UK Freight Carve-Outs: Separating Routing Algorithms, Fleet Data and Customer Contracts

A transaction framework for defining the sale perimeter, protecting service continuity and converting separation evidence into price, protection and execution decisions

Authored by Chennakeshav Adya
Independent Researcher
September 2026

Abstract

Road-freight businesses increasingly depend on routing software, telematics, customer interfaces, depot systems, driver processes, licences and group services that do not sit neatly inside the legal entity being sold. A conventional asset list can therefore transfer vehicles and contracts while leaving the buyer without the code, data rights, people, infrastructure or consents needed to operate them. The result can be an apparently complete transaction with an incomplete business.

This paper develops a Freight Carve-Out Separation Framework for UK transactions. It begins with the operating promise made to customers, traces each service through algorithms, data, contracts, people, fleet and infrastructure, and classifies every dependency as transferring, remaining, duplicated, licensed, novated or supported temporarily. It connects the perimeter to customer consent, data-controller obligations, intellectual-property rights, TUPE, competition and national-security screening, cyber controls, transition services, stranded costs and valuation.

An illustrative seven-depot freight division demonstrates the method. Management assumptions include annual revenue of GBP 420 million, reported EBITDA of GBP 38 million, 64 enterprise customers, 1,280 powered and unpowered fleet units, 18 material software services and a routing platform shared with the seller. Evidence-based standalone adjustments reduce maintainable EBITDA to GBP 31 million. A hypothetical headline enterprise value of GBP 285 million is then tested for algorithm-rights restrictions, customer-consent attrition, data remediation, separation expenditure and executable mitigation. The resulting values are management assumptions created solely to demonstrate the framework. They are not observed company data, a valuation opinion, a fairness opinion, an investment recommendation or a forecast of any identified business.

The analysis finds that separation quality is a value driver rather than an administrative workstream. The buyer should be able to prove, before signing or through enforceable conditions, that it can accept orders, optimise routes, dispatch vehicles, use historical data lawfully, invoice customers, pay drivers, maintain regulatory compliance and withstand a seller-system outage. The sale agreement, transition-services agreement, data plan and valuation model should use the same controlled dependency register. This makes the economic bargain visible and gives the parties a practical route from diligence to Day One and exit from transitional support.

JEL Classification: G34, L86, L91, L92, K12

Keywords: UK freight carve-out, logistics M&A, routing algorithms, fleet data, customer contracts, transaction separation, transition services agreement, data protection, intellectual property, standalone cost, purchase price

1. Define the transaction decision

The transaction decision is whether the proposed perimeter constitutes an operable freight business at completion and whether the price and protections reflect what actually transfers. Legal ownership of vehicles and customer contracts does not answer that question. The buyer must identify the capabilities required to quote, plan, dispatch, track, deliver, evidence, invoice and collect each service, then prove that the rights, systems, people and controls supporting those capabilities will be available.

The board paper should state the transaction form, target perimeter, intended completion date, regulatory path, operating model and value thesis. An asset purchase, business transfer, share sale and internal reorganisation create different consent, tax, employment and separation consequences. Qualified counsel, tax advisers, accountants, technology specialists, pensions advisers and operational experts must determine the treatment of an actual transaction.

The decision framework separates six questions: what transfers, what remains, what must be copied or recreated, what requires third-party consent, what needs transitional access and what changes the price or risk allocation. Every diligence finding should resolve into one of these decisions. A long issue list without a transaction response creates activity but does not establish an executable carve-out.

2. Start with the customer service promise

The perimeter should begin with services rather than assets. A freight contract may promise timed collection, route optimisation, temperature control, proof of delivery, live tracking, customs support, returns management, emissions reporting or dedicated capacity. Each promise depends on a chain of technology, data, fleet, people, licences, depots and external suppliers.

For every material service, the team should map the order-to-cash and incident-to-resolution paths. The map should identify who receives the order, how capacity is confirmed, which engine selects the route, where driver and vehicle data originate, how exceptions are managed, which evidence supports invoicing and who owns the customer relationship. Shared parent systems can appear invisible until the service is traced end to end.

The output is a minimum viable operating perimeter. It defines the capabilities that must work on Day One even if the buyer plans a later platform migration. Optional enhancements, synergies and future transformation should remain separate. This protects the closing decision from relying on improvements that have not yet been delivered.

Table 1. Carve-out perimeter classes and transaction response

Perimeter class	Typical freight example	Required evidence	Principal transaction response
Transfer	Vehicles, depot leases, assigned employees	Title, condition, lease and employment records	Include in transfer instruments and completion evidence
Novate or consent	Customer and supplier contracts	Assignment, novation and change-of-control clauses	Obtain consent, condition completion or allocate attrition risk
Licence	Routing code, databases, brands or mapping rights	Ownership, permitted use, territory and sublicensing rights	Execute durable licence with support, audit and exit rights
Duplicate	Interfaces, data stores and operating procedures	Architecture, lineage, build plan and acceptance tests	Fund separation plan and prove independent operation

Perimeter class	Typical freight example	Required evidence	Principal transaction response
Transitional service	Hosting, payroll, finance, cyber monitoring	Service catalogue, capacity, security and exit dependencies	Define TSA service levels, charges, remedies and exit milestones
Retain with seller	Group treasury, unrelated customer data	Boundary evidence and access controls	Exclude cleanly and prevent continuing access or economic leakage

The final legal and accounting treatment requires transaction-specific professional advice.

3. Establish the legal-entity perimeter

The legal-entity map should list each company, branch, partnership, depot vehicle, employee population, contract, licence, permit, bank account and asset relevant to the freight operation. A division may trade through several seller entities while vehicles are leased by one company, employees sit in another and customer invoices are raised centrally. Financial reports prepared by management can combine these elements without showing their legal ownership.

The map should distinguish a transfer of shares from a transfer of selected assets and liabilities. In a share sale, contracts and licences may remain with the same legal entity but change-of-control clauses can still apply. In an asset sale, assignment or novation may be required and some liabilities may remain by law or contract. The transaction documents should reconcile the commercial perimeter with the legal transfer mechanism.

