Who Owns the Plant Data? Value-Sharing in India-GCC Industrial AI JVs

A governance, intellectual-property and economics framework for cross-border industrial AI partnerships

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Industrial AI joint ventures between Indian technology and engineering businesses and Gulf Cooperation Council industrial operators can combine plant access, process knowledge, software capability and regional distribution. Their economics depend on a question that conventional ownership clauses often leave unresolved: who may use which plant-derived information, for what purpose, in which environment and after the relationship ends? Raw sensor readings, contextualised operating records, engineered features, model parameters, synthetic data, operator feedback and validated savings have different legal, technical and commercial characteristics. Treating all of them as one asset called data creates avoidable disputes and weakens the investment case.

This paper develops a Plant Data Value-Sharing Framework for India-GCC industrial AI joint ventures. It replaces a single ownership debate with a governed bundle of rights covering access, control, permitted use, model improvement, disclosure, localisation, security, audit, portability and exit. The framework connects those rights to the industrial asset graph, the source-of-truth hierarchy, application readiness, validated outcomes and joint-venture economics. It also addresses personal-data rules, confidential process knowledge, operational-technology security, foreground and background intellectual property, competition constraints, accounting, valuation, deadlock and termination.

A wholly hypothetical case covers 20 industrial sites, 58 production units and 96 proposed AI applications. Management assumes USD 18.0 million of annual customer benefit and USD 7.2 million of joint-venture revenue and synergy. Evidence gates reduce the application population from 96 proposed cases to 61 deployed and validated cases. After baseline, attribution, persistence and cash-conversion adjustments, the framework retains USD 9.2 million of customer benefit and USD 3.1 million of joint-venture revenue and synergy. Every figure is an illustrative management assumption created to demonstrate the method. It is not observed company data, a market benchmark, a forecast or a valuation opinion.

The evidence base includes official India-UAE industrial cooperation and trade instruments; data-protection and cross-border-transfer rules in India, the United Arab Emirates and Saudi Arabia; ISO standards for manufacturing digital twins, asset management and AI management systems; IEC 62443 and NIST operational-technology guidance; ISA-95 and OPC UA interoperability frameworks; IFRS requirements for joint arrangements, intangible assets, revenue and fair value; and current competition regimes. The conclusion is that industrial data creates durable joint-venture value when the parties

define an auditable chain from physical asset and authorised data use to validated operating outcome and distributable cash.

JEL Classification: G32, G34, L23, L60, M15, O31, O32

Keywords: industrial AI, joint ventures, India, GCC, plant data, intellectual property, digital twins, value sharing, operational technology

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 JOINT-VENTURE DECISION

The governing decision is how an Indian technology or engineering partner and a GCC industrial partner should allocate rights, obligations and economics when plant data is used to develop and deploy industrial AI. The answer affects contribution valuation, governance, exclusivity, regulatory compliance, delivery capacity, customer trust and exit value. A clause stating that one party owns the data rarely resolves the operating questions that determine cash flow.

The joint venture should identify the asset, decision and benefit attached to each application. A predictive-maintenance model may use vibration data from customer-owned equipment, engineering features created by the technology partner, failure labels verified by plant staff and a model trained across several sites. Each layer can carry a different right and restriction. The transaction model should therefore price a documented rights stack rather than an undefined data pool.

The framework tests six propositions. The data population is identifiable. Source authority and provenance are reliable. Permitted purposes and transfer routes are lawful. Background and foreground intellectual property are allocated. Operating outcomes are independently validated. Value sharing follows those outcomes without transferring unsafe plant authority. Failure at any layer reduces the scope, timing or certainty of value.

Table 1. Plant-data rights stack for joint-venture diligence

Right	Diligence question	Minimum evidence	Economic consequence
Access	Who can retrieve the record and through which interface?	Access matrix and technical architecture	Defines feasible application scope
Control	Who can approve, correct, suspend or delete use?	Authority and escalation record	Protects plant accountability
Use	Which operational, training and commercial purposes are allowed?	Purpose schedule and consent basis	Defines addressable value
Improvement	Can derived features or parameters improve other deployments?	Model-rights schedule	Determines scalability
Disclosure	Which affiliates, vendors and customers may receive outputs?	Recipient and confidentiality map	Constrains delivery model
Portability	What can each party retain or export at exit?	Exit package and format standard	Supports continuity and terminal value

Each right should be defined by data class, site, purpose, territory, duration and exit treatment.

2. DEFINE THE PLANT DATA POPULATION

The data population begins with sites, units, equipment, instruments, control loops, historians, maintenance systems, laboratory records, operating procedures, alarms, work orders, production accounts and financial outcomes. The joint venture should link these elements to a common asset hierarchy. Connected-tag counts alone do not establish that records are accurate, contextualised or available for the proposed purpose.

The parties should distinguish raw observations from contextualised records. A pressure tag becomes more useful when linked to equipment identity, engineering units, calibration state, operating mode and maintenance history. That context may embody the operator's confidential process knowledge or the engineering partner's taxonomy. Rights should follow the contribution that created each layer.

The population register also needs exclusions. Safety-system records, employee information, export-controlled designs, third-party licensed datasets and customer-confidential recipes may require separate handling or prohibition. A defined exclusion does not destroy value. It gives the joint venture a reliable boundary within which applications can be developed, financed and sold.

