

Omnichannel Carve-Outs: Separating Digital Growth from Legacy Retail Infrastructure

A channel-to-separation framework for defining the perimeter, rebuilding stand-alone economics and protecting customer continuity

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

An omnichannel retailer rarely contains a clean digital business beside a clean store business. Customer identity, loyalty, pricing, inventory, fulfilment, returns, payments, supplier terms, media, technology and labour often operate as one system. A transaction that separates a digital channel, brand or growth platform without reconstructing those dependencies can transfer revenue without the assets needed to serve it, leave the seller with stranded costs, and expose both parties to customer and data failures.

This paper develops a Channel-to-Separation Omnichannel Carve-Out Framework. It maps value from customer acquisition through order, inventory, fulfilment, return and cash; defines a legally and operationally executable perimeter; rebuilds stand-alone financial statements; identifies stranded and duplicated costs; designs transition services around explicit exits; and converts the separation into valuation, transaction protection, Day 1 controls and a twenty-four-month implementation roadmap. The framework treats the proposed perimeter as a hypothesis that must be proved through data, contracts and operating evidence.

The worked case is wholly hypothetical. A retailer considers selling a digital growth business with USD 480 million of channel-originated revenue. After reallocating store fulfilment, shared technology, loyalty, payment, logistics and corporate services, the central case produces USD 31 million of stand-alone EBITDA. The downside case produces USD 13 million after weaker customer transfer, duplicated capabilities and slower TSA exits. Every amount, rate, timetable and valuation is an illustrative management scenario. The case is not observed company data, a forecast, legal advice, tax advice, accounting advice or investment advice.

JEL Classification: G24, G32, G34, L22, L81, M15, M21

Keywords: omnichannel carve-out, retail M&A, digital commerce, separation perimeter, customer data, fulfilment economics, transition services agreement, stand-alone costs, stranded costs, Day 1 readiness

1. Define the separation decision

The board decision is whether a channel, brand or digital platform can become a viable business without damaging customer value in the seller or buyer. Revenue labels do not define a perimeter. The analysis must establish which customers, contracts, people, assets, systems, inventory and obligations are required to originate an order, fulfil it, accept a return and collect cash. The decision should state the intended transaction form, jurisdictions, control model, financing constraints and target operating model. It should also identify which capabilities remain shared on Day 1 and which must be duplicated, migrated or replaced. Approval requires an evidence-backed answer to four questions: what transfers; what remains; what temporarily connects the parties; and what each business costs after those connections end. A

perimeter that cannot be expressed in legal schedules, system rules and financial statements is not ready for pricing.

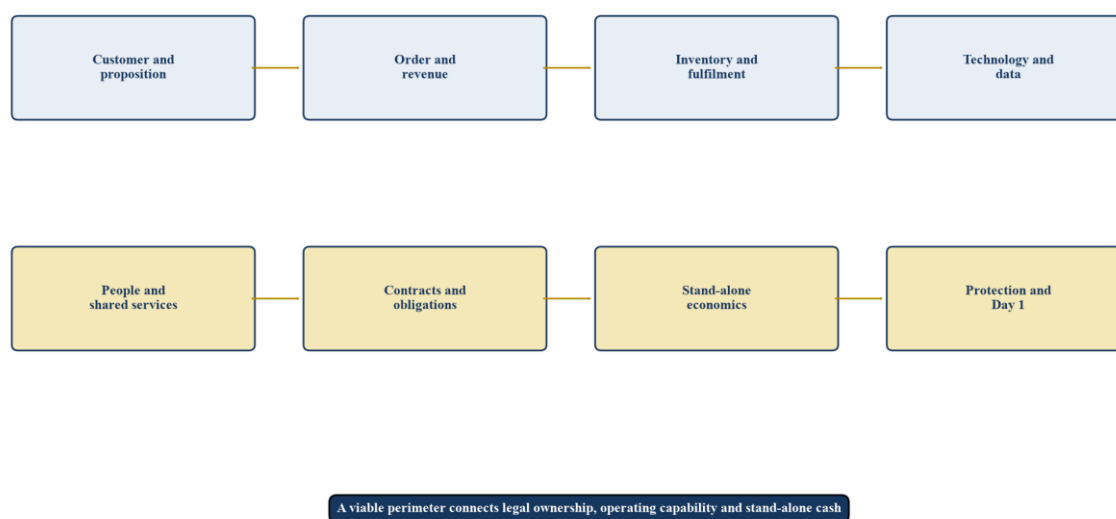
The decision memorandum should record the preferred perimeter, rejected alternatives, evidence gaps, downside exposure and authority to proceed. The board should see the commercial thesis, execution path and funded contingency in one view so that approval conditions can be tested at every subsequent gate.

2. Use the Channel-to-Separation Framework

The proposed framework has eight linked gates: customer and proposition; order and revenue; inventory and fulfilment; technology and data; people and shared services; contracts and obligations; stand-alone economics; and transaction protection. Each gate produces a perimeter decision, an evidence pack, a financial consequence and an owner. The gates should run together because a change in one layer can alter every other layer. Allocating digital revenue to the buyer, for example, may require store inventory, pick-and-pack labour, delivery contracts, returns capacity, loyalty data and payment credentials. The framework begins with a transaction-level value chain and ends with a controlled Day 1 model. It prevents a visually simple channel split from becoming an operationally incomplete carve-out. Exceptions remain visible in a decision log, with an explicit resolution before signing, closing or TSA exit.

Gate completion requires named evidence rather than percentage-complete reporting. A gate stays open when a critical dependency lacks a disposition, contract, cost or owner. This discipline prevents timetable pressure from turning unresolved assumptions into the signed transaction perimeter.

Figure 1. Channel-to-Separation Omnichannel Carve-Out Framework



Eight evidence gates connect the commercial perimeter to Day 1 and the end state.

