Sovereign Networks, Open Vendor Choice: Structuring GCC Telecom-AI JVs

A transaction framework for preserving national control, multi-vendor interoperability and measurable capability transfer in intelligent network joint ventures

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Gulf telecommunications operators are moving toward cloud-native, programmable and AI-enabled networks while governments treat connectivity, data and cyber resilience as national infrastructure. Joint ventures can combine licensed market access, network assets and local operating authority with specialist software, radio, cloud and AI capability. The transaction challenge is to obtain technology and execution capacity without replacing one closed dependency with another.

This paper develops a Sovereign Network Joint Venture Framework for boards, operators, public investors, technology vendors and transaction teams. It separates legal sovereignty, operational control, architectural openness, technical interoperability, data governance, cybersecurity, intellectual-property rights, economics and capability transfer. The framework translates these dimensions into reserved matters, interface baselines, acceptance tests, staffing obligations, source-code and continuity protections, commercial milestones and exit rights.

Primary sources establish the direction of travel and the constraints. The UAE Telecommunications and Digital Government Regulatory Authority has placed artificial intelligence, virtualization, sensing, security and standards collaboration within its 6G roadmap. Saudi Arabia's communications authorities have published an Open RAN framework centred on interoperability, innovation and sovereignty. O-RAN ALLIANCE Release 5, completed in June 2026, adds AI and machine-learning workflow services, security controls and features for commercial deployment. ITU material emphasises open interfaces, programmable networks, AI-enabled operation and global interoperability. GCC licensing, data-transfer and critical-system rules also require transaction structures to respect local regulatory, security and ownership conditions.

A wholly hypothetical joint-venture case uses USD 360 million of committed capital. The local operator contributes spectrum-linked operating rights, sites, data access under applicable law, customer relationships and deployment authority. The technology partner contributes a disaggregated network stack, orchestration, AI models, engineering capability and global supplier access. The model releases capital against tested interoperability, local operational readiness, service levels, security assurance and knowledge-transfer outcomes. Every amount and operating assumption in the case is illustrative management input. It is not observed company data, a market forecast, a valuation opinion or an offer of financing.

The central conclusion is that sovereignty and open vendor choice require engineered rights and evidence. Local incorporation, a government-linked shareholder or an open-interface claim does not by itself establish control, portability or capability transfer. A durable joint venture assigns decision rights to the party that bears national obligations, makes interfaces and data rights testable, rewards

production outcomes, and provides credible continuity if a supplier, model, component or geopolitical condition changes.

JEL Classification: G31, G32, G34, L22, L51, L63, L96, O31, O32, O33

Keywords: sovereign networks, open RAN, telecom AI, joint ventures, vendor choice, capability transfer, GCC, network control, interoperability, technology transfer

This paper is an educational and structural analysis prepared for research purposes. It is not investment advice, an offer, or a solicitation. It contains no client information.

1. DEFINE THE SOVEREIGN-NETWORK TRANSACTION

A sovereign-network joint venture is an operating arrangement in which local and technology partners combine assets to build, modernise or operate nationally important telecommunications capability. Its purpose can include radio access, cloud RAN, edge infrastructure, network automation, AI operations, private networks or a broader intelligent-network platform.

The transaction thesis should state which services will be supplied, which licences and spectrum rights remain with the operator, where data and control planes reside, which components are open to substitution, and how local capability increases over time. A broad promise of digital sovereignty is too imprecise for investment approval.

The board should define sovereignty as a bundle of enforceable controls: lawful authority, operational command, data control, security assurance, technology portability, talent depth, supply continuity and the ability to change vendors without interrupting essential service.

Table 1. Sovereign-network value layers and transaction treatment

Value layer	Required evidence	Principal transaction question	Contractual treatment
Regulatory authority	Licence, spectrum and approval map	Who may operate each regulated function?	Condition precedent and reserved matter
Operational control	Command rights, credentials and runbooks	Can the local party direct and recover the network?	Control matrix and step-in right
Open vendor choice	Interface baseline and substitution test	Can a component be replaced at tolerable cost?	Acceptance test and portability covenant
Data and AI control	Data map, model lineage and access rights	Who may use network data and models?	Data schedule and audit right
Capability transfer	Role matrix, proficiency tests and succession	Can local teams perform critical work?	Milestone and payment gate
Economic durability	Service revenue, cost and capital plan	Does openness create resilient returns?	Funding tranche and performance covenant

Each layer requires a named evidence owner, contractual right and operational test.

2. SEPARATE SOVEREIGNTY FROM OWNERSHIP

Equity ownership influences governance and economics. It does not establish operational sovereignty on its own. A locally controlled joint venture can remain dependent on foreign credentials, proprietary tools, remote engineering, unavailable source code or a single hardware and software combination.

The diligence team should trace control from the constitutional documents into production. It should identify who can change configurations, approve software, rotate certificates, access

telemetry, deploy AI models, restore service and authorise a supplier. It should also identify which decisions require regulatory or security approval.

The operating model should show whether local teams can exercise those rights without exceptional consent or unavailable knowledge. Ownership should therefore be assessed beside operating authority, technical capability and continuity arrangements.

3. DEFINE OPEN VENDOR CHOICE PRECISELY

Open vendor choice means that identified components can be competed, introduced, upgraded or replaced through documented interfaces and acceptance criteria. It does not require every component to come from a different supplier. It requires credible choice at the boundaries that matter.

The relevant boundaries can include radio unit to distributed unit, cloud infrastructure to network functions, service management and orchestration, RAN intelligent controllers, model lifecycle services, observability, identity, security and data platforms. Each boundary has a specification, implementation profile, performance envelope and test burden.

The target architecture should name the baseline release, optional features, extensions and deviations. An interface can be open in specification and commercially closed through integration tooling, support dependencies, certification limits or contract restrictions.

