

Sovereign by Design: Control, Localisation and Exit in GCC Defence-AI JVs

A transaction framework for durable partnership economics across technology, data, manufacturing and national control

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Defence-AI joint ventures in the Gulf must produce local capability while preserving lawful access to foreign technology, reliable mission delivery and investable economics. Equity ownership alone cannot answer who controls software releases, model weights, training data, technical decisions, export permissions, customer relationships, manufacturing quality, cyber operations or crisis support. A venture can appear locally controlled while remaining operationally dependent on a foreign parent. It can also transfer substantial know-how without building an economically sustainable local business.

This paper develops a Sovereign-by-Design JV Framework for acquisition, formation, recapitalisation and exit decisions. It separates eight control layers: legal ownership; board and reserved matters; technology and intellectual-property rights; data and model governance; engineering and release authority; manufacturing and supply; customer and mission control; and capital, cash and exit. Each layer is tested against evidence, operating responsibility, regulatory permission, failure states and value allocation. Localisation is measured as an operating capability with named people, facilities, tooling, suppliers, documentation, test authority and recurring customer demand.

A wholly hypothetical case examines a proposed UAE defence-AI joint venture between a GCC industrial sponsor and a foreign autonomy-software company. The illustrative venture begins with a USD 420 million commercial pipeline, USD 72 million of proposed partner contributions and a five-year localisation plan. Evidence review reduces executable risk-adjusted pipeline to USD 196 million, places USD 23 million of technology and market value behind regulatory, acceptance and localisation milestones, and creates separate economics for licensed technology, local engineering, manufacturing, sustainment and export sales. Every financial value is an illustrative management assumption. It is not observed company data, a market forecast, a military assessment, a valuation opinion or evidence of customer commitment.

The evidence base includes the UAE Tawazun Economic Program; Saudi Arabia's General Authority for Military Industries strategy and Industrial Participation Policy; current public GCC defence-technology joint-venture announcements; U.S. Directorate of Defense Trade Controls guidance for technical-assistance and manufacturing-licence agreements; U.S. Bureau of Industry and Security guidance on advanced computing and AI-related export controls; UAE and Saudi AI-governance sources; the NIST AI Risk Management Framework; UAE commercial-company and personal-data legislation; IFRS requirements for joint arrangements and business combinations; and OECD guidance on intangibles.

The conclusion is that sovereignty should be contracted, funded, tested and auditable. Durable partnership value comes from operational capability, lawful rights, accepted mission performance and collected cash.

JEL Classification: G34, L14, L64, O32, O38, H56

Keywords: defence AI, GCC joint ventures, technology sovereignty, localisation, export controls, data governance, intellectual property, joint control, M&A, exit rights

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 TRANSACTION DECISION

The transaction decision is whether a proposed defence-AI joint venture can create a locally controlled operating capability without severing the technology, supply, approval and support relationships that make the product viable. The parties need an answer before they agree valuation, ownership, governance, contributions, exclusivity, customer allocation, capital calls and exit.

The framework applies to a new joint venture, a minority investment, a technology-licensing vehicle, a manufacturing partnership, a regional sales company or the acquisition of an existing local platform. The legal form matters. The operating design matters more because the customer buys an outcome delivered through software, data, hardware, integration, sustainment and accountable people.

The buyer or sponsor should define the required sovereign outcome in observable terms. Examples include local mission-data custody, authorised release engineering, domestic manufacturing, local test authority, national cryptographic control, local sustainment, independent incident response or the ability to continue service when a foreign parent cannot provide support. Each outcome requires rights, resources and evidence.

Table 1. The eight-layer sovereign-control evidence stack

Control layer	Core question	Minimum evidence	Transaction consequence
Legal ownership	Who owns and consolidates the venture?	Articles, shareholder agreement, cap table and control analysis	Defines formal control and accounting
Governance	Who decides relevant activities?	Board rights, reserved matters, delegated authorities and deadlock rules	Defines decision power
Technology and IP	What may the venture use, change and commercialise?	Licence schedules, source access, field and territory rights	Defines technical freedom
Data and models	Who controls data, weights, prompts, logs and outputs?	Data map, model registry, licences and retention rules	Defines lawful learning and reuse
Engineering	Who can build, test, release, patch and recover?	Repositories, pipelines, keys, test authority and local team	Defines operational autonomy
Manufacturing and supply	What can be produced, qualified and sustained locally?	Bill of materials, tooling, suppliers, quality records and spares	Defines delivery resilience
Customer and mission	Who holds the contract and mission authority?	Customer agreements, acceptance, security and tasking rights	Defines executable demand
Capital, cash and exit	Who funds, receives value and can leave?	Funding plan, transfer pricing, distributions and exit mechanics	Defines investable economics

Each layer requires contractual rights, operating resources, regulatory permission and tested execution.

2. DISTINGUISH SOVEREIGNTY FROM SHAREHOLDING

A local majority shareholding can satisfy a legal or policy requirement while leaving critical operating power elsewhere. The foreign partner may control source code, model updates, cloud access, export authorisations, technical staff, cyber tooling, specialised components or the only customer-approved test environment. Formal ownership and operational autonomy should therefore be reviewed separately.

Sovereignty is also broader than independence. A rational joint venture can remain connected to a global technology network while holding sufficient local authority to meet customer, security and continuity requirements. The objective is a deliberate dependency model with understood triggers, substitutes and remedies.

The evidence file should list every dependency that can stop delivery. For each dependency it should identify the provider, contractual right, approval, lead time, replacement path, data exposure, cost and effect of termination. A dependency that is lawful, reliable and competitively priced can support value. An undocumented or revocable dependency can become a valuation discount or closing condition.