Intercompany balances, guarantees, cash-pooling arrangements, insurance, tax grouping and shared registrations require separate treatment. The buyer should not assume that an operating licence, credit line or insurance programme follows the activity. The seller should identify what will terminate, be replaced, be released or remain temporarily, together with the party responsible and the deadline.

4. Build a controlled dependency register

The dependency register is the central record for separation. Each row should identify the capability, asset or service, current owner, user, location, contractual basis, data involved, transfer route, Day One requirement, target-state solution, accountable owner, cost, decision date and evidence status. A controlled identifier should link the same item across diligence, the sale agreement, TSA, technology plan and valuation model.

Dependencies should be recorded at a level that supports action. “IT separation” is too broad. “Routing optimisation production environment,” “vehicle-position message broker,” “customer proof-of-delivery portal” and “invoice-rating table” can each have different owners and transfer routes. The register should distinguish software code, configured instances, credentials, documentation, data, interfaces, hosting, support and underlying third-party licences.

The programme office should retain the closing baseline and log changes. New dependencies often emerge when interfaces are tested or customer terms are reviewed. A change should state its effect on Day One, separation cost, timing, price, consent and risk allocation. This prevents late discoveries from disappearing into narrative status reports.

5. Decompose the routing algorithm

The routing capability should be decomposed into source code, compiled services, optimisation logic, model parameters, maps, traffic feeds, constraint libraries, customer rules, configuration, interfaces, testing assets, monitoring and documentation. Ownership can differ across these components. A seller

may own the orchestration layer while using third-party solvers, map data and open-source libraries under separate licences.

The buyer should identify whether the business needs ownership, a perpetual licence, a term licence or only transitional access. The right to use code can be more important than nominal ownership when the licence covers the required fields, territories, users, modifications, interfaces, hosting models and successors. UK government IP guidance similarly emphasises case-specific rights and the practical importance of licences [8-10].

Algorithm diligence should examine reproducibility and operating control. The buyer needs build instructions, deployment pipelines, model versions, change logs, test suites, incident history and the people able to maintain the service. A code repository without the data, keys, infrastructure and expertise required to run it does not create an independent routing capability.

6. Test intellectual-property ownership and licences

The IP schedule should identify copyright, database rights, patents, trademarks, domains, know-how, confidential information and contract-based rights. Software created by employees, contractors, vendors and joint-development partners can carry different ownership terms. The transaction team should trace material components to executed employment, assignment, development and licence documents.

Third-party licences require special attention to assignment, change of control, affiliate use, territory, processing volume, hosting, sublicensing and termination. Open-source dependencies require a complete bill of materials and compliance record. HMRC software standards note the need to understand ownership and adhere to open-source licences, particularly during contract transitions [11].

Database rights can protect the contents of qualifying databases separately from copyright in their selection or arrangement [9,12]. The buyer should therefore assess both the right to receive data and the right to extract, reuse and continue enriching it. Legal rights, contractual restrictions and data-protection obligations should be analysed together.

7. Define the fleet-data perimeter

Fleet data includes vehicle identity, location, speed, fuel or energy use, maintenance, defects, driver interactions, route execution, loading, temperature, incident and proof-of-delivery records. It can originate from vehicle manufacturers, telematics providers, mobile devices, depot equipment, subcontractors and customer systems. The seller may possess the data without owning every right needed to transfer or reuse it.

The register should record each dataset’s source, controller, processor, contractual owner, lawful purpose, retention period, refresh frequency, geography, security classification and intended buyer use. Personal data should be separated from operational data wherever feasible. Driver location and performance records can identify individuals and require a lawful, fair and transparent processing basis.

Historical data can support route calibration, pricing, maintenance and valuation. Its usefulness depends on completeness, continuity and permitted use. A buyer should not pay for a machine-learning advantage that cannot be transferred, reproduced or lawfully applied. The data room should contain field definitions, lineage, quality metrics, licences and a sample extraction that can be reconciled to source systems.

8. Apply data-protection diligence to the transaction

The ICO states that M&A due diligence should establish what personal data transfers, the original purposes, lawful basis, data-protection principles, documentation, security and communication to data subjects [5]. The Data (Use and Access) Act 2025 has changed parts of the UK data-protection regime,

and the ICO notes that related guidance remains under review [5-7]. Current legal advice is therefore required at signing, completion and migration.

The parties should distinguish diligence disclosure from completion transfer. Clean teams, aggregation, redaction, controlled access and staged disclosure can reduce risk before completion. The buyer should identify whether it becomes a new controller, joint controller or processor for each activity and update notices, records, contracts and rights-handling processes accordingly.

Data migration should be tested for completeness, accuracy, access control, retention and deletion. The seller must remove buyer data from retained systems according to the agreed plan while preserving records it is legally required to keep. The buyer should prove that it can answer data-subject requests and investigate incidents after separation.

9. Map customer contracts to operating dependencies

Customer contracts should be reviewed beyond headline revenue. The schedule should capture legal entity, service scope, volume commitment, pricing, indexation, term, renewal, termination, assignment, novation, change of control, exclusivity, subcontracting, service levels, data terms, audit, cyber requirements, liability, insurance and governing law.

Each contract should link to the systems and data required to perform it. A contract may transfer legally while the seller retains the customer portal, tariff engine or reporting process needed for delivery. Conversely, a routing platform may transfer while the contract prohibits subcontracting or customer data migration. The perimeter is complete only when rights and operating capability align.

Revenue quality should be assessed at the contract-service lane level. Minimum volume, spot pricing, pass-through fuel mechanisms, claims, penalties and loss-making lanes can change the economic value of a customer relationship. IFRS 3 requires identifiable acquired assets and liabilities to be recognised and measured, including qualifying customer-related and contract-based intangibles [19-21]. Transaction valuation should use the actual rights and economics that transfer.