4. START WITH THE NATIONAL OBLIGATIONS MAP

The transaction team should map obligations before selecting the legal vehicle. The map should cover telecommunications licensing, spectrum, equipment approval, cybersecurity, data protection, lawful access, service continuity, national-employment requirements, procurement and foreign-ownership conditions.

In the UAE, operating a public telecommunications network or providing regulated telecommunications services requires TDRA licensing. The application framework requests ownership, management, network, spectrum, financing and economic-benefit information. Saudi critical-system controls address governance, resilience, third parties and cloud use. These rules affect who may hold authority and where functions may operate.

The map should identify regulator, obligation, accountable entity, evidence, approval lead time and change trigger. It becomes the basis for conditions precedent, reserved matters and compliance reporting.

5. CHOOSE THE RIGHT JOINT-VENTURE PERIMETER

The perimeter can include assets, employees, licences, contracts, software, intellectual property and services. A narrow services joint venture can launch quickly while leaving most capability with the technology partner. A wider operating joint venture can support deeper transfer and requires more capital, governance and regulatory work.

The team should compare at least three structures: a contractual alliance, a separate operating company, and an asset-owning joint venture with long-term service agreements. Rights and obligations should drive the classification and accounting assessment. IFRS 11 defines joint control through unanimous consent over relevant activities and distinguishes rights to assets and obligations for liabilities from rights to net assets.

The selected perimeter should match the decisions that truly affect returns, service continuity and national responsibility.

6. BUILD THE CONTROL ARCHITECTURE

Control should be allocated by decision rather than through a generic list of board approvals. Decisions can be grouped into national control, ordinary operations, technology evolution, financing and shareholder protection.

National-control matters can include regulated services, security architecture, data location, network shutdown, lawful access, critical supplier changes and continuity events. Technology matters can include interface baselines, model releases, component certification and architecture exceptions. Financing matters cover budgets, additional capital, debt and distributions.

The control matrix should identify proposer, reviewer, approver, emergency authority and escalation path. Unanimity should be reserved for decisions that require genuine joint control. Excessive unanimity can turn routine engineering into shareholder deadlock.

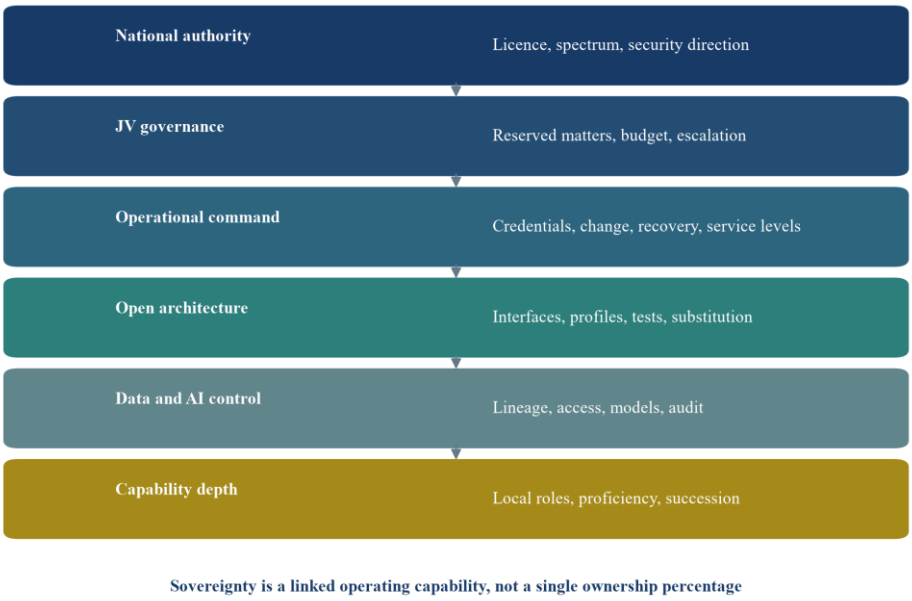

Figure 1. Sovereign control stack for a telecom-AI joint venture

Control becomes credible when legal authority, operational command, architecture, data, security and talent operate as one system.

7. ALLOCATE RELEVANT ACTIVITIES

Relevant activities are the decisions that significantly affect the joint venture's returns. In an intelligent-network venture, they may include architecture, vendor selection, deployment sequencing, pricing, customer contracting, model release, data use and capital allocation.

The legal documents should distinguish relevant activities from protective rights. A shareholder can receive veto rights that protect its investment without sharing control over ordinary operations. Conversely, a technology partner can exercise practical control through indispensable systems even when it lacks formal voting power.

The team should test the allocation under normal conditions, budget failure, cyber incident, supplier failure and shareholder dispute. The result should be consistent across the shareholders' agreement, operating agreements, licence obligations and accounting analysis.

8. PRESERVE THE OPERATOR'S REGULATED ACCOUNTABILITY

The licensed operator normally remains accountable for network and customer obligations. Outsourcing technology or creating a joint venture should not obscure that accountability. The operator requires information, intervention and audit rights proportionate to its exposure.

The operating agreement should define service levels, incident classification, regulatory reporting, access to records, change management, subcontractor approval and emergency command. It should also preserve the operator's ability to comply with lawful directions and security requirements.

Technology-partner protections remain important. Emergency rights should have clear triggers, duration, evidence and post-event review. Persistent discretionary intervention can undermine operating efficiency and the economics promised to the partner.

9. TRANSLATE STANDARDS INTO AN IMPLEMENTATION PROFILE

O-RAN and other standards contain mandatory, optional and evolving elements. A transaction cannot rely on the existence of a specification alone. It needs an implementation profile that defines the exact release, interfaces, functions, security controls, timing and conformance requirements used by the venture.

O-RAN Release 5 includes AI and machine-learning workflow services across non-real-time and near-real-time controllers, security enhancements and commercial-deployment features. These capabilities create choice and increase integration responsibility.