3. CLASSIFY DATA BEFORE ALLOCATING RIGHTS

Classification should precede ownership language. A practical taxonomy includes public information, ordinary business data, confidential commercial data, personal data, plant-operating data, safety-critical data, engineering intellectual property, customer data and regulated information. The same record can change classification when combined with other records. Equipment output may reveal proprietary throughput or production economics after contextualisation.

The register should record origin, custodian, sensitivity, residency, contractual restrictions, retention, permitted processing and authorised recipients. It should also identify whether a record is observed, manually entered, calculated, inferred or generated by a model. This distinction matters because a predicted failure probability is not the same asset as the underlying vibration signal.

Classification drives controls and economics. Broad reusable rights can support platform value. Narrow site-specific rights support only contracted delivery. Restricted safety or personal data may require local processing and limited retention. The valuation should therefore apply different probabilities, margins and useful lives to different data classes rather than capitalising a single undifferentiated asset.

4. BUILD THE INDUSTRIAL ASSET GRAPH

An industrial asset graph connects legal entity, site, unit, equipment, component, sensor, work order, operating event, model, recommendation and economic outcome. It provides the structure needed to answer which physical asset generated the record, who operated it, what model used it and which cash-flow claim followed. Without that chain, portfolio-level benefit claims are difficult to reproduce.

The graph should use stable identifiers and versioned relationships. Equipment may be renamed, replaced or transferred between units. Sensors can be recalibrated or mapped to new tags. Models

can change features and objectives. A durable graph preserves history while showing the current state, which supports audit, cyber response, model monitoring and dispute resolution.

The graph also exposes contribution. The GCC operator may contribute physical access, operating context and validated outcomes. The Indian partner may contribute engineering ontology, connectors, algorithms and delivery staff. The joint venture may create deployment templates and cross-site benchmarks. Mapping those contributions provides a reasoned basis for licensing, transfer pricing and value sharing.

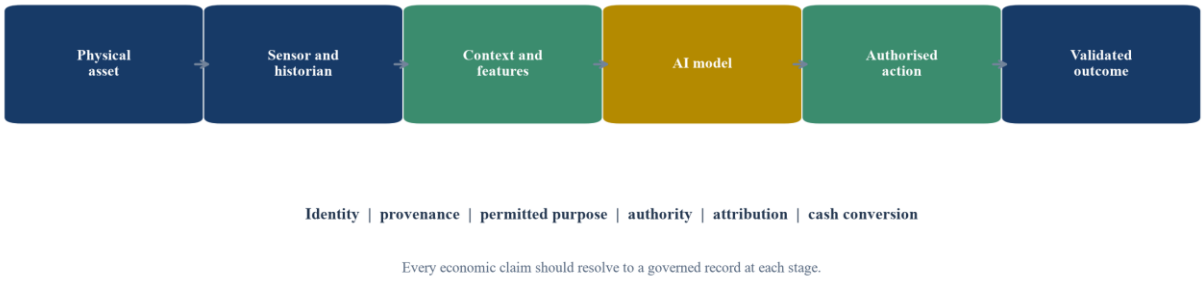

Figure 1. Industrial asset graph and rights lineage

Rights and economics can be traced from the physical asset to the validated outcome.

5. IDENTIFY SOURCE AUTHORITY

The parties should establish a source-of-truth hierarchy for each material field. A historian may be authoritative for timestamped process values, while a maintenance system governs work completion and an enterprise resource planning system governs invoiced production. Model outputs, spreadsheets and dashboards should not silently replace those records.

Source authority includes correction rights. A plant engineer may correct an equipment mapping. Finance may approve a savings baseline. The joint venture may correct a feature pipeline while preserving the original observation. Every correction should retain the previous value, reason, approver and effective time. This protects reproducibility and reduces disputes about whether a reported benefit arose from the model or from revised accounting.

Data quality should be measured against the intended decision. Missing temperature readings may be tolerable for a monthly reporting model and unacceptable for real-time control. The service level should specify completeness, timeliness, calibration and context requirements by application. The party controlling the deficient source should own the remediation obligation or the economics should adjust accordingly.

6. SEPARATE ACCESS FROM OWNERSHIP

Ownership is only one element of the rights stack. A plant operator can retain ownership while granting the joint venture controlled access for defined purposes. A technology partner can retain its software while granting the joint venture deployment rights. The joint venture can own new

implementation assets while each parent receives limited use rights. These combinations are more precise than a forced transfer of every input and output.

Access should be granted through named systems, identities, zones and interfaces. The agreement should identify whether data may be viewed, copied, transformed, aggregated, exported or used to train a model. It should state whether access is continuous, event-based or subject to plant approval. Technical controls should reflect the negotiated scope.

Economic rights can also be separated. A parent may receive a royalty for background technology, the joint venture may earn service revenue and the industrial customer may retain most validated operating savings. The value-sharing formula should compensate actual contributions and risks without using ownership as an indirect substitute for pricing.

7. DEFINE PERMITTED PURPOSES

Purpose schedules should describe the decisions the data may support. Examples include monitoring, maintenance planning, energy optimisation, quality prediction, operator assistance, model validation and product improvement. A broad phrase such as business purposes gives limited protection to either party and can conflict with customer contracts or data-protection principles.

Each purpose should name the legal entity, site, application, data class, processing location, recipient, duration and retention rule. Secondary use for benchmarking or cross-customer training needs an explicit basis. Aggregation and anonymisation can reduce exposure, although the parties should test whether sensitive operating patterns remain identifiable.

