Saudi Industrial JVs: Digital-Twin Governance for Technology Transfer and Localisation

A transaction framework for allocating control, access, validation and exit rights across process models, operating data and industrial know-how

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Industrial joint ventures in Saudi Arabia increasingly combine foreign process technology with local capital, market access, procurement capability, people and industrial infrastructure. A digital twin can become a critical part of that bargain because it joins engineering models, equipment identities, operating data, control logic, maintenance history and decision rules. The transaction problem is that these elements rarely share one owner, one legal character or one economic life. A joint venture that receives software access without durable data rights, validation capability or trained people may remain operationally dependent. A technology provider that transfers unrestricted source code, models and derived know-how may lose control of valuable intellectual property beyond the agreed localisation purpose.

This paper develops a Digital-Twin Joint-Venture Governance Framework for industrial technology transfer and localisation in Saudi Arabia. The framework maps the rights stack, aligns localisation milestones with independently testable operating capability, separates accounting recognition from transaction value, and connects reserved matters, access controls, cybersecurity, data protection, licensing economics and exit arrangements. It applies Saudi investment, local-content, data-governance, intellectual-property, competition and operational-technology requirements together with international manufacturing digital-twin, joint-control and AI-governance principles.

The method is demonstrated through a hypothetical Saudi manufacturing joint venture. Management assumptions include total project capital expenditure of SAR 620 million, a foreign technology contribution, a Saudi operating partner, 140 critical manufacturing assets and a five-year operating model. The illustrative digital-twin programme requires SAR 18 million at completion and SAR 7 million in the first year. Gross recurring benefit at maturity is SAR 22.3 million, recurring operating cost is SAR 6.2 million and net recurring benefit is SAR 16.1 million. A five-year model with a management-assumed fourteen-percent discount rate produces an illustrative net present value of approximately SAR 14.9 million before tax, financing, terminal value, transfer pricing and negotiated value sharing. These figures demonstrate the method only. They are not observed company data, a valuation opinion, accounting advice, engineering advice, legal advice or investment advice.

JEL Classification: F21, G34, L24, L60, M15, O32, O33

Keywords: Saudi industrial joint ventures, digital twins, technology transfer, localisation, industrial data, intellectual property, joint control, operational technology, local content, M&A governance

1. Define the transaction decision

The transaction decision is how an industrial joint venture should allocate control, access, validation and exit rights over the digital twin that supports technology transfer and localisation. The parties must decide what the joint venture will own, what it will license, what it may modify, which data it may retain, who can validate changes, what capabilities must be localised and what happens when the relationship ends. These choices affect the value of each contribution, operating resilience, local capability, regulatory compliance, dividend capacity and the risk of strategic dependence.

The decision is narrower than whether the joint venture will use digital-twin software. A factory can display a sophisticated virtual model while depending on the foreign technology provider for every material update, fault investigation and optimisation. It can also hold large volumes of operating data that it cannot combine, interpret or reuse. Conversely, a broad transfer may expose the technology provider's background intellectual property, global model improvements or trade secrets beyond the agreed field, territory and duration.

The framework therefore tests five conditions. The rights stack must cover every material component. The joint venture must possess enough operating evidence and trained capability to perform the agreed decisions. Localisation milestones must measure usable capability rather than document delivery. Reserved matters and deadlock arrangements must preserve safety, cybersecurity and continuity. The expected cash benefit must exceed implementation, governance, licensing and operating costs after execution risk.

Table 1. Digital-twin rights stack for an industrial joint venture

Rights layer	Typical subject matter	Core transaction question	Minimum evidence
Background technology	Pre-existing process models, libraries, algorithms and source code	What remains owned by each party and what licence reaches the joint venture?	IP schedule, provenance, registration and licence scope
Manufacturing configuration	Plant-specific asset hierarchy, parameters, recipes and engineering rules	Who controls the configured twin and modifications created for the plant?	Configuration baseline, change history and acceptance record
Operating data	Sensor, event, quality, maintenance and production records	Who may collect, combine, export, retain and reuse the records?	Data inventory, classification, purpose and access matrix
Derived outputs	Features, simulations, model weights, alerts and optimisation recommendations	Does the joint venture own outputs or receive a limited use right?	Derivation logic, version record and permitted-use schedule
Local know-how	Work instructions, tuning practices, failure libraries and trained capability	What capability must remain in Saudi Arabia without continuing external intervention?	Competency matrix, witnessed tests and operating records
Improvements	New methods, code, models and inventions developed during the venture	How are improvements owned, licensed and commercialised?	Invention disclosure, contributor record and improvement policy

Each layer requires a defined owner, permitted use, accountable decision maker and exit treatment.

2. Distinguish the digital twin from its components

A digital twin is not one indivisible asset. The ISO 23247 series describes a manufacturing digital-twin framework that links observable manufacturing elements, data collection, device control, models and user applications [1-2]. In a transaction, the twin usually consists of several assets and services with different owners and restrictions. It may include mechanical and process models, control logic, equipment master data, interfaces, data pipelines, vendor software, cloud services, simulation tools, maintenance rules, operator judgement and evidence created after commissioning.

This distinction matters because delivery of one component does not establish operating independence. A joint venture may receive a plant model but lack the live interfaces needed to update it. It may receive executable software but not source code or rights to modify it. It may own site data but rely on a vendor-held ontology or calibration method. A trained local team may operate the system during normal production but remain unable to recover it after a major upgrade or cyber incident.

The transaction documents should therefore define the governed capability, not merely the platform name. The capability is the ability to maintain an authoritative plant representation, connect approved operating evidence, run agreed analyses, validate outputs, manage changes and recover service. Rights, people, systems and operating procedures must work together. The absence of one critical element can make another contribution economically stranded.

3. Establish the joint-venture thesis

The parties should state why a joint venture creates more value than a supply contract, licence, distribution arrangement, contract manufacturing relationship or wholly owned investment. The thesis may combine foreign process technology with Saudi capital, demand, local procurement, industrial land, utilities, customer relationships and workforce development. The digital twin can support the thesis by accelerating commissioning, transferring operating knowledge, improving asset reliability, validating local inputs and documenting process capability.

