Transition Services from a Failing Group: Designing Continuity without Dependency

An Operating, Rights and Liquidity Framework for Distressed Carve-Outs

Authored by Chennakeshav Adya
Independent Researcher
September 2026

Abstract

Acquiring a viable business from a failing group creates a specific continuity problem: legal ownership can transfer before the systems, people, contracts, data rights and payment controls required to operate have become independent. A transition services agreement can bridge the separation, but its provider may be losing liquidity, vendors and employees. This paper proposes an operating, rights and liquidity framework for sustaining the acquired business while reducing provider dependency from completion.

The framework begins with customer-facing business services and maps the people, processes, technology, facilities, information and third parties required to deliver them. It converts residual dependencies into a modular service catalogue, tests legal and technical access separately, protects personal data and privileged access, and builds the standalone plan backwards from service exit. Current UK Government, CMA, FCA, ICO and NCSC materials support the bounded principles concerning distress, transitional support, service mapping, data governance and supply-chain security. Their legal and regulatory scope remains specific to the issuing body and context.

An original hypothetical model compares service exit at months four, seven and ten across six workstreams. It combines monthly transition charges, standalone build, two months of dual running, contingency and an author-assigned dependency measure. A sensitivity grid varies exit timing and build-cost overrun. All numerical inputs are author assumptions without transaction probability, supplier quotation or empirical calibration. The model demonstrates how delay can increase cash requirements and prolong reliance even when the acquired operation remains commercially attractive. The resulting decision record reconciles business-service continuity, provider authority, rights, access, replacement milestones and acquisition liquidity.

JEL Classification: G34, G33, L23, M15

Keywords: transition services agreement, distressed acquisition, carve-out, operational continuity, standalone build, data separation, cyber access, liquidity

1. Frame continuity as a separability problem

The purchaser of a business from a failing group may acquire a viable operation without acquiring the systems, people, contracts and permissions that keep it trading. The legal perimeter can move at completion while the operating perimeter remains embedded in the seller. A transition services agreement can bridge that gap, but the bridge inherits the financial weakness, governance constraints and operational fragility of the group providing the service. The buyer therefore needs a transition design that sustains the acquired business and reduces reliance on the provider from the first day.

This paper treats continuity as a separability problem. The analysis begins with the products and services that customers must continue to receive. It maps each service to people, processes, technology, facilities, data, contracts and cash. It then identifies which components transfer, which remain with the group and which require a third party. This service-to-resource map is more useful than an application list because it connects every dependency to an operating outcome and a tolerable interruption.

The proposed method combines five records: a minimum viable continuity map, a transition service catalogue, a rights-and-access schedule, a standalone build plan and a cash model. The records share identifiers and owners so that a service cannot appear operationally green while its contract, funding or data rights remain unresolved. The framework is analytical infrastructure for a particular transaction team to tailor with legal, tax, regulatory, cyber, technology and employment advice.

2. Start with the services the buyer must preserve

A distressed carve-out can encourage a systems-first response. Teams inventory applications, servers and licences because those items are visible. Customers experience an order, a payment, a delivery, a claim, a report or another end-to-end business service. A system can be available while the service fails because a bank mandate, supplier account, employee permission or data feed has not transferred. The continuity map should therefore begin with business services and work backwards to their supporting resources.

For each service, the buyer records the accountable owner, customer or regulatory consequence, peak operating period, maximum tolerable interruption and minimum output. A distributor may need to accept orders, allocate inventory, dispatch goods, invoice customers and collect cash. Each outcome has different dependencies and recovery needs. The map should distinguish a short manual workaround from a sustainable replacement. A workaround can reduce immediate interruption while creating capacity, control and reconciliation risks that require an expiry date.

The FCA's operational-resilience guidance offers a useful bounded analogy for regulated financial firms. It requires relevant firms to identify important business services, set impact tolerances and map the resources needed to deliver them, including third parties [5]. A buyer outside that regulatory perimeter can still use the service, tolerance and resource logic as a management framework. The paper does not extend the FCA rules to companies outside their stated scope.

3. Define minimum viable continuity

Minimum viable continuity is the smallest controlled operating state that can meet critical obligations after completion. It is not the seller's complete service environment reproduced under a new name. The buyer should specify the transactions, users, locations, data, approvals and reporting needed during the first operating cycle. Optional functionality, historical convenience and low-priority automation can move to later releases when their absence does not breach a legal, customer or control requirement.

