GCC Defence JVs: AI Capability Transfer under Export-Control and Data-Sovereignty Constraints

A Transaction and Operating-Control Framework for Ownership Technology Access Training Cybersecurity and Exit

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Defence joint ventures in the Gulf Cooperation Council can combine sovereign demand, local industrial capacity and international technology. The transaction succeeds only when the parties define which capability may transfer, which technical data and defence services require authorisation, which information must remain segregated, who may access source code and models, how training becomes local decision authority, and what happens when a licence, partner or security assumption changes. Equity ownership alone does not establish an export right, a right to use controlled technical data, or an operationally independent local capability.

This paper develops a GCC Defence Joint-Venture Capability Transfer Framework for sovereign investors, defence groups, original equipment manufacturers, technology companies, boards, lenders and transaction advisers. It begins with the sovereign capability outcome and decomposes the joint venture into product, design, manufacturing, software, data, model, training, certification, maintenance and decision-authority layers. It connects partner and partner diligence to source-country export controls, end use and end user, local cybersecurity and privacy rules, classified or sensitive information, intellectual property, operating architecture, reserved matters, funding, performance milestones, remedies and exit.

Artificial intelligence is treated as both a capability and a controlled operating dependency. Training data, model weights, source code, prompts, evaluation sets, interfaces, update rights, safety cases and human decision authority can be governed differently. AI can assist configuration review, predictive maintenance, quality assurance, logistics and simulation. It cannot create an export authorisation, determine legal classification, replace professional security assessment or authorise a consequential defence decision.

The worked case is wholly hypothetical. A GCC industrial group and an international defence-technology partner consider a joint venture with assumed initial funding of USD 180 million. The local partner contributes USD 105 million and facilities; the international partner contributes USD 45 million and defined licences, while USD 30 million is reserved for secure infrastructure, training, validation and working capital. Capability is released through six evidence gates rather than a single closing event. A hypothetical central case reaches USD 92 million of annual revenue and USD 16 million of EBITDA in year five. A licensing delay and lower local qualification case reaches USD 61 million of revenue and USD 3 million of EBITDA. Every amount, percentage, timetable, authorisation outcome and operating result is an illustrative assumption.

The central conclusion is that a credible defence joint venture needs a capability ledger, an authorisation matrix, a sovereign data architecture and milestone-linked economic rights. The board should be able to

show what the venture may know, do, modify, manufacture, support and export at each stage; who approved it; which evidence proves it; and which remedy applies when an assumption fails.

JEL Classification: F23, G34, L64, O32, O33

Keywords: GCC defence joint ventures, capability transfer, export controls, technical data, artificial intelligence, data sovereignty, cybersecurity, localisation, M&A, joint venture governance

1. Define the sovereign capability decision before structuring the venture

The sponsoring board should begin with a specific capability outcome. Examples include maintaining a platform without external field support, producing a defined component locally, modifying mission software within an authorised boundary, training and certifying local engineers, securing availability of spares, or building an exportable regional support capability. Each outcome needs a date, operational consequence, evidence standard and accountable owner.

The decision record should separate strategic aspiration from the minimum investable outcome. A joint venture can create employment and assembly while remaining dependent on imported design authority, controlled software, specialist tooling, remote diagnostics or foreign approvals. The board should state which dependency is acceptable, which must decline over time and which must remain with the international partner because law, safety or commercial policy requires it.

Alternatives should use the same evidence and cash-flow test. They can include direct procurement, licensed production, maintenance agreement, technical-assistance arrangement, minority investment, joint venture, prime-subcontractor model, government-to-government route or internal development. The joint venture should be selected because its rights, economics, resilience and governance outperform those alternatives under central and downside cases.

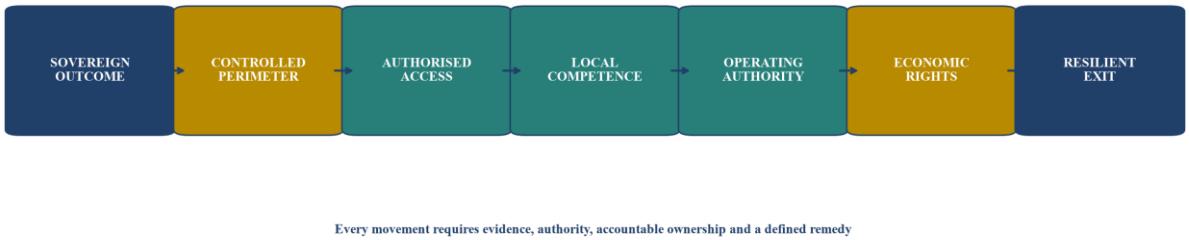
The opening gate should identify the intended end user, product and service perimeter, source countries, controlled components, proposed local activities, people requiring access, data locations, AI use cases, funding envelope and walk-away conditions. Qualified counsel and relevant authorities determine the applicable legal position. The transaction team maintains the evidence and decision trail.

2. Use the GCC Defence JV Capability Transfer Framework

The framework links eight questions: what sovereign capability is required; what lawfully transfers; which technical data and services are authorised; where data and compute reside; who holds design and release authority; how local competence is demonstrated; how economics respond to delayed capability; and how the parties separate or exit without disrupting operational support.

A joint-venture agreement should not carry this burden alone. The operating design needs linked schedules for controlled items, permitted activities, territories, end users, sublicensees, data domains, named roles, training, tooling, validation, cybersecurity, audit, reporting, milestones, remedies and transition. Each schedule should reference the governing approval or evidence.

Figure 1. GCC Defence Joint-Venture Capability Transfer Framework



Proposed framework; transaction-specific law, authorisations and security requirements determine the actual design.

3. Separate equity ownership from operational capability

Equity establishes economic and governance rights in the legal entity. It does not by itself transfer export-controlled technology, technical data, defence services, source code, model weights, design authority, certification rights, tooling, know-how or permission to supply another end user. The transaction model should value each capability layer separately.