Purpose changes require governance. A model developed for maintenance should not be reused for employee performance scoring or autonomous control without new review. The reserved-matters schedule should identify which changes management can approve and which require parent or customer consent. The technical platform should block unapproved uses and preserve an audit record.

8. SET THE PERSONAL DATA PERIMETER

Industrial datasets can contain employee identifiers, access logs, shift patterns, video, voice, maintenance notes and user activity. India's Digital Personal Data Protection Act 2023 and the Digital Personal Data Protection Rules 2025 establish obligations for digital personal data in their respective scope [4][5]. The UAE personal-data law regulates processing and cross-border transfer [6]. Saudi Arabia's Personal Data Protection Law and transfer regulation apply where relevant [7].

The joint venture should minimise personal data at ingestion, separate identity from equipment events and document its lawful basis, notices, processors, retention and rights-handling procedures. Local counsel should confirm the applicable rules for each deployment. A contractual statement that the dataset is industrial does not remove personal-data obligations when identifiable people remain present.

Personal data should not become an unpriced platform asset. Where model development does not require identity, tokenisation or aggregation can reduce risk. Where operator identity is necessary for

safety or competence controls, access should remain limited and purpose-bound. The transaction model should include compliance, localisation and deletion costs.

9. PROTECT CONFIDENTIAL PROCESS KNOWLEDGE

Plant data can reveal recipes, yields, bottlenecks, maintenance practices, energy intensity and operating constraints. These features may have competitive value even when they fall outside a registered intellectual-property right. Confidentiality therefore needs operational controls, not only a general non-disclosure clause.

The joint venture should map data rooms, support channels, engineering notebooks, model features and customer reports in which process knowledge appears. Access should follow need, territory and customer scope. Cross-customer benchmark products need threshold rules that prevent reconstruction of a plant's performance. Staff movement and subcontracting should be governed because expertise can transfer through people as well as files.

At exit, confidential material should be returned, deleted or retained under a defined archive exception. Trained models require special treatment because parameters may preserve information about the training population. The parties should decide whether a model can continue operating, requires retraining or must be retired when underlying rights expire.

10. DESIGN CROSS-BORDER TRANSFER ARCHITECTURE

Cross-border architecture should follow data classification and purpose. Options include processing entirely within the plant, using a GCC-hosted environment, transferring selected features to India, using federated learning or exporting aggregated results. The lowest-friction technical design may not be the lawful or commercially acceptable design.

The India-UAE Comprehensive Economic Partnership Agreement includes a digital-trade dialogue and provisions relevant to electronic transactions, personal-data protection and intellectual property [2][3]. It does not replace sectoral, personal-data, cybersecurity or customer restrictions. The UAE personal-data law includes cross-border transfer provisions, and Saudi rules apply to relevant Saudi personal data [6][7]. Each route requires a documented basis and current legal review.

The architecture register should show where data is collected, decrypted, processed, backed up, monitored and supported. Remote administrative access is part of the transfer analysis. Costs for local hosting, duplicated pipelines, key management and audit should enter the joint-venture model before pricing customers or parent contributions.

11. SECURE OPERATIONAL TECHNOLOGY

Industrial AI can connect sensors, historians, engineering workstations, edge devices, cloud services and remote support. NIST SP 800-82 Rev. 3 addresses operational-technology security while recognising safety, reliability and performance constraints [8]. IEC 62443 provides a lifecycle framework for industrial automation and control-system security [9]. The joint venture should translate these principles into a shared security responsibility matrix.

The matrix should cover asset inventory, identities, network zones, conduits, encryption, certificates, vulnerability handling, backup, recovery, monitoring, incident response and supplier access. It should identify which parent operates each control and which party bears remediation cost. A customer should not face an unclear division between software support and plant-network accountability during an incident.

Security changes require plant coordination. Patching, endpoint controls and identity changes can affect validated systems or production availability. The joint venture should test changes in a representative environment, schedule plant approvals and preserve safe fallback. Cyber service levels should measure verified control performance and recovery capability rather than the volume of alerts.

12. PRESERVE PLANT OPERATING AUTHORITY

The industrial operator remains accountable for safe production. A joint venture can provide models, recommendations and integration services while preserving the plant's operating procedures, engineering limits and control hierarchy. The agreement should state which outputs are informational, advisory, supervisory or capable of direct control.

Authority should be mapped by application and operating mode. A model may provide advice during stable production and be disabled during start-up, shutdown or abnormal conditions. The record should name who can approve a model, change a constraint, accept a recommendation, suspend service and return the process to manual operation. These controls should be visible in the interface and audit log.

Commercial incentives should not reward unsafe authority expansion. Outcome fees based on throughput or energy savings need boundaries for safety, quality, emissions and equipment life. Any proposal to move from advisory use to automated action should pass the plant's engineering review and management-of-change process before it enters the revenue or valuation case.

13. ALLOCATE BACKGROUND INTELLECTUAL PROPERTY

Background intellectual property includes software, algorithms, libraries, connectors, engineering methods, ontologies, templates, patents, trade secrets and know-how that existed before the joint venture or was developed outside its funded scope. Each parent should disclose the relevant background assets and grant the rights needed for the agreed business plan.

The licence should address field, territory, customer group, exclusivity, sublicensing, modification, support, source-code access, royalties and termination. A contribution described as technology can be commercially weak if the joint venture cannot modify it, support customers or continue operating after parent exit. The valuation of an in-kind contribution should reflect the rights actually transferred.