The definition should be quantitative where evidence permits. Examples include orders processed per day, payroll completed by a stated date, cash receipts reconciled within an agreed period, customer incidents answered within a stated window and regulatory submissions produced from

an identified source. The numbers must come from verified operating records or be marked as management assumptions. A generic statement that services will continue as normal hides the exact performance the transition arrangement must support.

The minimum state also needs a failure boundary. The team identifies which loss of function stops trading, which creates accumulating exposure and which reduces efficiency. This classification controls the order of standalone work. Identity, payments and order-to-cash may require immediate redundancy; historical analytics may tolerate a staged migration. The classification remains transaction-specific and should be approved by accountable operating, finance, risk and technology owners.

Table 1. Proposed transition service catalogue

Field	Required content	Acceptance evidence
Business output	Testable result, volume and timing	Observed end-to-end transaction
Provider resources	People, systems, vendors and facilities	Named owner and available capacity
Rights and access	Contract, licence, data and credentials	Executed right and access test
Service control	Level, incident route and fallback	Monitoring record and rehearsal
Exit	Replacement, milestone and termination	Accepted cutover and closure pack

Proposed analytical record. Actual terms depend on the transaction documents, provider authority and specialist advice.

4. Build a transition service catalogue

The catalogue converts operational dependencies into contractible services. Each service has a defined output, volume assumption, hours of operation, service level, provider asset, buyer obligation, charge, term, exit date and evidence of delivery. The description should state the result rather than merely name a department. “Finance support” is too broad. “Generate the weekly accounts-receivable ageing from the specified ledger and deliver it in the agreed format by Tuesday 10:00” is testable.

Service boundaries must address interactions. An ERP service may depend on identity, network, data warehouse, help desk and vendor support. If those components are divided among separate schedule lines, the contract and operating plan should identify the party responsible for restoring the end-to-end service. Otherwise each component provider can meet its narrow obligation while the buyer cannot process a transaction. A named service integrator and incident escalation route reduce this gap.

The United Kingdom's Model Services Contract guidance describes a joint transition team spanning operations, legal, human resources, finance, service design, technology, facilities, commercial and project management expertise. It also addresses termination assistance, data return and orderly transfer [4]. The model contract is designed for specified public-sector services; it supplies useful drafting and governance prompts rather than terms that can be copied into a distressed acquisition without adaptation.

5. Separate transfer, transition and replacement

Every dependency should have one of three primary treatments. Transfer moves the resource or right into the acquired business. Transition keeps the group providing a bounded service for a limited period. Replacement creates a new internal or third-party capability. The team should document why the selected route is executable and what evidence would trigger a change. A licence that cannot be assigned may require a new vendor contract even if the associated data and configuration transfer.

The three routes can coexist. The buyer may transfer employees and data, receive temporary hosting from the seller and procure a new software subscription. The plan needs a responsibility matrix that follows the complete service through these layers. It should identify who maintains data integrity, who approves changes, who resolves incidents and who pays each vendor. Without this matrix, legal transfer can leave operational accountability divided.

Replacement work should start before completion where access and process rules allow it. The buyer can define requirements, select vendors, establish bank and tax registrations, prepare identity domains and design interfaces without copying protected data. The plan must identify activities that depend on completion, regulatory approval or seller consent. The critical path should distinguish preparatory work from steps that legally or technically cannot begin early.

6. Account for a failing provider

A conventional transition services agreement assumes that the provider remains able and willing to perform. A failing group may lose trade credit, banking facilities, key employees and supplier confidence. UK Government guidance identifies these effects of financial distress and notes that they can intensify the problem [1]. The buyer should treat provider capacity as a changing exposure and create evidence that can be monitored during the transition.

The provider assessment should cover cash needed to deliver the service, critical staff, third-party contracts, licences, infrastructure, insurance and authority. A charge paid to the group may not reach the employee or vendor on whom the service depends. The agreement can require specified pass-through payments, evidence of settlement, direct-pay rights or another controlled funding arrangement where lawful and commercially agreed. The actual structure requires insolvency and transaction advice.