The capability ledger should describe the current holder, legal basis, classification, source country, permitted recipient, purpose, territory, access method, modification right, derivative-work treatment, update right, support obligation, evidence and expiry. It should also identify dependencies that cannot be transferred and the operating consequence of losing them.

Table 1. Equity and capability-rights bridge

Layer	Equity ownership provides	Separate evidence required	Board consequence
product and hardware	interest in the venture	item classification, licence and end-use scope	what may be received or made
technical data	no automatic access	approved agreement, licence or other lawful basis	who may inspect or use
software and source code	no automatic delivery or modification	licence, access boundary and change rights	local support and upgrade resilience
AI data and models	no automatic ownership or reuse	data rights, model rights, evaluation and deployment authority	permitted learning and decisions
design authority	no automatic delegation	documented engineering and release authority	who approves configuration
training and defence services	no automatic service right	authorised scope, people and location	competence transfer timetable
export and territory	no automatic onward sale	destination, end-user and retransfer permission	addressable market and exit value

Proposed diligence structure; qualified advisers should determine the applicable classification and authorisation.

4. Prove sovereign demand and the authorised use case before price

The commercial case should start with an evidenced requirement, procurement path, budget authority, qualification process, expected quantities, acceptance criteria, support obligation and payment route. Strategic importance does not remove demand risk. A local production plan can become uneconomic when volumes, timing, configuration or export opportunity are assumed rather than contracted.

For AI-enabled capability, define the precise function and consequence. Predictive maintenance, visual quality inspection, logistics planning, document search, simulation and decision support can require different data, model assurance, human review and security. The team should avoid a single broad AI label that conceals distinct access and risk profiles.

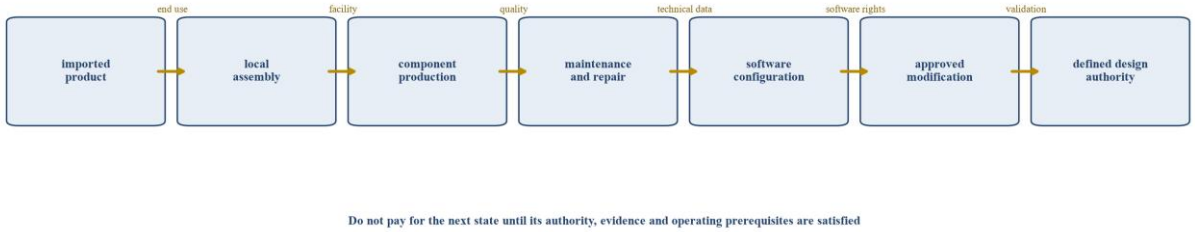
Customer and authority evidence should identify whether local content, security accreditation, facility clearance, personnel approval, test range, certification, interoperability or sovereign hosting affects award or operation. The investment committee should see the difference between a policy ambition, a funded programme, an awarded contract and accepted recurring revenue.

5. Map the capability-transfer chain as a sequence of authorised states

Capability transfer should be represented as states that can be tested. A venture may begin with imported finished goods, progress to local assembly, then component production, maintenance, software configuration, approved modification and defined design authority. Each transition needs authorisation, facilities, people, tooling, data, quality evidence and customer acceptance.

The chain should expose bottlenecks. Local technicians may complete training while still lacking approved technical data. A secure facility may be accredited while a model update remains accessible only through the partner. Local manufacture may depend on a controlled test fixture or cryptographic key. The board should see the dependency that limits the next state.

Figure 2. Capability-release chain for a defence joint venture



Proposed stage architecture; actual release depends on applicable approvals, security and customer acceptance.

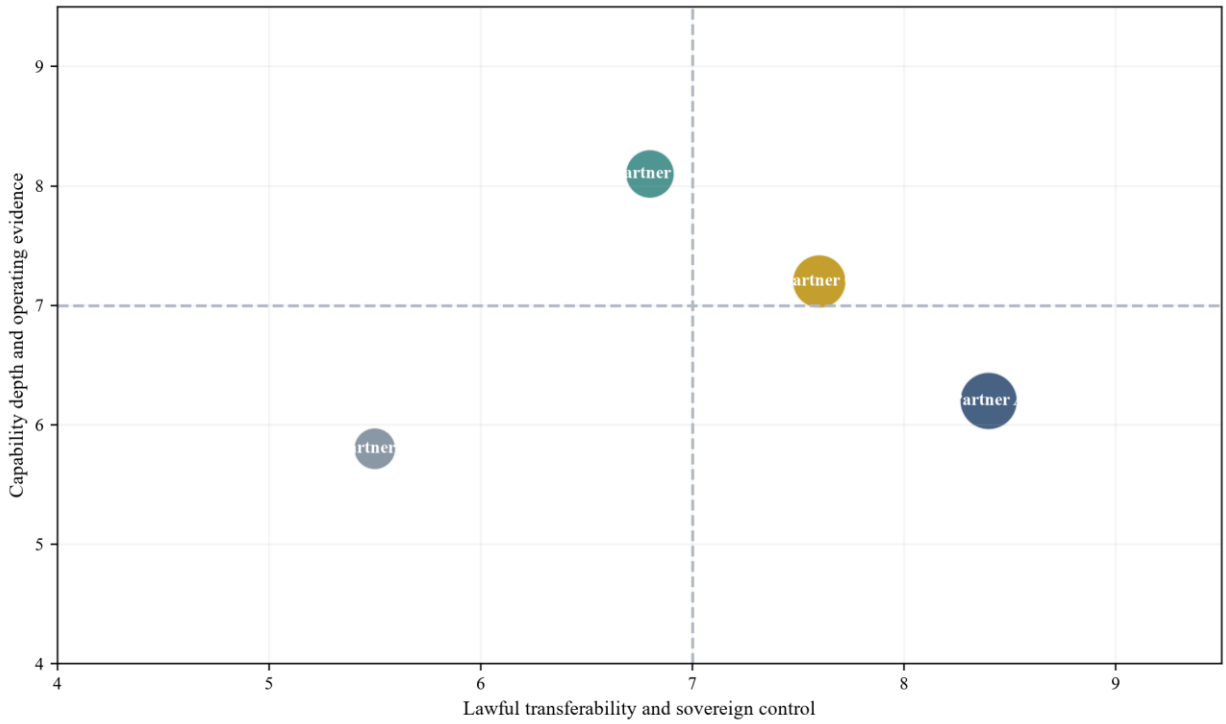
6. Rank partners through a controlled-capability scorecard

Partner selection should reflect capability depth, lawful transferability, sovereign demand, security maturity, training capacity, supply resilience, economics and exit continuity. A high-performing product can rank poorly when the required technical data cannot be released, key personnel cannot access it, or the partner retains an unpriced unilateral right to withdraw support.