The profile should be version controlled and approved as a reserved technical baseline. Supplier deviations should identify commercial effect, migration path and test evidence. The profile becomes a diligence artefact, procurement document and post-completion control.

10. TEST INTEROPERABILITY IN PRODUCTION CONDITIONS

Conformance proves behaviour against a specification. Interoperability proves that selected implementations work together. Production readiness also requires performance, resilience, security, operations and lifecycle management under the venture's actual conditions.

The acceptance programme should cover functional tests, load, latency, timing, radio performance, failover, upgrades, observability, certificate rotation, model rollback and incident response. It should include multi-vendor combinations and defined adverse conditions.

The test catalogue should identify owner, environment, data, threshold, evidence and remediation. A demonstration assembled by exceptional vendor engineers should remain a trial until local teams repeat the procedure using production runbooks and normal support channels.

11. MEASURE SUBSTITUTION COST

Vendor choice has economic value when substitution is feasible. The venture should estimate the time, capital, service risk and engineering effort required to replace each critical component.

The substitution model should include procurement, integration, certification, retraining, data migration, parallel operation and decommissioning. It should identify proprietary extensions, bundled licences and operational dependencies that increase cost.

A low theoretical switching cost can conceal high service risk. The board should therefore track a portability coefficient: the share of interfaces, automation, data, tests and runbooks reusable with the replacement component. It should also track elapsed time from supplier selection to production acceptance.

The model should be maintained at component and service level. A radio unit can be technically replaceable while the affected service remains dependent on a proprietary management layer, accelerator or optimisation feature. The team should identify the smallest substitutable unit, the operational boundary around it and every shared dependency. Periodic replacement exercises can begin in a laboratory and progress to a limited production cluster. Results should record engineering hours, failed tests, temporary capacity, customer impact and residual remediation. This evidence gives the investment committee a more credible basis for pricing vendor-choice optionality.

12. DESIGN THE MULTI-VENDOR INTEGRATION FUNCTION

Disaggregation moves integration responsibility. The joint venture must decide whether the operator, technology partner, neutral systems integrator or dedicated internal team owns end-to-end performance.

The integration authority should control architecture, configuration baselines, test environments, defect triage, release coordination and root-cause analysis. It requires contractual access across suppliers and enough technical independence to challenge them.

The commercial model should avoid gaps between component warranties. A service incident can cross radio, cloud, transport, orchestration, security and AI layers. The venture needs one accountable incident process and a method for allocating cost after evidence is collected.

13. GOVERN THE AI LIFECYCLE

AI-enabled network control creates model-specific dependencies. The venture should record training data, features, model version, objective, performance envelope, deployment scope, approval, monitoring, drift and rollback.

The decision rights should distinguish advisory analytics from automated network action. Models that change radio parameters, resource allocation or security posture require defined human authority, guardrails and safe fallback.

The O-RAN architecture supports AI and machine-learning workflows across controllers and orchestration. Transaction value depends on whether those workflows are documented, portable and operated by the joint venture. A proprietary model endpoint without lineage, monitoring or replacement rights can become another control dependency.

14. DEFINE NETWORK-DATA RIGHTS

Network data can include topology, configuration, performance, faults, location, traffic metadata, customer information and derived model outputs. The venture should classify each dataset and define controller, processor, permitted purpose, location, access, retention, transfer and deletion.

The data schedule should separate personal data, security-sensitive data, commercially confidential information and reusable technical telemetry. The technology partner may need data to improve models. That purpose requires explicit authority and safeguards.

Saudi data-transfer rules and standard contractual clauses address transfers outside the Kingdom. UAE requirements should be assessed for each use. The commercial contract should not treat data ownership as a substitute for lawful processing and operational access.

15. DESIGN CYBERSECURITY INTO THE VENTURE

Open interfaces increase transparency and can expand the attack surface. O-RAN security work covers interface controls, zero-trust architecture, certificates, software integrity, threat assessment and testing. The venture should adopt a security baseline linked to its implementation profile.

The baseline should cover identity, privileged access, encryption, secure update, software bills of materials, vulnerability management, segmentation, logging, incident response and supplier assurance. AI components also require model, data and pipeline controls.

Saudi critical-system rules explicitly address third parties and cloud computing. The joint venture should map such obligations into contracts and technical evidence. Security approval should be a release gate, not a post-deployment review.

16. BUILD SUPPLY-CHAIN RESILIENCE

Open choice can diversify supply and introduce more suppliers. The venture should map component origin, manufacturing capacity, export restrictions, licences, support locations, financial health and replacement options.

Resilience planning should identify single points of failure across hardware, accelerators, software repositories, certificates, cloud regions and specialist personnel. Inventory and spares policy should follow criticality and replacement lead time.

The joint venture agreement should require notice of material supply changes and preserve rights to alternative sources. Multi-vendor design creates value when the venture maintains tested alternatives. A list of nominal suppliers without qualified replacement paths offers limited resilience.

17. PROTECT INTELLECTUAL PROPERTY AND FREEDOM TO OPERATE

The venture will combine background intellectual property, jointly developed assets and operational know-how. The agreements should define ownership, licence scope, territory, duration, sublicensing, improvement rights, enforcement and post-termination use.

Background intellectual property should remain identifiable. Joint developments need a decision on ownership and exploitation outside the venture. Operational scripts, interface adapters, data models and test assets can carry more continuity value than broad patent language.

Freedom-to-operate work should cover software dependencies, open-source obligations, standards-essential patents and third-party licences. Open-source use can accelerate capability and still create compliance obligations. The data room should include inventories, notices and licence scans.

18. CREATE CONTINUITY PROTECTIONS

Continuity protections should match the components whose loss would interrupt service. Options include source-code escrow, object-code continuity rights, build documentation, configuration exports, key-person replacement, transition assistance, mirror repositories and step-in licences.