The plan should also identify who can bind the provider after an insolvency event. The appointment of an administrator changes control. UK guidance explains that an administrator oversees the process and that access to third-party data may require a direct contract or the administrator's support [1][2]. The buyer should obtain advice on the office holder's authority and statutory duties. A pre-completion promise from prior management may not remain an executable service commitment.

7. Design services that can be terminated individually

A transition programme becomes difficult to exit when services are bundled. The buyer should define modules that correspond to standalone capabilities and can end independently. Identity, hosting, order processing, payroll, finance reporting and facilities access may have different replacement dates. Modular termination lets the buyer reduce exposure and cost as each capability becomes ready.

The service schedule should specify notice mechanics, testing requirements, data handover and final reconciliation for each module. A module is ready to terminate when the replacement has passed defined tests, users have been migrated, data has been reconciled, support ownership has moved and a fallback has been approved. Calendar expiry alone does not establish operational readiness. Equally, a provider should not remain indefinitely responsible because the buyer has delayed a replacement.

The CMA's merger-remedies guidance states that transitional access to key inputs or services may be permitted for a limited period to allow a divestment business to operate effectively. It also identifies risks and monitoring burdens where ongoing links substitute for a standalone business [3]. The regulatory context differs from a distressed acquisition, but the principle is relevant: transitional support should enable independence and remain bounded in scope and duration.

Table 2. Rights and access evidence map

Layer	Question	Minimum evidence
Legal	May the buyer receive or use the service?	Executed contract, consent or authority
Commercial	Are price, term and volumes defined?	Service schedule and charge basis
Data	May the parties transfer and process the data?	Approved data map and agreement
Technical	Can authorised users administer the service?	Access test, logs and revocation path
Continuity	Can the service survive provider failure?	Fallback test and independent data copy

Proposed evidence structure. It does not determine a legal right or regulatory obligation.

8. Secure rights before relying on access

Operational access has legal, contractual and technical layers. The buyer may receive a user account without the right to use the underlying software for the acquired business. It may have a licence but lack the administrator credentials needed to manage users. It may have credentials but no lawful basis to process personal data. The rights-and-access schedule should test each layer separately.

For every critical dependency, the schedule records ownership, contract party, assignability, consent, licence metric, user population, data classification, technical access method, authentication control and termination requirement. It also records the evidence relied on, such as an executed consent, vendor order form, data-sharing agreement or administrator approval. An expected consent should remain a condition or risk until executed.

The schedule should include source code, configuration, interfaces, domain names, certificates, encryption keys, cloud tenants, telephone numbers and physical access. These items often sit outside the main asset register. The buyer should establish the ability to administer and revoke access, not merely to consume a service. A right that depends on a named employee or shared group credential is fragile and should receive an early replacement plan.

9. Govern personal data during separation

The transfer and continued sharing of personal data require a defined legal and operational basis. The ICO states that organisations should consider data sharing as part of M&A due diligence, establish what data transfers, identify original purposes and lawful basis, document the sharing and secure the information [6]. It also notes the practical difficulty of managing shared data while systems differ or integration is incomplete.

The transition plan should create a data map for employees, customers, suppliers and other individuals. It identifies controller and processor roles, purpose, fields, location, recipients, retention, access, transfer mechanism and deletion evidence. The team should minimise shared fields and users to the service actually provided. A full database copy may be faster technically while creating unnecessary legal, security and reconciliation exposure.

Data separation needs a closing record. At each service termination, the provider should return or make available the agreed data, preserve material records where required and delete residual copies in accordance with applicable obligations and the contract. The buyer should verify the result through logs, attestations or testing appropriate to the risk. This paper does not determine the lawful basis, notification duty or international-transfer mechanism for any transaction.

10. Control privileged and third-party access

A transition agreement often leaves seller personnel with access to the buyer's systems or buyer personnel inside the seller's environment. Privileged accounts can change configurations, export data and create users. The access design should use named identities, least privilege, strong authentication, time limits, logging and a documented approver. Shared administrator credentials weaken accountability and complicate revocation.

The NCSC Cyber Assessment Framework states that relevant security requirements should be met whether an internal organisation or a third party operates the function and highlights protection against unauthorised access, modification and deletion [7]. The framework can inform transition controls even where it is not mandatory. The buyer should align controls to the actual threat, data and service consequence.