3. TRANSLATE NATIONAL POLICY INTO OPERATING OBLIGATIONS

The UAE Tawazun Economic Program describes industrial participation intended to create sustainable economic, social and strategic benefit, including long-term partnerships, innovation, research and development, technology transfer and new capability. Saudi Arabia's General Authority for Military Industries links procurement, manufacturing and technology development to military readiness, strategic autonomy, spending efficiency and a sustainable domestic sector.

These policies create a direction for transaction design. They do not by themselves define which software component, production activity, job, supplier or right qualifies as localisation for a specific programme. The parties should convert policy goals into a programme schedule that can be measured and audited.

The schedule should identify the baseline, target state, accountable party, budget, customer acceptance, timing and remedy. It should distinguish direct local spend from capability creation. Rent, payroll and assembly can increase local expenditure. Sovereign capability also requires knowledge, authority, tooling, documentation, quality, security and continuing demand.

4. MAP THE PRODUCT AS A MISSION SYSTEM

Defence AI is rarely a standalone model. The delivered system can combine sensors, communications, compute, data pipelines, training data, simulation, models, autonomy software, operator interfaces, cyber controls, effectors, test infrastructure and sustainment. A joint venture that controls one layer can remain dependent on several others.

The parties should map the complete mission chain from sensing to authorised action. The map should show which entity owns each component, who operates it, what information crosses organisational or national boundaries, which approvals apply and what happens when a component is unavailable.

The system map should also identify assurance boundaries. A model can perform well in a laboratory and fail when data changes, communications degrade, adversarial conditions emerge or human operators use it differently. Mission value requires representative testing, configuration control, monitoring, override and incident response.

5. ALLOCATE LEGAL AND ACCOUNTING CONTROL DELIBERATELY

The shareholder agreement should reflect the activities that significantly affect returns and mission delivery. Relevant activities can include programme bidding, technology roadmaps, model releases, major suppliers, customer contracts, security architecture, capital expenditure, financing, data use, export applications and appointment of senior technical leaders.

IFRS 11 describes joint control as contractually agreed sharing of control where decisions about relevant activities require unanimous consent. Legal ownership percentages alone do not settle the accounting outcome. The parties should analyse the contractual arrangement, separate vehicle, rights to assets, obligations for liabilities and decision requirements before signing.

Accounting classification influences consolidation, reported revenue, leverage, covenants and exit expectations. It should follow the actual control design. A structure created to obtain a desired accounting presentation can fail when operational rights tell a different story.

6. BUILD A RESERVED-MATTERS ARCHITECTURE

Reserved matters should protect both sovereign requirements and the venture's ability to operate. A list that requires unanimous approval for every meaningful decision can create paralysis. A narrow list can allow one partner to change technology, markets or economics without adequate protection.

Matters should be grouped by purpose. Mission and security matters can require customer or sovereign approval. Technology matters can require the owner of controlled IP to confirm lawful release. Commercial matters can follow an approved business plan within thresholds. Capital matters can use pre-agreed funding and dilution rules.

The agreement should define information standards, decision deadlines and escalation. A veto should identify the protected interest and should not become an indefinite option to delay. Failure to decide can trigger an expert determination, a customer referral, a temporary operating rule or a structured exit process.

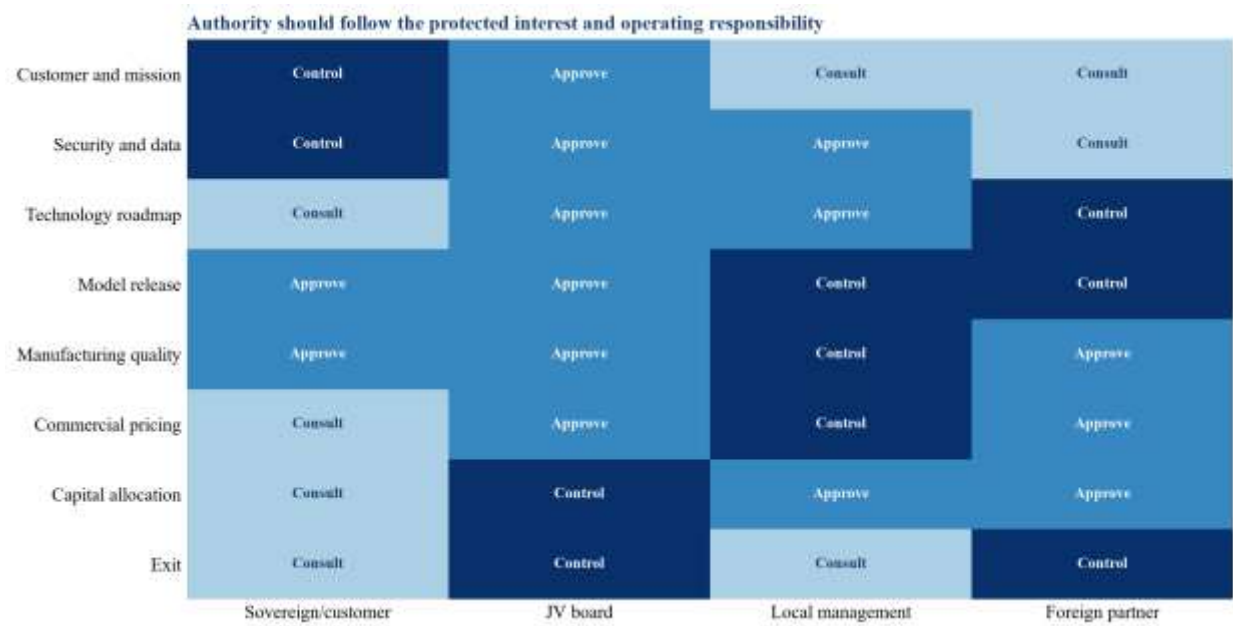


Figure 1. Illustrative allocation of decision authority across the JV control stack
The allocation is a management-design example and does not describe any existing venture or legal requirement.