Escrow has value only when materials are complete, current and buildable. The venture should test retrieval and reconstruction. It should also cover models, training pipelines, infrastructure code, documentation and credentials where relevant.

Triggers can include insolvency, prolonged service failure, sanctions, licence termination, abandonment or material breach. Exercise should be limited to continuity purposes and structured to respect intellectual-property rights.

19. CONVERT CAPABILITY TRANSFER INTO DELIVERABLES

Capability transfer should be measured through work performed, proficiency demonstrated and authority assumed. Training attendance and headcount do not prove operational independence.

The transfer plan should list critical roles, starting capability, target proficiency, evidence, assessor and date. Local staff should progressively lead architecture, integration, deployment, security, model operations, incident response and vendor management.

Evidence can include independent execution of a release, recovery exercise, component substitution, model rollback and production incident. Payments, partner fees or exclusivity can be linked to these outcomes. The venture should retain records that allow boards and regulators to test progress.

The plan should also address institutional capability. Individual proficiency can disappear through turnover, while an operating organisation preserves recruitment, documentation, peer review, laboratories, repositories, decision forums and succession. The joint venture should therefore test whether knowledge survives a change in named personnel. A mature milestone can require a second qualified local team, an independently reproduced build and successful execution during the technology partner's absence. This prevents a small group of trained specialists from being presented as a durable national capability.

Table 2. Capability-transfer evidence ladder

Stage	Evidence	Typical weakness	Transaction response
Exposure	Workshops and documentation access	Knowledge remains theoretical	No valuation credit
Assisted delivery	Local team performs tasks with vendor support	Dependency remains high	Partial milestone
Supervised ownership	Local lead directs a production release	Escalation still depends on vendor	Conditional payment
Independent operation	Local team deploys, monitors and recovers service	Limited exposure to abnormal events	Operating value
Independent change	Team integrates or substitutes a component	Capability may be concentrated in a few people	Strategic-control premium

Capability is demonstrated through independent operation under defined conditions.

20. RETAIN AND DISTRIBUTE CRITICAL KNOW-HOW

Capability concentrated in a small number of individuals remains fragile. The venture should map key people, succession, documentation, access and teaching responsibilities.

Retention packages can combine incentives, career pathways and meaningful authority. Restrictive covenants should be proportionate and enforceable. The operating model should prevent the technology partner from keeping essential knowledge within a rotating remote team.

Documentation quality should be tested through use. A new qualified engineer should be able to follow a runbook, reproduce an environment and complete a defined task. Knowledge should be distributed across teams and locations that satisfy continuity requirements.

21. DESIGN THE OPERATING MODEL

The operating model should define which activities sit with the joint venture, operator, technology partner and third parties. It should cover product, architecture, engineering, operations, security, commercial, finance, procurement and regulatory functions.

Every critical process needs an accountable owner and service interface. Shared responsibility without a named decision maker creates delay and weakens incident response. The model should also state where personnel are located and which functions require local presence.

The team should test the model against the target deployment schedule and cost base. A structure that depends on undeclared partner support can understate operating expense and overstate transferred capability.

22. CONNECT THE TECHNICAL MODEL TO ECONOMICS

Open architecture can create procurement leverage, shorter innovation cycles and resilience. It can also increase integration, testing and lifecycle costs. The economic case should show both effects.

The model should separate hardware, cloud, software licences, integration, assurance, operations, support, security and refresh capital. It should identify partner transfer pricing and related-party services.

Benefits should link to observable drivers: site cost, energy, deployment time, service reliability, vendor pricing, automation or enterprise revenue. General claims of lower total cost should remain hypotheses until compared with a defined baseline over the full lifecycle.

23. BUILD THE SOVEREIGNTY SCORECARD

The scorecard should combine authority, portability, data, security, capability and economics. Each measure needs a source, owner, baseline, target and threshold.

Measures can include the share of critical actions executable locally, tested interface combinations, substitution time, unresolved security findings, local leadership of production changes, model rollback success, supplier concentration and contribution margin.

The scorecard should support board oversight, funding tranches and regulator engagement. Definitions should be fixed before completion. Changing a metric after a milestone is due creates disputes and weakens accountability.