Table 2. Customer-contract consent matrix

Consent position	Operating position	Day One risk	Possible response
No consent required and capability transfers	Service can continue on existing terms	Low, subject to verification	Confirm transfer evidence and customer communication plan
Consent required and obtained	Service can continue after novation or approval	Moderate implementation risk	Make consent effective at completion and test billing and data migration
Consent required and pending	Revenue and service continuity are uncertain	High	Condition completion, exclude contract, escrow value or allocate attrition risk
Contract transfers but capability remains with seller	Buyer lacks independent delivery capability	High operational risk	TSA, licence, personnel transfer and tested exit plan
Capability transfers but data use is restricted	Performance or optimisation may be impaired	High compliance and value risk	Amend data terms, minimise data, rebuild model or adjust value

Contract interpretation and transfer mechanics require qualified legal advice.

10. Prioritise consents by value and critical path

Consent management should prioritise economic materiality, operational dependency and lead time. A simple count of obtained consents can mislead when the remaining contracts represent most EBITDA or contain the longest notice periods. The tracker should show revenue, margin, service dependency, consent route, counterparty, owner, request date, conditions and fall-back plan.

The seller should decide when to approach customers with regard to confidentiality, competition and deal certainty. The buyer should prepare a credible continuity narrative and avoid promising capabilities that depend on untested separation. Material amendments sought by customers should be quantified and approved before acceptance.

The sale agreement can address missing consents through conditions, delayed transfer, agency arrangements, economic pass-through, price retention, escrow or specific indemnity. Each method has legal, tax, accounting and operational consequences. The chosen response should match the customer's value and the time needed to obtain a durable solution.

11. Assess supplier and subcontractor continuity

Road freight commonly relies on vehicle lessors, fuel-card providers, maintenance networks, tyre suppliers, subcontracted carriers, warehouse operators, map and traffic-data providers, telecommunications, payment services and insurance. Supplier dependencies can be as critical as customer contracts because a failure can interrupt the entire service chain.

The buyer should test assignment, minimum commitment, credit support, pricing tiers, volume rebates, data rights, audit rights and termination. Group purchasing power may not transfer. A new standalone entity can face higher unit costs, reduced credit limits or collateral requirements. These effects belong in standalone EBITDA and working-capital analysis.

Subcontractor diligence should include operator credentials, insurance, safety, cyber access, data processing and customer approval. The buyer needs the right to supervise and replace providers. Where a seller remains the contractual counterparty during transition, the TSA should state authority, liability, payment flow and the route to direct contracting.

12. Identify people and TUPE consequences

The people perimeter should map roles to capabilities and systems. Routing engineers, transport planners, dispatchers, depot managers, fleet compliance specialists, pricing analysts, customer teams, finance staff and cyber personnel may support both the carved-out business and retained operations. Organisational charts alone do not reveal actual time allocation or critical knowledge.

TUPE may protect employees when a UK business transfers. Government guidance states that employment terms and continuity generally transfer, subject to the applicable facts and exceptions [13-16]. The outgoing employer must provide specified employee-liability information, and consultation obligations can apply before transfer [14-16]. Qualified employment counsel should determine the affected population and process.

The buyer should plan for roles that do not transfer but remain essential. Options include recruitment, secondment, retention, knowledge transfer and managed service. The plan should distinguish temporary capacity from permanent capability. Named-person dependencies require a succession response rather than an assumption that individuals will remain.

13. Confirm transport licensing and compliance

The operating model should identify every operator licence, transport manager, vehicle base, maintenance arrangement, driver process, safety system and regulatory record required to continue operating. A licence held by the seller or another group entity may not be available to the buyer at completion. Vehicle movement without the correct authority can destroy the Day One plan.

Compliance diligence should cover vehicle roadworthiness, inspections, defects, driver hours, tachograph records, dangerous goods where relevant, permits, insurance and subcontractor controls. The buyer should reconcile fleets across asset registers, licensing records, telematics and maintenance systems. Exceptions should be assigned to remedy, exclusion or pricing.

Regulatory readiness belongs in the completion evidence. The buyer should have accepted applications, responsible managers, insurance, maintenance providers, operating centres and system access in place to the extent required. Any reliance on seller licences or staff should be reviewed by counsel and the regulator rather than assumed under a commercial TSA.

14. Screen competition and national-security issues

The CMA's merger guidance requires a case-specific assessment of whether a transaction may substantially lessen competition [1-4]. In technology-enabled freight, relevant issues can include customer access, capacity concentration, commercially sensitive data, routing algorithms and foreclosure. The 2026 guidance specifically recognises that access to rival information, including pricing strategies, algorithms and technical specifications, can affect competition [2].

The clean-team design should therefore restrict access to competitively sensitive customer, lane, price and capacity information before clearance. The separation plan should preserve independent decision-making when interim measures apply. Integration activity should follow legal advice and the applicable CMA process.

The National Security and Investment regime can be relevant where an acquired entity undertakes specified activities in transport, AI, data infrastructure, advanced robotics or other mandatory sectors [17-18]. Asset acquisitions are treated differently from entity acquisitions for mandatory notification, although call-in powers can still matter [18]. The parties should screen the actual target and technology early.

15. Protect cyber security through separation

Carve-outs create privileged-access changes, duplicated environments, temporary interfaces and compressed timelines. These conditions increase cyber risk. The NCSC advises boards to consider cyber risk in mergers, acquisitions, suppliers and partnerships and to identify access, sensitive data and security requirements across those relationships [22-23].

The programme should maintain an identity and access register covering employees, vendors, service accounts, application keys, certificates, devices and administrative privileges. Access should follow the target operating model and be revoked at defined milestones. Shared credentials and undocumented integrations should be treated as separation defects.

The buyer should test incident detection, logging, backups, vulnerability management and recovery in the separated environment. The TSA needs cyber-notification, cooperation, evidence preservation and audit provisions. A legal right to receive a system is insufficient if the buyer cannot detect compromise or recover service.