The thesis should identify the relevant operating decisions. These may include production scheduling, recipe approval, energy optimisation, quality release, predictive maintenance, debottlenecking and engineering change. Each decision requires a defined evidence chain and a named accountable owner. The parties should avoid claiming broad digital transformation when the investment case depends on a small number of high-value decisions.

Saudi Arabia's updated Investment Law identifies intellectual-property rights and contractual rights as forms of capital and protects investor rights, including intellectual property and trade secrets [3-4]. This supports a contribution architecture in which each party can identify and value the rights it makes available. The law does not by itself determine whether a particular licence, dataset or improvement is transferable, sufficient or economically valuable. The joint-venture agreement and supporting schedules must do that work.

4. Map the observable manufacturing perimeter

The digital-twin perimeter should begin with the physical production system. The parties should identify the plant, line, cell, machine, tool, utility, material flow, product family and quality stage represented by the twin. Each observable manufacturing element needs a persistent identity and relationship to drawings, bills of material, sensors, controls, work orders and operating limits. The map should distinguish equipment owned by the joint venture from leased assets, vendor-controlled systems and shared infrastructure.

The data perimeter should then identify every source used to initialise, calibrate, update or validate the twin. Typical sources include engineering design files, programmable-controller tags, historians, manufacturing execution systems, laboratory systems, maintenance systems, operator logs, energy meters, inspection records and original-equipment-manufacturer portals. For each source, the map should record ownership, legal control, security classification, location, retention, export capability, format, quality and dependency.

The model perimeter should identify the representations used for geometry, physics, process behaviour, controls, statistics and machine learning. A model may be reliable only within specified products, loads, ambient conditions or equipment configurations. The parties should record intended use, calibration evidence, validation population, limitations and change authority. A twin that lacks a controlled perimeter can produce plausible outputs that refer to an obsolete configuration or an operating state outside the validated range.

5. Build the rights architecture

The rights architecture should separate ownership from access, use, modification, commercialisation and control. Ownership may remain with a party while the joint venture receives a durable, paid-up licence for a defined field and territory. A licence can be exclusive or non-exclusive, transferable or personal, perpetual or time-limited, and capable or incapable of surviving termination. These dimensions should be negotiated independently.

The architecture should also distinguish background technology from foreground improvements. Background technology exists before the venture or is developed independently outside it. Foreground improvements arise through venture-funded work, plant operation or collaboration. A simple rule that all improvements belong to one party can create disputes when employees, contractors, operating data and pre-existing code contribute together. The agreement should define contribution records, invention disclosure, ownership tests, licence-backs and rights to general learning.

Source-code access requires particular care. Full assignment may be unnecessary if continuity can be protected through escrow, step-in rights, documented interfaces, local build capability and a licence that activates on defined events. Escrow alone is weak when the deposited code is incomplete, cannot be compiled or excludes required dependencies. A verification plan should test build instructions, third-party components, credentials, update cadence and release triggers.

6. Align the structure with Saudi investment and localisation policy

Saudi industrial policy emphasises economic diversification, local manufacturing, human-capital development and localisation of emerging technologies. The National Industrial Development and Logistics Program describes local-content objectives that include increasing the contribution of local manufacturers and service providers, developing human capital and attracting investment to localise new technologies [5]. These objectives create a reason to make localisation evidence part of the venture's economic and governance architecture.

Localisation should be defined through capabilities that the joint venture can demonstrate. Relevant measures may include Saudi engineering roles, approved local suppliers, local maintenance capability, domestic software or integration work, local ownership of plant-specific configurations, Arabic operating documentation and the ability to validate routine changes without external intervention. Procurement percentages can be important, but they do not by themselves prove technology transfer.

The Ministry of Investment's investor guidance identifies technology transfer and localisation among relevant investment considerations [6]. Incentive eligibility, procurement treatment and sector approvals can vary by project and authority. Transaction counsel and local-content specialists should confirm current requirements for the specific venture. The investment case should treat incentives as conditional until eligibility, measurement, evidence and timing are established.

7. Create a localisation capability scorecard

A useful scorecard measures whether the joint venture can perform defined tasks with decreasing dependence on the technology provider. Capability can be assessed across people, process, data, tooling, authority and evidence. The parties should identify the level required at each milestone and the evidence that an independent reviewer can inspect.

The scorecard should avoid equating attendance with competence. Training hours show exposure, not performance. A stronger test requires local personnel to complete a task using controlled procedures and evidence, under defined operating conditions and escalation rules. Examples include restoring a model from an approved baseline, adding an asset, validating a parameter change, investigating a quality deviation, executing a simulation and reconciling the result to plant evidence.

Table 2. Illustrative localisation capability scorecard

Capability	Initial state	Milestone test	Acceptance evidence	Governance consequence
Plant model administration	Provider-operated	Saudi team updates asset hierarchy and rolls back a change	Change ticket, validation report and recovery log	Routine administration delegated locally
Data engineering	Shared support	Local team connects and quality-checks an approved source	Lineage record, quality metrics and access approval	New approved sources can be onboarded locally
Model validation	Provider-led	Joint team validates a defined use case on local evidence	Test set, error analysis, limits and approval	Model release authority becomes shared
Maintenance analytics	Advisory use	Local engineers investigate alerts and close the evidence loop	Alert, inspection, action and outcome record	Routine decisions move to plant governance
Cyber recovery	Provider-dependent	Local team restores service from a clean baseline	Recovery exercise and security sign-off	Continuity step-in right becomes operational
Improvement development	Limited	Local team develops an approved plant-specific enhancement	Contributor record, code review and benefit evidence	Improvement ownership rule is applied

Milestones are accepted through witnessed performance and controlled evidence rather than document delivery alone.

8. Govern data classification and permitted use

Industrial data can contain several legal and commercial interests at once. A production event may reveal process know-how, customer demand, employee activity, equipment performance and supplier quality. The joint venture should classify data by sensitivity, owner or controller, permitted purpose, territory, retention and access role. Classification should travel with exports, backups and derived datasets.