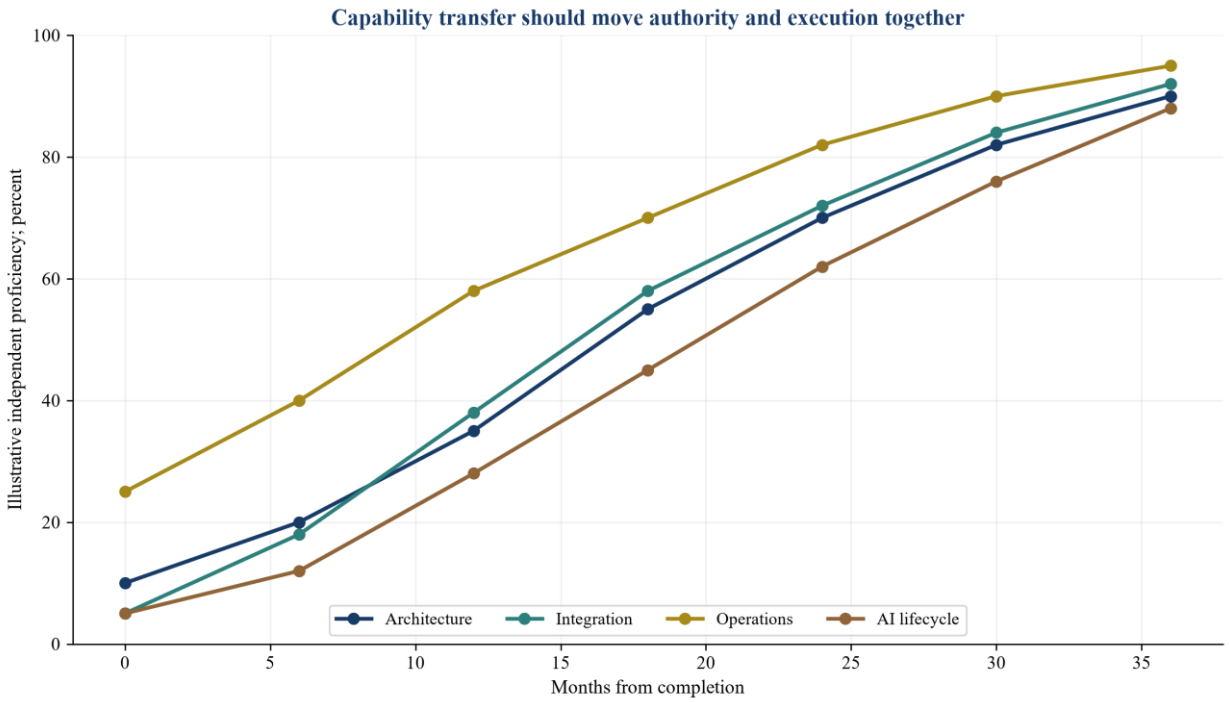

Figure 2. Hypothetical capability-transfer path over 36 months

Illustrative management assumptions; proficiency means independent completion of defined production tasks.

24. DEFINE THE CAPITAL PROGRAMME

Capital should be committed against a deployment plan and released against evidence. The plan should distinguish initial platform investment, site rollout, integration, security, capability transfer and expansion.

The funding agreement should specify equity, shareholder loans, external debt, cost overruns and unused commitments. It should also state whether contributed assets are valued, licensed or provided as services.

A joint venture can fail when one partner controls a required input and the other funds overruns. The budget should expose related-party pricing and require comparable evidence for material procurements. Capital calls should follow an approved business plan and defined exceptions.

25. ALLOCATE CONTRIBUTION ECONOMICS

The operator can contribute market access, sites, customers, regulated authority and network integration. The technology partner can contribute software, hardware access, intellectual property, engineers and product roadmap. Their economic contributions should be valued separately.

Returns can include dividends, service fees, licences, equipment margin and performance payments. The board should understand total economics to each partner, not only equity ownership.

Transfer pricing should remain transparent and benchmarked. A low technology licence fee can be offset by exclusive equipment margin or mandatory support. The venture's standalone economics should be visible after all related-party charges and replacement costs.

26. AVOID EXCLUSIVITY TRAPS

Limited exclusivity can justify investment and protect market development. Broad exclusivity can undermine vendor choice and expansion.

The agreement should define product, territory, customer, duration, performance thresholds and exceptions. Exclusivity can step down when deployment, service, capability-transfer or pricing obligations are missed.

The venture should preserve the right to procure alternative components for interoperability, security, resilience and regulatory reasons. The technology partner can receive fair testing and matching rights without an unconditional veto over substitution. Exit and post-termination provisions should prevent exclusivity from surviving after the commercial basis has failed.

27. STRUCTURE PERFORMANCE OBLIGATIONS

Performance obligations should combine technical, operational and commercial measures. Technical measures include interface conformance, performance and security. Operational measures include availability, recovery and incident closure. Commercial measures include deployment, revenue and cost.

Capability-transfer obligations require independent assessment. A partner should not certify its own completion without evidence. Acceptance can use a joint committee with an expert mechanism for disputes.

Remedies should follow materiality: cure plan, service credit, payment deferral, loss of exclusivity, step-in or termination. The contract should avoid incentives that encourage narrow metric optimisation at the expense of network resilience.

28. PRICE SOVEREIGN-CONTROL VALUE

Sovereign control can reduce disruption, supply concentration and policy risk. It can also require duplicated capability and higher near-term cost. The valuation should identify which cash flows and risk reductions are attributable to the structure.

Value can arise through avoided outage, procurement leverage, faster local change, lower transition cost, better regulatory alignment and access to protected demand. Each item requires a baseline and evidence.

The model should avoid adding strategic value that the buyer cannot capture. National resilience may justify investment for a public shareholder while producing no direct commercial revenue. The investment committee should keep financial return, policy value and option value distinct.

The policy-value case should state the beneficiary, measurement method and governance owner. Examples can include continuity of essential services, domestic engineering employment, local research capacity, supplier diversity and reduced exposure to external interruption. These outcomes should not be converted automatically into enterprise value. They can inform public-capital allocation, required return, procurement policy or the acceptable cost of resilience. A transparent separation allows the board to compare commercial performance with national objectives without using one to conceal weakness in the other.

29. MODEL VENDOR-SWITCHING OPTIONALITY

Vendor choice is an option to respond when price, performance, security or geopolitical conditions change. Its value depends on the cost and time to exercise.

The team can model trigger probability, avoided loss, substitution cost and service interruption. The option should be capped when interfaces remain untested or alternative suppliers are not qualified.

Exercise milestones can include successful lab interoperability, pilot substitution, production acceptance and independent local operation. The venture should maintain these capabilities through periodic tests. Dormant rights and obsolete artefacts lose value.

30. CONSTRUCT THE USD 360 MILLION CAPITAL BRIDGE

The hypothetical venture commits USD 360 million across the platform, rollout, capability and contingencies. The bridge releases capital as control and capability become evidenced.

The first tranche funds incorporation, architecture and test facilities. Later tranches follow production interoperability, local operational readiness, security assurance and commercial deployment. A contingency remains available for substitution or remediation.

The amounts explain the method and do not represent observed costs. A real case requires site counts, spectrum, traffic, architecture, supplier quotations, staffing and approvals. The bridge should be rebuilt for each transaction.