Access reviews should follow the exit plan. When a module terminates, associated accounts, tokens, certificates, interfaces, firewall rules and remote-support paths must be removed or changed. The team should maintain a live register and test high-risk revocations. A contractual statement that access ends does not itself close a technical connection. Evidence of closure should enter the completion pack.

11. Protect order to cash

Order-to-cash is frequently distributed across customer portals, pricing tools, inventory, logistics, invoicing, tax, banking and collections. A buyer that migrates the general ledger while leaving customer master data, bank details or electronic data interchange with the seller can interrupt cash generation. The service map should trace a representative transaction from customer instruction to settled cash and accounting entry.

The buyer should establish who can accept orders, issue invoices, change bank details, grant credit, process returns and chase debts. Customer communications need controlled timing and

anti-fraud measures. A change in payment instructions creates impersonation and diversion risk. The programme should use verified contact routes, dual approval and reconciliation of the first payment cycles.

The cutover plan should include open orders, accrued revenue, deposits, rebates, credits and disputed receivables. It should allocate economic ownership and operating responsibility across the completion date. The buyer's liquidity model should reflect any collection delay caused by new bank accounts, customer onboarding or invoice reissuance. These effects need transaction-specific evidence rather than a generic working-capital percentage.

12. Establish independent finance and payments

Finance independence begins with authority over cash. The buyer needs bank accounts, mandates, payment controls, receipts, payroll funding, tax processes and a chart of accounts that supports statutory and management reporting. A temporary ledger service can help produce reports, but it should not leave the acquired business unable to approve a supplier payment or identify its cash position.

The transition catalogue should specify posting cut-offs, interfaces, reconciliations, reporting dates, accounting policies and the treatment of shared balances. It should name the system of record for each period and provide a controlled route for corrections. The buyer should reconcile opening balances to the transaction perimeter and preserve the audit trail from source records to the standalone ledger.

Payments delivered through the seller require particular control. The schedule should identify the bank account, beneficial ownership of funds, approval chain, segregation, timing and evidence of release. The buyer needs a fallback for a frozen account or revoked mandate. Legal and insolvency advice should determine whether a proposed payment arrangement is permissible and how funds are protected.

13. Retain the people who know how the service works

Transition knowledge may be concentrated in a small number of employees who understand undocumented interfaces, customer exceptions or month-end procedures. Distress can accelerate departures. The resource map should identify critical roles and knowledge, employment status, transfer position, retention risk, access and replacement plan. Names belong in a restricted operational schedule rather than a public paper.

The buyer should distinguish service delivery from knowledge transfer. Paying for the provider to run payroll for six months does not automatically train the buyer's team or document the process. Each service should include explicit knowledge artefacts, shadowing, reverse-shadowing and acceptance tests. The receiving employee should demonstrate the process before the service terminates.

Retention arrangements require consistent authority and funding. Promises made by a failing group may not be paid. The transaction plan should identify who offers the arrangement, who bears the cost and what event earns the payment. Employment, tax and insolvency advice should address the actual structure. The analytical model can include the verified cost once terms and responsibility are established.

14. Manage suppliers and licences

The business may rely on contracts held centrally by the seller. Cloud hosting, telecoms, maintenance, insurance, software, logistics and professional services can be shared across multiple entities. The buyer should inventory each supplier against the business service it supports, contract party, term, payment status, assignability, consent and replacement lead time.

A vendor may suspend service because the failing group has unpaid invoices. The buyer should determine the amount attributable to the acquired business and the condition for continued supply. A direct payment, novation or new contract may solve the operational issue while creating value-transfer, priority or double-payment questions. Qualified advisers should determine the permissible transaction response.

Licence metrics can also change after separation. A group enterprise licence may not permit a carve-out entity to continue use. A new agreement may price users, revenue, compute, locations or transactions differently. The standalone cost model should use a supplier quote or clearly labelled author assumption. The team should not carry the seller's allocated charge into the investment case as though it were the buyer's future market price.

15. Test facilities and physical continuity

Technology receives attention because it is complex, yet a business can stop when it loses a warehouse gate, laboratory permit, security pass, utility account or spare part. The continuity map should include land and building access, leases, licences, utilities, environmental controls, safety systems, inventory, tools, records and security. Each facility should have a day-one operating checklist and emergency contacts independent of the seller.

