reporting process | Regulatory and customer assurance failure |

*Proposed minimum evidence for a transaction decision.*

## Table 2. Critical rights and operating mechanisms

| Decision | Governance right | Operating mechanism | Evidence owner |
|---|---|---|---|
| Mission scope | Board reserved matter | Approved service and architecture baseline | Chief executive and design authority |
| High-consequence command | Delegated dual control | Role-based command authority and key custody | Mission operations |
| Emergency isolation | Incident authority | Predefined technical containment path | Security operations |
| Critical release | Design and assurance approval | Reproducible build and acceptance evidence | Design authority |
| Supplier replacement | Board threshold and delegated procurement | Step-in rights and qualified alternative | Chief operating officer |

*Proposed alignment of governance and system capability.*

### Table 3. Hypothetical programme funding

| Source or reserve | Illustrative amount | Intended use | Evidence condition |
|---|---|---|---|
| Shareholder equity | USD 120 million | Development, integration and working capital | Approved programme budget |
| Asset financing | USD 70 million | Eligible ground and payload equipment | Acceptance, security and lender conditions |
| Prepayments and grants | USD 50 million | Contracted customer and capability milestones | Executed documents and milestone evidence |
| Continuity reserve | USD 20 million | Mirrored operations and dependency remediation | Released only after board-approved tests |
| Conditional partner economics | USD 16 million | Technology and capability contribution | Four verified USD 4 million tranches |

*Wholly hypothetical management assumptions; not observed financing terms.*

### Table 4. Technology-access schedule

| Access class | Purpose | Minimum material | Principal condition |
|---|---|---|---|
| Operational | Run approved service | Procedures, interfaces and credentials | Authorised users and end use |
| Diagnostic | Investigate anomaly | Logs, tools and engineering support | Controlled environment and records |
| Modification | Correct or improve system | Source, build chain and test assets | Export permission and change control |
| Manufacturing | Produce authorised item | Drawings, process and quality data | Manufacturing authority and supplier controls |
| Continuity | Maintain service after trigger | Verified package, tools, keys and support | Objective trigger and continuing authorisation |

*Proposed categories; actual rights depend on law and authorisation.*

### Table 5. Dependency-to-transaction mapping

| Dependency | Risk | Mechanic | Release evidence |
|---|---|---|---|
| Non-reproducible mission build | Inability to maintain software | Holdback and source verification | Independent reproducible build |
| Shareholder identity tenant | Access and incident concentration | Funded mirrored identity | Loss-of-provider exercise passed |
| Shareholder-only suppliers | Continuity and pricing exposure | Novation or direct step-in rights | Executed supplier arrangements |
| Unauthorised technology promise | Invalid value assumption | Closing condition and valuation adjustment | Required approval obtained |
| Unassigned spectrum dependency | Service interruption or weak asset claim | Licence and filing condition | Regulator-confirmed operating rights |

*Proposed transaction treatments.*

### Table 6. First 180-day board dashboard

| Measure | Day 30 | Day 90 | Day 180 |
|---|---|---|---|
| Authority | Delegations and reserved matters aligned | High-consequence actions exercised | Exception log closed or funded |

| Measure | Day 30 | Day 90 | Day 180 |
|---|---|---|---|
| Technology | Access schedule reconciled | Permitted build reproduced | Continuity package verified |
| Operations | Roles and permissions mapped | National team completes supervised mission | Independent operations test passed |
| Suppliers | Critical dependency register approved | Direct rights negotiated | Disruption exercise passed |
| Regulation | Authority map and conditions confirmed | Required filings and permissions current | Regional expansion gates approved |