The Saudi Data and AI Authority and the National Data Management Office publish national data-management and data-protection policies, including data classification, data sharing, data monetisation and personal-data rules [7]. The Saudi Personal Data Protection Law applies to processing within the Kingdom and can also reach processing of data relating to individuals residing in the Kingdom by parties outside it [8-9]. Employee identifiers, biometric access records, video, shift histories and detailed operator-performance records may therefore require specific handling even when the main purpose is industrial optimisation.

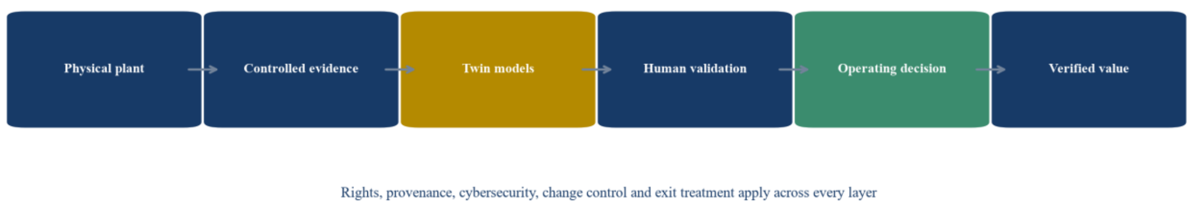
Permitted use should be described precisely. The technology provider may need access to diagnose faults and improve the licensed service. The joint venture may need the right to retain records, benchmark assets and continue local models after termination. The parties should define whether provider learning may be used for other customers, whether data must be aggregated or anonymised, and whether the joint venture receives benefits from global improvements. Cross-border transfers and remote support require a current legal and security assessment.

9. Use a controlled digital-twin architecture

The architecture should create a traceable path from the physical plant to the decision. ISO 23247 provides a manufacturing digital-twin framework with observable manufacturing elements, data-collection and device-control entities, core entities and user entities [1]. For a joint venture, the architecture should add transaction controls: rights metadata, provenance, version history, jurisdiction, approval state, access role and exit treatment.

The authoritative configuration should be identifiable at any time. Plant changes, software releases, sensor replacements and model updates can create divergence between the physical system and its virtual representation. The change process should show who proposed the change, what evidence supported it, which tests were run, who approved release and how the prior state can be restored. Safety and production controls should remain independent where appropriate.

Figure 1. Digital-twin joint-venture governance architecture



The architecture connects the physical plant, controlled evidence, models, human decisions and transaction rights.

10. Protect intellectual property and trade secrets

The intellectual-property schedule should identify patents, software, copyright works, databases, designs, confidential know-how, trademarks and contractual rights used by the venture. The Saudi Authority for Intellectual Property provides services and guidance for protecting, managing and licensing intellectual property, including registration of contractual patent-licensing arrangements [10-12]. The parties should confirm which rights require registration, recordal or other formalities and which depend on contractual confidentiality and practical secrecy controls.

Trade-secret protection depends on behaviour as well as drafting. Access should follow role, purpose and need. Repositories should separate venture-specific material from the provider's broader libraries. Download, export and administrative actions should be logged. Contractors should receive only the information required for their tasks and should return or destroy it at the end of access. Sensitive design and process information should not move through unmanaged collaboration tools.

The agreement should address reverse engineering, benchmarking, publication, patent filing, employee inventions and third-party claims. It should also define the response when plant data reveals an improvement to background technology. The parties may agree that the inventor owns the improvement while the joint venture receives a permanent plant-use licence, or that specified classes of plant-specific improvements belong to the venture. The rule should follow the economic bargain and remain workable after exit.

11. Design knowledge transfer as operating capability

Technology transfer becomes durable when the recipient can perform the required operating and engineering tasks. Documents and classroom sessions support that outcome but do not prove it. The plan should identify the decisions, tasks and failure situations that local teams must handle. It should define prerequisite skills, supervised practice, independent performance, assessment criteria, refresher requirements and escalation limits.

Tacit knowledge deserves explicit attention. Experienced engineers often recognise abnormal behaviour through context that is absent from a formal manual. The transfer plan can capture this knowledge through paired investigations, structured failure reviews, annotated operating cases, decision journals and witnessed shutdown or commissioning work. A failure library should record symptoms, conditions, diagnosis, action, outcome and lessons without turning one local event into a universal rule.

Retention also matters. A venture can meet a training milestone and lose the capability when key personnel leave. The operating model should identify critical roles, succession, minimum staffing, protected learning time and a method for maintaining competence. Incentives for the technology partner can be linked to capability outcomes that remain valid after a defined period, rather than completion of training inputs.

12. Control cross-border access and personal data

Remote support can improve speed and provide scarce expertise, but it changes the data and security perimeter. The joint venture should identify which users outside Saudi Arabia can access systems, which data are visible, whether sessions are recorded, where support logs are retained and whether files can be downloaded. Privileged access should be time-limited, approved, monitored and capable of rapid revocation.

The personal-data assessment should focus on identifiable people in industrial records. Maintenance work orders may name technicians. Video analytics may show employees. Access-control logs and shift records can reveal attendance and behaviour. The parties should establish a lawful purpose, limit collection, provide required information, manage retention and rights, and apply appropriate technical and organisational safeguards under the Saudi framework [8-9].

The operating-data assessment should also cover national data classifications, sector restrictions, customer confidentiality and critical-infrastructure requirements. A dataset that is not personal can still be highly sensitive. The data-sharing schedule should define approved purposes, recipients, environments, aggregation and return or destruction. Any proposed secondary use for product development, global model training or commercial benchmarking should have a separate approval path.

13. Secure operational technology

The Saudi National Cybersecurity Authority's Operational Technology Cybersecurity Controls establish minimum cybersecurity requirements for industrial control systems and extend the Essential Cybersecurity Controls [13-14]. The controls include governance, risk management, asset management, identity, access, network protection, vulnerability management, incident response, business continuity and third-party requirements. A digital-twin architecture that connects operating technology to enterprise or remote environments should be assessed against the applicable control set.