3. Map value from customer to cash

A defensible carve-out begins with the full order lifecycle. The team should map discovery, marketing, identity, basket creation, pricing, promotion, payment authorisation, inventory reservation, pick, pack, delivery, collection, customer service, return, refund, fraud management and settlement. Every step should identify the legal entity, system, data set, employee group, third party, accounting entry and cash account involved. Target reports that stores fulfil the majority of digitally originated sales and that store fulfilment supports availability, speed and cost [1]. Walmart similarly describes an integrated store and e-commerce

model with same-day pickup and delivery across substantially all United States stores [2]. These disclosures are company-specific. They demonstrate that channel origin and operational fulfilment can be different. The separation model must therefore follow the order through the network rather than treating website revenue as a self-contained business.

Sampling should cover ordinary orders, peak periods, split shipments, cancellations, promotions, fraud reviews, store collection and cross-channel returns. The resulting maps should reconcile to system logs and accounting entries. Exceptions can then be costed and assigned before they become customer incidents.

4. Freeze the proposed perimeter

The perimeter register should list every legal entity, brand, domain, application, store, warehouse, office, customer contract, supplier agreement, licence, data set, employee, asset, liability and service proposed to transfer. Each item needs a disposition: transfer, remain, duplicate, replace, terminate or provide temporarily. Ambiguous items require a named decision owner and deadline. The register should reconcile to the general ledger, contract repository, HR system, application inventory, asset register and customer-facing terms. It should record consent, novation, regulatory and tax requirements without assuming that operational use equals legal ownership. A good perimeter is both economically coherent and executable. The buyer receives the minimum viable capabilities needed to trade; the seller retains sufficient capability to operate; and neither party relies on an asset or right that has no documented access after closing.

Version control matters because transaction negotiations continually change scope. Every perimeter movement should update legal schedules, financial statements, employee lists, system dispositions, TSA services, separation cost and valuation. A change accepted in one workstream should not remain invisible elsewhere.

Table 1. Minimum executable perimeter register

Layer	Evidence	Core decision	Financial consequence
Customer	Terms, consent, history, loyalty	Transfer, share or retain	Revenue retention and liability
Operations	Stores, warehouses, returns	Transfer, contract or replace	Fulfilment cost and capex
Technology	Applications, interfaces, licences	Clone, migrate, TSA or replace	Separation cash and recurring cost
People	Roles, skills, authority, location	Transfer, retain or recruit	Stand-alone and duplicated cost
Contracts	Suppliers, logistics, payments	Assign, novate or procure	Terms, deposits and continuity
Finance	Assets, liabilities and allocations	Carve-out and pro forma treatment	Valuation, working capital and debt

Every item requires a disposition, evidence owner and Day 1 route.

5. Establish customer ownership and proposition

Customer ownership is wider than an email address. The team should determine which entity contracts with the customer, controls loyalty terms, issues promotions, bears product and refund obligations, owns service history, and decides future use of personal data. Customers may move across web, app, marketplace, call centre and store within one purchase journey. A carve-out that assigns customers only by last order can fragment the relationship and distort lifetime value. The analysis should segment active customers by acquisition source, purchase channel, fulfilment method, return behaviour, consent, loyalty status and geographic eligibility. It should define how joint customers are treated and how customer

communications avoid confusion. Any proposed transfer of data requires a documented lawful basis, purpose, transparency plan, security control and retention treatment. The commercial model should then test acquisition, retention, cross-channel migration and service cost under the proposed ownership rules.

Customer cohorts should be analysed using behaviour observed across a sufficiently representative period. Management estimates for retention or migration should be identified as assumptions and sensitised. No customer-transfer case should depend on marketing access or consent that the buyer cannot legally or technically use.

6. Reconstruct revenue by origin and fulfilment

Revenue should be decomposed by order origin, merchant of record, fulfilment node, delivery method, product category, geography, payment method, return location and accounting entity. The bridge must reconcile gross merchandise value to recognised revenue, discounts, loyalty awards, tax, delivery income, marketplace commission, refunds, cancellations and cash settlement. Channel-originated sales are not necessarily channel-earned profits. Store inventory, store labour and store occupancy may fulfil an online order; the digital platform may generate demand for a store purchase; and returns may be processed by a different entity. The model should therefore show commercial attribution and operational causation side by side. It should retain transaction identifiers so that allocation rules can be rerun. Management judgments belong in a controlled policy table, supported by sensitivity analysis where more than one allocation is plausible.

The revenue bridge should be reproducible for each reporting period and selected transaction samples. Finance, commercial and technology owners should approve the same allocation logic. A model that changes when extracted by a different team is not ready for purchase-price or financing use.

7. Define inventory ownership and availability

Inventory separation requires product-level clarity. The register should identify legal title, physical location, reservation rules, transfer pricing, shrink responsibility, markdown authority, supplier restrictions, consignment terms and return rights. A single stock pool can support stores, direct delivery, click-and-collect and marketplace orders. Splitting that pool can reduce availability, duplicate safety stock and weaken purchasing scale. The buyer should model inventory by SKU, node and ageing band; reconcile quantity to the subledger and ledger; and test the cash needed for a stand-alone assortment. Cut-over rules must address orders in flight, goods in transit, customer returns and intercompany transfers. The transaction documents should define inventory counts, valuation, obsolete stock, post-close access and claims. A digital business without dependable product availability may lose revenue even when the website and customer list transfer intact.

Inventory scenarios should test peak demand, supplier lead time, minimum orders and node failure. Management should separate permanent inventory required by the new network from temporary duplication during cut-over. Both amounts affect funding, risk and the credibility of the growth plan.