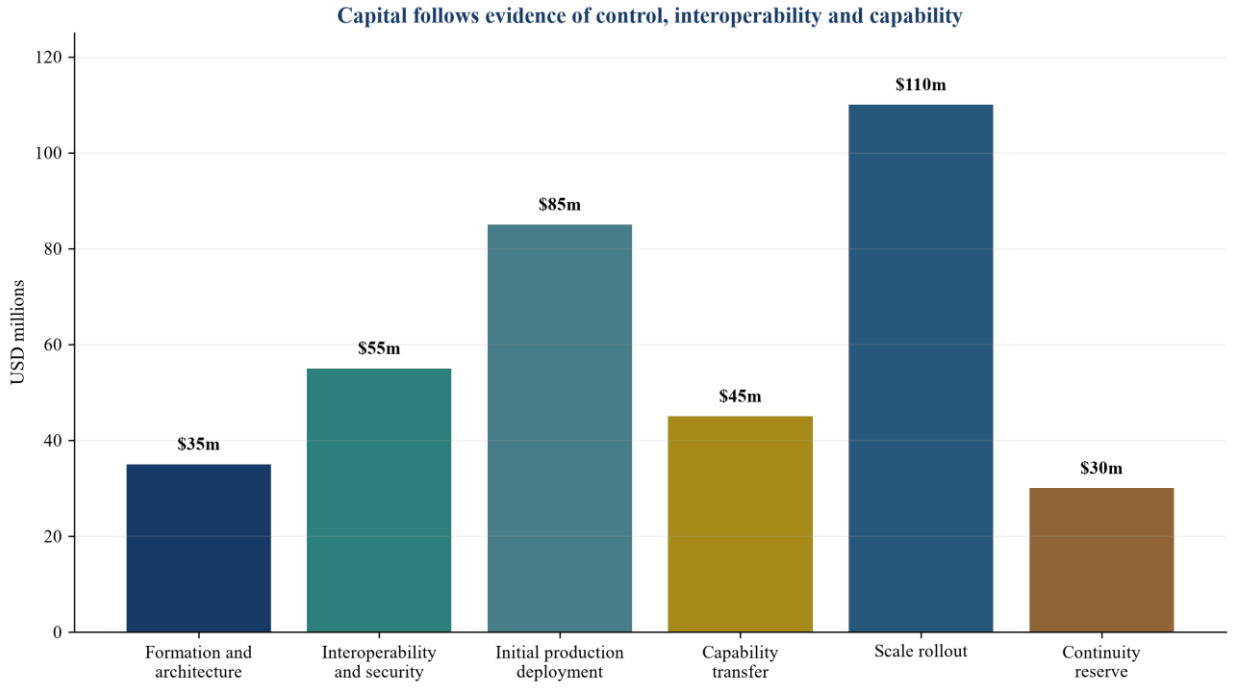

Figure 3. Hypothetical USD 360 million joint-venture funding bridge

Illustrative management assumptions; releases depend on verified milestones.

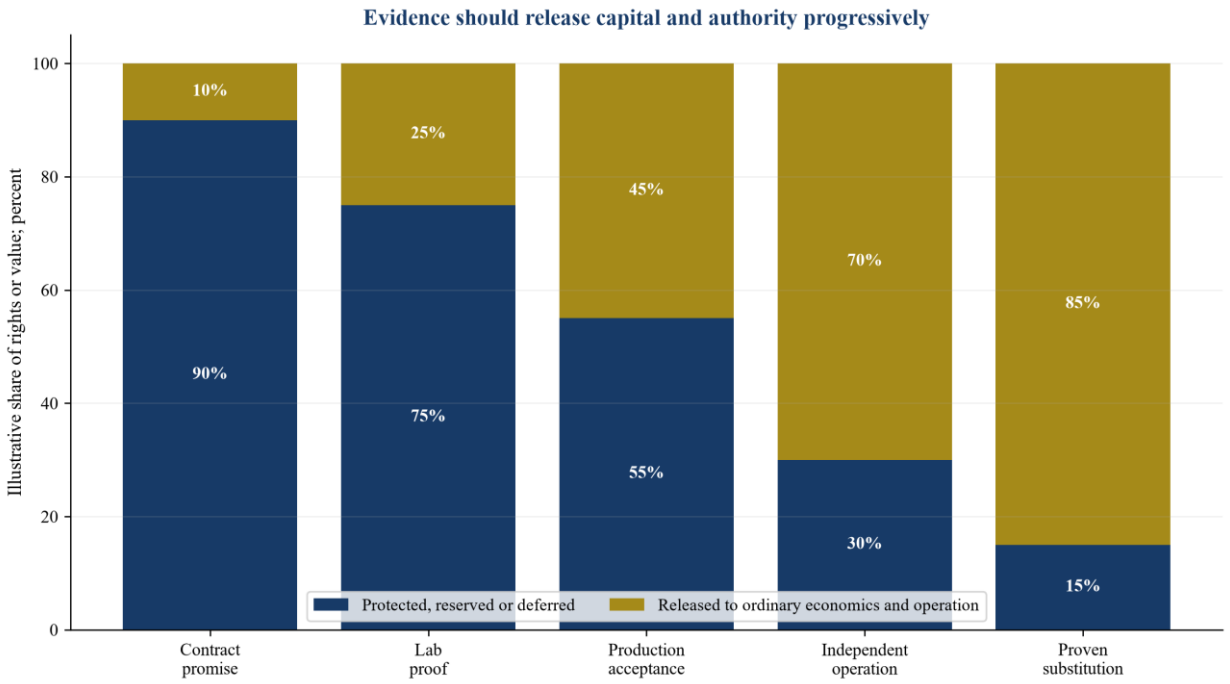

Figure 4. Transaction protections by evidence maturity

Illustrative governance design; stronger evidence allows economics and authority to move from protected to ordinary operating treatment.

31. STAGE CONSIDERATION AND PARTNER ECONOMICS

Upfront value should reflect contributed assets and proven capability. Deferred value can reward production milestones, cost performance, capability transfer and commercial expansion.