The transaction should identify every new connection, service account, gateway, historian interface, cloud component and remote-support path. It should record data direction, protocol, authentication, encryption, logging and failure behaviour. The architecture should preserve safe local operation when analytics or remote services are unavailable. Models and recommendations should not bypass established safety interlocks or authorised control procedures.

Cybersecurity responsibilities should be reflected in the joint-venture governance model. The technology provider may control software development and vulnerability remediation. The joint venture may control plant networks and identities. A managed-service provider may operate monitoring. The agreement should allocate patching, incident notice, evidence preservation, recovery, regulatory engagement, audit and cost. Shared responsibility should not become unassigned responsibility.

14. Govern models and human accountability

A model can support a decision without owning it. The joint venture should assign accountable people for model approval, engineering interpretation, operating action and financial recognition. Model documentation should state intended use, prohibited use, inputs, assumptions, training or calibration population, performance measures, limitations, monitoring and override procedures.

The OECD AI Principles emphasise human-centred values, transparency, traceability, robustness and accountability across the AI lifecycle [15]. These principles are relevant when a twin incorporates predictive models, optimisation or generative interfaces. The parties should retain sufficient records to reconstruct important outputs and subsequent decisions. They should also provide a safe method to override, repair or withdraw a model that behaves outside expectations.

Joint ownership of a model does not automatically create joint accountability. The governance schedule should identify who can propose, validate and approve changes. A provider should not be able to push a material update into production without plant approval. A local team should not be able to alter safety-relevant parameters outside the validated process. Independent challenge is useful for high-consequence use cases and for disputes over whether a milestone has been met.

15. Align joint control and digital decision rights

IFRS 11 defines joint control as the contractually agreed sharing of control when decisions about relevant activities require unanimous consent of the parties sharing control [16]. The accounting classification depends on rights and obligations and may differ between a joint operation and a joint venture. The transaction team should obtain accounting advice on the actual arrangement. The digital-governance design should be consistent with the commercial decision rights rather than creating hidden control through technical dependency.

Relevant activities can include approval of annual budgets, production plans, major technology changes, licensing outside the field, material data sharing, cybersecurity architecture and appointment of key executives. Some digital-twin decisions may affect returns significantly. If one party can unilaterally withhold access, disable the service or prevent a required update, technical rights can influence control even when the constitutional documents appear balanced.

The parties should map corporate reserved matters to system privileges and operating procedures. A unanimous board decision should not be undermined by an administrator who can implement the opposite result. Likewise, routine plant decisions should not require board consent merely because the technology platform is material. Delegations, limits and escalation thresholds should allow efficient operation while protecting the core bargain.

Table 3. Digital-twin joint-venture decision-rights matrix

Decision	Proposer	Independent challenge	Approver	Required record
Background-technology release	Technology partner	IP and security review	Joint-venture board under reserved matters	Licence schedule, provenance and dependency assessment
Plant-specific configuration	Joint engineering team	Process-safety and quality review	Joint-venture technical director	Change request, tests and rollback plan

Decision	Proposer	Independent challenge	Approver	Required record
New data source or cross-border access	Data owner	Privacy and cybersecurity review	Data-governance committee	Purpose, classification, lineage and access decision
Model release	Model owner	Independent validation	Engineering and AI governance owner	Test report, limitations and monitoring plan
Operating action	Plant function	Discipline specialist where required	Authorised plant manager	Evidence, decision, action and outcome
External commercialisation	Rights owner	Competition, IP and valuation review	Joint-venture board under reserved matters	Market scope, licence economics and conflict assessment

Corporate authority, technical privilege and operating accountability should point to the same decision owner.

16. Select the valuation approach

The value of the digital-twin contribution depends on the rights and capabilities transferred. A relief-from-royalty approach can estimate the present value of avoided licence payments for a legally protectable technology right. A cost approach can estimate the cost to recreate documented software, models, data preparation and engineering knowledge, adjusted for obsolescence and economic utility. An incremental cash-flow approach can estimate buyer-specific operating benefits after implementation, recurring cost, ramp time and risk.

The methods answer different questions. Replacement cost does not prove that the capability will produce cash benefits. A royalty benchmark may not reflect the restricted field, territory, exclusivity or dependence in the actual venture. Incremental cash flow can capture operating value but is sensitive to the baseline, attribution and execution assumptions. A robust analysis uses the method appropriate to the right being valued and reconciles differences.

Accounting recognition should remain separate from transaction value. IAS 38 defines an intangible asset through identifiability and requires probable future economic benefits and reliable measurement for recognition [17]. A contractually protected licence may be recognisable while a broader operating capability is not a separate accounting asset. Conversely, a joint venture can derive economic value from integrated know-how and data even when no separate asset appears on the balance sheet. Accounting specialists should assess the specific facts.

17. Build the operating baseline

The valuation should begin with expected performance without the digital-twin contribution or incremental localisation programme. The baseline should cover availability, throughput, yield, energy, maintenance cost, spare-parts use, quality loss and service risk. It should reflect the planned plant design and operating ramp, not a mature benchmark imported from another country or factory.

The evidence should separate technical loss from commercial loss. A production interruption has economic value only when it constrains saleable output, causes incremental cost or changes customer outcomes. Spare labour or inventory may absorb some events. A quality improvement may reduce scrap, rework, claims or lost contribution, but these effects should not be counted several times. Energy benefit should be measured against production mix and operating conditions.