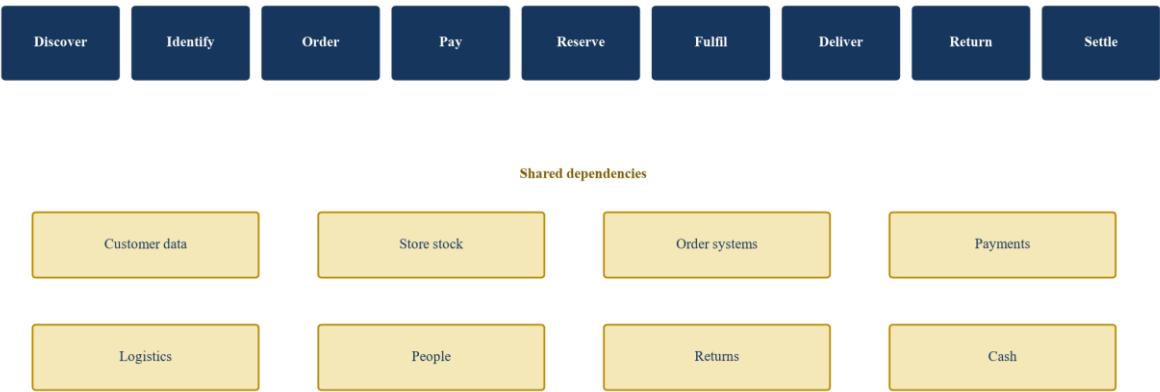
8. Allocate stores and fulfilment nodes

Stores may be sales locations, marketing assets, collection points, return centres and micro-fulfilment nodes at the same time. The team should quantify each role by store and order cohort. It should calculate pick-and-pack labour, inventory handling, last-mile cost, failed delivery, customer collection, return processing, occupancy and incremental capex. Where stores remain with the seller, the buyer may need a fulfilment agreement with service levels, capacity rules, pricing, audit rights and exit provisions. Where fulfilment transfers, the buyer may need leases, systems, employees, licences and vendor contracts. Network modelling should test delivery promises, peak volumes and failure scenarios. A transitional rate

based only on current average cost can underprice peak demand or capital requirements. The economic model should compare continued shared fulfilment, dedicated capacity and third-party replacement.

Service pricing should distinguish variable handling, fixed capacity, dedicated capital and exceptional work. Performance credits alone do not restore lost customer trust. Capacity reservations, forecasting duties and emergency prioritisation therefore belong in the commercial agreement and the operating runbook.

Figure 2. Customer-to-cash dependency map



Order origin, operational fulfilment and legal responsibility can sit in different parts of the group.

9. Separate returns, refunds and customer service

Returns can create one of the sharpest boundary failures. The team should identify who accepts the item, verifies condition, refunds the customer, bears fraud, restores inventory, records markdown and manages warranty claims. Cross-channel returns may depend on store systems and trained staff even when the original order is digital. A transaction cut-off should allocate pre-close and post-close orders, returns and chargebacks. Customer communications should preserve a simple experience while the legal and financial responsibilities remain precise behind the scenes. Service-level agreements should cover response times, escalation, data exchange, cash settlement and evidence retention. The model should quantify handling cost, recovery value and working-capital timing. A high-return category can make an apparently asset-light digital business dependent on physical infrastructure and seller liquidity.

A returns control account should reconcile physical items, customer refunds, processor settlements, inventory entries and supplier recoveries. This creates a single evidence trail across both parties. It also helps detect duplicate refunds, delayed cash and stock that has disappeared between systems.

10. Map technology by business capability

The application inventory should connect each system to business capability, users, data, interfaces, licences, infrastructure, support teams, resilience and cost. Core layers may include commerce, product information, pricing, promotions, order management, warehouse management, store point of sale, customer identity, loyalty, payments, fraud, customer service, analytics, finance and HR. Each application needs a disposition and a Day 1 access route. Shared instances require logical separation, cloned environments, contractual access or replacement. The architecture should identify hard dependencies such

as identity services, master data, API gateways, batch jobs and security tooling. The technology plan must include capacity, monitoring, disaster recovery, cyber response and records retention. A system can be technically available yet commercially unusable if licences, data rights, interfaces or support people do not transfer.

Architecture decisions should include the end-state date and the temporary path. Teams should avoid cloning unnecessary legacy complexity merely to accelerate Day 1. Where replacement is chosen, data migration, controls, reporting, training and decommissioning should be included in scope and budget.

11. Protect data rights and privacy

The data workstream should create a record of data sets, purposes, controllers, processors, lawful bases, retention periods, locations, transfers and security controls. The UK Information Commissioner's Office states that mergers, acquisitions and changes of controller require data-sharing due diligence, including purpose, lawful basis, transparency, governance and security [3]. The carve-out should therefore identify what data can transfer, what must be separated, what can be shared temporarily and what must be deleted or anonymised. Consent language and customer expectations should be reviewed before assuming reuse for a new brand or owner. Data-room access should be minimised and logged. Cut-over plans need reconciliation totals, exception handling and evidence of successful migration. Privacy, cyber and commercial teams should sign the same data-perimeter decision.

Data migration should use defined record counts, control totals, sampling, reconciliation and exception ownership. Access granted for diligence should be removed or converted at closing. Breach-response responsibilities should identify notification decision rights, evidence preservation and cooperation across both organisations.

12. Allocate identity, loyalty and personalisation

Identity and loyalty platforms often connect customers across channels and brands. The team should map account credentials, authentication, loyalty balances, tier status, vouchers, recommendations, preference centres, customer-service history and fraud signals. It should define which balances and obligations transfer, how joint customers authenticate, and whether accounts split or remain interoperable. Customer confusion can increase abandonment, service contacts and fraud. The financial model should include the liability for points, vouchers and expected redemptions; it should also test the effect of losing cross-brand data on conversion and marketing efficiency. Personalisation models require training-data, model, feature and decision-right analysis. A buyer cannot assume that access to outputs includes the right or ability to reproduce them. A migration should preserve security, customer notice and a reversible exception process.

Loyalty liabilities should reconcile membership records, outstanding units, expected redemption and accounting balances. Commercial teams should also test whether changes to earning or redemption create customer detriment. Any transitional interoperability needs fraud controls, settlement mechanics and a fixed route to independence.

