UK Utilities Carve-Outs: Separating Digital Twins, Operational Data and Regulated Assets

A transaction framework for perimeter design, operational continuity, regulatory control and transition-service exit

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

A UK utility carve-out can transfer pipes, wires, substations, treatment works, licences and employees while leaving the operating capability behind. Modern utility operations depend on operational technology, sensor histories, engineering models, digital twins, cloud services, data rights, cyber controls and group-wide support functions. These elements often cross the legal and regulatory perimeter proposed for sale. If the separation plan treats them as ordinary information-technology assets, the buyer may receive a regulated business that cannot safely operate, report or invest without the seller.

This paper develops a Utility Carve-Out Control Framework for boards, sponsors, strategic buyers, regulated utilities, lenders and advisers. It places the data, systems and model perimeter alongside physical assets, people, contracts, licences and financing. The method starts with the statutory and licence perimeter. It then maps each essential service to the physical asset, operational process, data source, model, decision right, accountable role and third-party dependency required to deliver it. The resulting evidence controls diligence, valuation, transaction documents, transition-service agreements, Day 1 readiness and the path to operational independence.

The framework distinguishes a digital twin from a visual model or asset register. A digital twin remains tied to a specific physical counterpart, operates within a stated validation envelope and uses two-way data flows appropriate to the decision. That dependency creates separation questions about telemetry, model ownership, interfaces, calibration history, cyber access, safety approval and post-completion accountability. The buyer needs enough rights and capability to operate the transferred asset safely from Day 1 and to maintain the model after the transition period.

The worked case is wholly hypothetical. A seller proposes to carve out a regional regulated utility platform at an enterprise value of GBP 1.80 billion. The proposed perimeter contains GBP 1.15 billion of regulatory asset value, GBP 120 million of identified digital and operational-technology assets, GBP 84 million of separation expenditure, GBP 32 million of stranded seller cost, GBP 18 million of transition-service charges and a GBP 65 million buyer risk adjustment before remediation. The model compares three separation designs and shows how data rights, model validation, cyber assurance and transition-service exit affect value. Every amount, percentage, date and result in the case is a hypothetical management assumption. The case is not observed transaction data, a valuation, legal advice, regulatory advice, cyber assurance, tax advice or investment advice.

JEL Classification: G34, L94, L95, L97, K23, K24, M15, O32

Keywords: UK utilities, carve-out, digital twin, operational technology, regulated assets, operational data, transition services, M&A, cyber resilience, regulatory ring-fence

1. Define the transaction decision

The board decision is whether a specified utility business can transfer to a buyer with a complete and independently operable perimeter at an agreed value, risk allocation and timetable. The answer requires evidence about the regulated service, the assets that deliver it and the systems that control those assets. A legal-entity boundary or fixed-asset register is an incomplete starting point when operating data, applications and specialist teams are shared across a group.

The decision should allow four outcomes: proceed with the proposed perimeter, enlarge the perimeter, redesign the transition architecture, or defer signing until a material dependency is resolved. Each unresolved dependency needs an owner, closing consequence and quantified value effect. A generic undertaking to provide reasonable assistance after completion gives a buyer little protection when a model, licence or cyber dependency is essential to service continuity.

The CMA states that a carve-out package used as a merger remedy must contain the assets, functions and capabilities needed for the purchaser to operate successfully and compete effectively [1,2]. The same operational logic applies to a voluntary utility carve-out. The transaction team should test whether the buyer receives a functioning business rather than a collection of assets.

Table 1. Utility carve-out decision framework

Decision area	Evidence required	Separation question	Approval condition
Regulated perimeter	Licences, appointments, price-control records and regulatory correspondence	Which entity, assets, obligations and revenues must remain together?	Regulator-tested perimeter and responsibility map
Operating capability	Service map, asset register, process inventory and accountable roles	Can the buyer deliver the essential service safely on Day 1?	Signed Day 1 operating model
Data and models	Lineage, rights, retention, interfaces and validation records	Can the buyer lawfully use and maintain every required dataset and model?	Transferable rights and tested data products
Technology and cyber	OT inventory, architecture, identities, suppliers and assurance evidence	Does separation preserve resilience while removing seller access?	Approved cyber separation plan
Economics	Carve-out accounts, RAV bridge, capex, opex, TSAs and stranded costs	Does price reflect standalone cost and remediation?	Board-approved value bridge
Execution	Critical path, approvals, migration tests and cutover plan	Can dependencies exit within the agreed timetable?	Gated closing and exit milestones

Original framework. Requirements vary by sector, licence, transaction structure and regulatory direction.

2. Start with the regulated service

The perimeter should begin with the service that the licensed or appointed entity must provide. Electricity and gas networks operate under sector licences and price controls. Water undertakers operate under instruments of appointment. Those frameworks assign obligations, information duties, financial protections and customer outcomes to defined entities [14-18]. A separation plan should map each obligation to the assets, people, data and decisions needed to discharge it.

This service-first approach avoids two common errors. The seller may assume that an application is a group service because the contract sits at parent level, even though the regulated entity cannot operate without it. The buyer may assume that ownership of a substation, treatment works or network

automatically includes the telemetry, engineering model and historical records required to manage it. Neither assumption establishes an operable perimeter.

The evidence room should contain a regulatory obligation register. Each entry should identify the source obligation, accountable entity, operational process, supporting technology, data inputs, reporting output and proposed treatment at completion. A regulator may require notification, consent, licence modification or assurance. Legal advice should confirm the applicable process for the actual transaction.

3. Map the legal and regulatory perimeter

The legal perimeter identifies shares, assets, contracts, licences, permits, land rights, intellectual property and employees proposed for transfer. The regulatory perimeter identifies the obligations and protections that must remain effective. The operating perimeter identifies what the business actually needs. A robust carve-out reconciles all three rather than treating the legal schedule as the complete answer.

Utility ring-fences add constraints. Ofwat licence conditions can restrict transactions with owners and associates, require information and protect financial resilience [15,16]. Ofgem's network ring-fence framework seeks legal, financial and operational independence for regulated licensees and restricts cross-subsidisation and asset transfers that could compromise licence obligations [17]. Transaction teams should test intercompany arrangements, shared assets, cash pooling, guarantees, service charges and data access against the relevant conditions.