7. SEPARATE BACKGROUND IP, CONTRIBUTED IP AND FOREGROUND IP

The intellectual-property schedule should identify what each partner owns before formation, what is licensed or assigned to the venture, what the venture develops and what each partner may use after development. General clauses referring to each party's technology are insufficient for a complex AI system.

Background IP can include source code, model architecture, training methods, interface specifications, patents, trade secrets, simulation assets, design data and manufacturing processes. Contributed IP should be itemised with version, scope, territory, field, term, sublicensing, modification, support and termination rights.

Foreground IP should be allocated according to contribution, funding and intended market. Joint ownership can create uncertainty over enforcement, licensing and exit. A cleaner design can assign ownership to the venture with defined licences back to the partners, or assign by technical field while preserving the venture's continuing rights.

8. DESIGN SOURCE-CODE AND MODEL-WEIGHT ACCESS

Access to source code or model weights is not the same as the ability to operate them. The venture also needs build instructions, dependencies, development environments, data schemas, test suites, signing keys, deployment tooling, model cards, evaluation records and authorised personnel.

The access model should have ordinary and contingency states. Ordinary access can remain within controlled repositories operated by the technology partner. Contingency access can activate after insolvency, prolonged support failure, sanctions, licence termination, unresolved cyber incident or an authorised national-security direction.

Escrow should be tested. A deposited archive has limited value when it cannot be built, deployed or supported. Periodic reproducibility exercises should demonstrate that the designated local team can restore a defined version in an approved environment without relying on undocumented assistance.

9. ALLOCATE DATA AND LEARNING RIGHTS

AI value can shift through use. Operational data can improve models, expose failure modes and generate new products. The data schedule should distinguish customer data, sensor data, synthetic data, annotations, telemetry, operator interactions, test results, derived features, model outputs and incident records.

For each category, the schedule should identify controller, processor, custodian, permitted purpose, location, access, retention, deletion, training rights, sharing, classification and export status. Customer contracts may restrict use even when the venture physically holds the data.

The UAE Personal Data Protection framework and Saudi data-governance requirements add obligations where personal data is processed. Defence and security contracts can impose stronger requirements. The venture should design the data architecture to meet the applicable customer and jurisdictional rules rather than assume one regional standard.

10. GOVERN MODELS AS CONTROLLED ASSETS

The model registry should identify each production model, owner, version, training data, intended use, prohibited use, evaluation results, deployment location, approvals and rollback path. Model updates should pass defined technical, security, safety and mission-acceptance gates.

The UAE AI ethics guidance addresses fairness, transparency, accountability, explainability, human-centred values, privacy, robustness, safety, security and sustainability. Saudi AI ethics sources

address reliability, safety, privacy, security, transparency and accountability. NIST's AI Risk Management Framework provides a voluntary process for governing, mapping, measuring and managing AI risks.

These frameworks can inform the venture's controls. Mission assurance still requires a product-specific test plan, named authority and customer acceptance. A policy statement does not demonstrate performance under representative operating conditions.

11. PRESERVE HUMAN ACCOUNTABILITY FOR CONSEQUENTIAL DECISIONS

The operating concept should state where AI recommends, prioritises, navigates, detects, tracks or controls, and where authorised people decide. The boundary should be explicit for normal, degraded and emergency states.

Accountability requires more than a human interface. The operator needs sufficient information, training, time and authority to understand a recommendation, reject it and recover safely. Logs should record model version, inputs, confidence, user action, override and outcome where lawful.

The joint venture should allocate responsibility across developer, integrator, operator and customer. Liability cannot be managed through a broad disclaimer when the system design, data, integration and mission use are shared across parties.

12. TREAT EXPORT PERMISSION AS A PRODUCTION DEPENDENCY

Technology transfer, technical assistance, foreign-person access, manufacturing, re-export and support can require approvals. U.S. Directorate of Defense Trade Controls guidance distinguishes technical-assistance agreements, manufacturing-licence agreements and distribution arrangements for controlled defence articles, technical data and services. U.S. Commerce controls can also apply to dual-use technology, advanced computing and certain AI-related items.

The venture should build an export-control classification and authorisation matrix before assigning work. It should list hardware, software, technical data, services, people, facilities, destinations, end users and end uses. The matrix should show what is authorised, pending, excluded or subject to provisos.

Regulatory permission should not be assumed from partner intent. A contribution that cannot lawfully reach the venture should remain outside base valuation and operating plans until approval is obtained. The transaction documents should address delay, partial approval, restrictive provisos and denial.

13. RING-FENCE CONTROLLED TECHNOLOGY WITHOUT CREATING AN EMPTY VENTURE

Technical-control plans can restrict access by nationality, role, location, network and programme. The venture can use secure enclaves, segregated teams, clean rooms, controlled repositories and approved interfaces. These controls should preserve compliance while enabling the venture to deliver a real product.

An overly narrow interface can reduce the local entity to assembly or sales. The localisation plan should therefore identify which capabilities can be transferred immediately, which require approval, which can be developed independently and which should remain with the foreign partner.

The economic model should follow the actual division. The venture should not pay a full technology premium for a black-box component while carrying customer, integration and performance risk. Fees should reflect the rights, support, performance and continuing accessibility provided.