Dependencies require separate review. Open-source components, third-party simulation engines, cloud services and customer-owned interfaces can limit sublicensing or change-of-control rights. The joint venture should maintain a software and licence register and include renewal, replacement and escrow costs in its plan.

14. ALLOCATE FOREGROUND INTELLECTUAL PROPERTY

Foreground intellectual property arises through joint-venture activity. Examples include deployment code, customer-specific connectors, engineered features, synthetic datasets, digital-twin configurations, validation protocols, user interfaces and new models. Automatic joint ownership can create deadlock because exploitation rules differ by jurisdiction and asset type.

A practical allocation follows creation and future use. The joint venture can own reusable platform improvements. A customer can retain site-specific configuration and confidential process content. A parent can receive a non-exclusive licence for defined territories or fields. Inventor and employee assignment processes should support the intended allocation.

The development workflow should classify new assets when created. Repository metadata, invention disclosures, model cards and design approvals can record contributors, funding source, dependencies and permitted use. Delayed classification increases exit risk because the parties may disagree only after an asset becomes valuable.

Table 2. Intellectual-property allocation by asset layer

Asset layer	Typical origin	Practical allocation	Key diligence evidence
Raw plant records	Industrial operator or customer	Operator ownership with purpose-bound access	Data schedule and customer contract
Context and labels	Joint operational work	Defined site rights plus limited reusable method rights	Provenance and contributor record
Background software	Technology or engineering parent	Retained ownership with field licence	Code, dependency and licence register
Deployment configuration	Joint venture and customer	Site continuity rights with reusable templates separated	Configuration repository and acceptance
New reusable model	Joint-venture development	Joint-venture ownership or exclusive field right	Training lineage and invention record
Validated outcome ledger	Plant, joint venture and finance	Shared audit access; restricted external use	Baseline and approval workflow

The appropriate structure depends on contribution, customer terms and continuing support obligations.

15. GOVERN MODELS AND IMPROVEMENTS

A model register should link each production version to training data, features, code, validation, permitted sites, operating regimes, monitoring, approvers and rollback. The register is the operational bridge between data rights and intellectual property. It shows whether a model can lawfully and safely be reused in another deployment.

Improvement rights require precision. A party may learn a general engineering method without retaining customer data. A jointly trained model may be deployable only after removing restricted features or retraining on an authorised population. Federated learning can keep records local while sharing parameter updates, although it introduces aggregation, security and validation obligations.

Change governance should distinguish maintenance, recalibration, feature change and new purpose. Material changes should trigger renewed technical, legal, cyber and plant review. The joint venture

should retain failed tests and rejected versions. A clean history of limitations supports trust and provides a more credible valuation basis than a register containing only successful deployments.

16. MEASURE DATA QUALITY AND PROVENANCE

Data quality should be measured against the application decision. Completeness, accuracy, timeliness, consistency, calibration and context can matter differently for predictive maintenance, quality prediction and energy optimisation. A universal quality score can conceal a critical weakness in the feature that drives a specific model.

Provenance should trace each material feature to the source record and transformation. It should preserve timestamps, units, quality flags, code version and responsible party. Manual labels require reviewer identity and supporting evidence. Synthetic or imputed data should remain identifiable so that validation does not treat generated observations as independent plant outcomes.

The commercial model should assign remediation cost. Instrument repair may belong to the operator. Pipeline correction may belong to the joint venture. A new connector may become reusable foreground intellectual property. Clear allocation reduces disputes and reveals whether a profitable-looking subscription depends on extensive unfunded data engineering.

17. VALIDATE DEPLOYMENT READINESS

Deployment readiness is wider than model accuracy. The site needs a defined problem, adequate instrumentation, authorised data, integration capacity, named operating owner, cyber approval, engineering validation, user workflow, benefit baseline and support plan. Applications should pass these gates before management counts them as deployable pipeline.

The readiness register should use evidence states such as proposed, data-qualified, technically validated, site-approved, commissioned, adopted and outcome-validated. Progression should require documentary evidence. This prevents a long list of ideas from being presented as revenue-ready applications.

Readiness also determines sequencing. High-value applications with weak instrumentation can consume capital before they produce revenue. Lower-value applications with strong data and repeatable workflows may generate earlier proof and cash. The joint venture should prioritise a balanced portfolio that builds reusable capability while meeting customer operating needs.