The National Security and Investment regime may also apply. Government guidance explains how the regime interacts with sector regulation and identifies energy, data infrastructure and other sensitive activities [19-23]. The perimeter assessment should consider the target, acquirer and control being transferred. Notification analysis belongs on the transaction critical path rather than in a late closing checklist.

4. Define regulated assets and associated rights

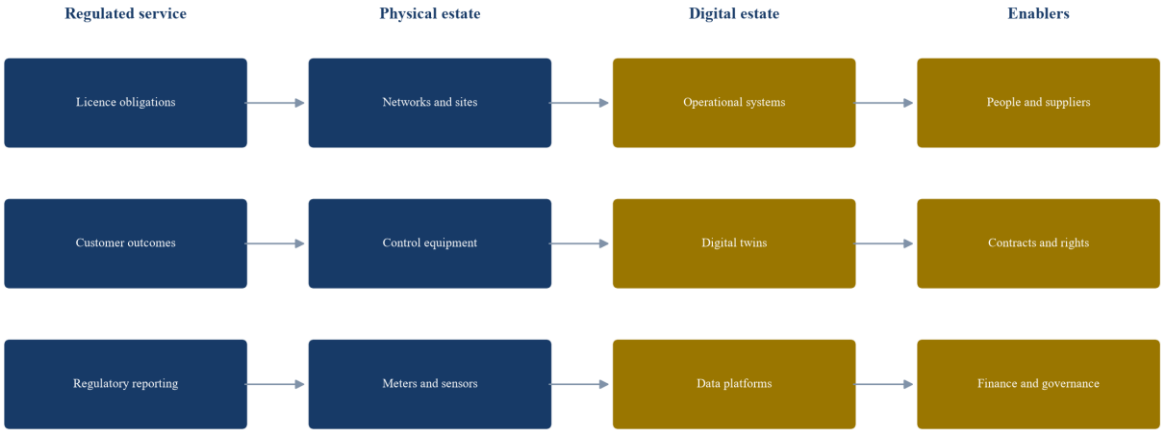
Regulated asset value is a regulatory financial construct rather than a complete operating asset list. Ofgem's reporting explains that RAV reflects accumulated investment under the price-control framework and supports the calculation of allowed returns [18]. A transaction perimeter must also capture assets that carry little accounting value but remain operationally essential, including control logic, network models, configuration records, cyber keys, maintenance histories and specialist tools.

The regulated-asset map should connect each physical asset to ownership, licence treatment, location, condition, regulatory value, accounting value, maintenance duty, telemetry, model representation and operating authority. It should record assets owned by third parties or shared with retained businesses. A right to use can matter more than title when an interface, communications circuit or software licence supports continuous service.

The map should also identify assets that cannot transfer without consent, novation, licence modification or technical reconfiguration. The separation team should avoid a binary transfer-versus-retain classification. Some items require duplication, transitional access, escrow, substitution or a new operating agreement. Those treatments need costs, dates and failure consequences.

Figure 1. Proposed utility carve-out perimeter map

A service-led perimeter connects regulation, assets, data and capability



Original framework. The nodes and connections are illustrative and do not describe an actual utility or transaction.

5. Treat the digital twin as an operating capability

The UK government's 2025 definition requires a digital twin to remain tied to a real-world counterpart, use a two-way data flow, operate within a stated validation envelope and carry an assumption set [5]. A static three-dimensional model, dashboard or asset register may support the business, but it does not meet that definition by itself. The distinction matters because a true twin depends on live interfaces, calibration, data quality and governance after completion.

The separation inventory should describe the physical counterpart, purpose, owner, users, source data, output decisions, update frequency, validation envelope, assumptions, model version, software stack and fallback process for each twin. It should identify whether the model only advises operators or sends instructions back to the physical system. A model that influences control settings, maintenance intervals or safety decisions requires stronger assurance than a visual planning tool.

National Digital Twin Programme principles emphasise security, trustworthiness, adaptability and interoperability [6,7]. Transaction documents should therefore address provenance, validation, change control and lifecycle support. Delivery of source code without telemetry rights, model documentation or skilled operators may leave the buyer with an unusable artefact.

6. Build the data-lineage map

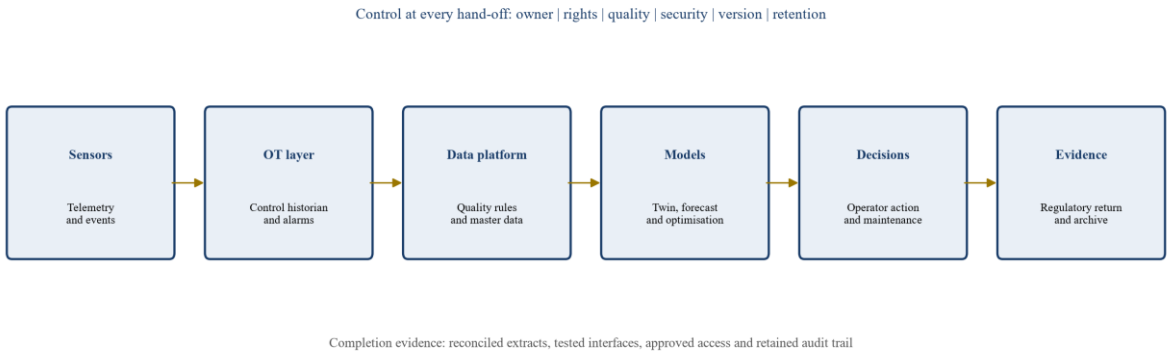
Operational data should be traced from sensor or source record to each system, transformation, model, decision, regulatory report and archive. The map should show owner, controller, processor, licence, retention period, security classification, quality rule and permitted use. It should also identify group data lakes, shared master data, manual spreadsheets and third-party feeds that sit outside the proposed legal perimeter.

Ofgem's Data Best Practice guidance treats data as an asset that should be discoverable, interoperable and governed under licence obligations [3,4]. Ofwat describes data, together with the people, processes and technology that support it, as an important asset for the water sector [14]. These policies support a separation design in which data products have clear ownership, standards and accountability.