13. Separate payments, fraud and cash

The payment perimeter should identify merchant accounts, acquirers, gateways, payment tokens, alternative payment methods, chargeback rights, reserves, settlement accounts, fraud rules and PCI responsibilities. Payment credentials may be contractually or technically non-portable. The buyer may need new merchant identifiers and token migration, with customer reauthentication where required. The cut-over plan should reconcile authorisations, captures, refunds, chargebacks and cash by transaction date. Fraud models and blacklists require data-right and performance testing. The liquidity model should include settlement delays, acquiring reserves and higher early-stage chargebacks. Transaction documents

should allocate legacy claims and customer refunds. Day 1 readiness requires successful end-to-end tests across every material tender, geography and refund route, supported by fallback procedures.

End-to-end testing should include low-value and high-value orders, partial captures, cancellations, refunds, chargebacks and alternative tenders. Finance should reconcile each test through settlement. Cyber and compliance teams should confirm that credentials, encryption, monitoring and incident ownership meet the new control model.

14. Rebuild logistics and supplier contracts

The team should map inbound freight, distribution centres, parcel carriers, same-day delivery, click-and-collect, drop-ship suppliers, packaging and reverse logistics. Contracts may price volume across the combined group, restrict assignment or depend on seller guarantees. Separation can therefore change unit cost and credit support. The buyer should reprice the stand-alone network using expected volumes, service levels, zones, fuel, surcharges, peak capacity and claims. Supplier analysis should cover terms, rebates, minimum orders, exclusivity, data exchange, product compliance and intellectual property. Shared purchase orders and goods in transit require cut-off rules. A transition agreement can preserve service while replacement contracts are completed, but it should not conceal an uneconomic end state. Every temporary service needs a target contract, owner, date and tested exit.

Supplier and carrier consent should be tracked against the critical path. Where a counterparty can reprice, terminate or require security, the downside case should reflect that outcome. Procurement savings should enter the base case only after supportable terms and an executable implementation plan exist.

15. Define people, roles and decision rights

A role map should link employees and contractors to processes, systems, locations, legal entities and decision rights. Shared teams may support merchandising, digital product, data, technology, customer service, logistics, finance, HR, legal, tax and procurement. Headcount allocation alone can miss critical knowledge or authority. The carve-out should identify named critical roles, transfer requirements, retention risk, consultation obligations, replacement needs and duplicated leadership. The stand-alone design should specify accountability for pricing, promotions, inventory, customer incidents, cyber response and cash. TSA service recipients still need competent people to govern the provider and prepare exit. The cost model should include recruitment, retention, contractors, severance, training and productivity ramp. Day 1 organisation charts should connect to system access and delegated authorities.

The people plan should respect applicable information, consultation and transfer requirements. Legal advice is jurisdiction-specific. From an operating perspective, each critical role needs a successor, access plan and retention response. Knowledge-transfer milestones should be measurable rather than described only as workshops.

16. Reconstruct shared services and stranded cost

Shared-service allocation should distinguish consumption, causation, capacity and avoidability. Historical corporate charges may not equal the cost of a stand-alone function or the saving available to the seller. The team should build each function from required activities, service levels, volumes, people, applications, vendors and facilities. It should identify costs that transfer, costs that remain and can be removed, costs that remain stranded, and costs duplicated during transition. Seller and buyer cases should reconcile to the same baseline. Removal plans require actions, owners, timing and cash costs; unsupported stranded-cost savings remain outside the base case. The board should see EBITDA before and after stranded cost, implementation cash and timing. This prevents both parties from pricing the same synergy or ignoring the cost of operating two complete businesses.

Seller cost removal should be tested at cost-centre and contract level. Vacant capacity, minimum vendor commitments and duplicated management layers can persist after the service ends. The seller case should therefore distinguish addressable cost, action cost, timing and the residual amount that remains stranded.

17. Prepare carve-out and pro forma financials

The financial workstream should produce historical carve-out statements, an opening balance sheet, stand-alone management accounts, cash flow and a bridge to the proposed perimeter. The SEC Financial Reporting Manual states that carve-out financial statements generally include identifiable assets and liabilities plus reasonable allocations where a discrete business is acquired, and that Article 11 pro forma information may be required [4][5]. Applicable requirements depend on the transaction and jurisdiction. The model should document allocation bases for shared payroll, technology, occupancy, logistics, marketing, financing and tax. It should distinguish historical allocations from future stand-alone costs and transaction accounting adjustments. Working capital, capital expenditure, leases and contingencies should reconcile to operational schedules. The resulting statements must be auditable enough for pricing, financing and post-close control.

Accounting policies should be applied consistently across historical periods and the opening balance sheet. Material judgments should be documented with responsible reviewers. The finance plan should include the first monthly close, consolidation, tax reporting, controls certification and audit support in the separated environment.

Table 2. Stand-alone cost reconstruction

Cost category	Historical evidence	Stand-alone question	Required control
Fulfilment	Store labour, warehouse and carrier cost	Which network serves the buyer?	Order-level attribution and SLA
Technology	Applications, licences and support	What must be cloned or replaced?	Architecture disposition register
Customer	Loyalty, service and marketing	Which obligations and data transfer?	Customer-perimeter reconciliation
Corporate	Finance, HR, legal and procurement	What capability must exist independently?	Activity-based operating model
Seller stranded cost	Capacity that does not transfer	When can cost be removed?	Action, owner, date and cash cost

Historical allocations and future costs should remain distinct.

18. Establish stand-alone working capital

Working capital should be rebuilt from the operating model, not copied from a consolidated percentage. The buyer should model receivables, payment settlement, inventory by node, supplier terms, returns, gift cards, loyalty liabilities, tax, payroll and intercompany balances. Separation can shorten supplier terms, create new deposits, extend cash-settlement cycles and increase safety stock. Cut-over rules should identify ownership of inventory, customer cash, refunds, chargebacks and accrued expenses. The purchase-price mechanism should use definitions that match the perimeter and accounting policies. Seasonal and peak periods require monthly or weekly analysis. A minimum liquidity reserve should cover the lowest cash point plus operational disruption. The board should receive a bridge from reported working capital to stand-alone needs, with every material assumption linked to a contract or operating driver.