14. DEFINE LOCALISATION AS A CAPABILITY LADDER

Localisation should progress through measurable levels. Level one can be local sales, programme management and support. Level two adds assembly, integration and test. Level three adds repair, configuration, software integration and supplier development. Level four adds design authority for defined modules, model evaluation, release engineering and product improvement. Level five adds independent development and exportable products within authorised scope.

Each level requires people, process, infrastructure, rights and demand. Training completions alone do not establish capability. The evidence should include competency assessment, completed work, quality records, customer acceptance and repeat delivery.

The ladder should match programme economics. A capability with no forecast workload can become a permanent cost centre. The customer and venture should connect localisation milestones to procurement, sustainment and export opportunity without treating an announced pipeline as committed revenue.

Table 2. Localisation scorecard for a defence-AI joint venture

Capability	Baseline evidence	Target evidence	Value test
Local engineering	Headcount and job descriptions	Named team completes accepted releases	Reduced foreign engineering dependence
Model evaluation	Imported reports	Local test datasets, harnesses and approvals	Faster mission-specific assurance
Manufacturing	Assembly records	Qualified suppliers, tooling and first-pass yield	Reliable local output and lower lifecycle risk
Sustainment	Foreign support tickets	Local diagnostics, spares and mean-time-to-repair	Improved availability and response
Data governance	Informal storage map	Approved lineage, access, retention and deletion controls	Lawful reuse and customer confidence
Design authority	Partner-controlled decisions	Local authority for defined modules and interfaces	Product adaptation and export potential

Evidence should demonstrate repeatable delivery under the applicable security and quality regime.

15. CONNECT LOCALISATION MILESTONES TO ECONOMIC VALUE

Milestones should affect price, fees, exclusivity, customer allocation or equity only when they create measurable capability. Examples include regulatory approval, successful local build, first accepted local release, supplier qualification, customer-approved test authority, defined design authority and completed sustainment transfer.

The parties can use staged equity vesting, contingent consideration, fee reductions, performance credits or additional market rights. The mechanism should identify the evidence, evaluator, deadline, cure period and economic consequence.

Milestones should remain within the contributing party's control. A milestone dependent entirely on a government procurement decision can create dispute. Customer acceptance can still be an outcome gate when the parties separately allocate bid, delivery and approval responsibilities.

16. MEASURE WORKFORCE TRANSFER THROUGH DELIVERED WORK

The workforce plan should cover roles, security eligibility, competence, retention, succession and workload. A target number of local employees can be met without transferring the critical capability if senior architecture, release, test and customer authority remain elsewhere.

Capability transfer should be assessed through completed tasks. Local engineers should reproduce builds, resolve defects, integrate interfaces, conduct evaluations, release authorised configurations and support field incidents. Manufacturing teams should meet quality, traceability and delivery measures.

Retention economics matter. Scarce personnel may be recruited by the venture and then remain dependent on one foreign technical leader. The plan should include documented processes, paired roles, succession, incentive alignment and restrictions consistent with applicable law.

17. BUILD THE SUPPLY-CHAIN SOVEREIGNTY MAP

The bill of materials should identify country of origin, sole sources, long-lead components, controlled content, obsolescence, cyber exposure, qualification status and substitutes. AI systems also depend on compute, cloud, development tools, mapping, communications and data services.

Local assembly can coexist with concentrated foreign inputs. The venture should calculate the time and cost required to replace each critical dependency. Inventory can bridge short disruption. It cannot replace unavailable design data, test authority or software support.

Supplier localisation should begin with components and services where the GCC base can meet quality, security and economic requirements. Forced substitution without qualification can increase mission risk. The customer should distinguish resilience value from local-spend volume.

18. CREATE DURABLE CUSTOMER AND PROGRAMME ECONOMICS

The venture's right to bid, contract and serve customers should be documented. The parties should allocate existing customers, regional leads, prime relationships, channels and future opportunities. Ambiguous customer ownership creates conflict when both parents sell overlapping products.

Pipeline should be rebuilt opportunity by opportunity. Each item should show customer, mission need, budget source, procurement route, competitive position, approval requirements, localisation conditions, bid cost, expected margin, acceptance and collection profile.

Public announcements can demonstrate strategic intent. They do not establish funded demand. EDGE and Anduril announced a UAE joint venture and an initial acquisition plan for 50 systems in

2025, subject to required approvals. EDGE and EM&E announced a UAE co-production venture in 2026 with a stated commercial pipeline and divided manufacturing roles. These disclosures illustrate transaction structures; the underlying contracts, approvals and delivery economics require diligence.

19. SEPARATE LICENCE, SERVICE AND PRODUCT ECONOMICS

The foreign partner may receive an upfront licence fee, recurring royalty, engineering fee, component margin, software subscription or share of profits. The local partner may contribute facilities, capital, market access, personnel, customer relationships and programme execution.

Each payment should correspond to a defined contribution and should survive an arm's-length review. An excessive royalty can prevent the venture from funding localisation. Underpriced technology can shift value away from the contributing partner and create tax, governance or minority-protection concerns.

The operating model should show gross margin by product, customer and contribution. It should also show which costs sit in parent companies, which are recharged and which remain with the venture. Transfer-pricing policies should follow functions, assets, risks and the value created by intangibles.

20. FUND THE CAPABILITY BEFORE DISTRIBUTING CASH

A new venture often needs facilities, tooling, compute, security, certification, inventory, bid costs and working capital before it can deliver. The funding plan should identify initial contributions, milestones, capital-call obligations, debt capacity, customer advances and contingency reserves.