Lineage should reach the decision layer. If a leakage model, outage forecast or network simulation uses a derived feature, the buyer needs the transformation logic and historical version. If a regulatory return

draws from a data mart, the separation plan should preserve reconciliation to source. A simple database export rarely meets these needs.

Figure 2. Proposed operational-data lineage for separation



Original framework. The flow shows the controls required to transfer data into an independently governed buyer environment.

7. Allocate data rights and responsibilities

The seller may own a database while lacking unrestricted rights to transfer every record. Customer information, employee data, licensed geospatial data, vendor feeds and jointly created engineering records can carry different restrictions. The buyer needs a record-level or dataset-level rights analysis for material data products. The analysis should cover ownership, database rights, confidentiality, privacy, contractual restrictions and post-completion use by both parties.

The ICO's data-sharing code states that a merger or acquisition involving a change of controller requires due diligence on the original purpose, lawful basis, changed use, transparency, governance and security [8]. A disclosure in the transaction data room does not establish permission for operational migration. The parties should define which personal data transfers at signing, completion and TSA exit, and how data-subject rights and retention obligations will be handled.

Shared historical data may support both the sold and retained businesses. The parties should choose among transfer, duplication, clean-room access, aggregation, anonymisation or continued service. The chosen treatment should preserve regulatory evidence while limiting use to agreed purposes.

8. Separate operational technology safely

Operational technology includes the hardware and software that monitors or controls physical processes. In a utility, it can include supervisory control and data acquisition, distributed control, telemetry, protection, remote terminal units, engineering workstations and safety systems. Separation changes identities, networks, supplier access and responsibilities around systems that support essential services.

The NCSC Cyber Assessment Framework provides a structured basis for assessing cyber security and resilience [9]. Its operational-technology guidance recognises the distinctive safety, availability and lifecycle constraints of these systems [10]. Ofgem's 2026 NIS guidance requires operators to identify the systems, components, interfaces, people and third parties on which the essential service depends and to manage security throughout the engineering lifecycle [11,12].

The separation plan should classify each connection as transfer, duplicate, isolate, replace or retire. It should specify the final identity authority, privileged-access model, remote-support route, monitoring, incident response and recovery responsibility. Cutover should be rehearsed in a representative

environment. A buyer should not discover after completion that a retained seller account remains the only route to a critical controller.

9. Preserve essential-service continuity

Continuity is the primary operating constraint. The NIS Regulations apply to essential services in energy and water and require appropriate security and incident-management measures [11-13,24]. A transaction cannot treat a prolonged outage as an acceptable migration failure. Every cutover plan needs a safe fallback and a defined decision authority.

The business should decompose each essential service into minimum viable operating capabilities. For each capability, the team should identify the maximum tolerable disruption, manual fallback, data recovery point, cyber controls, staffing, supplier support and regulatory notification path. These requirements become acceptance criteria for separation tests.

Day 1 readiness should be evidenced through scenario tests rather than status reporting alone. Tests should cover loss of seller connectivity, failure of migrated interfaces, compromised credentials, corrupt telemetry, supplier unavailability and delayed regulatory approval. The board should receive unresolved critical findings and the specific mitigations required before completion.

10. Validate models before and after transfer

A model can produce technically plausible outputs while depending on undocumented preprocessing, stale calibration or unavailable data. The model inventory should record purpose, decision owner, inputs, outputs, training or calibration period, validation method, performance limits, change history, override process and fallback. Digital twins require additional evidence about the physical counterpart and validation envelope [5].

The separation team should run three tests. Reproduction confirms that the buyer can generate the same output from the agreed inputs. Portability confirms that the model operates in the buyer environment with permitted data and licences. Operational validation confirms that qualified users can interpret the output and recognise conditions outside the model's limits. Passing one test does not prove the others.

Where machine learning is used, the parties should preserve feature definitions, evaluation data, monitoring thresholds and human accountability. OECD AI principles emphasise transparency, robustness and accountability [26]. Transaction documents should identify who bears the cost and risk if a transferred model cannot be validated in the buyer environment.

11. Allocate intellectual property and software licences

The digital estate can include proprietary models, configuration, scripts, interfaces, vendor software, open-source components and group-developed platforms. Ownership and the right to operate are separate questions. A seller may own custom code while a third-party licence restricts assignment. A buyer may receive a perpetual licence but lack the tools or knowledge needed to maintain the system.

The intellectual-property schedule should link each right to the systems and processes it supports. It should identify source-code availability, object-code rights, documentation, derivative-work rights, data rights, maintenance obligations, escrow and territorial limits. The schedule should also record open-source obligations and any components whose terms require source disclosure or restrict commercial use.

Software contracts should be reviewed for assignment, change of control, user metrics, hosting, data export, audit rights, support and termination. A temporary seller licence can support Day 1, but the TSA should contain a funded replacement path and a realistic exit date.

12. Design the transition service architecture

A TSA buys time to complete separation. It should not hide an undefined target operating model. Each service needs scope, volumes, service levels, security rules, charging, change control, liability, data treatment, exit assistance and a named owner on both sides. The service catalogue should separate critical operations from convenience services.

Dependencies should be mapped at application and process level. An operational dashboard may rely on group identity management, a shared data lake, vendor support, telecommunications and a retained analytics team. The TSA should specify how each dependency will transfer or be replaced. A single end date for the entire catalogue can create either excessive cost or premature exit.