Scores should carry evidence confidence and a critical-failure flag. A low-confidence score cannot be averaged away by strong commercial presentation. The committee should see which conclusion comes

from an authority, executed document, technical demonstration, customer evidence or management representation.

Figure 3. Hypothetical partner capability and transferability matrix



Hypothetical management assumptions; bubble size represents assumed five-year cash commitment.

7. Build one jurisdiction and authorisation matrix

The transaction team should map source-country export controls, reexports and retransfers, destination and end-user restrictions, sanctions, foreign-investment review, competition, procurement, industrial licensing, cybersecurity, privacy, classified information, employment, immigration, tax, customs and intellectual-property rules. The matrix identifies the competent authority, responsible applicant, required evidence, sequencing, conditions, duration, expiry and change events.

U.S. ITAR and EAR questions can arise through origin, item, technology, technical data, defence service, software, person, end use, end user, destination and retransfer. UK and European controls can apply to goods, software, technology, technical assistance and military end use. The exact result is transaction specific. The parties should avoid treating country of incorporation as the only relevant fact.

Table 2. Cross-border control and authorisation matrix

Question	Evidence	Owner	Transaction gate
what is controlled	item, software, technology and service classification	originating partner and counsel	before diligence access
who may receive it	entities, people, nationalities, end users and sublicensees	compliance and security	before data-room admission
what may they do	manufacture, maintain, modify, train, test, integrate or export	programme and counsel	before operating design
where may it occur	approved sites, systems, cloud, networks and countries	security and IT	before build commitment

Question	Evidence	Owner	Transaction gate
what approval applies	licence, agreement, exception, authorisation or prohibition	applicant and authority liaison	condition to signing or closing
what changes require action	ownership, control, scope, product, people, place or end use	company secretary and compliance	continuing covenant
what happens at expiry	renewal, suspension, return, deletion, transition or stop work	board and programme office	resilience and exit plan

Illustrative categories only; qualified advisers and competent authorities determine the applicable requirements.

8. Sequence source-country export control and end-use work

Export-control work should begin before the joint venture promises localisation, technical access or a delivery date. The originating partner should identify controlled items and activities, proposed parties, end users, locations, nationalities, technical scope, manufacturing rights, defence services, training and retransfers. The local partner should supply accurate ownership, governance, facilities, security, personnel and intended-use evidence.

An authorisation can be narrower than the commercial term sheet. It can limit products, data, parties, sites, purposes, territories, duration, foreign nationals, subcontractors or onward transfers. The financial model and milestone schedule should use the authorised scope, with explicit treatment for unresolved items. A closing condition should not assume that approval will be granted or granted on the requested terms.

Controls continue after closing. Changes in ownership, board rights, personnel, end use, product configuration, cloud architecture, subcontractors or export destination can require review. The compliance operating model should maintain classifications, approvals, provisos, access lists, training, records, screening, audit and escalation.

9. Design sovereign data and AI architecture before integration

The parties should classify data by legal control, national-security sensitivity, customer restriction, intellectual-property ownership, personal-data status, operational consequence and permitted processing. The architecture can separate public, enterprise, customer-controlled, export-controlled, classified or specially protected domains. Identity, device, network, storage, compute, model, interface and support access should follow the classification.

AI requires additional lineage. Record training and evaluation data, preprocessing, model and weight provenance, code and library versions, prompts, retrieval sources, deployment environment, permissions, human review, performance limits, security tests, updates and retirement. A model hosted locally can still depend on foreign weights, remote telemetry, licence servers, specialists or cloud tooling. Sovereign hosting and sovereign operational control should be tested separately.

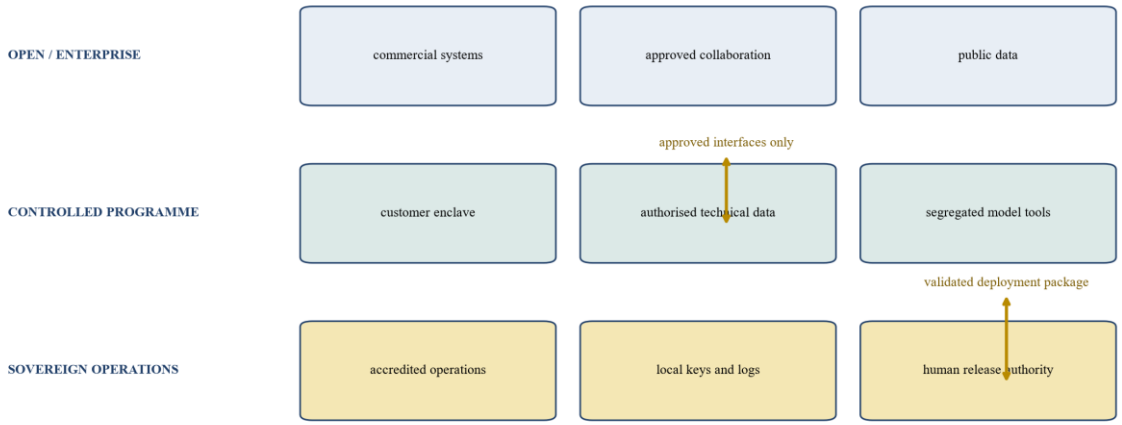
Table 3. Sovereign data and AI control architecture

Domain	Typical content	Permitted environment	Decision control
open and commercial	public specifications and ordinary enterprise data	approved enterprise services	business owner
customer restricted	programme, configuration and operational records	customer-approved enclave	programme security owner
export controlled	technical data, source code or defence-service records	authorised people, systems and sites	export compliance owner

Domain	Typical content	Permitted environment	Decision control
classified or specially protected	authority-designated information	accredited environment	designated security authority
AI training and evaluation	approved datasets, labels and test results	segregated model-development environment	model owner and validator
AI deployment	weights, inference logs, interfaces and updates	authorised operational environment	accountable operational authority

Proposed control model; actual classification and handling depend on applicable authority and contract requirements.