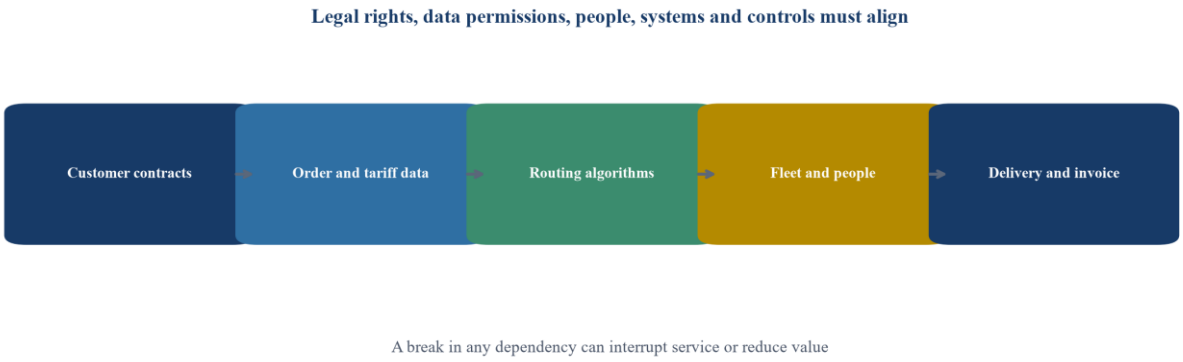
16. Design the target technology architecture

The target architecture should show applications, data stores, interfaces, infrastructure, identities, networks, vendors and owners for every critical capability. It should distinguish Day One from the final state. A temporary replicated environment can be acceptable when it is secure, supported and tied to an executable exit plan.

The architecture decision should compare clone, migrate, replace, retain and consume-as-a-service options. Clone can preserve functionality but duplicate technical debt. Replacement can improve the platform but increases delivery risk. A licence to use the seller's service may accelerate completion while creating dependency and information-separation issues.

Acceptance criteria should be operational. The buyer should demonstrate order intake, route calculation, dispatch, tracking, exception management, proof of delivery, invoicing and management reporting using representative data. Interface success alone does not prove that the end-to-end service works.

Figure 1. Freight carve-out dependency architecture



The architecture is a decision framework and does not represent an identified company.

17. Create the data-separation plan

The data plan should classify records as transfer, copy, retain, delete, anonymise, aggregate or provide under transitional access. Rules should operate at dataset and field level where customer, employee and retained-business information coexist. The plan should preserve referential integrity so transferred orders, journeys, invoices and claims remain usable.

Extraction should be repeatable from a defined cut-off with controlled deltas between test, signing and completion. Reconciliations should compare record counts, control totals and economic balances. Samples should trace from customer contract through route, delivery and invoice to cash collection.

Deletion and access termination are part of acceptance. The seller should prove that buyer-only data is removed from retained environments subject to legal-retention obligations, and the buyer should remove seller data outside the agreed perimeter. Exceptions require an owner, lawful basis, security control and expiry.

18. Separate models, parameters and operational judgement

Routing performance often depends on more than an algorithm. Dispatchers may apply local restrictions, customer preferences, loading rules, driver knowledge and exception judgement that are absent from the

code. The buyer should capture these operating rules and determine which are contractual, regulatory, technical or experiential.

Model parameters and training data should be versioned and linked to the relevant service. The team should test whether the transferred model reproduces expected routes and service levels in the buyer environment. Differences should be explained through data, configuration or infrastructure rather than accepted as unexplained variance.

Human decision rights should remain explicit. Automation can recommend routes, prices or capacity, while authorised staff approve exceptions and safety-critical decisions. The separation should preserve escalation, override records and accountability. A model that cannot be governed after transfer is not a complete operating asset.

19. Define the transition-services agreement

The TSA should be a service contract linked to the dependency register. Each service needs a scope, user population, operating window, capacity, data boundary, service level, security control, charge, change process, remedy, exit dependency and termination date. Broad labels such as “IT support” or “finance services” create disputes and weak exit accountability.

Charges should distinguish cost recovery, pass-through costs, one-off separation work and volume-dependent pricing. The buyer should model both TSA cost and the cost of the target replacement. A low monthly TSA fee can conceal an expensive exit if documentation, licences or people are withheld.

The parties should establish service governance, incident escalation and evidence requirements before completion. Critical services need continuity and recovery obligations. The TSA should not give either party uncontrolled access to the other’s commercially sensitive information.

20. Make TSA exit measurable

Every TSA service should have an exit criterion that can be tested. Examples include successful data migration, buyer acceptance of interfaces, completion of parallel runs, receipt of third-party consents, transfer of licences, user training and recovery testing. Calendar expiry alone does not establish readiness.

The exit plan should identify the longest critical path and the dependencies among services. Routing may depend on telematics, identity, map data and customer interfaces. Exiting hosting before those dependencies are ready can interrupt operations. Sequencing should follow capability rather than organisational convenience.

Readiness reviews should use evidence and named decision rights. Waivers should state risk, duration, mitigation and accountable approver. Extension pricing can increase over time to encourage exit, but it should not create coercive economics where the seller controls essential deliverables.

21. Quantify standalone operating cost

Standalone cost analysis should rebuild the target cost base by capability. Allocated seller charges can be higher or lower than the resources required after separation. The buyer should identify direct costs, transferred employees, replacement hires, vendor contracts, infrastructure, insurance, compliance, public-company or group functions and one-off separation expenditure.

The model should distinguish recurring standalone cost, temporary TSA expense, stranded seller cost, dis-synergy and synergy. These categories have different valuation and negotiation consequences. Seller stranded cost does not automatically belong in target EBITDA, while buyer integration savings should not be used to conceal an incomplete perimeter.

Each adjustment should have an owner, source, timing, confidence and implementation plan. A run-rate claim supported only by a future programme belongs in a separate case from contractual savings already available at completion.