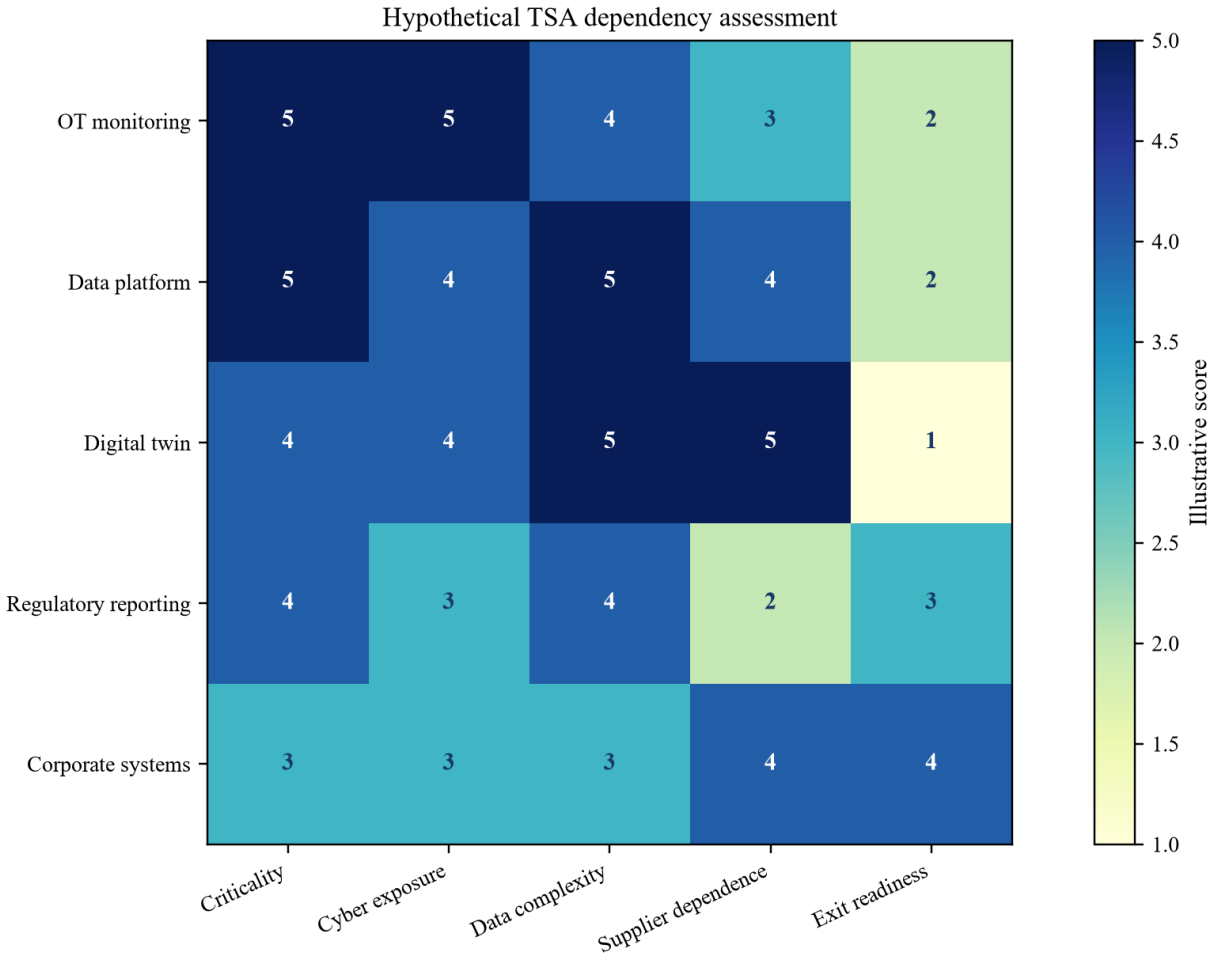
The buyer should define objective exit criteria: migrated data reconciled, interfaces tested, users trained, suppliers contracted, cyber controls approved, regulatory reports produced and service continuity demonstrated. Exit should be governed through evidence and acceptance, with escalation for missed dependencies.

Table 2. Transition-service design matrix

Service	Operational criticality	Proposed term	Principal exit evidence	Failure response
OT monitoring and incident support	Critical	12 months	Buyer monitoring centre passes resilience test	Extend only the affected service with remediation plan
Data-platform hosting and feeds	Critical	15 months	Reconciled migration and lineage approval	Parallel run and controlled rollback
Digital-twin platform and model support	High	18 months	Portable model, validated outputs and trained owner	Escrow support and funded replacement
Regulatory reporting	High	Two reporting cycles	Buyer produces accepted return from source records	Seller review under controlled access
Finance, HR and procurement	Medium	6 to 9 months	Standalone systems and supplier controls live	Short extension subject to step-up pricing

Original framework. Timing and controls are hypothetical and require transaction-specific confirmation.

Figure 3. Hypothetical transition-service dependency and exit matrix



Hypothetical scores from one to five. They illustrate prioritisation and are not observed performance data.

13. Build standalone cyber governance

Cyber separation is a governance change as well as a technical migration. The buyer becomes accountable for risk acceptance, incident decisions, regulator engagement and supplier oversight. Policies copied from the seller may refer to unavailable teams, tools or escalation paths. The buyer needs a functioning control system that matches its actual organisation.

The governance design should identify the accountable executive, security operations, OT security leadership, data protection role, incident commander and board reporting. It should map controls to the systems in scope and record residual risks. Privileged accounts, certificates, keys, remote-access tools and shared domains require explicit cutover treatment.

The assurance plan should combine design review, configuration evidence, vulnerability management, access testing, recovery exercises and independent challenge. A penetration test alone cannot establish resilience. Where essential-service regulation applies, the team should align evidence to the competent authority's current framework [9,11,24].

14. Create reliable carve-out financials

Historical management accounts often reflect group allocations, shared procurement, central financing and services that change after separation. The buyer needs financial statements that reconcile to the proposed perimeter and a standalone cost model that identifies replacement services, duplicated functions, dis-

synergies and remediation. Regulatory accounts, statutory accounts and transaction carve-out accounts serve different purposes and should be bridged.

The model should separate recurring standalone cost from one-off separation expenditure. It should identify seller stranded cost without assuming that the buyer will reimburse it. It should also distinguish costs already funded through a price control from costs that may require future regulatory treatment. Regulatory value and enterprise value should not be treated as interchangeable.

Each material adjustment needs a source, basis, owner and sensitivity. Data-platform cost, software licences, cyber operations, model support and telecommunications are often dispersed across group budgets. The digital perimeter workstream should feed the financial model rather than operate as a technical appendix.

15. Bridge regulatory value to transaction value

Regulatory asset value can anchor analysis in network transactions because it reflects the regulator's treatment of qualifying investment. Enterprise value also reflects allowed returns, performance, capital requirements, financing, service quality, growth, risk and buyer assumptions. A premium or discount to RAV needs a clear explanation based on expected cash flows and risks.