Milestones should rely on records available to both parties. Network performance and local proficiency require agreed test methods. Revenue milestones should specify related-party treatment, collection and margin.

The structure can include seller or partner rollover, preferred returns, service-fee adjustment and earn-out. It should avoid creating incentives to delay knowledge transfer or protect proprietary dependency. Governance rights and economics should move together when milestones change the parties' roles.

32. DESIGN DEADLOCK MECHANISMS

Deadlock is a material risk when national control and proprietary technology meet. The agreement should define escalation from operating committee to board, chief executives and expert determination.

Technical disputes can use an independent expert. Valuation or accounting disputes may use a different specialist. National-security matters can require local authority and regulator engagement.

Buy-sell mechanisms should be used cautiously where a regulated or sovereign shareholder cannot freely sell. Alternative remedies include scope separation, loss of exclusivity, structured transition and call options following defined breaches. The mechanism must remain workable under foreign-ownership, licence and approval constraints.

33. PREPARE EXIT AND SEPARATION AT ENTRY

The venture should be designed so that termination does not threaten service continuity. The separation plan should map assets, employees, contracts, data, credentials, intellectual property, customer obligations and suppliers.

Exit rights can include trade sale, public offering, put, call, transfer restrictions and dissolution. Each route may require regulatory approval. The agreement should address valuation, continued services and stranded assets.

Transition assistance should have scope, duration, pricing and service levels. Data return, deletion and verification should be planned. A tested separation plan strengthens bargaining power and confirms whether vendor choice is real.

34. BUILD THE FIRST 100-DAY PLAN

The first 100 days should establish decision rights, baselines and evidence. Priorities include governance activation, regulatory engagement, architecture freeze, security plan, data classification, supplier inventory and capability assessment.

The venture should select initial production use cases and define acceptance tests. It should also reconcile the approved budget with contracts and staffing.

Capability transfer begins immediately through paired roles and documented work. The board should receive a scorecard showing open issues, milestone evidence, capital release and continuity risks. Early discipline reduces later disputes about what was promised.

35. CREATE THE BOARD DASHBOARD

The dashboard should track service, control, portability, capability, security, capital and commercial performance. Measures should be few enough to govern and detailed enough to expose dependency.

Examples include production availability, critical incidents, tested vendor combinations, substitution time, local change leadership, open security findings, capital deployed, forecast-at-completion and contribution margin.

Every exception should have an owner, due date and decision. The dashboard should show trends and thresholds. It should distinguish observed results from management forecasts and avoid combining policy outcomes with commercial returns.

36. ESTABLISH THE DILIGENCE WORKPLAN

The diligence team should include commercial, technical, regulatory, cybersecurity, data, intellectual-property, finance, accounting, tax and human-capital specialists. Workstreams should share one dependency register.

Technical diligence should inspect architecture, interfaces, performance and lifecycle. Commercial diligence should test customers, pricing, partner economics and procurement. Regulatory work should identify approvals and operating constraints. Human-capital work should test who can perform critical tasks.

The workplan should prioritise deal-breakers: licence incompatibility, unavailable data rights, non-portable architecture, unremediated security exposure, unaffordable integration and capability that cannot be transferred.

37. PREPARE THE DATA ROOM

The data room should include constitutional documents, licences, approvals, architecture, interface profiles, test evidence, supplier contracts, software inventories, data maps, security assessments, operating records, budgets and staffing.

Intellectual-property materials should include background rights, development records, open-source inventories, third-party licences and continuity assets. Capability materials should show roles, assessments, training records and independent execution.

Documents should be dated, attributable and linked to the transaction claim they support. Presentations should not substitute for raw evidence. A request list should identify missing, stale and inconsistent records.

38. APPLY A GO, REPRICE OR STOP DECISION

A go decision requires a lawful structure, credible control, tested architecture, fundable economics and measurable capability transfer. A reprice decision is appropriate when issues can be quantified or placed behind milestones.

A stop decision is appropriate when the venture cannot comply with regulation, secure critical systems, obtain necessary rights, sustain service or reduce an unacceptable dependency. Strategic importance should increase the quality threshold.

The investment committee should record facts, assumptions, unresolved matters, mitigations and owners. It should state which value depends on future evidence and how the contract protects capital.

Table 3. Hypothetical sovereign-network joint-venture case

Item	Illustrative assumption	Diligence condition	Deal response
Total committed capital	USD 360 million	Approved deployment and funding plan	Tranche by evidence
Initial release	USD 35 million	Vehicle, approvals, architecture and test plan	Fund at completion
Production release	USD 85 million	Tested multi-vendor production acceptance	Fund after acceptance
Capability release	USD 45 million	Independent local operation of defined functions	Defer until proficiency
Scale release	USD 110 million	Service, unit economics and rollout thresholds	Stage by deployment
Continuity reserve	USD 30 million	Board-controlled substitution or remediation need	Restricted reserve

All values and milestone amounts are illustrative management assumptions.

39. RECOGNISE LIMITATIONS

This framework supports transaction analysis. It does not determine whether a network architecture, AI model or supplier is safe, compliant, secure or suitable for a specific deployment. Qualified technical, regulatory, security, legal, tax, accounting and valuation advice is required.

Standards and national requirements continue to evolve. Published trials and vendor results apply to their stated configurations. They should not be generalised without independent reproduction.

The hypothetical case demonstrates a method. Actual capital, costs, benefits, probabilities, approvals and terms require transaction-specific evidence. No figure in the case is a forecast, valuation opinion or recommendation.

40. CONCLUDE WITH ENGINEERED SOVEREIGNTY

Sovereign telecommunications capability emerges from enforceable authority, tested architecture, lawful data control, secure operations, transferable knowledge and credible supplier choice. Joint ventures can assemble these elements when the parties make them explicit.

Open interfaces provide a foundation. The transaction must convert that foundation into implementation profiles, interoperability tests, portable assets, operational authority and measurable local proficiency. Governance should allocate national obligations clearly and preserve efficient technical execution.