Dividend policy should follow capability and liquidity requirements. Early distributions can leave the venture unable to complete localisation or sustain programmes. A retained-cash threshold can cover committed capex, working capital, warranty, security remediation and programme downside.

Failure to fund should have a proportionate consequence. Options include dilution, shareholder loans, suspended distributions, loss of selected rights or a structured sale. Forced transfer at punitive value can discourage reasonable governance and may not solve the operating problem.

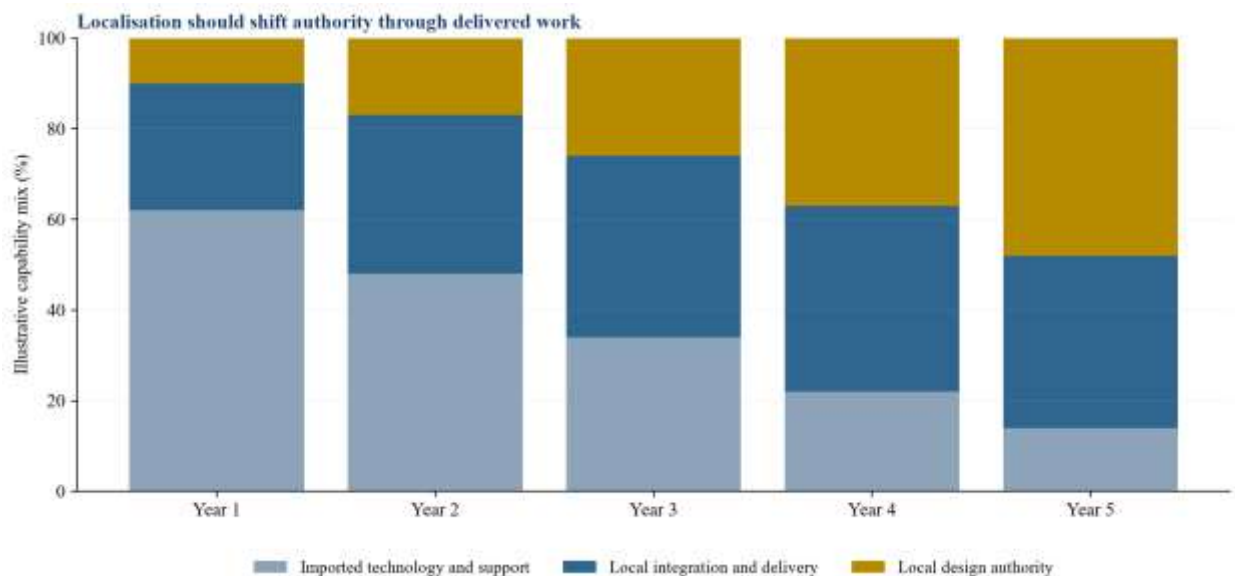


Figure 2. Illustrative five-year progression from imported support to local design authority
Percentages are hypothetical management assumptions and represent an example capability mix.

21. TEST THE HYPOTHETICAL VENTURE ECONOMICS

The hypothetical venture begins with a USD 420 million five-year pipeline. The amount includes announced programmes, qualified opportunities, framework access and early concepts. The parties propose USD 72 million of contributions: USD 30 million of cash and facilities from the local sponsor; USD 27 million of technology rights and engineering support from the foreign partner; and USD 15 million of anticipated customer-funded development.

Evidence review removes unfunded concepts, probability-weights qualified opportunities, separates approval-dependent technology and models customer acceptance. The resulting illustrative executable risk-adjusted pipeline is USD 196 million. This is a transaction-planning scenario, not a forecast.

The contribution review values only rights and support that the venture can lawfully access and use. USD 23 million of proposed technology and market value is placed behind export authorisation, reproducible local builds, customer acceptance, supplier qualification and collected revenue milestones.

22. BUILD AN EVIDENCE-ADJUSTED VALUE BRIDGE

Valuation should separate operating value, technology access, customer access, localisation capability and strategic option value. Each component needs its own evidence and downside. Applying one multiple to the announced pipeline can reward opportunities that are unfunded or inaccessible.

The base case should use accepted revenue, maintainable contribution, required lifecycle investment and continuing parent charges. Scenario value can cover regional exports, adjacent missions or expanded design authority when the required approvals and customer routes are visible.

Strategic value should remain outside the operating case unless the buyer can identify a right, action, cost, timing and cash consequence. Milestones can preserve upside while protecting the venture from paying for unsupported ambition.

Table 3. Hypothetical contribution and value allocation

Value component	Announced or proposed amount	Evidence-adjusted treatment	Transaction mechanism
Five-year pipeline	USD 420m	USD 196m risk-adjusted executable pipeline	Reprice through funded orders and acceptance
Local sponsor cash and facilities	USD 30m	Recognise verified cash, usable facilities and committed services	Equity contribution with completion evidence
Foreign technology and support	USD 27m	Recognise USD 12m at close; defer USD 15m	Vest through approvals, builds and acceptance
Customer-funded development	USD 15m	Exclude until contracted and collectible	Add when funding and rights are documented
Regional market option	USD 18m	Defer USD 8m behind export and customer milestones	Earn-out or staged equity
Localisation premium	USD 10m	Defer until design and sustainment authority is accepted	Milestone payment

All values are illustrative management assumptions; they are not market evidence, forecasts or valuation advice.

23. ALLOCATE PROGRAMME AND BID RISK

The venture should have a bid authority matrix covering price, technical commitments, localisation, offset obligations, warranties, liquidated damages, security and export assumptions. A parent should not commit the venture to a programme without approved capacity and risk.