The carve-out value bridge should show the effect of standalone cost, separation expenditure, TSA charges, stranded-cost negotiations, required capital, pension or environmental obligations, model remediation and cyber risk. It should avoid treating all digital expenditure as value creating. Some spending restores a minimum operating capability and should be assessed as a necessary cost.

The buyer should test whether data and digital capability improve operational outcomes that the regulatory framework rewards. The seller should provide evidence linking a model or platform to service, cost or investment decisions. A technology narrative without measured operational evidence should not support a valuation premium.

Table 3. Hypothetical transaction value bridge

Item	GBP million	Treatment in the worked case
Headline enterprise value	1,800	Starting commercial assumption
Identified regulatory asset value	1,150	Regulatory reference, not a valuation conclusion
Digital and OT assets within perimeter	120	Included subject to rights and operability
Separation expenditure	(84)	Buyer-funded central assumption
TSA charges	(18)	Expected transition cash cost
Buyer risk adjustment before remediation	(65)	Data, model, cyber and exit uncertainty
Potential adjustment after verified remediation	42	Released only after specified evidence

All amounts are hypothetical management assumptions in GBP millions. They do not represent an actual company or valuation.

16. Quantify separation expenditure

Separation expenditure should be estimated from the dependency map. Categories may include data extraction and cleansing, interface development, cloud migration, OT isolation, telecommunications, identity redesign, licences, digital-twin portability, cyber assurance, test environments, parallel running and specialist retention. Each category should have quantities, rates, contingency and timing.

Correlation matters. A delayed identity platform can hold back several applications. A disputed data right can prevent model validation and regulatory reporting. A critical vendor may control both software support and integration capacity. The cost model should preserve these dependencies instead of applying independent contingencies to each line.

Governance should distinguish scope growth from estimate refinement. When diligence reveals an omitted system, the perimeter has changed. When a known migration task receives a firmer quotation, the estimate has improved. Both affect value, but they require different board decisions and contractual protection.

17. Conduct buyer diligence around decisions

Buyer diligence should test the decisions the board and financing parties must make. It should establish whether the perimeter operates, what must be remediated, how long independence takes and how the findings affect value and documents. A questionnaire that produces thousands of files without a dependency model delays these decisions.

The buyer should select end-to-end service journeys for testing. An electricity network case could trace an alarm through telemetry, control, dispatch, incident management, customer communication and regulatory reporting. A water case could trace a quality or leakage event from sensor to operator response, laboratory data, customer impact and regulatory evidence. Each journey exposes cross-functional dependencies.

Red findings should have quantified consequences. Examples include a condition precedent, purchase-price adjustment, escrow, specific indemnity, TSA obligation, remediation covenant or walk-away right. The board should see which findings remain subject to legal, regulatory or technical confirmation.

18. Prepare the seller evidence package

Seller readiness begins with one controlled perimeter model. Legal, finance, operations, digital, cyber, property, tax and people workstreams should use the same asset and dependency identifiers. Separate lists create reconciliation effort and allow material gaps to remain hidden between teams.

The seller should prepare an evidence index linking each claim to an authoritative source. Claims about system independence, data ownership, model accuracy, service cost and separation timing should be reproducible. Management estimates should be labelled with their basis and range. Sensitive operational data can be staged through clean teams or controlled environments.

Early readiness can improve negotiating leverage because it reduces uncertainty around the asset being sold. It can also expose a need to redesign the perimeter before launch. The seller should treat that outcome as transaction preparation rather than a disclosure failure.

19. Translate findings into transaction documents

The sale agreement should describe the business being transferred in operational terms. Asset and contract schedules remain necessary, but warranties and covenants should address the completeness and usability of data, documentation, interfaces, licences, models and access. Disclosures should identify known limits precisely.

Conditions precedent may include regulatory consent, NSI clearance, licence transfer or modification, material contract novation and specified separation tests. Completion deliverables can include reconciled data extracts, access revocation, keys, runbooks, model documentation and regulator correspondence. Where a dependency cannot be completed before closing, the TSA should carry the obligation and exit criteria.

Risk allocation should follow control. A seller that controls migration before completion may bear delay and accuracy risk. A buyer that changes the target architecture may bear resulting cost. Shared dependencies require governance and dispute mechanisms. Transaction-specific legal advice is essential.

20. Govern Day 1 readiness

Day 1 is the first operating state under buyer control. The plan should identify which systems, data, people and suppliers are buyer-owned, seller-provided or operating under temporary access. Each critical process needs a named owner and escalation route. Service continuity, safety and regulatory compliance take priority over a cosmetically complete migration.

The readiness dashboard should use evidence-based gates. A green status requires passed tests, approved documentation and accepted residual risk. Time elapsed or percentage complete does not establish readiness. Critical defects should remain visible to the board even when a workaround exists.

The cutover command structure should define who can stop, continue or roll back each migration. Communications should cover employees, suppliers, regulators and customers where applicable. The first reporting cycle and incident exercise should be planned before completion.

21. Control TSA exit

TSA exit transfers accountability as well as workload. The buyer should demonstrate that it owns the relevant contracts, controls identities, receives required data, operates monitoring, manages incidents and can evidence regulatory compliance. The seller should remove access and retain only records it is entitled or required to keep.

Exit sequencing should follow dependencies. Corporate applications may exit early while OT monitoring, data platforms and digital-twin services remain longer. The commercial terms can include step-up pricing to encourage exit, but pricing should not force a premature cutover. Extension rights should be narrow, documented and linked to remediation.

The exit certificate should list accepted services, unresolved defects, archived evidence, transferred records, revoked access and continuing obligations. Board oversight should continue until all critical services have exited and post-exit tests have passed.