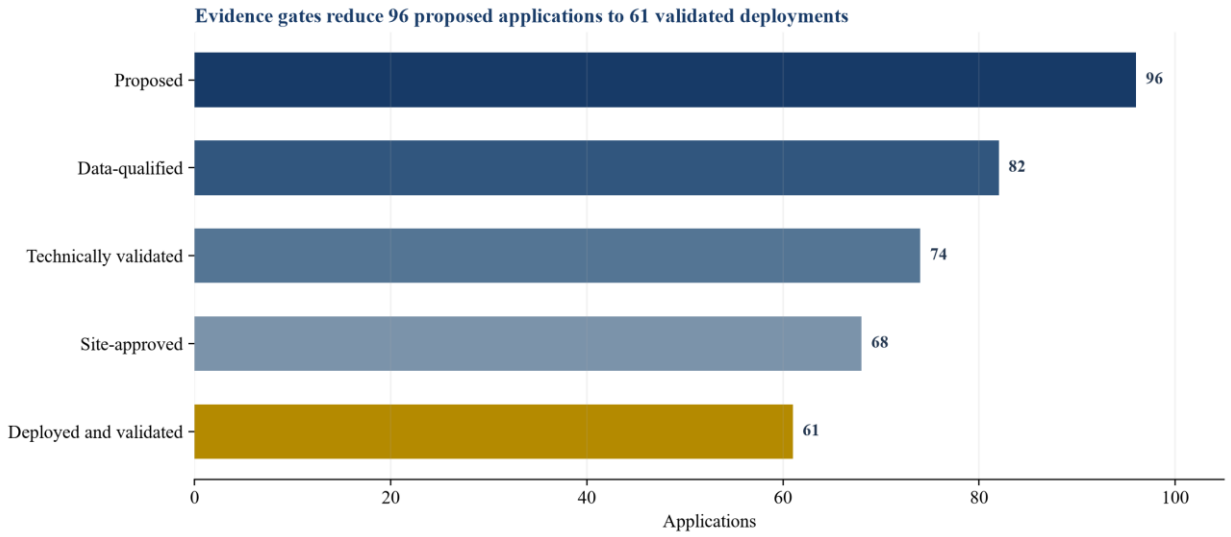

Figure 2. Hypothetical application readiness funnel

Counts are illustrative management assumptions for demonstrating evidence gates.

18. RECONCILE REPORTED SAVINGS

Every savings claim requires a counterfactual. The joint venture should state what would have happened without the application, over which period and under which operating conditions. Baselines may use matched operating periods, engineering models, controlled trials or approved budgets. Each method carries limitations that should remain visible in the evidence record.

The outcome ledger should link baseline, model output, authorised action, physical result, price effect, operating cost and finance approval. It should separate yield, throughput, energy, maintenance, quality and avoided downtime to prevent overlap. A physical improvement does not always become cash when another plant constraint or market condition blocks monetisation.

Outcome validation should cover a representative cycle and regime change. A short trial can establish feasibility while providing limited evidence of persistence. Retained economics should reflect adoption, attribution, duration, service effort and customer payment. The joint venture should disclose excluded cases and failed applications when presenting portfolio results.

19. DESIGN VALUE SHARING

Value sharing can combine subscription fees, implementation charges, royalties, cost-plus services, milestone payments and outcome fees. The structure should compensate the party that contributes the relevant asset and bears the relevant risk. A fixed software fee can suit a repeatable product. An outcome fee can suit measurable operating gains, provided the baseline and cash-conversion rules are agreed.

The formula should state the benefit population, measurement period, exclusions, price source, approval process, payment timing, cap, floor and dispute mechanism. It should also account for operator investment, instrumentation, downtime, engineering effort and third-party costs. Gross benefit is not distributable value until these items are recognised.

Parent economics should remain transparent. Background-technology royalties, seconded staff, hosting, sales commissions and support charges can move value away from the joint venture. Reserved matters and transfer-pricing evidence should govern these flows. Minority protections should focus on verifiable related-party terms and cash distributions rather than broad vetoes over ordinary delivery.

20. SET SERVICE LEVELS AND CONTINUITY

Service levels should cover data availability, model availability, response, restoration, accuracy where measurable, approved change windows and recovery. Industrial consequences vary by application. A delayed monthly report differs from a failed advisory service during a production constraint. Severity should follow operating impact.

Continuity requires source code, model artefacts, configuration, documentation, credentials, keys, dependencies and trained personnel. The parties should identify what the joint venture needs to operate if a parent stops supporting it. Escrow can support continuity only when deposits are complete, current and usable.

Exit service levels should include data export, model handover, revocation, deletion and transition assistance. Customers may require continuity beyond parent disputes. The business plan should fund duplicated expertise and recovery tests rather than relying on a small number of individuals whose departure could suspend service.

21. DEFINE JOINT CONTROL AND RESERVED MATTERS

Governance should reflect whether the parties have joint control over the relevant activities. IFRS 11 distinguishes joint operations and joint ventures by the parties' rights and obligations [16]. Legal form, contractual arrangements and other facts should be assessed together. Accounting classification should follow the arrangement rather than the commercial label.

Reserved matters should cover business plan, capital, borrowing, material contracts, related-party transactions, territory, exclusivity, intellectual-property changes, new data purposes, major cyber events, model authority, acquisitions, disposals and distributions. Thresholds should protect strategic interests while allowing management to deliver approved work.

Technical governance needs equal attention. A data and model committee can approve classifications, transfer routes, model changes and reusable assets. A plant authority can approve deployment and operating scope. An audit committee can review value-sharing calculations. Escalation timelines and independent expert processes can prevent ordinary evidence disputes from becoming shareholder deadlock.

22. MANAGE RELATED-PARTY ECONOMICS

Joint ventures often depend on their parents for technology, staff, facilities, customers or distribution. These relationships can accelerate formation and create continuing conflicts. Every material related-party flow should have a service description, pricing method, benchmark, approval path, performance evidence and termination right.

Seconded staff require clarity on employer, direction, confidentiality, invention assignment and cost. A technology royalty should correspond to a documented licence and continuing support. A sales commission should correspond to customer origination and collection. Hosting charges should identify infrastructure, utilisation and margin. Undefined management fees weaken accountability and distributable cash.

The parties should model economics before and after parent charges. A profitable customer contract can leave the joint venture unable to fund product development when royalties and services absorb its gross margin. Independent review and minority access to records can reduce this risk. Transfer-pricing and tax advice should be obtained for the actual jurisdictions and structure.