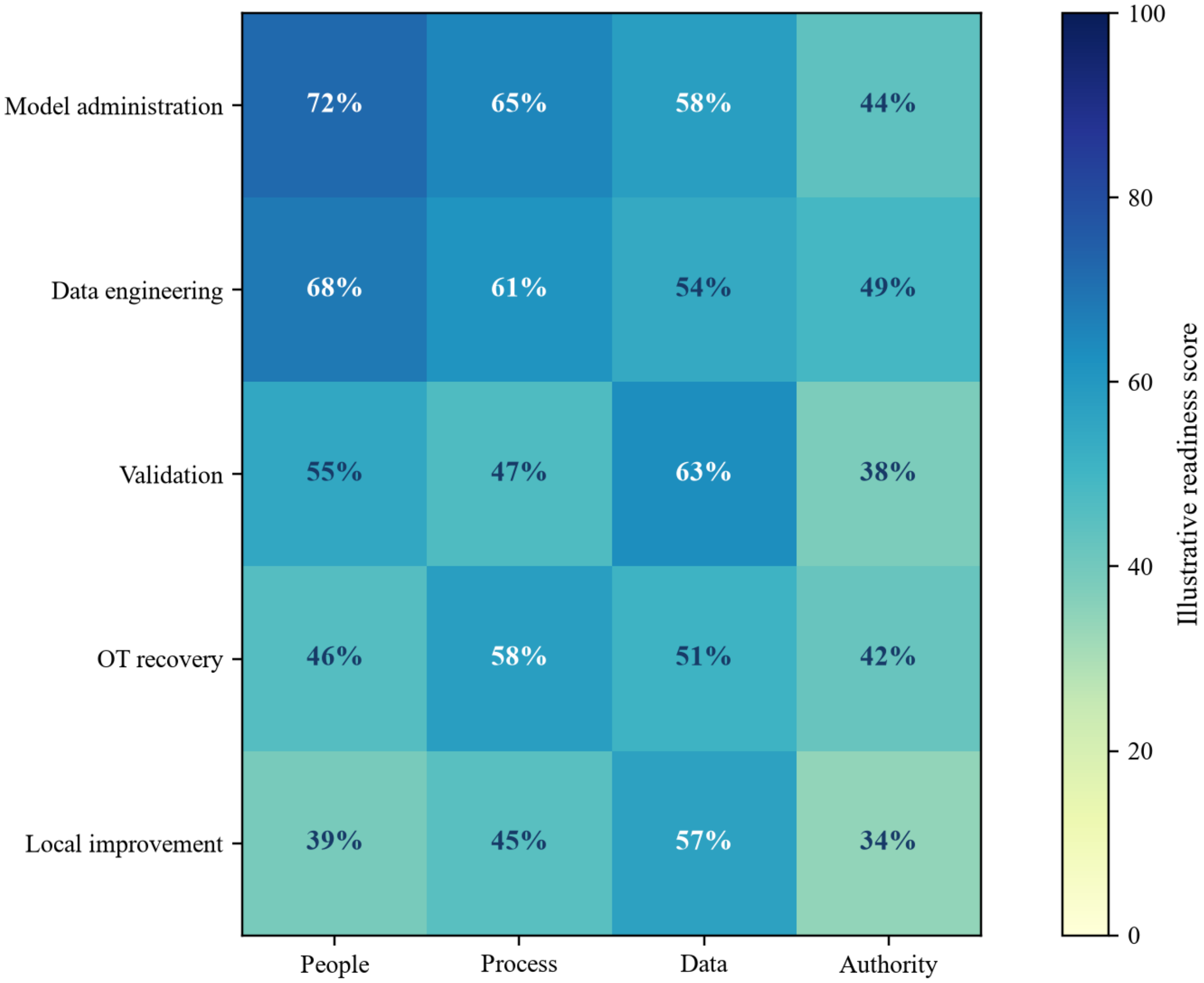
The baseline should also show what existing systems and people would achieve. A digital twin may accelerate diagnosis but not replace sound maintenance, process control or competent engineering. Benefits created by the broader factory ramp should not be attributed to the twin. Finance, engineering and operations should agree the evidence ledger before benefits are included in the investment case.

18. Link milestones to contribution value

Contribution value should vest as the joint venture receives usable rights and capability. A single contribution value at signing can overstate delivery when material elements depend on later integration, training or validation. Staged recognition can link value, royalties, equity credit, earn-out or other economics to defined milestones.

Milestones should be objective enough to test. Examples include delivery of an approved configuration baseline, verified data interfaces, successful recovery, local administration, validated use cases and sustained performance over an agreed period. A milestone should identify the acceptance authority, evidence, cure period and consequence of failure. It should also distinguish a provider delay from a plant-access or data-quality delay controlled by the joint venture.

Figure 2. Illustrative localisation-readiness heat map



Management-assumed readiness scores identify capabilities that require evidence before economic value can vest.

19. Demonstrate the hypothetical case

The illustrative transaction forms a Saudi manufacturing joint venture between a foreign industrial-technology provider and a Saudi operating partner. Management assumes total project capital expenditure of SAR 620 million and 140 critical manufacturing assets. The technology contribution includes a plant-specific digital-twin configuration, process-model access, interfaces, validation support and a structured knowledge-transfer programme. The Saudi partner contributes local execution capability, industrial infrastructure, workforce development, procurement relationships and market access.

Management assumes the programme creates four steady-state gross benefits: SAR 9.2 million from availability and throughput, SAR 5.6 million from yield and quality, SAR 3.4 million from energy optimisation and SAR 4.1 million from maintenance and spares. Gross recurring benefit is therefore SAR 22.3 million. Recurring software, support, data-engineering, security and validation cost is SAR 6.2 million, producing a net recurring benefit of SAR 16.1 million.