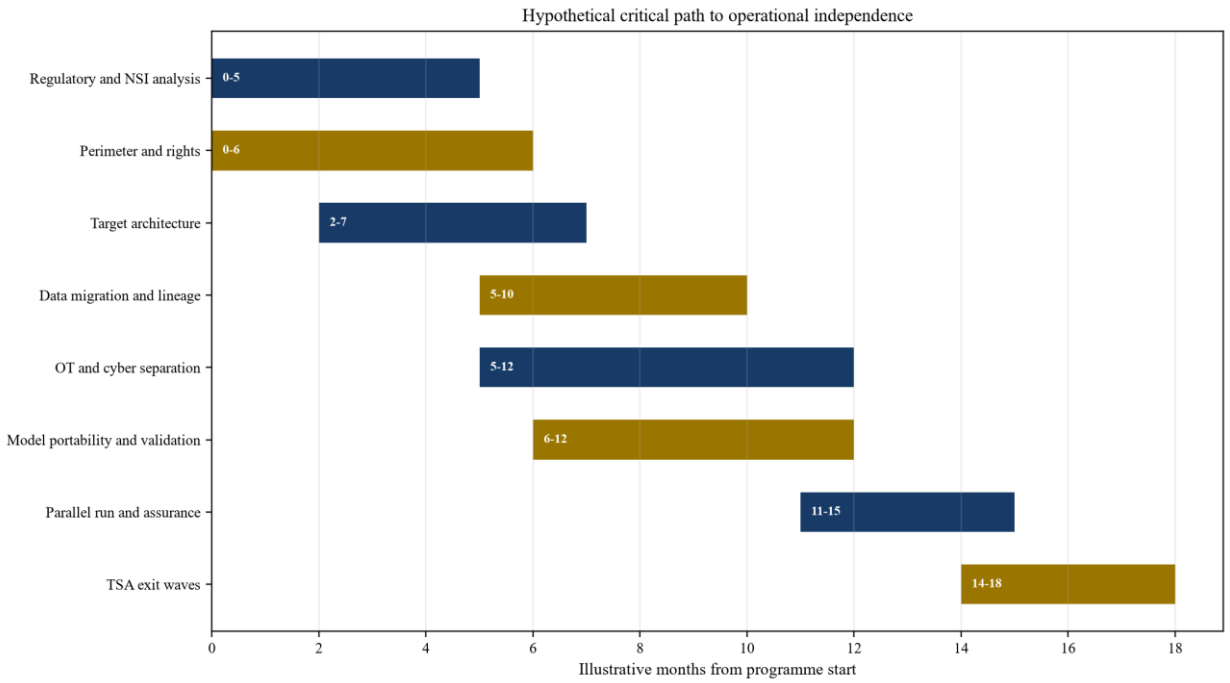
22. Apply the hypothetical worked case

The hypothetical seller proposes a regional platform containing regulated networks, field operations, customer-service interfaces, an operational data platform and several digital models. The first perimeter contains physical assets and employees but relies on seller-hosted identity, data, model and cyber services. The buyer identifies GBP 84 million of separation expenditure and applies a GBP 65 million risk adjustment.

Three designs are tested. Design A transfers the physical and legal perimeter with an 18-month TSA. It has the lowest pre-completion work but the highest dependency and extension risk. Design B duplicates the core data and identity platforms before completion, transfers model rights and uses targeted TSAs. It costs more before completion and reaches independence sooner. Design C transfers the wider shared digital platform and selected teams. It reduces duplication but creates a more complex retained-business separation.

The board selects Design B as the planning case. This is a hypothetical decision. The value adjustment can release GBP 42 million if the buyer receives verified data rights, reproducible models, approved cyber architecture and tested TSA exits before the agreed milestones. The remaining adjustment covers execution uncertainty that the hypothetical evidence does not remove.

Figure 4. Hypothetical separation critical path



Hypothetical months and dependencies. They demonstrate the framework and are not a commitment or observed timetable.

23. Set board gates and reporting

The board should approve the perimeter, value bridge, regulatory path, Day 1 model and TSA exit plan at defined gates. Each gate should present evidence, residual risk and the decision requested. Reports should distinguish confirmed facts, management assumptions and items awaiting external approval.

The board needs a small set of operating indicators: critical dependencies without funded treatment, unresolved rights, failed migration tests, high cyber risks, regulatory conditions, TSA services without exit plans, separation-cost movement and value at risk. Detailed workstream data should remain available beneath those indicators.

Escalation thresholds should be agreed before signing. A change to the regulated perimeter, loss of a required licence, inability to validate a control model or failure of an essential-service test should return to the relevant approval body. Governance should remain active after completion until independence is verified.

Table 4. Board approval gates for a utility carve-out

Gate	Board evidence	Minimum decision	Consequence of failure
Perimeter approval	Service map, regulatory boundary, asset and dependency registers	Approve or redesign perimeter	Stop launch or exclude unsupported value
Signing approval	Diligence findings, value bridge, approvals path, documents and funded plan	Authorise signing with stated conditions	Renegotiate structure, price or risk allocation
Completion readiness	Regulatory status, Day 1 tests, cyber assurance, data rights and people readiness	Authorise completion	Defer completion or activate contractual remedy

Gate	Board evidence	Minimum decision	Consequence of failure
TSA exit	Reconciled migration, independent operations, revoked seller access and accepted residual risk	Accept transfer of accountability	Extend affected service under remediation governance

Original framework. Evidence and approval bodies should be adapted to the actual governance and transaction documents.

24. Use a ninety-day action plan

During the first thirty days, appoint accountable workstream leads, confirm the service and regulatory perimeter, create common identifiers and launch the dependency inventory. Identify regulatory and NSI advice, critical suppliers, shared OT connections and digital twins. Establish controlled data-room access and evidence standards.

During days thirty-one to sixty, complete end-to-end service maps, data lineage, model inventory, target architecture and preliminary standalone costs. Test the proposed treatment of the highest-risk systems. Draft TSA services and identify conditions precedent. Feed quantified findings into valuation and transaction documents.

During days sixty-one to ninety, rehearse critical migrations, validate buyer capability, close material rights gaps and agree exit evidence. Present the board with the complete perimeter, value bridge, residual risks and gated execution plan. The timetable is an illustrative management sequence and should be changed for the actual transaction.