*Proposed milestone evidence.*

**Table 7. Board decision thresholds**

| Decision area | Green evidence | Amber condition | Red condition |
|---|---|---|---|
| Sovereign control | Authority, access and continuity tested | Time-bound dependency with funded plan | Formal control without executable capability |
| Architecture | One baseline and accountable design authority | Defined temporary interface exception | Fragmented systems without ownership |
| Technology | Rights and approvals match operating need | Limited access accepted with continuity | Material promise cannot be authorised |
| Regulation | Permits, filings and accountable holders confirmed | Approval pending with protected timetable | Critical activity lacks viable authorisation path |
| Economics | Contributions reconciled and milestones objective | Residual dependency priced and reserved | Value depends on unsupported contribution |

*Proposed decision framework.*

## Frequently asked questions

Q: Does 51 percent ownership give a GCC sponsor sovereign control over a space joint venture? A: Majority ownership can support board and economic control. Operational sovereignty also requires executable authority, access to critical systems and data, national capability, regulatory accountability and tested continuity. The transaction should evidence each capability separately.

Q: How can a venture protect national interests without duplicating the entire architecture? A: Define the specific national control points, including command authority, key custody, sensitive data, incident action and continuity. Preserve one system design authority, standard interfaces and common configuration control around those points.

Q: What technology should be transferred into the joint venture? A: The access schedule should follow the operating purpose. It can include operational, diagnostic, modification, manufacturing and continuity access. Each item requires a clear owner, authorised use, export status, control environment and exit treatment.

Q: How should export controls affect valuation? A: Value should reflect the rights that can lawfully be granted under the proposed ownership, workforce, end use and territories. A technology promise that lacks a viable authorisation path should not receive full operating-capability value.

Q: What is the role of a system design authority? A: The design authority maintains the end-to-end baseline, approves interfaces and changes, evaluates combined safety and security impact and resolves architectural conflicts. It helps the venture operate one integrated system across shareholder and supplier boundaries.

Q: How should the venture handle shareholder-supplied services? A: Use written related-party agreements with scope, price, service levels, evidence, audit, incident duties, continuity and termination rights. Material services should include executable step-in or replacement arrangements where feasible.

Q: What should happen if the technology partner exits or loses an export authorisation? A: The venture should activate a documented continuity plan covering notification, interim service, authorised access, source and tool release, supplier rights, replacement procurement, staffing and liquidity. The plan should identify rights that still depend on external approval.

Q: What should the board require before approving the joint venture? A: The board should require a control map, integrated architecture, authority and licence register, export analysis, technology-access schedule, capability-transfer plan, capital and valuation model, continuity reserve and tested conditions for material dependencies.

## References


**[1]** United Arab Emirates Government, Space Regulation and Federal Decree Law No. 46 of 2023 overview. https://u.ae/en/about-the-uae/science-and-technology/key-sectors-in-science-and-technology/space-science-and-technology/space-regulation

**[2]** United Arab Emirates Legislation, Federal Decree by Law No. 46 of 2023 Concerning the Regulation of the Space Sector. https://uaelegislation.gov.ae/en/legislations/2132/related-legislations

**[3]** United Arab Emirates Space Agency, National Space Strategy 2030. https://space.gov.ae/assets/download/ac4fd8ad/National%20Space%20Strategy%202030-compressed.pdf.aspx

**[4]** United Arab Emirates Legislation, National Space Policy. https://uaelegislation.gov.ae/en/policy/details/lsy-s-lotny-llfd-ldol-l-m-r-t-laarby-lmthd

**[5]** United Arab Emirates Space Agency, National Space Strategy and National Space Investment Plan announcement. https://space.gov.ae/en/media-center/news/15/10/2019/the-uae-space-agency-unveils-its-national-space-strategy-2030-and-national-space-investment-plan

**[6]** Communications Space and Technology Commission, Public Consultation on Space Sector Regulations and Guidelines, 2025. https://www.cst.gov.sa/en/media-center/news/N2025122502

**[7]** Communications Space and Technology Commission, Non-Terrestrial Networks Regulations. https://www.cst.gov.sa/media-center/news/CST-has-Published-the-Non-Terrestrial-Networks-Regulations