23. ADDRESS COMPETITION AND EXCLUSIVITY

Exclusivity can protect investment in market development while restricting customer choice, parent activity and future exit. The agreement should define product, field, customer, territory, channel and duration. Performance conditions can release exclusivity when the joint venture does not meet agreed investment or delivery milestones.

Competition review should cover information exchange, customer allocation, pricing coordination, non-compete provisions and access to essential inputs. India's Competition Commission issued the Competition Commission of India (Combinations) Regulations 2024 and publishes guidance relevant to combination filings and joint ventures [17][18]. The UAE competition regime includes Federal Decree-Law No. 36 of 2023 and implementing thresholds under Cabinet Resolution No. 59 of 2026 [19][20]. Current counsel should assess filing and conduct requirements for the actual transaction.

Data pooling can create both efficiencies and market power. Governance should prevent one parent from using competitively sensitive information outside the approved purpose. Clean teams, aggregation thresholds and access separation can support collaboration while limiting unnecessary disclosure.

24. PLAN EXIT AND TERMINATION

Exit planning should begin before deployment. Triggers can include term expiry, breach, insolvency, change of control, regulatory prohibition, persistent underperformance, deadlock or strategic sale. Each trigger should specify continuity, licence survival, customer service, employee treatment, data return and asset valuation.

The exit package should identify raw records, contextualised datasets, models, code, configurations, documentation, credentials, audit logs and validated outcome records. Formats and transfer time should be agreed. A party should not discover during termination that it lacks the identifiers or dependencies needed to use its own export.

Model retirement deserves specific treatment. If training rights expire, a deployed model may need retraining, restriction or deletion. If a customer requires continuing service, the contract may grant a transition licence. The joint venture should test exit procedures periodically and record deletion evidence. These obligations affect terminal value and should enter the transaction model.

25. APPLY ACCOUNTING AND VALUATION DISCIPLINE

IAS 38 requires identifiable intangible assets to satisfy recognition criteria and distinguishes research from development expenditure [15]. Plant data, contractual rights, software, customer relationships and models should be assessed separately. Expenditure creating internal capability does not automatically become a recognised asset. The accounting conclusion requires the actual facts and current professional advice.

IFRS 15 governs revenue from contracts with customers [14]. Outcome fees, implementation, licences, subscriptions and support may contain different performance obligations and variable consideration. Management should avoid treating an estimated customer saving as joint-venture revenue. Cash entitlement depends on the contract, measurement and payment terms.

IFRS 13 defines fair value and requires market-participant assumptions [13]. A contribution valuation should consider legal rights, technical readiness, replacement cost, obsolescence, useful life, customer restrictions, service dependency and probability of cash conversion. The value of broad rhetoric about proprietary data should be replaced with evidence for the specific rights that a market participant could use.

Table 3. Economic bridge from proposed application to distributable value

Stage	Customer benefit	Joint-venture revenue and synergy	Principal adjustment
Management case	18.0	7.2	Proposed application population
Data and rights gate	15.7	6.1	Availability, permission and provenance
Deployment gate	13.2	5.0	Site approval, integration and adoption
Outcome validation	10.6	3.8	Baseline, attribution and overlap
Persistence and cash conversion	9.2	3.1	Duration, service cost and collection

Values in USD millions are hypothetical management assumptions used only to demonstrate the framework.

26. CONSTRUCT A HYPOTHETICAL JOINT VENTURE

Consider a wholly hypothetical joint venture between an Indian industrial-technology business and a GCC industrial group. The programme covers 20 sites and 58 production units. Management identifies 96 applications across reliability, energy, quality, throughput and operator support. The initial case assumes USD 18.0 million of annual customer benefit and USD 7.2 million of joint-venture revenue and buyer synergy.

The readiness review finds 82 applications with adequate data, 74 with technical validation, 68 with site approval and 61 that are deployed with validated outcomes. Data-rights restrictions remove cross-site training for several customer-owned datasets. Instrumentation gaps delay part of the reliability portfolio. Outcome review removes overlapping energy and emissions claims and adjusts short trials for persistence.

The framework retains USD 9.2 million of annual customer benefit and USD 3.1 million of joint-venture revenue and synergy. These amounts include hypothetical service, hosting, royalty and deployment costs. They remain scenario assumptions rather than evidence about an actual company. Their purpose is to show how governance and technical evidence change the economics.