25. Appendix A diligence evidence register

The evidence register should contain the regulatory obligation map, licence and appointment records, regulatory correspondence, asset register, RAV bridge, intercompany arrangements, service catalogue, process maps, application and OT inventories, data lineage, model register, cyber architecture, supplier contracts, rights analysis, employee map, carve-out accounts, separation-cost model, TSA catalogue, Day 1 plan, testing evidence and critical path.

Each item should record owner, source, date, version, scope, access restriction, validation status and decision supported. A status of complete should require an identified reviewer and acceptance criterion. Material discrepancies between registers should be logged and resolved.

The register should remain active through completion and TSA exit. It becomes the transaction's audit trail and reduces reliance on personal knowledge. Sensitive operational information should remain protected through proportionate access controls.

26. Appendix B separation risk register

The risk register should connect each dependency to probability, impact, detection method, mitigation, owner, due date and contractual consequence. Risks should be stated as cause, event and consequence. For example, a non-transferable software licence may prevent the buyer from operating the network model after completion, leading to prolonged TSA dependence and additional cost.

The register should include regulatory, operational, safety, data, privacy, cyber, model, supplier, people, financial and timetable risks. Correlated risks should be identified. A failed data migration can affect model validation, regulatory reporting and operational continuity at the same time.

Residual risk should be accepted by the person with authority over the affected service. A workstream cannot close a board-level service-continuity risk by marking an action complete. Closure requires evidence that the risk is removed, transferred or accepted within the approved tolerance.

Regulatory and licence risks

Regulatory risk should identify the exact obligation, competent authority, proposed change and transaction consequence. A broad entry such as regulatory approval may conceal several distinct matters: change-of-control analysis, licence modification, information undertakings, ring-fence compliance, price-control treatment and national-security review. Each matter can have a different evidence requirement and timetable. The register should show whether the action is a legal requirement, a prudent engagement step or a management assumption awaiting advice.

Licence-related risks should connect to the operating model. A licence condition that requires resources, records or operational independence can affect which systems and people must transfer. The mitigation should therefore state the capability required and how it will be evidenced. A meeting held with a regulator is an activity; written confirmation, an approved modification or completion of a specified condition is evidence. The transaction timetable should carry sufficient time for questions, revised submissions and implementation of conditions.

Data and model risks

Data risks should distinguish missing records, poor quality, uncertain rights, incompatible formats and unavailable lineage. Each category needs a different response. Missing records may require reconstruction or a contractual remedy. Quality problems may require cleansing and validation. Rights problems may require consent, a new licence, anonymisation or restricted use. Format problems may require transformation and parallel testing. Missing lineage may limit the buyer's ability to reproduce a regulatory return or model output.

Model risks should state the decision affected. A demand model used for long-range planning may tolerate a different validation cycle from a control model that changes operating settings. The register should identify the relevant validation envelope, input dependencies, performance threshold, authorised users and fallback. The mitigation should include a reproducibility test and an operational-acceptance test in the buyer environment. Seller confirmation that the model ran successfully before separation does not prove that it will operate with the buyer's data, licences and controls.

Operational and cyber risks

Operational risks should be tested through service journeys. A dependency can appear minor in an application inventory while sitting on the only path between an alarm and an operator response. The register should identify the maximum tolerable disruption and the manual fallback. If no safe fallback exists, the dependency belongs on the critical path and may require duplication or continued seller support until a buyer capability is demonstrated.

Cyber risks should cover access, segmentation, monitoring, recovery, supplier connectivity, certificates, encryption keys and incident responsibility. Shared administrative domains and remote-support routes deserve specific entries because they can preserve unintended control after completion. The mitigation should define the target state, cutover sequence, test, evidence and rollback. The buyer should receive a current record of privileged access and confirm revocation or reassignment at the agreed point.

Financial and valuation risks

Financial risks should reconcile the perimeter to historical accounts and the standalone plan. A cost allocation can disappear from the seller's management accounts without disappearing from the business. The register should identify the service being replaced, expected volume, supplier or internal resource, implementation cost and steady-state cost. It should also record stranded seller costs separately because those costs do not automatically belong to the buyer.

Valuation risks should link directly to the model. If a data right remains uncertain, the model should show the cost of replacement, operating impact and timetable range. If TSA exit slips, the model should show

additional charges, duplicated cost and any delayed synergy. A risk adjustment should release only when agreed evidence is delivered. This approach makes the adjustment auditable and reduces arguments about whether an action is complete.

People and supplier risks

People risks should identify roles, named incumbents where appropriate, transfer treatment, retention needs, security clearance, on-call responsibility and knowledge concentration. A shared subject-matter expert may support several businesses and be unable to transfer. The mitigation may require documentation, shadowing, recruitment, a services agreement or a different perimeter. Completion bonuses alone do not create buyer capability unless the person and knowledge are available when needed.

Supplier risks should cover assignment, change of control, support capacity, data access, cyber obligations, subcontractors, termination and exit assistance. The team should confirm the supplier's role in operating or restoring the service. A vendor may own a connector, encryption key or model component that neither party can reproduce. Critical suppliers should be involved in planning under controlled confidentiality, with commercial terms and implementation capacity confirmed before the cutover becomes irreversible.

Evidence and escalation discipline

Every material risk should point to the evidence that would change its rating. The register should avoid circular mitigations such as continue monitoring or engage stakeholders. A useful mitigation states the document, test, consent, contract or operating capability required, who must accept it and when the transaction decision changes if it is absent. The programme office should preserve the source record and approval rather than relying on a dashboard entry that may lose context.

Escalation should follow consequence and decision authority. A workstream lead can manage routine delivery risk within an approved budget. A change that affects licence compliance, essential-service continuity, purchase price, closing conditions or the agreed risk appetite belongs with the transaction steering committee or board. The escalation paper should state the fact pattern, available routes, financial and operating effects, advice required and decision deadline. This discipline converts the risk register from an administrative list into a transaction-control instrument.

The final register should also distinguish transferred, retained and shared risk. A contractual indemnity can allocate financial loss while leaving the buyer exposed to service disruption. Insurance can fund certain losses while leaving regulatory and operational accountability unchanged. The board should therefore review both the economic allocation and the practical ability to prevent, detect and respond to the event after completion.