Figure 4. Segmented sovereign data and AI architecture



Proposed logical architecture; actual accreditation, connectivity and support design are transaction specific.

10. Protect customer authority and mission confidence

The venture should preserve a clear accountable interface with the government customer, end user and relevant security authorities. The customer may need visibility over ownership, foreign access, subcontractors, locations, system changes, incident response, continuity and exit. These rights should be reconciled with partner confidentiality and controlled-data obligations.

AI-enabled features need an approved concept of use. Define what the system observes, recommends or controls; the human role; performance boundaries; fallback mode; log retention; test evidence; change approval and incident response. Commercial demonstrations should not be treated as operational acceptance.

The board should track acceptance evidence alongside revenue. Contract signature, factory acceptance, site acceptance, operational evaluation, security accreditation and recurring service acceptance can have different cash and risk effects. The valuation should reflect the stage actually achieved.

11. Turn training into demonstrated local authority

Training hours do not prove capability. The transfer plan should identify each role, prerequisite, syllabus, controlled material, instructor authority, supervised task, examination, recertification, access approval and decision right. Competence is demonstrated through accepted work under the defined quality and security system.

Tacit knowledge needs deliberate capture through paired decisions, failure analysis, configuration reviews, maintenance events, customer issues and controlled modifications. The venture should retain evidence of what the local team can perform independently, what requires partner review and what remains prohibited.

Table 4. Training and authority-release matrix

Role	Demonstrated task	Evidence	Authority released
maintainer	diagnose and restore approved equipment	observed task and accepted record	defined maintenance action
manufacturing engineer	execute and control approved process	first-article and quality evidence	process release within limits
software engineer	configure approved parameters	controlled test and code review	bounded configuration change
data or model engineer	prepare approved data and run evaluation	lineage, test and validation record	model-development task
configuration authority	assess change and maintain baseline	supervised boards and audit trail	defined configuration approval
programme security owner	administer access and incidents	exercise, logs and authority acceptance	security decision within mandate

Proposed evidence framework; actual roles and release authority depend on product, law, contract and safety case.

12. Reconcile culture with operating design

Cross-border integration risk often reflects incompatible decision rights, incentives and work systems rather than national stereotypes. The buyer should compare how each organisation sells, prices, approves investment, manages risk, develops products, serves customers and escalates problems.

The partner operating model should define which decisions remain local, which move to group functions and which require joint governance. Protecting autonomy can preserve innovation while leaving duplicated controls. Immediate centralisation can damage speed and accountability. The choice should follow the value thesis.

Integration leaders need behavioural evidence from management interviews, employee listening, process observation and historical change. Generic culture scores have limited value unless they connect to specific execution dependencies such as tender approval, engineering sign-off or customer response.

The board should approve cultural and operating design together. Each proposed governance change should state the value enabled, decision owner, transition risk, measurable outcome and reversal plan.

13. Build the joint-venture operating model before signing

The partner operating model should allocate product management, engineering, configuration control, manufacturing, quality, supply chain, software, data, model governance, cybersecurity, programme security, sales, contracting, finance, compliance, audit and customer delivery. Each activity should identify decision owner, partner support, approval dependency, systems and evidence.

Reserved matters should focus on decisions whose consequence justifies joint control. Examples include product perimeter, new end users, export destinations, controlled-data access, material model changes, security architecture, critical subcontractors, intellectual-property licences, capital calls, debt, dividends, joint ventures, related-party contracts and exit. Routine operations need delegated authority so the venture can perform.

The operating model should include denial or delay. If a partner cannot provide an update, specialist or approval, the venture needs a safe operating mode, customer communication, inventory and cash response, cure timetable and escalation. The economics should price this dependency.

14. Underwrite localisation and supply resilience as an operating system

Localisation should distinguish local spend, local assembly, local manufacture, local engineering, local intellectual property, local decision authority and export capability. These outcomes require different investment and create different resilience. A percentage partner without a bill-of-materials and activity map can reward low-consequence spend while critical dependencies remain offshore.

The supply-chain model should identify controlled parts, single sources, long-lead items, test equipment, cryptographic material, approved vendors, obsolescence, repair loops, customs, quality release and minimum inventory. Local substitution requires engineering, qualification, customer and export-control review.

AI can assist demand forecasting, anomaly detection and maintenance planning. The approved operating process should retain source evidence, confidence, human review and fallback. A model forecast should not silently become an order, configuration change or safety decision.

15. Govern the AI and product road map as controlled configuration

The road map should distinguish product baseline, authorised local configuration, planned partner releases, security patches, model updates, data changes, interfaces and customer-specific variants. The venture should know which changes it can propose, develop, test, approve and deploy.

For each AI use case, maintain intended purpose, prohibited uses, data rights, performance measures, uncertainty, failure modes, human oversight, cybersecurity, validation, monitoring and decommissioning. NIST and OECD frameworks provide useful governance concepts; they do not replace defence-specific authority, safety, security or legal requirements.

Model drift and software dependency can change the economics after closing. The financial plan should include secure compute, data preparation, independent testing, red teaming where appropriate, model monitoring, update validation, licence cost, specialist retention and contingency for a partner-controlled component.

16. Preserve certification quality and configuration evidence

The venture should map every certification, approval, quality standard, facility status, personnel approval, test procedure and configuration record required to manufacture, maintain or support the product. Identify the holder, scope, transferability, renewal, audit right, change process and consequence of suspension.