Shared sites require clear boundaries. The agreement should define areas, hours, escorts, loading, health and safety, insurance, maintenance, visitor rules and incident control. Network and physical separation should progress together. A new system hosted in a room controlled by the seller remains dependent. The exit plan should state how equipment, cabling, records and access controls move or are replaced.

The buyer should test a plausible denial-of-access scenario. It needs a method for protecting people, serving customers, preserving assets and communicating with regulators or authorities where relevant. The scenario result informs inventory buffers, alternative locations and the order of migration. No generic resilience score can replace the local facts of the site and operation.

16. Set service levels around business outcomes

Service levels should reflect the consequences of failure. Uptime alone may not capture whether transactions are complete, data is accurate or support arrives before an operational deadline. The catalogue can combine availability, throughput, timeliness, accuracy, incident response and recovery evidence. Each measure needs a data source that remains available to both parties.

The buyer should define severity based on the affected business service. A payroll interface failure two weeks before payroll may be manageable; the same failure on payment day can be critical. Escalation should identify named roles, communication intervals, decision authority and fallback activation. The service provider should not control the only monitoring record used to demonstrate its own performance.

Credits and remedies should be considered with collectability in mind. A service credit against future charges may have little practical value if the provider fails or the service ends. The buyer may need step-in, direct-vendor engagement, escrowed materials, backup data or a funded continuity action. The appropriate contractual rights depend on law, bargaining position and administrator authority.

17. Price the service and fund delivery

Transition charges can be based on historical allocation, cost plus, unit price, fixed monthly amount or another agreed method. The buyer should understand which costs are incremental, which are shared and which arise from exit. A low monthly charge can hide a large build obligation or an unsupported provider subsidy. A high allocation can overstate the cost when the seller's group structure disappears.

The pricing schedule should state taxes, currency, indexation, pass-through costs, one-off changes, disputed amounts and payment timing. It should distinguish the cost of consuming the service from the cost of extracting data, transferring assets and supporting cutover. The Model Services Contract guidance notes the importance of clarity over exit charges and cost apportionment [4]. The actual transaction needs bespoke terms.

Funding design matters when the provider is distressed. The buyer should determine whether payment in advance is necessary, how unused amounts are protected and whether critical third-party vendors can be paid directly. Any controlled account, escrow or reserve requires legal and insolvency analysis. The cash model should include the agreed timing and identify exposure if the provider stops before earning an advance.

18. Build the standalone plan backwards from exit

Each service receives a target exit date, replacement route and acceptance criteria. The plan works backwards through design, procurement, build, data preparation, testing, user training, parallel run, cutover and stabilisation. It identifies which milestones depend on seller cooperation and which the buyer controls. The target date should reflect the critical path and resource capacity rather than a uniform programme deadline.

The plan should use progressive independence. The buyer first gains visibility and control, then duplicates critical data and access, then operates the replacement in parallel, and finally terminates the service. Some modules may use a clean cutover, while finance and order processing often need reconciliation across periods. The method should fit the process rather than enforce one migration pattern.

Every milestone requires evidence. A configured system is not ready until interfaces, security, data, controls, users and support have passed the agreed tests. The steering committee should see the evidence gap and the cash consequence of delay. A completion percentage without accepted deliverables can create false confidence.

19. Use cutover gates rather than optimism

A cutover gate is a dated decision with required evidence, accountable approvers, fallback and maximum deferral. Typical evidence includes successful end-to-end transactions, reconciled opening data, user access, vendor support, security review, training and a tested rollback or

continuity procedure. The gate should identify which defects can be accepted and who has authority to accept them.

The team should rehearse critical cutovers. A rehearsal tests timing, roles, files, scripts, communications and recovery. It also identifies hidden manual activity. The result belongs in an exception log with owners and retest dates. A rehearsal that succeeds on sample data may still require a production-volume test where capacity matters.

Deferral has a measurable cost. It extends transition charges, retains dependency exposure and can increase dual-running work. It may also move cutover into a peak trading, reporting or regulatory period. The decision paper should show these effects rather than framing delay as a schedule issue alone.