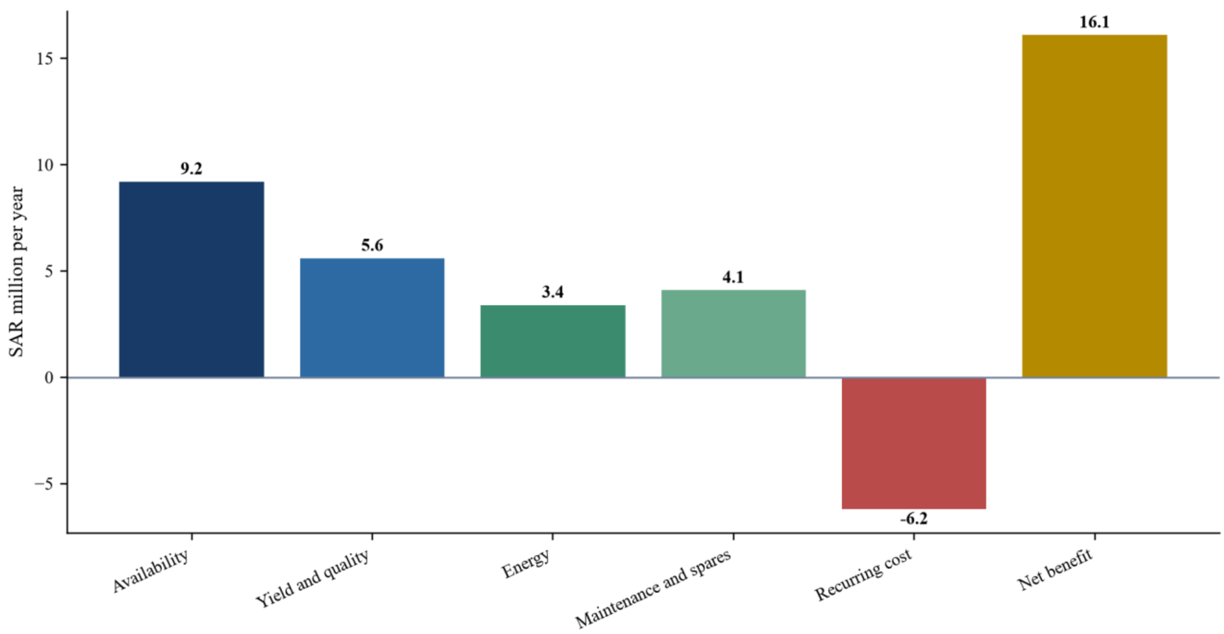
Initial programme investment is assumed at SAR 18 million on completion, with a further SAR 7 million in the first year. Net operating benefit is assumed at SAR 3.2 million in year one, SAR 9.7 million in year two and SAR 16.1 million in each of years three to five. A management-assumed fourteen-percent discount rate produces an illustrative five-year net present value of approximately SAR 14.9 million. The model excludes terminal value, tax, financing, working capital, transfer pricing, grant or incentive value, purchase-price allocation and negotiated sharing between the parties.

Table 4. Hypothetical digital-twin contribution valuation case

Item	Timing	Management assumption	Valuation treatment
Initial digital-twin enablement	Completion	18.0	Initial cash outflow
Additional integration and localisation	Year 1	7.0	Year-one cash outflow
Net operating benefit	Year 1	3.2	Discounted inflow
Net operating benefit	Year 2	9.7	Discounted inflow
Net operating benefit	Year 3	16.1	Discounted inflow
Net operating benefit	Year 4	16.1	Discounted inflow
Net operating benefit	Year 5	16.1	Discounted inflow
Illustrative discount rate	Five-year model	14 percent	Management assumption
Illustrative net present value	Five-year model	14.9	Capability value before excluded items

All figures are management assumptions in SAR millions and demonstrate the framework only.

Figure 3. Hypothetical steady-state annual benefit bridge



Management assumptions show how operating benefits become a recurring net benefit after programme cost.

20. Allocate economics without double counting

The valuation should distinguish the value of licensed technology, plant-specific configuration, knowledge transfer and future services. A royalty can compensate ongoing use of background technology. A contribution value can recognise rights committed at formation. Service fees can compensate continuing support. Milestone payments can reward completed localisation. Using all four mechanisms without reconciliation can charge the joint venture several times for the same economic benefit.

The parties should maintain a value bridge from each payment to a defined right or service. The bridge should show whether the consideration is fixed, usage-based, performance-linked or cost-plus. It should identify related-party pricing, withholding, tax and accounting implications for specialist advice. It should also show the effect of termination and step-in rights.

The operating-benefit model should avoid double counting. Availability and throughput may describe the same recovered production. Yield improvement and lower material cost can overlap. Reduced emergency maintenance may lower overtime and contractors without reducing salaried headcount. Energy benefit may partly arise from a separate equipment upgrade. Each benefit should appear once, with a baseline, owner, evidence source and attribution rule.

21. Design reserved matters and delegations

Reserved matters should protect decisions that can alter the venture's strategic rights, risk or value. Digital-twin reserved matters may include assignment or material amendment of core licences, use outside the agreed field, export of sensitive data, changes to cybersecurity architecture, external commercialisation, disposal of source code, abandonment of a material model and approval of large related-party technology contracts.

Routine operations require delegation. A plant should be able to replace an approved sensor, correct a mapping, tune a model within validated bounds and perform ordinary maintenance without repeated board approval. Delegations should specify thresholds, accountable roles, evidence and reporting. The technology partner may retain consent for changes that expose background intellectual property, while the plant retains authority over safety and production.

System privileges should follow the governance map. Administrative rights, signing keys, deployment pipelines and model registries can create practical control. The venture should maintain dual control for sensitive actions, emergency procedures for continuity and periodic review of access. A constitutional veto has limited value if one party can disable operations through an unmanaged technical dependency.

22. Prepare for deadlock and continuity

Digital-twin disputes can stop production or delay localisation. The agreement should define escalation paths for disagreements over model release, data access, milestone acceptance, security remediation, licence fees and improvements. A technical dispute may require an independent expert with the right discipline and access to the underlying evidence. A commercial deadlock may require executive escalation, mediation, buy-sell mechanisms or another agreed remedy.

Continuity measures should operate while the dispute is resolved. The joint venture may need a right to continue the last approved version, obtain critical support, access escrow materials or appoint an alternate provider. The technology partner may need protection against unauthorised copying, non-payment or use beyond scope. Interim rights should be limited to preserving safe operation and should not determine the final merits.

The deadlock matrix should distinguish safety-critical issues from commercial disputes. Safety, cybersecurity and legal compliance should have immediate protective procedures. A pricing disagreement should not automatically permit a shutdown. The agreement should also address what happens when a regulator, customer or insurer requires a change that one party has not anticipated.

23. Build transaction protections around evidence

Representations and warranties should address ownership or authority, disclosed third-party components, infringement claims, licences, material interfaces, cybersecurity incidents, data provenance, export capability and compliance with agreed development practices. They should be tailored to the actual contribution. A broad statement that the technology is fit for purpose may create uncertainty when intended uses and plant conditions are undefined.