Digital threads can improve traceability across requirement, design, part, process, test, release, field event and modification. Access still follows the applicable authorisation and security boundary. The venture should avoid creating a consolidated data lake that broadens access beyond permitted purpose.

AI-assisted inspection or anomaly detection needs validated inputs, representative evaluation, false-positive and false-negative analysis, human disposition, retained images or measurements, model version and audit trail. The accountable quality authority approves release.

17. Build the commercial synergy bridge

Commercial synergies should start with specific customers, products and channels. The buyer needs to show which relationship opens access, which product meets a known need, who owns the sale, what proof is required and when revenue can begin. Broad cross-selling percentages provide weak governance.

The bridge should separate price, volume, mix, retention, channel, new product and geographic expansion. It should include implementation cost, sales capacity, localisation, working capital, customer concentration and cannibalisation. Gross margin matters because low-margin expansion can inflate revenue without increasing value.

Evidence can include qualified pipeline, customer interviews, framework agreements, tender calendars and reference requirements. Each synergy should have an owner, probability, milestone and warning indicator. The buyer should reconcile the bridge with the partner's stand-alone forecast.

The central case should contain benefits supported by an executable route to market. Additional opportunities can remain in a separately disclosed upside case so that price does not capitalise uncertain demand.

Pipeline governance should distinguish buyer-introduced opportunities, partner-originated opportunities and joint wins. Attribution affects incentive, earn-out and synergy reporting. It also reveals whether the joint venture is genuinely opening access or whether the partner would have won the revenue without the buyer.

18. Build the cost and capability investment bridge

Cost savings can arise from procurement, facilities, systems, professional services, insurance and duplicated corporate functions. Capability joint ventures also require deliberate investment in people, product, localisation, marketing, compliance and delivery capacity. The net bridge should show both sides.

Each initiative should state baseline, owner, action, timing, one-off cost, recurring benefit, customer impact and dependency. Headcount reductions can conflict with capability retention. Platform consolidation can disrupt product development. Procurement changes can damage certified supply chains.

The model should distinguish avoidable cost from allocated accounting cost and should eliminate benefits already included in partner forecasts. Phasing should follow employee consultation, contract termination, migration and operational readiness.

A board-approved reinvestment envelope protects the strategic thesis from a narrow savings programme. Value comes from the capability earning more under the new owner while resilient operations and customer outcomes are preserved.

19. Value the venture through authorised capability states

Valuation should separate contracted cash, probable programme cash, option value and strategic value. Capability that depends on an ungranted approval, untested transfer, unaccredited environment, unavailable people or customer acceptance should not be valued as operating capability. The board can use probability-weighted cases while keeping the gating fact visible.

The model should connect revenue and margin to capability states: import, assembly, production, maintenance, configuration, modification and export. Each state has investment, working capital, approval, volume, price, cost, tax and delay assumptions. Terminal value should reflect continuing rights, support, renewal, obsolescence and exit restrictions.

Valuation lenses can include discounted cash flow, comparable transactions, replacement cost, contract economics and real-option analysis. Strategic value should be presented as identified cash flows, avoided cost, resilience or decision options, with an owner and evidence date. It should not become an unsupported premium.

20. Design financing around licence and milestone risk

Funding should match the staged release of capability. Equity can fund uncertain development and sovereign infrastructure. Working-capital facilities may become appropriate after accepted contracts and controllable receivables. Asset finance can support separable equipment. Project or programme finance requires dependable cash, security and step-in design.

Debt covenants should not force a prohibited disclosure or transfer. Lender diligence, security, enforcement, change of control and information rights need to respect export controls, national-security restrictions, customer consent and classified-information rules. The collateral package may exclude controlled intellectual property or require a pre-agreed transition mechanism.

Capital calls should link to evidence. A tranche for secure infrastructure follows design approval and procurement evidence. A training tranche follows authorised materials, instructors and access. A production tranche follows facility and quality gates. The board should retain liquidity for delay, remediation and customer continuity.

21. Link economic rights to evidence and capability delivery

Upfront equity should pay for rights delivered at closing. Deferred contributions, milestone shares, earn-outs, royalties, service fees or licence payments can respond to later capability. Each mechanism needs an objective definition, evidence, reviewer, dispute process, accounting and tax analysis.

The venture should avoid paying twice for the same contribution through equity valuation, recurring licence fees, mandatory services and transfer pricing. Related-party agreements should specify scope, service levels, benchmarking, audit, change, termination and transition.

A missed milestone can lead to extension, remediation, fee reduction, funding adjustment, restricted dividend, additional support, call or put right, or orderly wind-down. The remedy should fit the cause and preserve customer continuity.

22. Draft definitive documents as one control architecture

The joint-venture agreement, articles, intellectual-property licences, technical-assistance arrangements, supply, services, data, cybersecurity, facilities, employment, financing and customer documents should use consistent definitions and precedence. Capability schedules should tie commercial promises to the governing authorisation and operating evidence.

Key provisions include ownership and board rights, reserved matters, funding, business plan, product and territory, controlled access, personnel, subcontractors, audit, security incidents, model and software changes, data return or deletion, compliance, warranties, indemnities, suspension, force majeure, deadlock, change of control, exit and transition.

The documents should distinguish inability caused by authority decision from partner breach, poor planning or commercial choice. A party should not guarantee an authority outcome it cannot control. It can commit to accurate applications, timely cooperation, compliance, notification and defined contingency actions.

23. Build segregated operations and exit continuity before control changes

Integration should preserve the authorisation perimeter. Identity, networks, devices, repositories, development tools, support channels and physical spaces may need segregation. Shared corporate services should be assessed for data access, administrator privilege, logs, backups, incident response and exit.

The exit plan should identify customer continuity, inventory, spares, warranties, maintenance data, permitted technical records, software escrow where lawful, model access, keys, tooling, people, facilities,

licences, records, data return or deletion and authority notifications. A buyout right has limited value when the venture cannot operate after the partner exits.