22. Rebuild working capital and cash conversion

Freight working capital can depend on customer billing cycles, fuel cards, subcontractor terms, claims, duties, driver expenses and group treasury. The carve-out model should reconstruct receivables, payables, accrued revenue, deferred revenue, provisions and cash by contract and legal entity.

The buyer should test whether billing and collections can continue independently. Customer master data, tariffs, proof of delivery, tax configuration and bank details must align. A Day One failure in invoice generation can create liquidity pressure even when routes operate successfully.

The sale agreement should define normalised working capital and leakage consistently with the perimeter. Items settled centrally by the seller require a cut-over mechanism. The closing statement should avoid counting cash or liabilities that remain with the seller while transferring the related economic obligation.

23. Value customer relationships and technology separately

IFRS 3 identifies contractual and separable intangible assets that may require recognition apart from goodwill, including customer relationships, technology and contract-based rights [19-21]. Transaction valuation should similarly distinguish the cash flows attributable to customer relationships, routing technology, workforce, brand and physical assets.

The value of a customer relationship depends on enforceable terms, renewal behaviour, margin, service quality, switching cost and consent. The value of routing technology depends on ownership, licence scope, performance, replicability, data access and maintenance capability. Double counting can occur when technology benefits are embedded in customer cash flows and also valued separately.

The valuation should reconcile legal rights to economic benefits. A model may indicate high expected savings, yet a restricted licence or unavailable dataset can prevent their realisation. IFRS 13 fair-value principles and IAS 38 intangible-asset guidance provide relevant accounting concepts, while transaction pricing requires evidence specific to the deal [20-21].

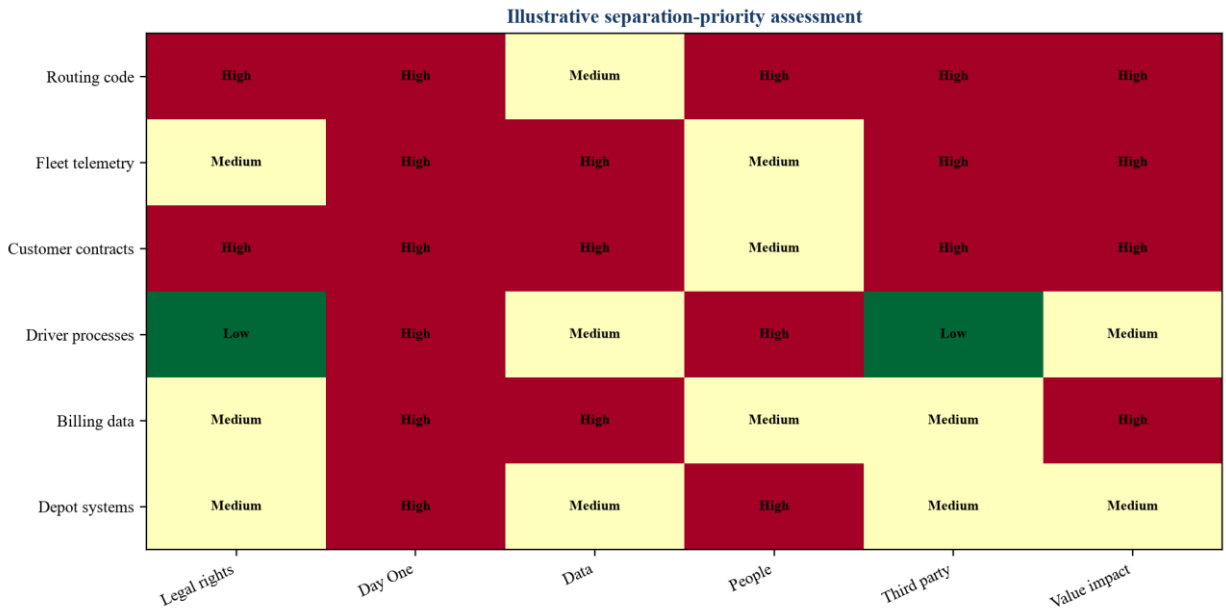
24. Translate dependencies into purchase-price decisions

Every material dependency should affect one or more deal levers: perimeter, price, condition, covenant, indemnity, escrow, retention, earn-out, TSA, licence, service level or termination right. The response should reflect likelihood, value at risk, controllability and duration.

A missing customer consent may justify a delayed transfer or value retention tied to receipt. An algorithm licence restriction may require a durable licence, replacement funding or price reduction. Uncertain data-transfer rights may require clean-room remediation and a limitation on intended use. The mechanism should be executable and measurable.

Price adjustments should avoid false precision. The team should show ranges and scenarios where probability or timing is uncertain. The investment committee needs to understand which value is paid at completion, which depends on future evidence and which remains exposed after contractual protection.

Figure 2. Hypothetical dependency heat map



Scores are management assumptions used to demonstrate prioritisation only.

25. Build the completion evidence pack

The completion pack should prove that the agreed perimeter and conditions are satisfied. It can include executed transfers and novations, IP assignments and licences, employee records, operator-licence evidence, insurance, bank accounts, data-migration reconciliations, access-control reports, TSA schedules and acceptance certificates.

Evidence should be indexed to the sale agreement and dependency register. A status of “complete” should identify the document, approver and date. Screenshots and informal assurances are weak evidence for rights, reconciliations or acceptance.

The buyer should retain post-completion access to evidence needed for audit, tax, claims and regulatory response. The seller should retain only information it is entitled or required to keep. The records protocol should address custody, retrieval, confidentiality and destruction.

26. Prepare Day One operations

Day One planning should cover the first order, first dispatch, first exception, first invoice, first payroll and first incident. Each scenario should have an owner, runbook, contact path and fallback. The buyer should know how to operate if a seller interface is unavailable.

Command-centre metrics should focus on service continuity and control: orders accepted, routes generated, vehicles dispatched, failed messages, proof-of-delivery completion, invoice exceptions, safety incidents, data incidents and customer escalations. Thresholds should trigger action rather than only reporting.