Bid costs should be budgeted and allocated. The party that controls customer access can contribute opportunity origination while the technology partner contributes solution design. Success fees can distort behaviour when they reward contract signature without regard to margin, delivery or collection.

Programme reviews should reconcile contracted scope to deliverable configuration, approvals, resources and cash. Changes should follow formal control because customer-driven customisation can fragment the product and consume localisation capacity.

24. DEFINE QUALITY, SAFETY AND CYBER ACCOUNTABILITY

The venture should identify design authority, airworthiness or product-assurance responsibility, configuration control, supplier quality, software assurance, cybersecurity and incident command. Responsibilities should align with access and competence.

AI assurance should cover data provenance, model behaviour, adversarial testing, drift, false positives, operator workload, fallback and recovery. The test set should represent intended environments and should be protected from inappropriate reuse.

Cyber events can cross partner boundaries. The incident plan should define detection, disclosure, containment, customer notification, evidence preservation, regulatory reporting, remediation and authority to suspend a system. Contractual indemnities should follow controllable failures and insurance coverage.

25. DESIGN DEADLOCK AROUND SERVICE CONTINUITY

Deadlock is particularly dangerous when the venture supports an operational customer. The agreement should distinguish strategic deadlock from day-to-day operating decisions. Existing approved configurations and customer obligations should continue safely while disputes are resolved.

The escalation path can move from management to board, chief executives, an independent expert and a defined buy-sell or sale process. Technical questions can go to an approved technical expert. Security and mission matters may require customer involvement.

Shotgun clauses can be unsuitable when partners have unequal capital, regulated ownership or non-transferable technology. A fair exit mechanism should recognise these asymmetries and should preserve licences, support and customer continuity during transition.

26. BUILD EXIT BEFORE FORMATION

Exit design should cover voluntary sale, strategic sale, initial public offering, partner default, loss of approval, sanctions, change of control, prolonged deadlock, technology discontinuation and failure to fund. Each event can require a different remedy.

Transfer restrictions should identify permitted buyers, competitors, sanctioned parties and ownership requirements. Rights of first refusal, first offer, tag, drag and put or call options should have clear pricing, timing and regulatory conditions.

The venture's continuing technology, data, customer and support rights are central to exit value. A buyer cannot value the company when core licences terminate automatically on a shareholder transfer. Change-of-control consents and transitional licences should be addressed before the first investment.

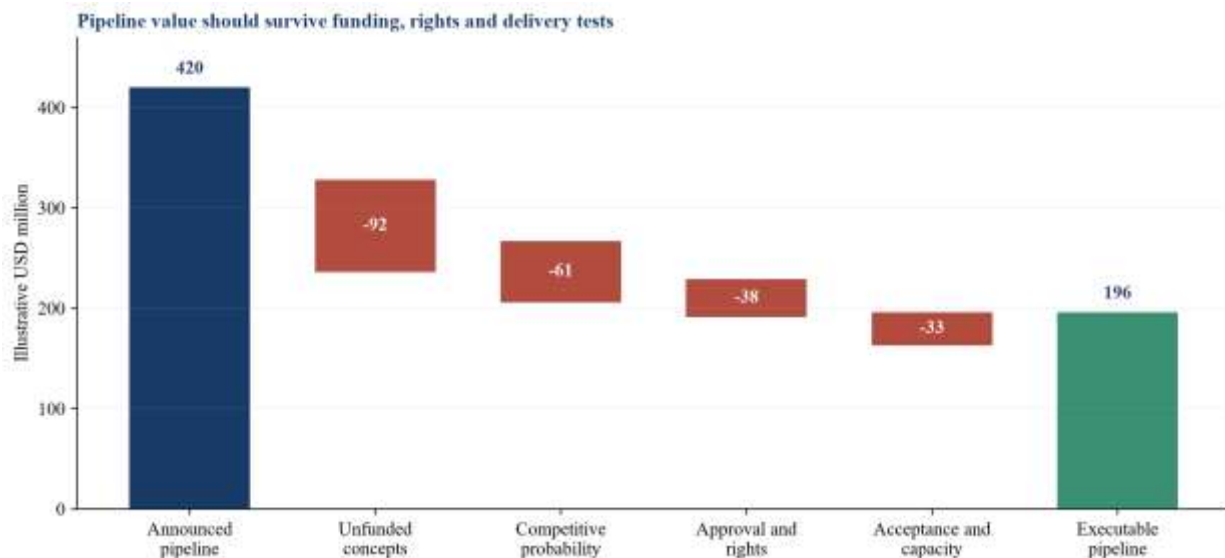


Figure 3. Hypothetical pipeline bridge from announced opportunity to executable programme value

Values are illustrative management assumptions and do not predict awards or revenue.

27. PROTECT THE VENTURE THROUGH CHANGE AND SEPARATION

The separation plan should preserve customer service, security, records, tooling, data and workforce. Transitional services should identify scope, service level, price, term, access, security, liability and exit assistance.

Technology should have a defined transition state. The venture may retain a perpetual licence for accepted products, a time-limited right to maintain installed systems or access to escrow material. Customer-specific rights and export approvals may constrain the option.

The parties should maintain a separability register throughout the venture's life. It should identify shared systems, people, contracts, facilities, data, IP and suppliers. Annual review reduces the cost and disruption of a future exit.

28. USE TRANSACTION PROTECTION FOR EVIDENCE GAPS

Conditions precedent can cover company formation, sector licences, export authorisations, customer consents, security approvals, IP schedules and committed funding. Covenants can govern applications, staffing, facility readiness and customer engagement between signing and closing.