Table 5. Joint-venture control and exit-continuity matrix

Dependency	Operating control	Failure signal	Continuity response
export authorisation	scope and expiry register	proviso breach or renewal risk	stop affected access and activate approved fallback
partner technical support	service level and named capability	missed response or unavailable specialist	local triage, inventory and authorised substitute
software and model updates	controlled release and validation	delayed patch or failed evaluation	freeze approved baseline and apply contingency
secure infrastructure	accredited boundary and monitoring	control failure or incident	isolate, investigate and restore under authority
critical supply	qualified source and buffer	delay, obsolescence or quality failure	approved reserve, repair or requalification plan
customer programme	acceptance and communication path	performance or security event	accountable notification and recovery plan

Proposed transaction schedule; enforceability and permitted transition depend on applicable law and authorisations.

24. Demonstrate a hypothetical staged-capability investment case

Assume initial committed funding of USD 180 million. The local partner contributes USD 105 million and facilities. The international partner contributes USD 45 million and defined licences. USD 30 million funds secure infrastructure, training, validation and working capital. The case assumes no value for unapproved technical data or export rights.

Capability is released through six gates: authorised perimeter, accredited environment, trained personnel, accepted assembly, accepted maintenance and approved configuration. Draws and economic rights follow evidence. In the central case the venture reaches USD 92 million of annual revenue and USD 16 million of EBITDA in year five. A licensing-delay and lower-qualification case reaches USD 61 million of revenue and USD 3 million of EBITDA. All amounts are hypothetical.

Table 6. Hypothetical staged capability and funding plan

Gate	Evidence	Cumulative funding	Capability state	Economic response
1 perimeter	parties, products, end users and activities defined	15	application and design	diligence and design spend only
2 secure environment	approved architecture and facility controls	55	controlled access available	infrastructure contribution released
3 people	authorised training and demonstrated competence	80	supervised local tasks	training milestone recognised
4 production	first article and quality acceptance	125	local assembly or production	production capital released
5 support	accepted local maintenance performance	150	defined sustainment authority	service economics begin
6 configuration	approved change and validation process	180	bounded local configuration	final contribution and option rights

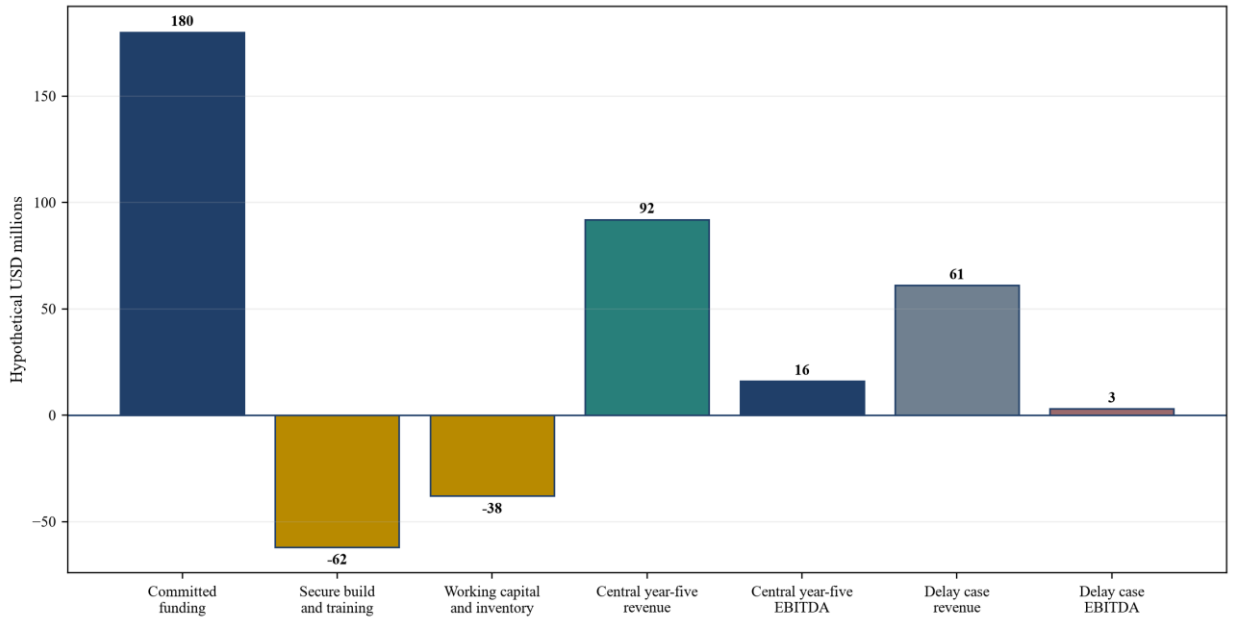
All amounts and outcomes are illustrative management assumptions in USD millions.

25. Run correlated downside scenarios across authority capability and cash

Downside should combine events that can occur together. A licence delay can defer technical access, training, facility acceptance, customer delivery and revenue while secure-infrastructure and payroll costs continue. A cyber incident can suspend access and create remediation. A partner change of control can trigger review. A customer configuration change can require new approval.

The model should show monthly liquidity, committed cost, revenue, EBITDA, working capital, capital calls and covenant headroom. Operational cases should show which capability remains safe and lawful. The board should understand the time available to cure before customer continuity or solvency is threatened.

Figure 5. Hypothetical central and licensing-delay cash bridge



All values are hypothetical management assumptions in USD millions.

26. Establish board governance and accountable AI control

The board should receive a capability ledger, approval status, access exceptions, security events, training authority, customer acceptance, supply resilience, model changes, milestone economics and liquidity. Reserved matters and delegated authority should align with consequence.

AI governance should identify system owner, operational authority, data owner, model developer, validator, cybersecurity owner, user and independent assurance. High-consequence output should reach an authorised person with source evidence, confidence, limitations and fallback. Overrides require reason, evidence, authority and retention.