Conditions precedent can require delivery of agreed licences, approvals, baseline documentation, data inventories, security assessments and escrow arrangements. Milestone conditions can govern staged contribution value or payments. Indemnities may address specific known risks such as a third-party licence gap or undisclosed infringement claim. Caps, exclusions, survival and remedies should reflect the negotiated risk allocation and local legal advice.

Acceptance testing should reproduce critical tasks. The joint venture should test installation, interfaces, model outputs, failure recovery, access controls and documentation. Performance tests should use agreed conditions and tolerances. A test that proves functionality on sample data does not establish plant performance. The acceptance record should distinguish software delivery from operating benefit, which requires evidence over time.

24. Protect competition and clean-team boundaries

Joint ventures can involve competitors, suppliers or customers sharing sensitive information. The Saudi General Authority for Competition's Economic Concentration Review Guidelines explain that merger-control provisions can apply to arrangements that transfer ownership, rights or decisive influence, including joint management [18]. The parties should obtain current competition advice on filing thresholds, control and information exchange.

Before approval and closing, clean-team controls can limit access to competitively sensitive information. Production costs, customer demand, pricing, future capacity, bids and strategic plans may require aggregation or specialist review. Technical diligence should receive the information needed to assess the digital twin without giving operating teams unnecessary visibility into competitive strategy.

Post-close information sharing should remain tied to the venture's purpose. A parent should not automatically receive detailed data that could influence competition outside the joint venture. The data-governance schedule should identify legitimate recipients, aggregation, delay and purpose. External commercialisation of combined models or benchmarks may require additional competition and confidentiality review.

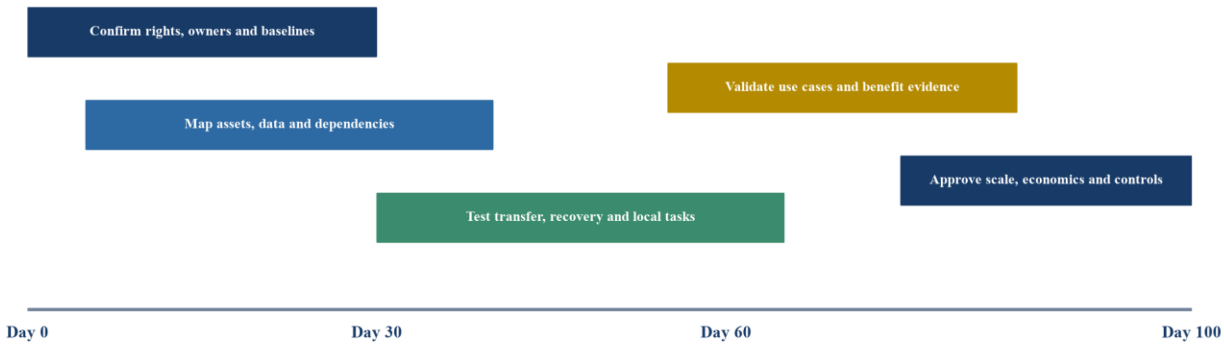
25. Execute the first hundred days

The first thirty days should preserve evidence and establish authority. The venture confirms licence schedules, IP provenance, data classifications, system owners, privileged access, approved baselines, security responsibilities and milestone evidence. It freezes undocumented changes to critical models and interfaces while allowing safe production. It also confirms training cohorts and the initial capability assessment.

Days thirty-one to sixty should establish controlled transfer. The team maps observable manufacturing elements, confirms data lineage, tests interfaces, validates recovery materials and runs the first witnessed capability tasks. It closes critical security gaps and identifies any third-party rights that prevent intended use. Finance establishes the operating-benefit baseline and evidence ledger.

Days sixty-one to one hundred should release limited use cases through the approved governance process. The venture validates outputs on local evidence, tests human review and rollback, measures early operating effects and records exceptions. The board receives a rights, capability, security and value report. Further economic credit or rollout depends on the evidence gates agreed in the transaction.

Figure 4. First hundred day digital-twin governance roadmap



The roadmap moves from rights and evidence preservation to controlled transfer, local validation and board-approved scaling.

26. Govern exit, termination and change of control

Exit should be designed when the rights architecture is agreed. A joint venture may end through sale, listing, partner buyout, insolvency, expiry or termination for breach. The continuing business needs clarity on plant data, configured models, interfaces, documentation, source code, licences, trained capability and support. The technology provider needs protection against use beyond the surviving scope.

The agreement should define licences that survive each exit path. A buyer of the joint venture may need consent or may inherit defined rights. A competing buyer may create legitimate restrictions. A technology-provider change of control may introduce a competitor, sanctions issue or security concern. Step-in, escrow or transition rights can protect continuity while the parties implement the agreed remedy.

Data exit should include format, metadata, lineage, credentials, derived outputs, retention and verified deletion. The joint venture should be able to reconstruct the last approved configuration and continue agreed operations. The provider should be able to separate its background technology and confidential information without deleting venture-owned records. A tested exit rehearsal is stronger evidence than a contractual promise that has never been operationalised.

27. Recognise limitations

The framework cannot determine the legal effect of a specific Saudi joint-venture agreement, licence, data transfer or intellectual-property arrangement. Applicable requirements depend on the parties, sector, data, technology, transaction structure and current law. Saudi legal, tax, accounting, competition, intellectual-property, cybersecurity and sector specialists should review the actual arrangement.

Digital-twin performance is context-dependent. A model validated on another plant may not transfer to local equipment, materials, climate, workforce, suppliers or operating practices. Documentation can be incomplete. Source code can depend on undisclosed libraries or services. Data may be biased toward stable operation and contain too few abnormal events. Cybersecurity or safety constraints can limit connectivity and automation.

The hypothetical case uses management assumptions and excludes terminal value, tax, financing, working capital, transfer pricing, grants, incentives and negotiated value sharing. It does not predict the value of any project. Commercial demand for a particular structure remains unverified until supported by project-specific evidence and agreed transaction terms.