The purchase-price mechanism should include example calculations and dispute procedures. Working-capital targets need seasonality, growth and perimeter adjustments. Intercompany balances that disappear

at closing should not be mistaken for permanent funding, and customer cash should follow the legally responsible entity.

19. Quantify capital expenditure and one-off cash

The separation budget should distinguish recurring maintenance, growth investment and one-off separation cash. Technology cloning, licences, data migration, cyber controls, new warehouses, store equipment, office moves, brand changes and contract deposits can be material. A business may show positive EBITDA while consuming cash to reach stand-alone readiness. Each project should have scope, owner, supplier, timing, dependency, contingency and acceptance criteria. Costs should be allocated between buyer, seller and TSA pricing without double counting. The model should also identify capital deferred during the sale process and investment required immediately after closing. Scenario analysis should test delay, inflation and scope expansion. Valuation and financing should use cash after required investment rather than a headline earnings measure.

A weekly separation cash forecast should connect purchase orders, payroll, vendors, projects and contingencies. Committed funding should remain available when milestones slip. Cost reports should distinguish approved scope changes from overruns so that the board can act before liquidity becomes constrained.

20. Design TSAs around executable exits

A transition services agreement should preserve continuity while driving separation. The service catalogue should define scope, recipient, provider, service level, data, volume, price, security, change control, incident management, audit rights, term and exit criteria. Each service needs a replacement solution, responsible owner, milestone plan and dependency map. Prices should reflect agreed principles and avoid incentives that delay exit. Capacity and peak-volume assumptions should be explicit. Termination mechanics should support service-by-service exit and controlled extensions. The governance forum should review performance, risks, disputes and exit readiness. A TSA should never be the only evidence that the buyer can operate independently. Before signing, the team should prove that each service has a feasible end state and funded implementation plan.

Exit rehearsals should prove that the recipient can operate without the service and that the provider can remove access without damaging retained operations. Data returns, archival obligations, final billing and residual incidents should be closed through a signed checklist. Extension should require a new risk decision.

Table 3. TSA design and exit controls

TSA element	Required definition	Exit evidence	Escalation trigger
Scope	Process, system, data and exclusions	Replacement service accepted	Material ambiguity or missing dependency
Service level	Volume, quality, timing and peak	Stable performance in new model	Repeated failure or capacity breach
Price	Cost basis, indexation and projects	Final settlement reconciled	Disputed allocation or unplanned spend
Security	Access, incidents, retention and audit	Access removed and data reconciled	Breach, unauthorised access or loss
Term	End date, extension and termination	Owner signs exit checklist	Milestone slippage threatens continuity

Service continuity and separation discipline should be governed together.

21. Protect brand, intellectual property and channels

The perimeter should identify trademarks, domains, apps, social accounts, creative assets, product content, software, algorithms, data rights, marketplace accounts and licences. Brand separation may require coexistence, rebranding, quality controls and geographic restrictions. Domain redirects and app migrations can affect search, conversion and customer trust. Marketplace ratings and seller histories may not transfer. The buyer should verify ownership, registration, assignment and third-party restrictions. Transitional licences need scope, term, territory, quality control, enforcement and exit. Product images, reviews and content should be linked to contractual rights. The operating plan should secure administrative credentials and change authority at closing. Valuation should distinguish owned intellectual property from temporary access and from benefits that depend on the seller's continuing brand.

Brand and channel cut-over should be sequenced across packaging, websites, apps, stores, marketplaces, customer service and legal notices. Search and redirect performance should be monitored. Transitional use should end only after customer-facing assets, ownership records and administrative control have reconciled.

22. Test competition, consumer and regulatory requirements

The legal workstream should identify merger control, foreign investment, consumer protection, product regulation, e-commerce, advertising, pricing, accessibility, payments, privacy, employment and sector-specific requirements. The FTC and US Department of Justice Merger Guidelines describe the agencies' analytical approach to mergers and market structure [6]. Actual filing and remedy requirements depend on facts and jurisdiction. The perimeter design can affect market definition, data concentration, supplier access and remedies. Consumer terms, warranties, subscriptions and refund rights must remain enforceable through the transition. Regulatory licences and registrations need transfer or replacement plans. Conditions precedent should track critical approvals and operational licences. The separation roadmap should include evidence owners and lead times rather than assuming legal completion automatically produces trading readiness.

Regulatory conditions should connect to the closing checklist and the implementation plan. A remedy or approval condition can change data, contracts, assets or governance. The model should therefore reserve capacity for required perimeter changes and test whether the business remains viable under them.

23. Build the Day 1 control room

Day 1 readiness should be tested by critical customer journeys and business processes. The control room needs named owners for order capture, payment, inventory, fulfilment, delivery, return, refund, customer service, pricing, promotion, supplier ordering, payroll, cash, financial close and incident response. Each process should have a success measure, monitoring source, escalation and fallback. Access lists, delegated authorities, bank mandates and vendor contacts should be complete. Rehearsals should cover peak volumes, unavailable interfaces, failed data loads, payment outages and customer communication. The buyer and seller should agree how shared incidents are diagnosed and resolved. A readiness status remains red until evidence demonstrates that the process can complete end to end under the new legal, technical and financial ownership.

Command-centre reporting should prioritise facts that indicate customer or cash harm. Metrics need thresholds and named escalation paths. Teams should pre-authorise emergency decisions within defined limits so that operational response is immediate while material perimeter or financial changes still receive governance.

24. Link valuation to customer and infrastructure transfer

Valuation should bridge from reported channel performance to stand-alone cash. The bridge should address customer transfer, revenue attribution, fulfilment charges, logistics rates, payment cost, loyalty liability, marketing efficiency, technology, people, corporate functions, working capital, capex and TSA exit. Multiples should be applied to earnings and cash flows that the buyer can operate and finance. A growth label does not remove infrastructure dependence. The model should separate value owned by the business from value provided temporarily by the seller. Customer retention and service continuity should be scenario variables because the separation itself can change behaviour. The investment committee should receive central, downside and severe-but-plausible cases, with transparent assumptions and no synergy counted twice.