The customer communication plan should identify new legal entities, bank details, portals, contacts, data notices and support channels. Fraud controls are important when bank details change. Communications should be timed with consent and competition advice.

27. Model the illustrative freight division

Consider a hypothetical UK road-freight division operating seven depots with 64 enterprise customers and 1,280 powered and unpowered fleet units. Management reports annual revenue of GBP 420 million and

EBITDA of GBP 38 million. Eighteen material software services support quoting, routing, telematics, dispatch, proof of delivery, billing and reporting.

The routing platform is shared with the seller and includes seller-owned orchestration, third-party mapping, telematics feeds and customer-specific rules. Nine customer contracts require consent or novation; five represent 38 per cent of division EBITDA. Payroll, treasury, procurement, cyber monitoring and finance operate through seller systems.

The scenario assumes that an asset transaction transfers selected fleet, depot rights, employees, customer contracts and operating records. The buyer receives a five-year routing licence and a twelve-month TSA with extension options. All figures are hypothetical management assumptions and do not describe an identified transaction.

Table 3. Hypothetical separation baseline

Measure	Reported position	Evidence-adjusted position	Principal dependency
Revenue	GBP 420m	GBP 397m at risk-adjusted consent case	Customer novations and retention
EBITDA	GBP 38m	GBP 31m maintainable standalone EBITDA	Standalone systems, procurement and central functions
Enterprise customers	64	55 transferable without unresolved material condition	Consent, data rights and capability continuity
Software services	18 material services	7 transfer, 5 licence, 6 TSA or replace	IP ownership, vendor consent and migration
Fleet units	1,280	1,214 verified for transfer at cut-off	Title, lease, condition and operator readiness

Values are management assumptions created to demonstrate the framework.

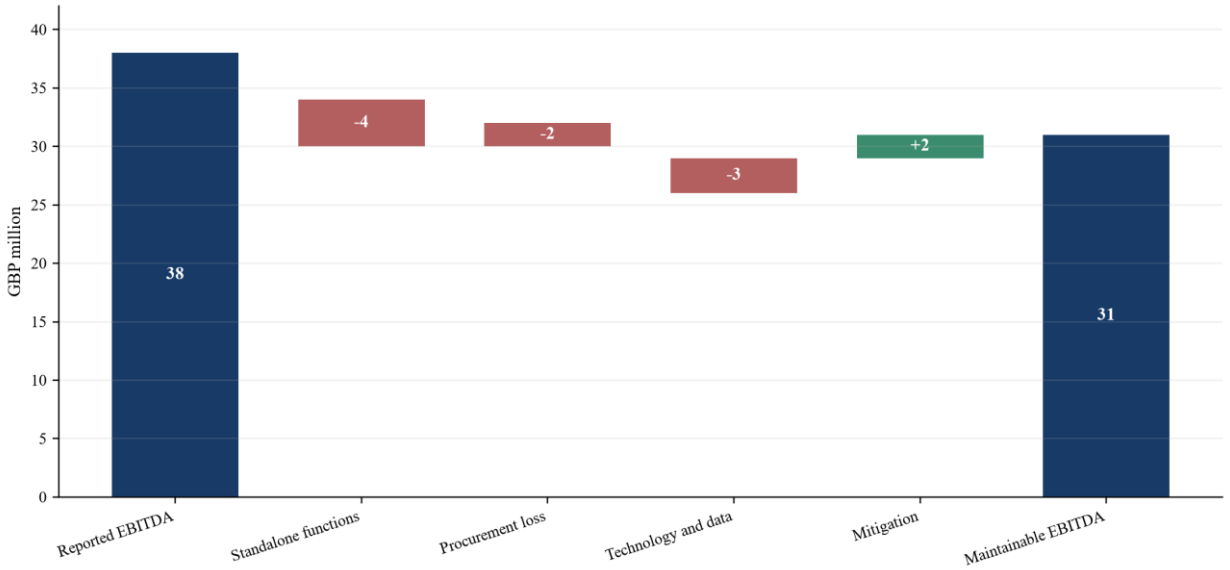
28. Reconcile reported to maintainable EBITDA

The illustrative bridge begins with GBP 38 million of reported EBITDA. It deducts GBP 4 million for unallocated standalone corporate and compliance costs, GBP 2 million for loss of group procurement economics and GBP 3 million for technology, cyber and data capability required outside the TSA. It adds GBP 2 million of identified, executable operating mitigation. Maintainable standalone EBITDA is therefore GBP 31 million.

TSA charges are modelled separately from recurring cost because they expire as target capabilities are delivered. One-off separation expenditure is also separate. The investment case should show the cash profile, rather than capitalising all transition cost or embedding temporary charges indefinitely.

The bridge is a management scenario. Actual treatment depends on the perimeter, accounting policies, evidence and contractual outcomes. Each adjustment should be reconciled to roles, systems, vendors or contracts in the dependency register.

Figure 3. Hypothetical standalone EBITDA bridge



Amounts are management assumptions in GBP million and are not observed company results.

29. Test price under separation scenarios

The hypothetical headline enterprise value is GBP 285 million. The central executable case deducts GBP 18 million for the restricted algorithm-rights package, GBP 22 million for customer-consent and attrition exposure, GBP 9 million for data remediation and GBP 12 million for separation expenditure. It adds GBP 15 million for mitigations supported by executed licences, customer evidence and a funded build plan, producing an illustrative value of GBP 239 million.

The downside case assumes delayed consent for two major customers, a six-month TSA extension and slower replacement of the routing platform. Maintainable EBITDA falls to GBP 27 million and value to GBP 205 million. The protected case uses completion conditions, contract-linked retention and seller-funded remediation to preserve GBP 252 million, subject to delivery.

These values do not constitute a valuation opinion. They demonstrate how perimeter evidence can affect price, deferred consideration and protection. The investment committee should view value together with cash outflow, completion probability and residual exposure.