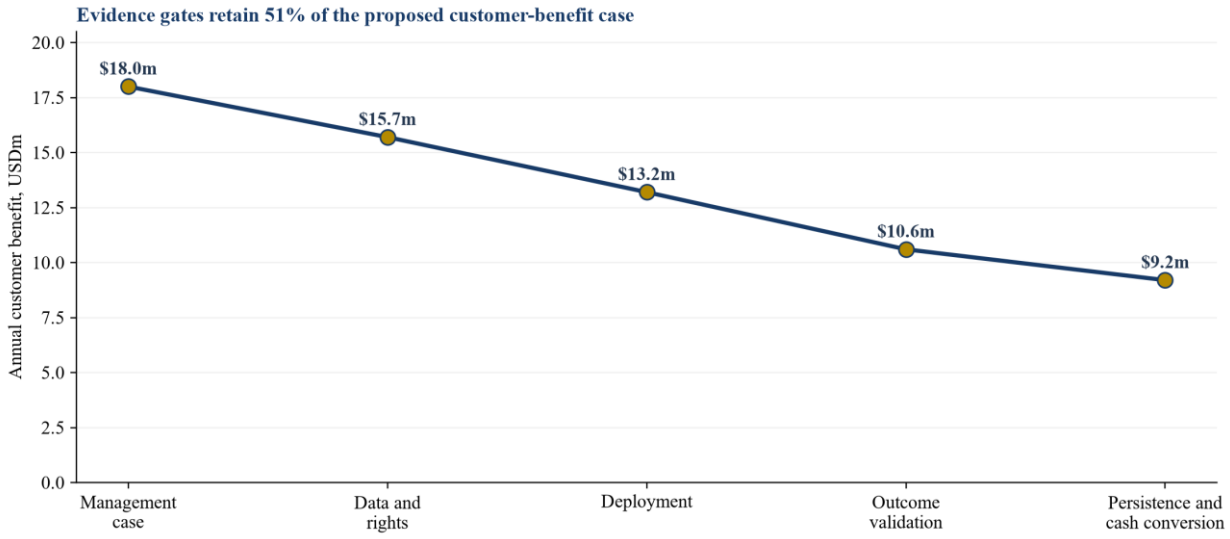

Figure 3. Hypothetical customer-benefit validation bridge

Values in USD millions are illustrative management assumptions.

27. TRANSLATE EVIDENCE INTO PRICE AND TERMS

Evidence should affect price, funding and risk allocation. Rights that are broad, durable, transferable and technically usable can support greater value. Rights limited to one customer or dependent on revocable parent support should receive lower weight. Unvalidated application pipeline can be funded through milestones rather than paid for at formation.

The contribution agreement can use staged equity issuance, earn-ins, preferred returns, royalties or contingent payments. Milestones should be within the responsible party's influence and tied to evidence such as customer consent, site commissioning, outcome validation or cash collection. Volume metrics without quality gates can reward low-value deployment.

Representations should cover authority, licences, data provenance, security incidents, model rights, customer restrictions and infringement claims. Indemnities and liability caps should reflect the actual risk allocation. Insurance can support selected risks, although exclusions and operating obligations require review. The commercial model should preserve sufficient joint-venture capital after parent consideration.

28. BUILD THE DILIGENCE REQUEST

The diligence request should begin with the business plan and trace each material claim to evidence. Core items include corporate documents, customer and parent contracts, data schedules, asset graph, system architecture, security assessments, intellectual-property register, software dependencies, model register, validation reports, plant approvals, outcome ledger, financial model and related-party agreements.

Sampling should follow risk and value. The team should inspect high-value applications, restricted datasets, automated authority, cross-border transfers, customer concentration and models supporting a large share of forecast revenue. It should reproduce selected outcomes from source records and interview plant, engineering, cyber, finance and customer personnel.

Exceptions should enter one register with owner, consequence, remediation, cost, timing and deal response. Some exceptions require a condition precedent. Others can become a covenant, price adjustment, holdback or post-close workstream. The investment committee should see unresolved rights and evidence gaps in the same language used in the valuation.

Table 4. Joint-venture diligence request and deal response

Workstream	Priority evidence	Typical exception	Possible response
Data rights	Customer terms, purpose schedule, transfer map	Cross-site training not permitted	Restrict use; reprice platform value
Technology	Architecture, code, dependencies, model register	Parent-controlled component lacks continuity	Licence, escrow or staged funding
Operations	Site approval, authority and support model	Application remains advisory pilot	Milestone before value attribution
Outcomes	Baseline, action and finance approval	Savings overlap or short observation	Adjust benefit and outcome fee
Security	OT assessment, identities and recovery test	Remote access outside approved route	Remediate before commissioning
Economics	Related-party terms and cash model	Parent charges absorb gross margin	Benchmark and reserve matter

The response should follow the economic and operating consequence of each gap.

29. EXECUTE THE FIRST ONE HUNDRED DAYS

The first thirty days should establish governance, freeze uncontrolled transfers and create the shared registers. The parties should confirm asset graph, classifications, source authority, contracts, model versions, privileged access, related-party services and active customer obligations. Critical continuity gaps should receive funded owners.

Days thirty-one to sixty should validate the highest-value applications and reconcile the economic baseline. The team should test data lineage, site approval, user adoption, outcome attribution and service effort. It should establish a single value ledger approved by plant and finance representatives. Unsupported claims should be removed from forecasts and customer materials.

Days sixty-one to one hundred should implement the target operating model. Work includes purpose approvals, transfer routes, security zones, model-change controls, foreground-asset classification, service levels, exit packages and board reporting. The programme should publish a repeatable deployment gate and use it for every new site. Management should report verified customer outcomes, joint-venture cash and unresolved risks separately.

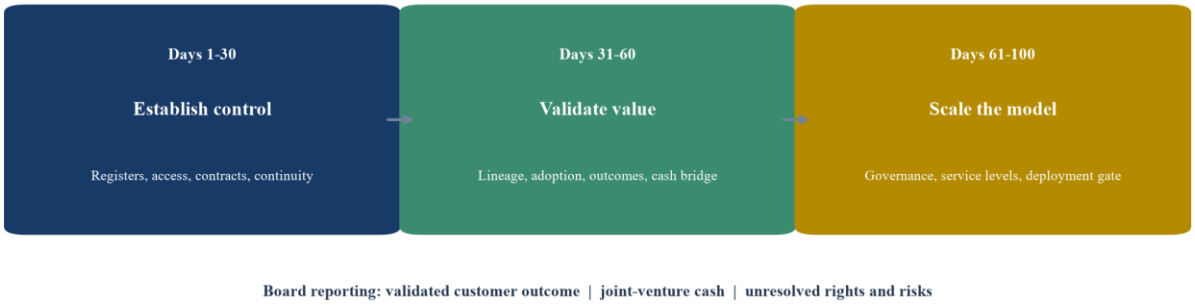

Figure 4. First one hundred days for the plant-data joint venture

The sequence establishes control before scaling new applications.