28. Draw the investment conclusion

A digital twin supports technology transfer and localisation when the joint venture receives a governed operating capability. The capability combines durable rights, plant-specific configuration, controlled data, validated models, trained people, change authority, cybersecurity, continuity and evidence of economic effect. Delivery of software or documents alone does not establish that result.

The investment case should define high-value decisions, map every component and dependency, separate background technology from venture improvements, and make localisation milestones independently testable. Reserved matters, technical privileges and operating delegations should align. Valuation should follow the rights actually transferred and use incremental cash flow after implementation, recurring cost, ramp time and risk.

The strongest transaction structure links economics to evidence. It rewards the technology provider for valuable rights and successful transfer, gives the Saudi operating venture the capability required for resilient local operation, and preserves accountability for safety, security and investment decisions. The resulting governance system can convert localisation from an aspiration into a measurable operating asset.

Frequently asked questions

What should a Saudi industrial joint venture own in the digital twin?

The answer depends on the commercial bargain. The venture commonly needs ownership or durable rights over plant-specific configurations, operating data, documentation and locally developed improvements, while the technology provider retains background intellectual property under a defined licence.

Is software access sufficient evidence of technology transfer?

No. The venture also needs controlled data, interfaces, documentation, trained people, validation capability, change authority and continuity arrangements for the agreed operating decisions.

How should localisation milestones be tested?

Use witnessed performance against defined tasks, conditions and evidence. Training attendance and document delivery can support a milestone but do not prove independent capability.

Who should own improvements created during the joint venture?

The agreement should define ownership by improvement type, contributors and use. A common structure preserves the inventor's ownership while granting the venture a durable plant-use licence, or assigns specified plant-specific improvements to the venture.

How should cross-border remote support be governed?

Define approved users, purposes, data classes, environments, session controls, downloads, logs, retention and incident duties. Confirm current Saudi data-protection, cybersecurity and sector requirements for the specific access.

Can the digital-twin contribution be valued through a royalty?

A relief-from-royalty method may suit a protectable licensed right. Plant-specific operating value may require incremental cash-flow analysis, while some documented capability may also be tested through replacement cost. The methods should be reconciled without double counting.

What happens if the parties disagree over model release?

The agreement should provide technical escalation, independent expert review where appropriate and interim continuity using the last approved safe version. Safety and cybersecurity procedures should remain immediately enforceable.

What should survive termination or a sale of the venture?

The documents should specify surviving plant-use licences, data rights, model and configuration access, escrow or step-in rights, transition support, retention, deletion and the treatment of improvements for each exit path.

References

[1] International Organization for Standardization, ISO 23247-1:2021 Automation systems and integration: Digital twin framework for manufacturing, Part 1 https://www.iso.org/standard/75066.html

[2] International Organization for Standardization, ISO 23247-5 Digital thread for digital twin, online browsing platform https://www.iso.org/obp/ui?_escaped_fragment_=iso%3Astd%3Aiso%3A23247%3A-5%3Adis%3Aed-1%3Av1%3Aen

[3] Ministry of Investment of Saudi Arabia, Updated Investment Law https://misa.gov.sa/activities/laws-regulations-copy/

[4] Ministry of Investment of Saudi Arabia, Investment Law https://misa.gov.sa/app/uploads/2025/07/Investment-Law.pdf

[5] Saudi Vision 2030, National Industrial Development and Logistics Program Annual Report 2022 https://www.vision2030.gov.sa/media/l2ulgrxt/ndlp-report-2022-english.pdf

[6] Ministry of Investment of Saudi Arabia, Investor Guide https://misa.gov.sa/app/uploads/2025/05/Investor-Guide-12-03en.pdf

[7] Saudi Data and AI Authority, Laws and Regulations https://sdaia.gov.sa/en/SDAIA/about/Pages/RegulationsAndPolicies.aspx

[8] Saudi Data and AI Authority, Personal Data Protection Law https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/PDPL/

[9] Saudi Data and AI Authority, Guide to the Saudi Personal Data Protection Law for Controllers and Processors https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/PDPLCP/

[10] Saudi Authority for Intellectual Property, Main services and institutional role https://www.saip.gov.sa/en

[11] Saudi Authority for Intellectual Property, Resources and licensing information https://saip.gov.sa/en/resources

[12] Saudi Authority for Intellectual Property, Contractual patent-licensing agreement service https://www.saip.gov.sa/ar/services/patents/patent15

[13] National Cybersecurity Authority, Operational Technology Cybersecurity Controls https://nca.gov.sa/en/regulatory-documents/controls-list/otcc/

[14] National Cybersecurity Authority, Operational Technology Cybersecurity Controls OTCC-1:2022 https://nca.gov.sa/otcc_en.pdf

[15] Organisation for Economic Co-operation and Development, OECD AI Principles https://www.oecd.org/en/topics/ai-principles.html

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

[17] IFRS Foundation, IAS 38 Intangible Assets https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/

[18] General Authority for Competition, Economic Concentration Review Guidelines https://gacbep.gac.gov.sa/cms/b9376edc-79a1-4573-a36d-4f3effaba838.pdf

[19] Ministry of Investment of Saudi Arabia, Investment Law Implementing Regulations 2025 https://misa.gov.sa/app/uploads/2025/06/THE-INVESTMENT-LAW-IMPLEMENTING-REGULATIONS.pdf

[20] National Cybersecurity Authority, Cybersecurity Toolkits https://nca.gov.sa/en/regulatory-documents/guidelines-list/cybersecurity-toolkits/

[21] Saudi Data and AI Authority, National Data Governance Platform https://dgp.sdaia.gov.sa/wps/portal/pdp/home/

[22] Saudi Authority for Intellectual Property, IP Licensing https://www.saip.gov.sa/en/services/ip-licensing

[23] IFRS Foundation, IFRS 11 supporting material https://www.ifrs.org/supporting-implementation/supporting-materials-by-ifrs-standards/ifrs-11/

[24] International Organization for Standardization, ISO/TR 23247-101:2026 manufacturing digital-twin use case https://www.iso.org/obp/ui?_escaped_fragment_=iso%3Astd%3Aiso%3Atr%3A23247%3A-101%3Aed-1%3Av1%3Aen

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.