The disciplined sequence is to map obligations, define the perimeter, allocate relevant activities, test interfaces, price full lifecycle economics, gate capital against evidence and prepare continuity and exit from the start. This structure allows GCC operators and investors to capture global technology while building national control that survives changes in suppliers, people and market conditions.

Table 4. Board and diligence scorecard

Domain	Minimum evidence	Red flag	Decision response
Authority	Licence map, reserved matters and emergency command	Regulated accountability is unclear	Restructure or stop
Architecture	Versioned profiles and production interoperability tests	Open claims without tested combinations	Defer capital
Data and AI	Data schedule, model lineage and rollback	Unauthorised access or non-portable models	Cure or stop
Security	Control baseline, findings and incident evidence	Critical unremediated exposure	Condition precedent
Capability	Independent local execution of defined tasks	Training without operational authority	Withhold milestone
Economics	Full related-party cost and lifecycle capital	Hidden support or integration burden	Reprice
Continuity	Tested escrow, alternatives and transition plan	Service depends on unavailable supplier	Require remedy

Minimum evidence should be agreed before signing and monitored after completion.

REFERENCES

[1] Telecommunications and Digital Government Regulatory Authority. TDRA Unveils the UAE's 6G Roadmap. 24 April 2024. https://tdra.gov.ae/en/media/press-release/2024/tdra-unveils-the-uaes-6g-roadmap

[2] Telecommunications and Digital Government Regulatory Authority and Khalifa University. Next-Generation Connectivity in the UAE. 2026. https://tdra.gov.ae/-/media/TDRA-Media/Brochures/2024/Whitepaper-by-TDRA-and-Khalifa-University--on-6G-Next-Generation-Connectivity-in-the-UAE-1.ashx

[3] Telecommunications and Digital Government Regulatory Authority. Issue Licences to Provide Telecommunication Services. https://tdra.gov.ae/en/Services/issue-licences-to-provide-telecommunication-services

[4] Telecommunications and Digital Government Regulatory Authority. Regulations and Rulings. https://tdra.gov.ae/en/About/regulations-and-ruling

[5] Communications, Space and Technology Commission. Open RAN: An Interoperable, Innovative, and Sovereign Architecture. 2023. https://www.cst.gov.sa/-/media/cst-website-app/data/media/Reports/Whitepaper/EN/Wireless-Technologies/Open-RAN-An-Interoperable-Innovative-and-Sovereign-Architecture---------Technology.ashx

[6] Ministry of Communications and Information Technology, Saudi Arabia. OpenRAN. 2024. https://mcit.gov.sa/sites/default/files/2024-07/OpenRan_1.pdf

[7] O-RAN ALLIANCE. O-RAN Specifications. https://www.o-ran.org/specifications

[8] O-RAN ALLIANCE. O-RAN ALLIANCE Completed its Specification Release 5. 8 June 2026. https://www.o-ran.org/blog/o-ran-alliance-completed-its-specification-release-5-o-ran-r005

[9] O-RAN ALLIANCE. O-RAN ALLIANCE Security Update 2026. 2026. https://www.o-ran.org/blog/o-ran-alliance-security-update-2026

[10] O-RAN ALLIANCE. Advances Open and AI-Driven RAN Standardization. 28 March 2025. https://mediastorage.o-ran.org/press-release/O-RAN.EC.2025-03-28.PR%20MWC25%20summit%20messages.pdf

[11] International Telecommunication Union. ITU-T Recommendation Y.2361: Requirements for fostering telecommunication and ICT services universalization using open networks and AI models. April 2025. https://www.itu.int/rec/dologin_pub.asp?id=T-REC-Y.2361-202504-I!!PDF-E&lang=e&type=items

[12] International Telecommunication Union. Focus Group on Artificial Intelligence Native for Telecommunication Networks. https://www.itu.int/en/ITU-T/focusgroups/ainn/Pages/default.aspx

[13] International Telecommunication Union. Towards autonomous open radio access networks. ITU Journal on Future and Evolving Technologies, 2023. https://doi.org/10.52953/GJII3746

[14] International Telecommunication Union. ITU-T Recommendation L.1391: IMT-2020 network sharing and co-construction. January 2024. https://www.itu.int/epublications/publication/itu-t-l-1391-2024-01-specification-of-imt-2020-network-sharing-and-co-construction-adapting-to-climate-change-mitigation

[15] du. Standalone Private 5G Network Solution Based on O-RAN. 13 October 2022. https://www.du.ae/about/media-centre/newsdetail/du-launches-a-standalone-private-5g-network-solution

[16] du. First Commercial 5G Cloud RAN Deployment in the Middle East and Africa. 2024. https://www.du.ae/about/media-centre/newsdetail/du-and-nokia-announce-the-first-commercial

[17] e& UAE and Nokia. Cloud RAN: Unlocking the Power of 5G for a Smarter, Connected Future. 2024. https://www.etisalat.ae/content/dam/eand/assets/docs/nokia-eand-cloud/wp-nokia-eand-cloud-ran-final-09272024.pdf

[18] National Cybersecurity Authority, Saudi Arabia. Critical Systems Cybersecurity Controls. https://nca.gov.sa/en/regulatory-documents/controls-list/cscc/

[19] Saudi Data and AI Authority. Regulation on the Transfer of Personal Data Outside the Kingdom and Standard Contractual Clauses. https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/

[20] IFRS Foundation. IFRS 11 Joint Arrangements. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-11-joint-arrangements/

[21] IFRS Foundation. IAS 28 Investments in Associates and Joint Ventures. https://www.ifrs.org/issued-standards/list-of-standards/ias-28-investments-in-associates-and-joint-ventures/

[22] IFRS Foundation. IFRS 12 Disclosure of Interests in Other Entities. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-12-disclosure-of-interests-in-other-entities/

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.