**[8]** Communications Space and Technology Commission, Provisioning of Operation Services of Non-Terrestrial Networks. https://www.cst.gov.sa/en/business/services/Provisioning-of-Operation-Services-of-Nonterrestrial-Networks-NTN

**[9]** Communications Space and Technology Commission, Regulations for the Provision of Broadband Satellite Services. https://www.cst.gov.sa/en/regulations-and-licenses/regulations/Document-499

**[10]** Communications Space and Technology Commission, Spectrum Outlook for Commercial and Innovative Use 2025 to 2027. https://www.cst.gov.sa/-/media/cst-website-app/data/media/Reports/CST%20Publications/EN/Spectrum%20Outlook%20for%20Commercial%20%20Innovative%20Use%202025%20%202027EN

**[11]** Saudi National Cybersecurity Authority, Essential Cybersecurity Controls 2 2024. https://nca.gov.sa/en/regulatory-documents/controls-list/ecc/

**[12]** Saudi National Cybersecurity Authority, Guide to Essential Cybersecurity Controls Implementation. https://nca.gov.sa/en/regulatory-documents/guidelines-list/1368/

**[13]** Communications Regulatory Authority Qatar, e-Spectrum Services Portal. https://www.cra.gov.qa/en/Services/Telecommunications/Spectrum-Management/e-Spectrum-Services-Portal

**[14]** Communications Regulatory Authority Qatar, Public Satellite Telecommunications Networks and Services License. https://www.cra.gov.qa/en/press-releases/public-satellite-telecommunications-networks-and-services-license

**[15]** International Telecommunication Union, Electronic Submission of Satellite Network Filings. https://www.itu.int/en/ITU-R/space/e-submission/FAQ/Pages/default.aspx

**[16]** United Nations Treaty Collection, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space. https://treaties.un.org/pages/showdetails.aspx?objid=0800000280128cbd

**[17]** United Nations Office for Outer Space Affairs, Space Law Treaties and Principles. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html

**[18]** National Institute of Standards and Technology, IR 8441 Cybersecurity Framework Profile for Hybrid Satellite Networks, 2023. https://csrc.nist.gov/pubs/ir/8441/final

**[19]** National Institute of Standards and Technology, IR 8401 Satellite Ground Segment Applying the Cybersecurity Framework to Satellite Command and Control, 2022. https://csrc.nist.gov/pubs/ir/8401/final

**[20]** National Institute of Standards and Technology, IR 8270 Introduction to Cybersecurity for Commercial Satellite Operations. https://csrc.nist.gov/pubs/ir/8270/final

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

**[22]** Consultative Committee for Space Data Systems, Security Architecture for Space Data Systems. https://ccsds.org/Pubs/351x0m1.pdf

**[23]** Consultative Committee for Space Data Systems, Charter and Standards Development. https://ccsds.org/about/charter/

**[24]** United States Department of State Directorate of Defense Trade Controls, Licensing and Agreement Guidance. https://deccs.pmddtc.state.gov/deccs?id=ddtc_search&q=itar

**[25]** United States Department of State Directorate of Defense Trade Controls, Manufacturing Licensing Agreement FAQ. https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_public_portal_faq_detail&sys_id=b8e5cf2f1b6909102dc36311f54bcb9e

**[26]** United States Bureau of Industry and Security, Export Administration Regulations Part 734 Scope of the EAR. https://www.bis.gov/regulations/ear/734

**[27]** United States Bureau of Industry and Security, Export Administration Regulations Part 742 Control Policy. https://www.bis.gov/regulations/ear/742

**[28]** Organisation for Economic Co-operation and Development, Guidelines on Corporate Governance of State-Owned Enterprises 2024. https://www.oecd.org/en/topics/corporate-governance-of-state-owned-enterprises.html

**[29]** International Organization for Standardization, ISO IEC 27001 Information Security Management Systems. https://www.iso.org/standard/27001

**[30]** International Organization for Standardization, ISO 22301 Security and Resilience Business Continuity Management Systems. https://www.iso.org/standard/75106.html

## 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.