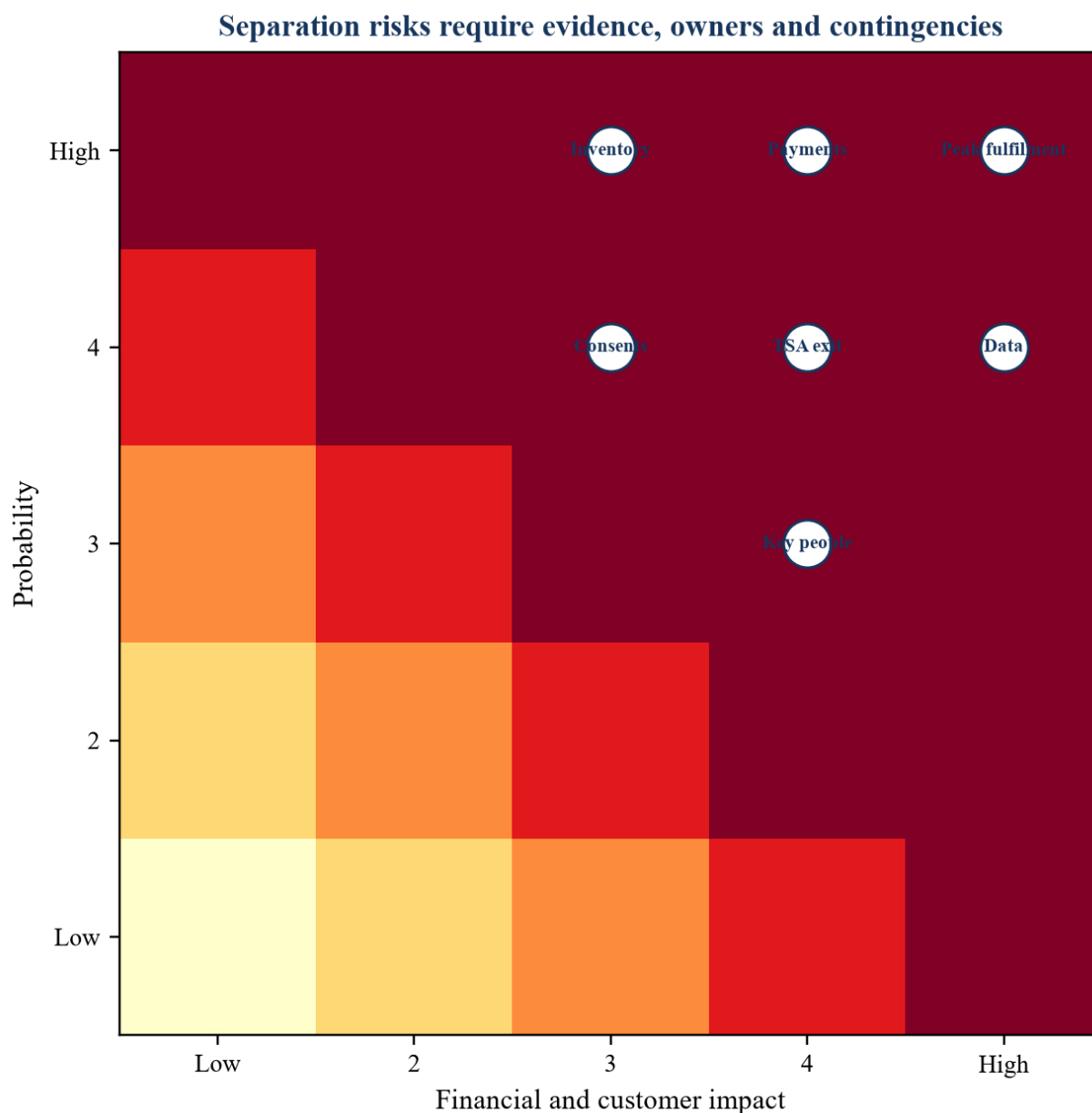
The valuation bridge should display each dependency as recurring cost, temporary cost, investment, risk or contingent benefit. This makes negotiation precise. It also allows diligence updates to flow into price and financing without rebuilding the model from narrative conclusions.

25. Use a separation risk heat map

The risk register should score probability, financial impact, customer impact, operational detectability, lead time and reversibility. High-priority risks commonly include customer-data legality, payment-token portability, inventory visibility, peak fulfilment, marketplace continuity, key-person loss, vendor consent, TSA exit and stranded cost. Each risk requires an owner, mitigation, trigger, contingency and valuation treatment. The heat map should connect to signing conditions, reserves, insurance, covenants and implementation milestones. Risks should be retired only after evidence, not after a meeting or plan. The board should receive movement over time and concentration by dependency. A small number of unresolved cross-functional risks can make the entire perimeter unexecutable.

Risks should be linked to specific evidence and tested at a regular cadence. Closing a risk requires proof that the mitigation is implemented and effective. If a risk cannot be mitigated before closing, the transaction response should be explicit in price, structure, covenant, reserve or condition.