The venture should maintain internal audit and partner audit rights appropriate to the sensitivity. Reviews can test access, classification, authorisation scope, model lineage, configuration, third parties, records, incident response and corrective action. Findings need owners and due dates. The board information design should separate a legal right from an operating condition. An approval can remain valid while an access-control failure makes continued use unsafe. A model can remain technically available while its evaluation evidence no longer supports the intended purpose. A customer contract can remain in force while a security incident requires suspension. The dashboard should therefore show authority, security, performance, customer acceptance and liquidity as distinct dimensions, together with their interactions.

Committee mandates should follow competence and consequence. The joint-venture board owns strategy, capital, reserved matters and continuity. A programme board owns delivery, acceptance and customer

commitments. A security committee owns accredited boundaries, access exceptions and incident response. A configuration or design authority owns approved baselines and bounded changes. A model-governance forum owns AI purpose, validation, monitoring and retirement. Each committee needs a defined escalation path when a decision crosses another mandate.

Change control should cover more than technical configuration. New investors, directors, nationalities, secondees, subcontractors, facilities, cloud services, development tools, data sources, models, interfaces, end users and territories can alter the approved risk position. The company secretary and compliance function should maintain a change trigger register and obtain review before implementation. Emergency action needs a narrow authority, retained evidence and prompt retrospective review.

Metrics should support intervention. Suitable measures can include approvals approaching expiry, access exceptions, overdue security actions, training authority achieved, rejected configuration changes, model-evaluation failures, customer acceptance delay, critical supplier coverage, cash to the next capability gate and time to execute the continuity plan. Targets should be interpreted with source evidence and consequence; a green average should not conceal one critical prohibited or unsafe condition.

27. Build the transaction data room as a controlled evidence system

The data room should separate commercial, corporate, technical, export-controlled, security-restricted and customer-controlled material. Admission should follow identity, nationality where legally relevant, need, authorisation, agreement and device or location controls. Download restrictions do not replace lawful access analysis.

Core records include ownership, products, classifications, licences, agreements, provisos, end users, technical-data registers, intellectual property, software bill of materials, model cards, data provenance, cybersecurity architecture, facility evidence, personnel approvals, training, quality, certifications, supply chain, contracts, finance, tax, insurance and disputes.

Every investment-committee conclusion should link to a dated source, reviewer, confidence and open condition. Management presentations are evidence of representation, not independent verification.

28. Execute a controlled first 100 days

Days 1 to 20 should confirm governance, authorised perimeter, people, sites, systems, customer interfaces and stop-work rules. Days 21 to 50 should establish segmented environments, access administration, records, security monitoring, programme controls and funding gates. Days 51 to 80 should run supervised training, quality and support cycles. Days 81 to 100 should conduct an operating exercise covering a configuration change, cyber event, supply interruption and authority escalation.

The first 100 days should avoid broad system integration or uncontrolled data migration. Each interface needs purpose, classification, approval, owner, logging and exit. Any temporary arrangement needs an expiry and accountable conversion plan.

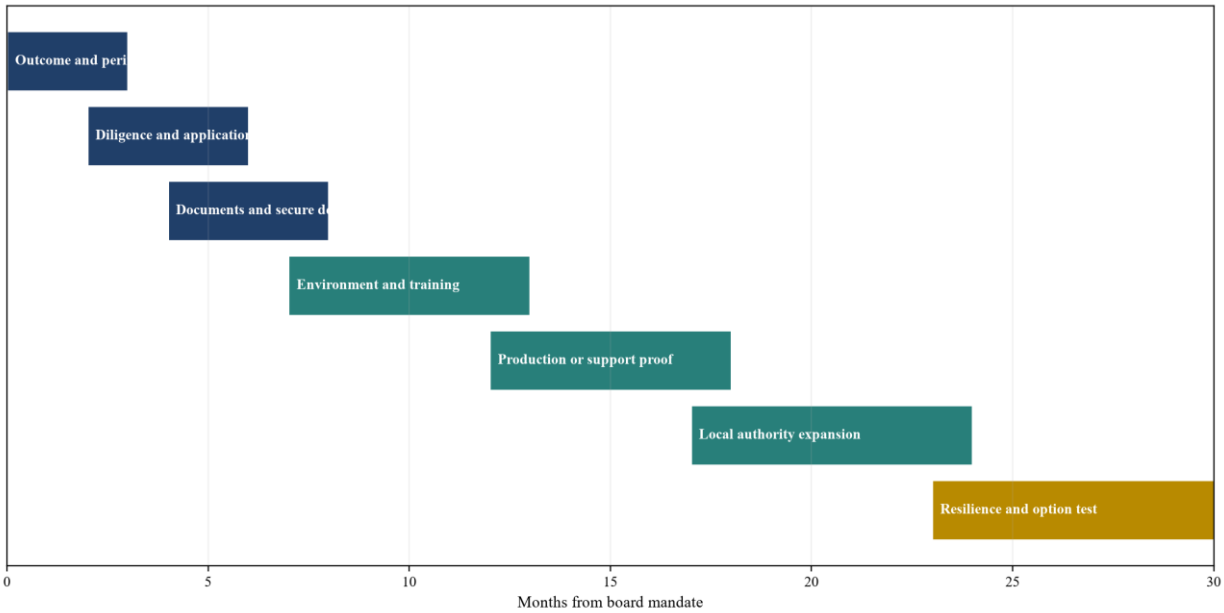
The board should receive evidence of what is operational, what remains supervised, what is pending authority, which milestone economics have been released and whether liquidity covers the next gate and downside case.

29. Use a thirty-month capability and transaction roadmap

The roadmap should connect transaction, approval, build, competence and customer gates. Months 0 to 3 define outcome, partner perimeter and preliminary classifications. Months 3 to 6 complete diligence, applications, operating design and definitive documents. Months 6 to 12 build the secure environment and begin authorised training. Months 12 to 18 demonstrate production or support capability. Months 18 to 24

expand accepted local authority. Months 24 to 30 test resilience, option rights and export readiness where permitted.

Figure 6. Illustrative thirty-month GCC defence JV capability roadmap



Timing is illustrative; authority, customer, product and security requirements determine the actual programme.