Table 4. Hypothetical separation scenarios and deal response

Scenario	Maintainable EBITDA	Illustrative enterprise value	Principal response
Central executable case	31	239	Licence, consent plan, funded separation and measured TSA exit
Downside delay case	27	205	Price reduction, greater retention and extended liquidity plan
Protected completion case	31	252	Conditions, customer-linked retention and seller-funded remediation
Unresolved perimeter	Not reliably measurable	Defer decision	Do not rely on headline value until rights and capability are evidenced

Values are management assumptions in GBP million and are not a fairness or valuation opinion.

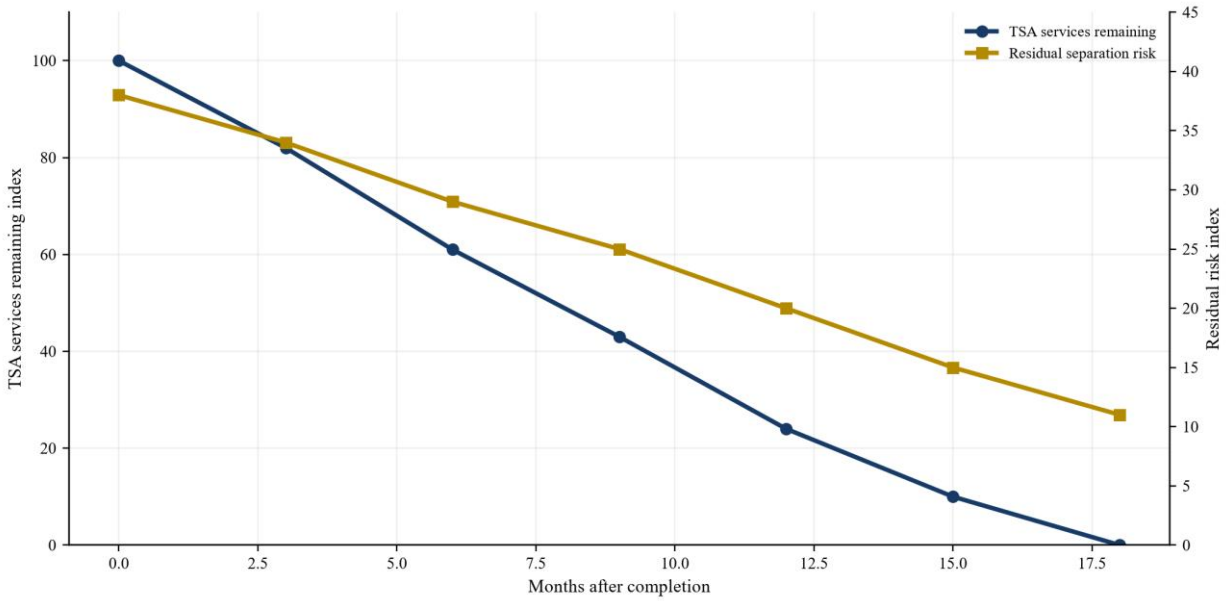
30. Reverse-stress the Day One plan

Reverse stress asks which failure causes the transaction thesis to break. For the illustrative case, the critical failures are loss of routing rights, non-transfer of the two largest customers, inability to lawfully use historical fleet data, delay in operator readiness and failure of the seller-hosted billing interface.

The team should model combinations rather than isolated issues. A routing delay can reduce service quality and trigger customer termination, while invoice failure increases working-capital needs. Correlation matters because multiple dependencies may share the same seller platform or specialist employees.

The board should define boundaries for price, timing and residual risk. If a failure cannot be prevented or protected contractually, the response may be to change the perimeter, defer completion or stop the transaction. Reverse stress turns operational evidence into an explicit investment decision.

Figure 4. Hypothetical TSA exit and residual-risk profile



Indices are management assumptions and demonstrate governance of transition only.

31. Establish post-completion governance

The separation governance body should own dependencies, customer consents, TSA performance, cyber incidents, data migration, cost, value and risk. It should include transaction, operations, technology, finance, legal, people and customer leaders with explicit decision rights.

Reporting should distinguish fact, management assumption, professional judgement and unresolved evidence. Measures should include service availability, customer retention, order and invoice exceptions, migration reconciliation, access closure, TSA exit, spend, standalone EBITDA and value protection.

Changes should follow a controlled process. A proposed extension, design change or scope transfer should state cost, timing, security, data, customer and value consequences. The closing baseline enables the board to see whether the thesis is being delivered or deferred.

32. Design the first 100 days

The first 100 days should stabilise service, close evidence gaps and accelerate exit from the highest-risk seller dependencies. The plan should prioritise customer continuity, regulatory compliance, cyber access, cash collection, data control and critical-person retention before discretionary transformation.

Workstreams should have measurable milestones. Examples include completing priority novations, validating fleet title and condition, moving privileged identities, reconciling opening data, parallel-running billing, transferring vendor contracts and accepting the target routing environment.

Value creation should remain linked to the transaction thesis. Route-density improvement, empty-mile reduction, customer repricing and fleet utilisation can follow once baseline controls are stable. Benefits should be measured against the evidence-adjusted closing baseline.

33. Recognise limitations

The framework does not determine the legal effectiveness of an assignment, the application of TUPE, the lawful basis for data processing, CMA jurisdiction, NSI notification, accounting classification, tax treatment, operator licensing or fair value. Those conclusions require current transaction-specific evidence and qualified professional advice.

Routing performance can change with customer mix, traffic, weather, network constraints, driver behaviour and data quality. Historical results may not reproduce in the buyer environment. The buyer should validate models and operations before relying on projected efficiencies.

The illustrative division, EBITDA, value, consents, systems and scenarios are hypothetical. They should not be attributed to an identified company. Commercial demand for an advisory mandate and resulting fees remain unverified until supported by executed and paid engagement evidence.