Representations should cover ownership, authority, IP, data rights, export compliance, sanctions, security incidents, customer contracts, pipeline classification, licences, related-party arrangements and localisation reporting. Known issues can be handled through disclosure, remediation, holdbacks or targeted indemnities.

Earn-outs and staged contributions should use observable measures. Suitable measures include funded orders, accepted local builds, approved releases, qualified suppliers, operational availability and collected cash. Broad strategic milestones invite dispute.

29. ESTABLISH A BOARD EVIDENCE PACK

The board should receive one integrated pack covering mission delivery, commercial performance, localisation, security, technology, approvals, workforce, supply chain, capital and cash. The information should reconcile to customer records and financial accounts.

Key measures can include accepted revenue, executable backlog, gross margin by contribution, cash collection, critical defects, model changes, availability, incidents, export-authorisation status, local engineering authority, supplier qualification, local spend and funding runway.

Measures should expose dependency as well as progress. A rising local-content percentage can coexist with continued reliance on foreign source code or release authority. The board needs both views to make capital and risk decisions.

Table 4. Reserved matters, evidence and failure remedies

Reserved matter	Required evidence	Decision route	Failure remedy
Technology or model release	Test results, security review, configuration and customer requirement	Technical authority plus defined board or customer approval	Retain accepted version and cure
New programme bid	Margin, capacity, approvals, localisation and cash profile	Management within plan; board above threshold	Reprice, partner support or decline
Related-party charge	Scope, benchmark, service level and invoice evidence	Independent director or audit committee	Adjust fee or procure alternative
Capital call	Approved plan, runway and milestone evidence	Board under pre-agreed funding rules	Shareholder loan, dilution or structured sale
IP sublicense or transfer	Rights, field, territory, security and export review	Both partners plus required authority	Restrict use or amend structure
Change of control or exit	Buyer eligibility, licence continuity, customer consent and valuation	Contractual transfer process	Transitional licence or alternative buyer

Thresholds and approval routes should be tailored to the venture, customer and applicable law.

30. SEQUENCE THE FIRST ONE HUNDRED AND EIGHTY DAYS

The first thirty days should establish corporate authority, bank controls, customer and licence registers, technology and data baselines, security access and a single programme portfolio. The venture should confirm what has legally transferred and what remains a parent service.

Days thirty-one to ninety should reproduce builds, validate data and model registers, qualify priority suppliers, confirm programme acceptance, finalise transfer-pricing arrangements and launch workforce capability assessments. Gaps should be linked to funded remediation.

Days ninety-one to one hundred and eighty should complete a representative local release, exercise incident response, test export and security workflows, present the first localisation evidence pack and refresh the capital plan. Progress should be accepted by named authorities rather than inferred from activity volume.

Sovereign control should be established through tested operating evidence

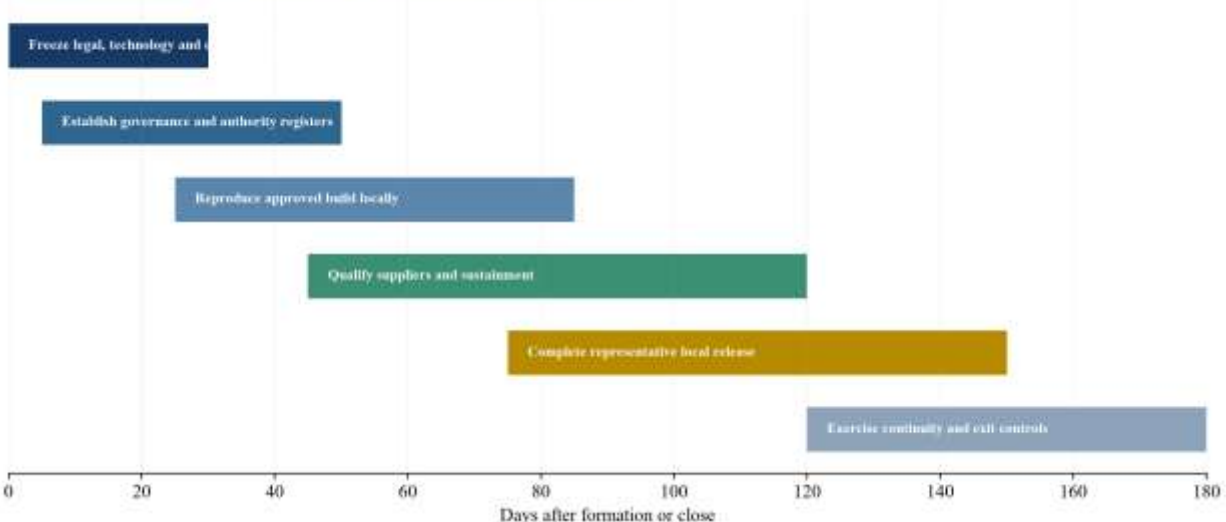


Figure 4. Hypothetical sequencing of sovereign-control implementation
Timing is illustrative and should follow regulatory, customer, security and programme requirements.

31. APPLY A CONFIRMATORY DILIGENCE CHECKLIST

Corporate diligence should cover formation, ownership, licences, control, related parties, disputes and financing. Technology diligence should cover architecture, source, model, data, build, release, cyber, testing, product roadmap and obsolescence. Commercial diligence should rebuild pipeline, backlog, pricing, margin, acceptance and collection.

Regulatory diligence should cover sector licensing, export classifications, authorisations, provisos, sanctions, end users, end uses, data, security and foreign ownership. Localisation diligence should test facilities, people, suppliers, tooling, authority, records and completed work.