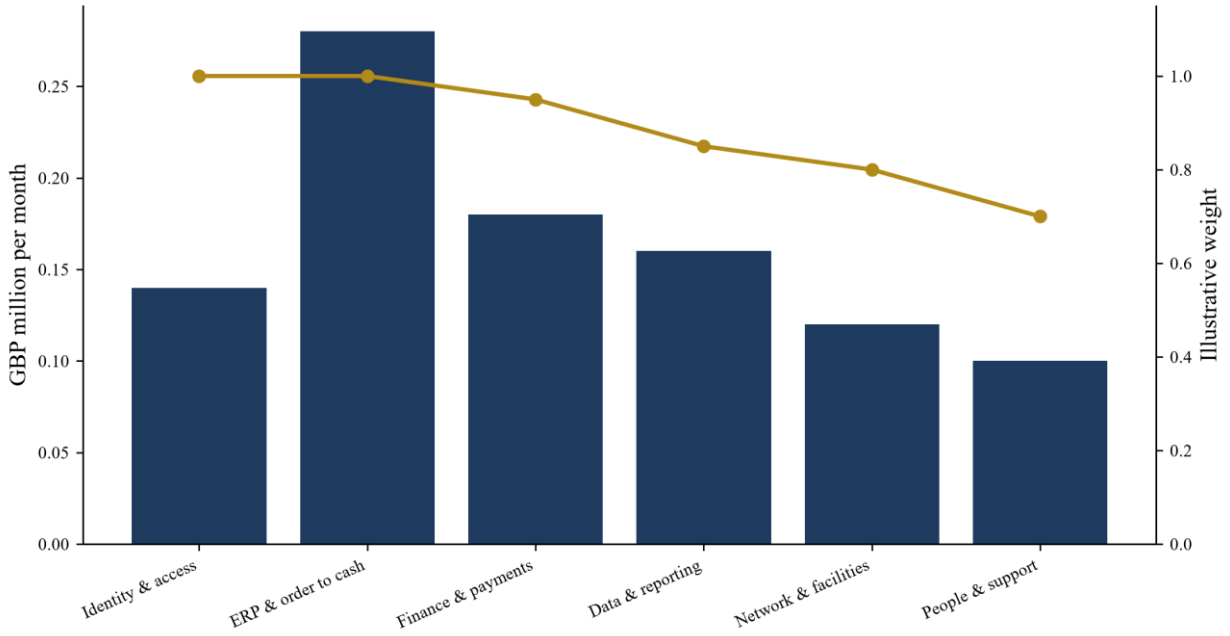
20. Create a controlled change process

The services defined before completion will change as the buyer learns more. The agreement should provide a fast process for clarifying scope, adjusting volume and resolving omissions. Each change should state the business need, service impact, cost, timetable, security and exit consequence. Emergency changes need retrospective documentation and a narrow authority.

A failing provider may lack resources for discretionary changes. The buyer should prioritise modifications that protect continuity or accelerate independence. Enhancements that reproduce the seller's legacy environment can consume scarce capacity and deepen dependency. The change board should assess whether the requirement belongs in the temporary service or the standalone build.

The change register should reconcile with the model and service catalogue. An approved new interface may create a one-off charge, additional access and a later exit milestone. Keeping these records linked reduces the risk that operational decisions occur outside the approved funding and risk case.

Figure 1. Illustrative monthly charge and dependency weight by workstream



Author assumptions only. Dependency weight is a planning measure, not a probability or monetary loss estimate.

21. Quantify dependency exposure

Duration alone does not describe transition risk. Seven months of access to a reporting archive differs from seven months of reliance on identity, payments and order processing. The proposed model uses weighted dependency-months: each workstream's duration multiplied by an author-assigned criticality weight. The measure is a planning tool, not an empirical probability or loss estimate.

The buyer can replace the illustrative weights with an approved scale tied to business consequences. A weight should reflect the service's interruption tolerance, fallback and concentration. The measure supports comparison among plans and highlights where a cheap transition service sustains a material operational dependency. It should not be aggregated into a monetary expected loss without calibrated data.

The register should show dependency declining as modules terminate. If a programme reports elapsed time while weighted dependency remains flat, the most critical services have not exited. The steering committee can then redirect resources to the bottleneck rather than celebrate low-priority completions.