30. Define the investable and executable defence joint venture

A defence joint venture becomes investable when the sovereign outcome, controlled perimeter, partner contribution, approvals, secure architecture, competence pathway, customer acceptance, economics, governance and exit continuity form one evidence chain. The board should avoid paying for capability that is described in a strategy deck but absent from an authorisation, operating design or demonstrated local task.

Proceed when the venture can identify what it may receive, know, do, modify, manufacture, maintain and export at each stage; when customer and authority dependencies are transparent; when AI and data remain within accountable controls; and when funding follows evidence. Defer when critical rights, data boundaries, people, facilities or approvals remain undefined. Reject when the commercial case depends on prohibited access, unsupported authority outcomes or an exit that cannot preserve customer support.

The practical output is a controlled transaction architecture rather than a promise of unrestricted transfer. That architecture can still create valuable local capability, resilient support, industrial learning and aligned economics when each party commits only what it can lawfully and operationally deliver.

Table 7. Board commitment gates for a GCC defence joint venture

Gate	Required evidence	Approver	Stop condition
sovereign outcome	funded requirement and capability definition	sponsor board	ambition without operating consequence
controlled perimeter	classifications, parties, activities and sites	compliance and counsel	unresolved prohibited access
operating design	segregated systems, roles and decision authority	JV boards and security owners	architecture cannot meet required controls
economics	milestone funding and downside liquidity	investment committee	value depends on ungranted capability

Gate	Required evidence	Approver	Stop condition
customer acceptance	qualification, security and delivery path	customer and programme authority	no executable acceptance route
closing	documents, approvals and readiness evidence	authorised boards	material condition remains unsupported
continuing operation	renewals, monitoring, audit and exit readiness	JV board	loss of lawful or safe operating basis

Proposed governance checklist; actual approvals and professional opinions are transaction specific.

Frequently asked questions

Does joint-venture ownership transfer defence technology automatically?

No. Equity ownership and export, reexport, retransfer, technical-data, defence-service, software, intellectual-property and end-use rights are separate questions governed by applicable law, authorisations and contracts.

What should a capability-transfer ledger contain?

It should identify each product, data set, software component, model, service, training element, tool and authority; its holder, classification, permitted recipient, purpose, place, people, evidence, restrictions, expiry and operating consequence.

How should AI capability be treated in the transaction?

Separate data, code, model weights, evaluation assets, interfaces, deployment environment, update rights, monitoring and human decision authority. Each can have different ownership, export-control, security and sovereign-data treatment.

Does local hosting establish sovereign control?

Local hosting addresses location. Sovereign operational control also depends on keys, administrators, remote access, model and software dependencies, update authority, logs, specialists, licences and the ability to continue safely when external support stops.

How should capability milestones affect economics?

Funding, shares, fees, royalties, earn-outs, dividends or option rights can follow objective evidence such as approval, secure-environment readiness, demonstrated competence, customer acceptance and released operating authority.

What happens when an export approval is delayed or narrower than requested?

The venture should use the authorised scope, preserve liquidity, stop affected access, activate an approved fallback, revise milestones and economics, communicate with the customer and follow the documented escalation and remedy process.

What should be planned before a partner exits?

Customer continuity, lawful records, inventory, spares, warranties, maintenance, software and model access, keys, tooling, people, facilities, licences, data return or deletion and authority notifications should have a tested transition path.

Is the hypothetical case a transaction recommendation?

No. It demonstrates a framework using hypothetical assumptions. A live transaction requires verified facts and current qualified legal, regulatory, security, technical, financial, tax, accounting, valuation and customer advice.

References

[1] U.S. Department of State, Directorate of Defense Trade Controls, International Traffic in Arms Regulations. https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987

[2] U.S. Department of State, Directorate of Defense Trade Controls, Agreement Guidance and DECCS industry resources. https://deccs.pmddtc.state.gov/deccs?id=ddtc_search&q=itar

[3] U.S. 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

[4] U.S. Department of Commerce, Bureau of Industry and Security, Export Administration Regulations Part 734. https://www.bis.gov/regulations/ear/734

[5] U.S. Department of Commerce, Bureau of Industry and Security, Export Administration Regulations Part 744. https://www.bis.gov/regulations/ear/744

[6] UK Government, Export controls: military goods, software and technology. https://www.gov.uk/guidance/export-controls-military-goods-software-and-technology

[7] UK Government, Military end-use controls. https://www.gov.uk/guidance/military-end-use-controls

[8] European Union, Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. https://eur-lex.europa.eu/eli/reg/2021/821/oj

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

[10] United Arab Emirates Cybersecurity Council, National Cloud Security Policy. https://uaelegislation.gov.ae/en/policy/details/lsy-s-lotny-llamn-lsh-by

[11] Saudi Data and AI Authority, Personal Data Protection Law and implementing resources. https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/

[12] Saudi Data and AI Authority, Regulation on Personal Data Transfer Outside the Kingdom. https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/PDPL2/

[13] Saudi National Cybersecurity Authority, Essential Cybersecurity Controls. https://nca.gov.sa/ecc-en.pdf

[14] Saudi National Cybersecurity Authority, Cloud Cybersecurity Controls. https://nca.gov.sa/ccc-en.pdf

[15] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework 1.0. https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10

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

[17] National Institute of Standards and Technology, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, SP 800-171 Rev. 3. https://csrc.nist.gov/pubs/sp/800/171/r3/final

[18] OECD, AI Principles. https://oecd.ai/en/ai-principles

[19] International Organization for Standardization, ISO/IEC 42001 AI management systems overview. https://www.iso.org/artificial-intelligence/ai-management-systems

[20] Wassenaar Arrangement, Control Lists. https://www.wassenaar.org/control-lists/

[21] United Nations Office for Disarmament Affairs, Arms Trade Treaty. https://disarmament.unoda.org/convarms/att/

[22] U.S. Department of Defense, Cybersecurity Maturity Model Certification programme. https://dodcio.defense.gov/CMMC/

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 closure.

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 and leads 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.