Figure 3. Hypothetical separation risk heat map



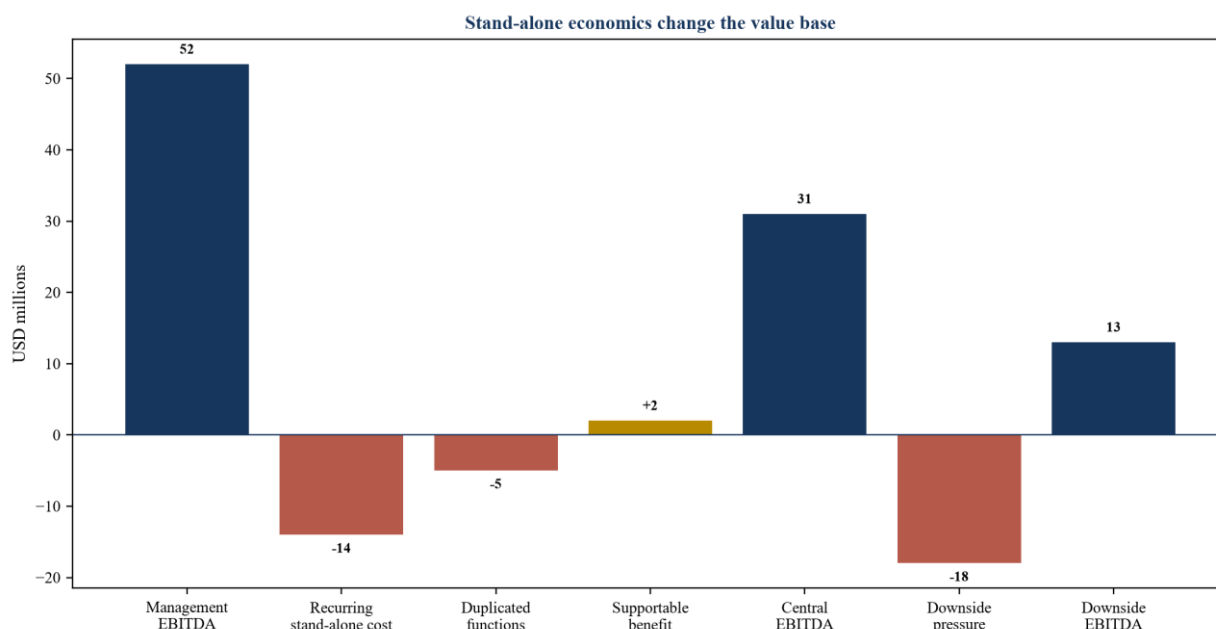
Scores are illustrative and should be replaced with transaction evidence.

26. Model a hypothetical digital carve-out

The hypothetical retailer records USD 480 million of channel-originated revenue and USD 52 million of management EBITDA. The reconstruction attributes store fulfilment, return handling, loyalty, payment, technology, logistics and corporate services to the business. Central stand-alone EBITDA is USD 31 million after USD 14 million of recurring cost additions, USD 5 million of duplicated functions and USD 2 million of supportable procurement benefits. The model includes USD 34 million of one-off separation cash and USD 22 million of incremental working capital. The downside assumes lower customer retention, higher logistics rates, duplicated technology for longer and delayed TSA exits; EBITDA falls to USD 13 million. All values are hypothetical management assumptions used to demonstrate method. They must be replaced with transaction evidence before any decision.

The worked case should be read as a modelling demonstration. It contains no claim about an actual company or market benchmark. Users should replace every assumption with verified target data, negotiated contract terms and advice appropriate to the transaction and relevant jurisdictions.

Figure 4. Hypothetical management EBITDA-to-stand-alone bridge



USD millions; all values are illustrative management assumptions.

Table 4. Hypothetical digital carve-out scenarios

Measure	Central	Downside	Decision meaning
Channel-originated revenue	480	420	Customer retention and proposition
Management EBITDA	52	52	Starting measure before reconstruction
Stand-alone EBITDA	31	13	Recurring separated economics
One-off separation cash	34	49	Funded path to independence
Incremental working capital	22	31	Liquidity created by new operating model
TSA exit period, months	18	30	Duration of seller dependency
Illustrative entry multiple	9.0x	7.0x	Risk-adjusted assumption
Illustrative enterprise value	279	91	Sensitivity to earnings and risk

USD millions; illustrative management assumptions only.

27. Convert findings into transaction protection

Perimeter findings should change the sale agreement. Asset and liability schedules should align with operational registers. Conditions precedent can address consents, licences, data transfer, key systems, merchant accounts and critical employees. Representations should cover customers, revenue, data, cybersecurity, inventory, suppliers, technology, intellectual property, employees, financial information and compliance. Specific indemnities or escrows may address identified exposures. Working-capital and completion mechanisms should reflect the carved business, not the seller's consolidated policies. Interim covenants should restrict material changes in pricing, promotions, inventory, suppliers, technology, data and staffing. TSAs and long-term commercial agreements should be negotiated with the main transaction

because they affect value. The buyer should preserve information and audit rights for allocations and service charges.

The disclosure schedules should be generated from controlled registers where possible. Manual re-keying creates divergence between operating reality and legal documentation. A final cross-functional reconciliation should confirm that the agreement, TSA catalogue, closing balance sheet and Day 1 plan describe the same business.

28. Size financing to separation cash flow

Financing should be based on stand-alone downside cash after working capital, recurring capex, TSA charges, separation investment, tax and contingency. Lenders need visibility into the customer-transfer assumptions, infrastructure dependencies, contract consents and Day 1 plan. Covenant definitions should exclude unsupported add-backs and should reflect the timing of duplicated cost and TSA exit. The capital structure may require committed equity, a revolving facility and a funded separation reserve. Minimum liquidity should cover seasonal peaks and operational disruption. Draw conditions should match closing and migration milestones. The financing case should test delayed systems, lower retention and higher fulfilment cost. Debt capacity based on management channel EBITDA can overstate resilience when infrastructure remains outside the perimeter.

The financing package should include a monthly cash model, covenant sensitivities and evidence for material add-backs. Separation reserves should have defined permitted uses and reporting. A lender waiver should not become the operating plan for risks that management already knows at signing.

29. Govern the first twenty-four months

The separation management office should maintain one integrated plan across customer, operations, technology, data, people, finance, legal, tax and communications. Milestones should show dependencies, acceptance criteria, cost, owner and risk. The board dashboard should track customer retention, conversion, service levels, order failures, inventory availability, fulfilment cost, returns, cash, working capital, duplicated cost, stranded cost, separation spend and TSA exits. Benefits and cost removal should be recognised only after actions complete and service remains stable. The roadmap should include Day 1, first 30 days, first 100 days, twelve months and twenty-four months. A change-control process should update valuation and liquidity when the perimeter or timing changes. The end state is reached when both parties operate independently with reconciled data, contracts, people, systems and financial control.