30. RECOGNISE LIMITATIONS AND CONCLUDE

The framework does not determine ownership or regulatory treatment for a specific joint venture. Applicable law depends on entity, sector, customer, data, processing activity, location and contract. Technology and regulatory requirements continue to evolve. The parties should obtain current legal, tax, accounting, cybersecurity, engineering and valuation advice before acting.

The hypothetical case is intentionally simplified. It does not estimate market demand, transaction value or likely savings. Industrial outcomes can change with plant condition, operator behaviour, feedstock, product mix, energy prices and capital investment. Model performance at one site does not establish performance elsewhere.

Implementation quality also depends on organisational capability. A carefully drafted rights schedule can fail when engineering teams exchange files through uncontrolled channels, models are deployed outside approved regimes or outcome calculations bypass plant finance. Boards should require periodic testing of the operating controls described in this paper. Internal audit or an independent reviewer can sample the chain from source record to model, authorised action, reported benefit and customer invoice. Exceptions should be reported with their financial consequence and remediation status.

The framework can also support future financing or sale. A lender or acquirer can evaluate contracted rights, customer concentration, continuity, model portability and verified cash conversion from the same evidence set used to operate the business. This reduces dependence on narrative claims about proprietary data. It also allows management to distinguish assets that can travel with the enterprise from site-specific rights that remain with a customer or parent.

The practical conclusion is that the value question is larger than who owns the plant data. A durable India-GCC industrial AI joint venture defines the asset graph, permitted purposes, control authority, transfer architecture, intellectual property, validation and cash-sharing rules as one operating system. That system converts collaboration into an auditable portfolio of rights and outcomes that customers, boards, investors and acquirers can evaluate.

REFERENCES

[1] UAE Ministry of Industry and Advanced Technology. UAE and India memorandum of understanding on industrial and advanced technologies, 2023. https://moiat.gov.ae/en/media-center/news/2023/10/05/uae-and-india-sign-mou-to-cooperate-on-industries-and-advanced-technologies

[2] Government of India, Department of Commerce. India-UAE Comprehensive Economic Partnership Agreement. https://commerce.gov.in/international-trade/trade-agreements/india-uae-comprehensive-economic-partnership-agreement/

[3] Government of India, Department of Commerce. India-UAE CEPA frequently asked questions. https://commerce.gov.in/wp-content/uploads/2022/05/FAQs-on-India-UAE-CEPA.pdf

[4] Government of India. Digital Personal Data Protection Act, 2023. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[5] Government of India. Digital Personal Data Protection Rules, 2025. https://www.meity.gov.in/data-protection-framework

[6] United Arab Emirates. Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data. https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws

[7] Saudi Data and Artificial Intelligence Authority. Personal Data Protection Law and implementing regulations. https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

[8] National Institute of Standards and Technology. Special Publication 800-82 Revision 3: Guide to Operational Technology Security, 2023. https://csrc.nist.gov/pubs/sp/800/82/r3/final

[9] International Electrotechnical Commission. IEC 62443 series: Security for industrial automation and control systems. https://www.iec.ch/cyber-security

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

[11] International Organization for Standardization. ISO 23247-5, Digital thread for digital twin, under development. https://www.iso.org/standard/89207.html

[12] International Organization for Standardization. ISO 55001:2024 Asset management; Management systems; Requirements. https://www.iso.org/standard/83054.html

[13] IFRS Foundation. IFRS 13 Fair Value Measurement. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-13-fair-value-measurement/

[14] IFRS Foundation. IFRS 15 Revenue from Contracts with Customers. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-15-revenue-from-contracts-with-customers/

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

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

[17] Competition Commission of India. Competition Commission of India (Combinations) Regulations, 2024. https://www.cci.gov.in/images/legalframeworkregulation/en/cci-combinations-regulations-20241725885607.pdf

[18] Competition Commission of India. Combination filing guidance and FAQs. https://www.cci.gov.in/combination/combination/faqs

[19] United Arab Emirates. Federal Decree-Law No. 36 of 2023 on the Regulation of Competition. https://uaelegislation.gov.ae/en/legislations/2169

[20] United Arab Emirates. Cabinet Resolution No. 59 of 2026 concerning economic concentration thresholds. https://uaelegislation.gov.ae/en/legislations/3185

[21] International Society of Automation. ISA-95 enterprise-control system integration. https://www.isa.org/standards-and-publications/isa-standards/isa-95-standard

[22] OPC Foundation. OPC Unified Architecture. https://opcfoundation.org/about/opc-technologies/opc-ua/

[23] International Organization for Standardization. ISO/IEC 42001:2023 Artificial intelligence management system. https://www.iso.org/standard/81230.html

[24] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework, 2023. https://www.nist.gov/itl/ai-risk-management-framework

[25] Indian Computer Emergency Response Team. Directions under section 70B of the Information Technology Act, 2000, 2022. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

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.