The approved register should be baselined at signing, refreshed before completion and reconciled after every critical TSA exit. Closed items should retain their evidence and approval history.

Frequently asked questions

What should define the perimeter of a UK utility carve-out?

The perimeter should begin with the regulated service and connect every obligation to the physical assets, people, contracts, data, systems, models, suppliers and decision rights required to deliver it. The legal entity and fixed-asset register are evidence within that analysis rather than the entire answer.

Why do digital twins require a separate separation workstream?

A digital twin depends on a specific physical counterpart, live or simulated data flows, validation limits, assumptions, software and qualified users. Transfer of a model file alone may leave the buyer unable to reproduce, validate or maintain the capability.

What operational data should transfer?

The required set depends on the service, legal rights and regulatory obligations. The buyer commonly needs current and historical telemetry, asset and maintenance records, model inputs and outputs, event histories, regulatory evidence, master data and the lineage needed to interpret them lawfully and reliably.

How should a TSA be structured?

Each service should state scope, service level, security, data treatment, charges, owner, change process, liability, exit assistance and objective exit evidence. Critical services should be separated from lower-risk corporate support and should follow their own dependency-led timelines.

How does cyber regulation affect a carve-out?

Energy and water operators may be subject to the NIS Regulations and competent-authority guidance. Separation changes networks, identities, suppliers and accountability. The transaction plan should preserve essential-service resilience and provide evidence that the buyer can manage risk and incidents after transfer.

Is regulatory asset value the same as transaction value?

No. RAV is a regulatory financial construct. Transaction value also reflects expected cash flow, allowed returns, performance, capital needs, financing, standalone costs, separation expenditure, liabilities and execution risk.

When should regulatory and national-security analysis begin?

It should begin during perimeter design. Sector approvals, licence changes and the National Security and Investment regime can affect structure, timetable, information access and closing conditions.

What evidence should the board require before completion?

The board should require an approved perimeter, regulatory path, standalone operating model, reconciled financial bridge, tested critical migrations, cyber assurance, transferable rights, Day 1 readiness and funded TSA exits. Residual risks should have accountable acceptance and contractual treatment.

References

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

[2] Competition and Markets Authority, Merger remedies guidance, 2025. https://assets.publishing.service.gov.uk/media/68f0a40f82670806f9d5e140/CMA_87_Merger_remedies_guidance.pdf

[3] Ofgem, Data Best Practice guidance. https://www.ofgem.gov.uk/guidance/data-best-practice-guidance

[4] Ofgem, Direction for Data Best Practice Guidance and Digitalisation Strategy and Action Plan Guidance, 2023. https://www.ofgem.gov.uk/sites/default/files/2023-08/Direction%20for%20Data%20Best%20Practice%20Guidance%20and%20Digitalisation%20Strategy%20and%20Action%20Plan%20Guidance.pdf

[5] UK Government, Digital Twin definition, 2025. https://www.gov.uk/government/publications/digital-twin-definition/digital-twin-official

[6] UK Government, National Digital Twin Programme principles, 2024. https://www.gov.uk/government/publications/what-a-digital-twin-is-and-how-you-can-contribute/national-digital-twin-programme-ndtp-principles

[7] UK Government, National Data Strategy. https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

[8] Information Commissioner's Office, Data sharing: a code of practice. https://ico.org.uk/media2/ictfahk2/data-sharing-a-code-of-practice-all-1-0-2.pdf

[9] National Cyber Security Centre, Cyber Assessment Framework. https://www.ncsc.gov.uk/collection/cyber-assessment-framework

[10] National Cyber Security Centre, Operational Technology guidance. https://www.ncsc.gov.uk/collection/operational-technology

[11] Ofgem, NIS guidance for Operators of Essential Services, updated January 2026. https://www.ofgem.gov.uk/guidance/nis-directive-and-nis-regulations-2018-ofgem-guidance-operators-essential-services

[12] Department for Energy Security and Net Zero, Implementation of the NIS Regulations for the energy sector. https://www.gov.uk/government/publications/security-of-network-and-information-systems-regulation-2018-implementation-in-the-energy-sector-for-great-britain

[13] UK Government, The NIS Regulations 2018 collection. https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

[14] Ofwat, Open data in the water industry. https://www.ofwat.gov.uk/regulated-companies/open-data-in-the-water-industry/

[15] Ofwat, Licences and licensees. https://www.ofwat.gov.uk/regulated-companies/ofwat-industry-overview/licences/

[16] Ofwat, Returns and dividends and the regulatory ring-fence. https://www.ofwat.gov.uk/households/your-water-company/returns-and-dividends/

[17] Ofgem, Energy Networks Ring-fence Review decision, 2026. https://www.ofgem.gov.uk/consultation/energy-networks-ring-fence-review-consultation

[18] Ofgem, RIIO-2 regulatory performance data 2025, published February 2026. https://www.ofgem.gov.uk/data/riio-2-regulatory-performance-data-2025

[19] UK Government, 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

[20] UK Government, National Security and Investment Act Section 3 statement. https://www.gov.uk/government/publications/national-security-and-investment-statement-about-exercise-of-the-call-in-power/national-security-and-investment-act-2021-statement-for-the-purposes-of-section-3--2

[21] UK Government, NSI Act guidance for downstream gas and electricity assets. https://www.gov.uk/government/publications/national-security-and-investment-act-2021-guidance-for-new-build-downstream-gas-and-electricity-assets/applicability-of-the-national-security-and-investment-act-2021-to-new-build-downstream-gas-and-electricity-assets

[22] UK Government, National Security and Investment Act Annual Report 2024 to 2025. https://www.gov.uk/government/publications/national-security-and-investment-act-2021-annual-report-2024-25/national-security-and-investment-act-2021-annual-report-2024-25-html

[23] UK Legislation, National Security and Investment Act 2021 Notifiable Acquisition Regulations. https://www.legislation.gov.uk/uksi/2021/1264/contents/made

[24] Drinking Water Inspectorate, Network and Information Systems enforcement policy. https://www.dwi.gov.uk/what-we-do/nis_enforcement_policy/

[25] Competition and Markets Authority, Utilities cases and projects. https://www.gov.uk/cma-cases?market_sector=utilities

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

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.