Benefits should be measured against the approved stand-alone baseline. Teams should avoid claiming both seller cost removal and buyer synergy from the same resource. Post-close reporting should preserve the original investment assumptions, approved changes and realised cash effect so accountability remains clear.

30. Conclude with an executable perimeter

Omnichannel carve-outs are separations of an operating system rather than transfers of a website and revenue line. Customer experience depends on connected stores, data, inventory, fulfilment, payments, returns, people and contracts. A successful transaction makes those dependencies visible, prices them and assigns a controlled route to independence. The Channel-to-Separation Framework gives boards a disciplined sequence: map customer-to-cash; freeze the perimeter; rebuild revenue and stand-alone cost; test data and technology; allocate inventory, logistics and people; design TSAs with exits; stress value and liquidity; and govern Day 1 through the end state. The result is an evidence-backed investment case with explicit limitations. It supports clearer negotiation, more credible financing and a separation plan that protects customer continuity while each business establishes its own economics.

The final board paper should state residual dependencies, unresolved limitations and the evidence supporting readiness. Independent sign-off across finance, operations, technology, data and legal workstreams reduces the chance that a locally complete plan masks a cross-functional failure.

Frequently asked questions

What is the first test in an omnichannel carve-out?

Map the complete customer-to-cash journey and prove which entities, systems, data, people, contracts and assets are required at every step. Use that evidence to test the proposed perimeter.

Can digital revenue be separated from stores?

Sometimes, subject to transaction evidence. The analysis should identify store fulfilment, returns, inventory, customer acquisition, loyalty, labour and occupancy that support digitally originated sales and provide an executable replacement or agreement.

How should customer data be transferred?

Create a data inventory and document controller roles, purposes, lawful bases, transparency, security, retention and migration controls. Applicable privacy advice should be obtained for the relevant jurisdictions and transaction.

What makes a TSA effective?

Each service needs precise scope, service levels, pricing, security, governance, a funded replacement solution, an accountable owner and measurable exit criteria. End-state readiness should be demonstrated before termination.

How should stand-alone EBITDA be calculated?

Start with reconciled carve-out financials; replace historical allocations with the cost of the target operating model; add recurring duplicated capabilities; remove unsupported benefits; and show implementation cash separately.

Which risks most often affect value?

Customer transfer, payment portability, inventory visibility, fulfilment continuity, data rights, vendor consents, critical people, stranded costs and delayed TSA exits can change revenue, cost, cash and risk.

How should acquisition debt be sized?

Use downside stand-alone cash after working capital, recurring capex, TSA charges, separation investment, taxes and contingency. Preserve liquidity for seasonal peaks and operational disruption.

What should the board monitor after closing?

Track customer retention, conversion, service failures, inventory availability, fulfilment and return cost, cash, working capital, separation spend, duplicated and stranded costs, and every TSA exit milestone.

References

- [1] Target Corporation. 2025 Annual Report, Item 1 Business and Management's Discussion and Analysis. <https://corporate.target.com/investors/annual/2025-annual-report/10-k-report/10-k-part-i/item-1-business>
- [2] Walmart Inc. Annual Report on Form 10-K for the year ended 31 January 2025. <https://stock.walmart.com/sec-filings/all-sec-filings/content/0000104169-25-000021/wmt-20250131.htm>
- [3] UK Information Commissioner's Office. Data sharing: a code of practice; due diligence following mergers and acquisitions. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/>

- [4] US Securities and Exchange Commission. Division of Corporation Finance Financial Reporting Manual, Topic 2. <https://www.sec.gov/corpfin/cf-manual/topic-2>
- [5] US Securities and Exchange Commission. Financial Reporting Manual, Topic 3; Regulation S-X Article 11. <https://www.sec.gov/about/divisions-offices/division-corporation-finance/financial-reporting-manual/frm-topic-3>
- [6] US Department of Justice and Federal Trade Commission. Merger Guidelines. https://www.ftc.gov/system/files/ftc_gov/pdf/2023_merger_guidelines_final_12.18.2023.pdf
- [7] IFRS Foundation. IFRS 3 Business Combinations. <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/>
- [8] IFRS Foundation. IFRS 5 Non-current Assets Held for Sale and Discontinued Operations. <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-5-non-current-assets-held-for-sale-and-discontinued-operations/>
- [9] IFRS Foundation. IFRS 15 Revenue from Contracts with Customers. <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-15-revenue-from-contracts-with-customers/>
- [10] IFRS Foundation. IFRS 16 Leases. <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-16-leases/>
- [11] European Union. Regulation (EU) 2016/679, General Data Protection Regulation. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [12] US Securities and Exchange Commission. Financial Disclosures about Acquired and Disposed Businesses. <https://www.sec.gov/resources-small-businesses/small-business-compliance-guides/financial-disclosures-about-acquired-disposed-businesses>
- [13] National Institute of Standards and Technology. Cybersecurity Framework 2.0. <https://www.nist.gov/cyberframework>
- [14] PCI Security Standards Council. Payment Card Industry Data Security Standard. <https://www.pcisecuritystandards.org/standards/pci-dss/>
- [15] US Federal Trade Commission. Protecting Personal Information: A Guide for Business. <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>
- [16] UK Competition and Markets Authority. Merger assessment guidelines. <https://www.gov.uk/government/publications/merger-assessment-guidelines>
- [17] Organisation for Economic Co-operation and Development. Guidelines for Multinational Enterprises on Responsible Business Conduct. <https://www.oecd.org/corporate/mne/>
- [18] International Organization for Standardization. ISO 22301 Security and resilience; business continuity management systems. <https://www.iso.org/standard/75106.html>
- [19] US Securities and Exchange Commission. Regulation S-X, Article 11. <https://www.ecfr.gov/current/title-17/chapter-II/part-210>
- [20] Target Corporation. Inside Target's supply-chain evolution: stores as hubs. <https://corporate.target.com/news-features/article/2025/09/evolving-stores-as-hubs>

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.