34. Conclude the carve-out case

A UK freight carve-out is executable when the buyer can prove that the transferred rights and capabilities support the customer promise on Day One and after TSA exit. Vehicles and contracts are necessary, while algorithms, data rights, people, licences, systems and controls determine whether those assets operate as a business.

The dependency register should connect diligence to transaction documents, separation design and value. Customer consents, IP rights, data permissions, operator readiness and cyber controls deserve the same investment-committee attention as EBITDA and purchase price.

The transaction should proceed when the perimeter is legally coherent, operationally tested, financially reconciled and protected against material gaps. A buyer that can trace every critical service from contract through route, delivery, invoice and cash has a defensible basis for price and execution. A seller using the same evidence can reduce uncertainty, protect value and shorten the path to completion.

Frequently asked questions

What is the first question in a UK freight carve-out?

The first question is whether the proposed perimeter can deliver the contracted customer service independently. The answer requires evidence across contracts, routing technology, fleet data, people, licences, depots, systems and regulatory controls.

Does ownership of routing source code make the capability transferable?

No. The buyer may also need third-party solvers, map and traffic licences, model parameters, data, deployment pipelines, credentials, documentation and skilled people. The relevant rights and operating components should be tested together.

Can fleet and driver data simply be copied to the buyer?

The parties must establish ownership, contractual rights, controller and processor roles, lawful purpose, transparency, security, minimisation, retention and deletion. The ICO identifies data sharing as a specific M&A due-diligence requirement.

How should customer consents affect value?

Material consents should be linked to revenue, margin, service dependency and timing. Missing consent can support a completion condition, delayed transfer, retention, escrow, price adjustment or another transaction-specific protection.

What makes a transition-services agreement effective?

Each service needs a precise scope, service level, data boundary, charge, security control, remedy, exit dependency and measurable acceptance test. The TSA should use the same dependency register as the separation plan.

How should standalone EBITDA be calculated?

Rebuild cost by capability and distinguish recurring standalone cost, temporary TSA charges, one-off separation expenditure, seller stranded cost, dis-synergy and buyer synergy. Each adjustment should be supported by an executable operating plan.

When can AI or routing technology trigger UK national-security review?

The NSI regime can apply when an acquired entity conducts specified activities in areas including AI, transport, data infrastructure or advanced robotics. The precise application depends on the entity, activity and control acquired, so qualified advice is required.

Is the illustrative transaction a valuation opinion?

No. All financial and operating figures are hypothetical management assumptions used to demonstrate the framework. An actual transaction requires verified data and qualified legal, tax, accounting, valuation, technology, employment, cyber and regulatory advice.

References

[1] Competition and Markets Authority, Merger assessment guidelines, updated 3 September 2026. https://www.gov.uk/government/publications/merger-assessment-guidelines

[2] Competition and Markets Authority, Merger assessment guidelines, HTML version, updated 3 September 2026. https://www.gov.uk/government/publications/merger-assessment-guidelines/merger-assessment-guidelines-html-version

[3] Competition and Markets Authority, Mergers: how they are investigated, updated 23 June 2025. https://www.gov.uk/government/publications/mergers-how-they-are-investigated/mergers-how-they-are-investigated

[4] Competition and Markets Authority, Mergers charter, 12 March 2025. https://www.gov.uk/government/publications/mergers-charter-how-to-work-with-the-cma-on-a-merger-investigation/mergers-charter

[5] Information Commissioner's Office, Due diligence when sharing data following mergers and acquisitions. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/due-diligence/

[6] Information Commissioner's Office, Data sharing: a code of practice. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/

[7] UK Parliament, Data (Use and Access) Act 2025. https://www.legislation.gov.uk/ukpga/2025/18/contents

[8] Intellectual Property Office, Licensing intellectual property, updated 1 April 2026. https://www.gov.uk/guidance/licensing-intellectual-property

[9] Government Office for Technology Transfer, KAM Guide: Intellectual property management. https://www.gov.uk/government/publications/knowledge-asset-management-kam-hub/kam-guide-intellectual-property-management

[10] Government Office for Technology Transfer, KAM Guide: IP in agreements. https://www.gov.uk/government/publications/knowledge-asset-management-kam-hub/kam-guide-ip-in-agreements

[11] HM Revenue and Customs, Software licensing standard, updated 21 March 2025. https://engineering.hmrc.gov.uk/standards/software-licensing/

[12] Intellectual Property Office, Sui generis database rights. https://www.gov.uk/guidance/sui-generis-database-rights

[13] UK Government, Business transfers, takeovers and TUPE: overview. https://www.gov.uk/transfers-takeovers

[14] UK Government, Business transfers, takeovers and TUPE: information about employees during transfers. https://www.gov.uk/transfers-takeovers/information-about-employees-during-transfers

[15] UK Government, Business transfers, takeovers and TUPE: transfers of employment contracts. https://www.gov.uk/transfers-takeovers/transfers-of-employment-contracts

[16] UK Government, Business transfers, takeovers and TUPE: consulting and informing. https://www.gov.uk/transfers-takeovers/consulting-and-informing

[17] Cabinet Office, National Security and Investment Act: details of the 17 types of notifiable acquisitions. https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions/national-security-and-investment-act-guidance-on-notifiable-acquisitions

[18] Cabinet Office, The National Security and Investment Act alongside regulatory requirements. https://www.gov.uk/government/publications/the-national-security-and-investment-act-alongside-regulatory-requirements/the-national-security-and-investment-act-alongside-regulatory-requirements

[19] IFRS Foundation, IFRS 3 Business Combinations. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/

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

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

[22] National Cyber Security Centre, Cyber Security Toolkit for Boards. https://www.ncsc.gov.uk/collection/board-toolkit

[23] National Cyber Security Centre, Assessing supply chain cyber security. https://www.ncsc.gov.uk/collection/supply-chain-security/assessing-supply-chain-security

[24] Driver and Vehicle Standards Agency, Guide to maintaining roadworthiness. https://www.gov.uk/government/publications/guide-to-maintaining-roadworthiness

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.