The review should use samples that connect the whole chain. Select a material programme and trace customer need, bid approval, technology rights, export permission, local work, delivery, acceptance, invoice and receipt. Select a production release and trace data, model, code, testing, approvals, deployment and incident monitoring.

32. RECOGNISE LIMITATIONS AND CONCLUDE

This framework does not determine the legality, security, safety, military suitability, accounting classification, tax treatment or valuation of a particular joint venture. Requirements vary by product, customer, jurisdiction, ownership, nationality, end use and technical configuration. Current legal, regulatory, export-control, security, technical, tax and accounting advice is required.

Public policy and company announcements establish context. They do not prove a private venture's contract coverage, customer commitment, approvals, technology access, performance or economics. The hypothetical values in this paper exist only to demonstrate the framework.

A durable GCC defence-AI joint venture connects sovereignty to observable operating capability. It gives the local venture the people, rights, systems and authority required to serve customers while maintaining lawful access to global technology and supply. It prices each partner's contribution, funds the localisation journey and protects service through deadlock, default and exit.

Sovereign control is therefore an evidence chain. The chain runs from legal rights through technical authority and accepted mission delivery to collected cash. Transactions that build and test that chain can create durable partnership value. Transactions that rely on ownership labels, announced pipeline or general transfer promises leave the most important risks unresolved.

REFERENCES

- [1] Tawazun Council. Tawazun Economic Program and Policy Guidelines. <https://www.tawazun.gov.ae/wp-content/uploads/2019/09/Tawazun-Economic-Program.pdf>
- [2] General Authority for Military Industries. GAMI Strategies. <https://www.gami.gov.sa/en/strategy>
- [3] General Authority for Military Industries. Industrial Participation Policy. https://www.gami.gov.sa/sites/default/files/2023-03/Industrial%20Participation%20Policy%20-%20English_0.pdf
- [4] General Authority for Military Industries. Localization of Military Spending in Saudi Arabia Increases to 24.89%. <https://www.gami.gov.sa/en/news/gami-reports-localization-military-spending-saudi-arabia-increases-2489>

- [5] EDGE Group. EDGE Group and Anduril Industries Form UAE-US Joint Venture to Develop Autonomous Systems, 13 November 2025. <https://edgegroup.ae/news/edge-group-and-anduril-industries-form-landmark-uae-us-joint-venture-develop-autonomous>
- [6] EDGE Group. EM&E Group and EDGE Establish Joint Venture in the UAE, 17 June 2026. <https://edgegroup.ae/news/eme-group-and-edge-seal-agreement-establish-joint-venture-uae>
- [7] U.S. Department of State, Directorate of Defense Trade Controls. Guidelines for Preparing Agreements, Revision 5.1. https://www.pmddtc.state.gov/sys_attachment.do?sys_id=5c7dfa1797eee21067b1791ad053af46
- [8] U.S. Department of State, Directorate of Defense Trade Controls. DECCS Agreement Guidance. https://deccs.pmddtc.state.gov/deccs?id=ddtc_search&q=itar
- [9] U.S. Department of Commerce, Bureau of Industry and Security. Department of Commerce Announces Rescission of AI Diffusion Rule and Strengthens Chip-Related Export Controls, 13 May 2025. <https://www.bis.gov/press-release/departments-commerce-announces-rescission-biden-era-artificial-intelligence-diffusion-rule-strengthens>
- [10] U.S. Department of Commerce, Bureau of Industry and Security. Export Administration Regulations, Part 734. <https://www.bis.gov/regulations/ear/734>
- [11] UAE Government. Federal Decree Law No. 32 of 2021 on Commercial Companies. <https://www.uaelegislation.gov.ae/en/legislations/1542>
- [12] UAE Government. Federal Decree Law No. 45 of 2021 on Personal Data Protection. <https://uaelegislation.gov.ae/en/legislations/1972>
- [13] UAE Office of Artificial Intelligence. AI Ethics: Principles and Guidelines. <https://ai.gov.ae/wp-content/uploads/2023/05/MOCAI-AI-Ethics-EN.pdf>
- [14] UAE Office of Artificial Intelligence. UAE Position on Artificial Intelligence Policy, 2024. <https://ai.gov.ae/wp-content/uploads/2024/10/UAE-Guiding-on-ai-policy-EN-V3.pdf>
- [15] Saudi Data and Artificial Intelligence Authority. AI Ethics Principles. <https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf>
- [16] Saudi Data and Artificial Intelligence Authority. AI Adoption Framework. <https://sdaia.gov.sa/en/SDAIA/about/Files/AIAdoptionFramework.pdf>
- [17] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework. <https://www.nist.gov/itl/ai-risk-management-framework>
- [18] National Institute of Standards and Technology. NIST AI RMF Playbook. <https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook>
- [19] IFRS Foundation. IFRS 11 Joint Arrangements. <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-11-joint-arrangements/>
- [20] IFRS Foundation. IFRS 3 Business Combinations. <https://www.ifrs.org/content/dam/ifrs/publications/pdf-standards/english/2022/issued/part-a/ifrs-3-business-combinations.pdf>
- [21] OECD. Guidance on Transfer Pricing Aspects of Intangibles. https://www.oecd.org/en/publications/guidance-on-transfer-pricing-aspects-of-intangibles_9789264219212-en.html
- [22] U.S. Department of State, Defense Trade Advisory Group. Joint Ventures and ITAR Compliance Issues, 9 November 2022. https://www.pmddtc.state.gov/sys_attachment.do?sys_id=8ca57c881b8029502b6ca932f54bcbea

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.