Table 3. Hypothetical transition model assumptions

Workstream	Monthly TSA charge	Standalone build	Two-month dual run
Identity and access	0.14	0.55	0.20
ERP and order to cash	0.28	1.20	0.44
Finance and payments	0.18	0.70	0.28
Data and reporting	0.16	0.65	0.24
Network and facilities	0.12	0.50	0.18
People and support	0.10	0.35	0.16

GBP million. All values are author assumptions without supplier quotations or empirical calibration. Contingency equals 12 percent of build and dual-running cost.

22. Establish the hypothetical cash model

The numerical example uses six workstreams: identity and access, ERP and order-to-cash, finance and payments, data and reporting, network and facilities, and people and support. It assigns each a monthly transition charge, standalone build cost, two months of dual-running cost and a dependency weight. Every figure is an author assumption in GBP millions without supplier quotations or empirical calibration.

The model compares exit at months four, seven and ten. Total transition cash equals charges through exit, standalone build cost, two months of dual running and a contingency equal to 12 percent of build and dual-running cost. Opening liquidity equals 60 percent of build cost, two months of transition charges and the dual-running amount. These formulas illustrate funding timing and do not prescribe a reserve for a real acquisition.

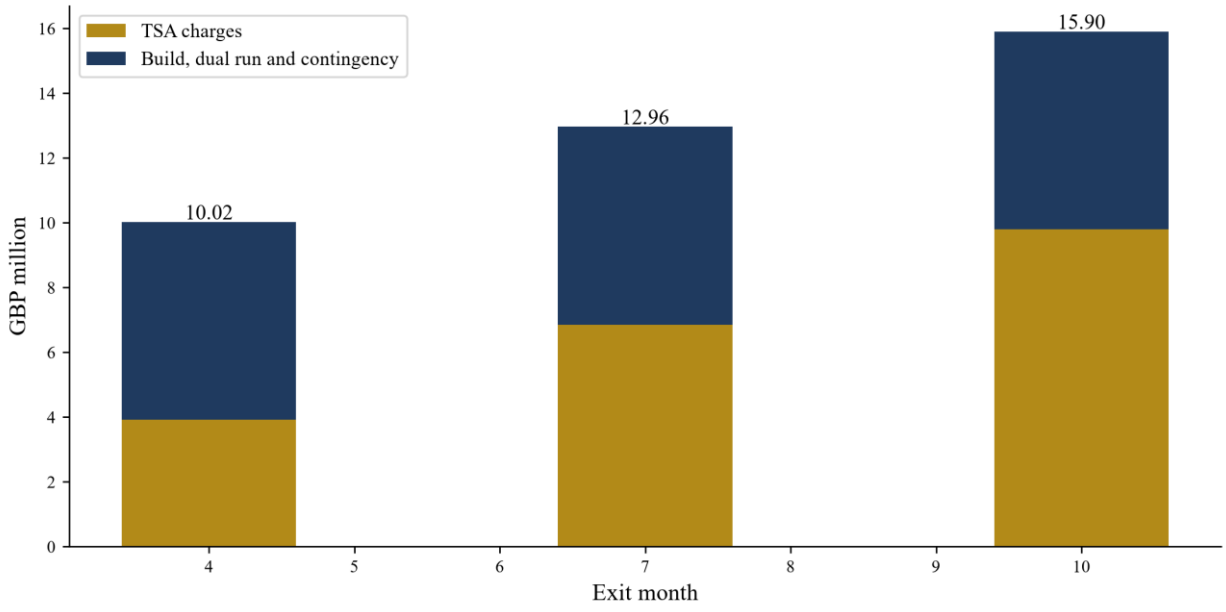
The sensitivity grid varies exit month from four to twelve and build-cost overrun from zero to 40 percent. It excludes taxes, financing costs, transaction fees, working-capital movements, service failure losses, recoveries and differences in expenditure timing. No likelihood is attached to any case. The model is designed to make assumptions visible and replaceable.

Table 4. Hypothetical transition cases

Exit month	TSA charges	Build plus dual run	Contingency
4	3.92	5.45	0.65
7	6.86	5.45	0.65
10	9.80	5.45	0.65

GBP million. No probability, financing cost, tax, working-capital effect or service-failure loss is included.

Figure 2. Hypothetical total transition cash by exit month



Author assumptions. The chart does not assign an execution probability or recommend an exit date.

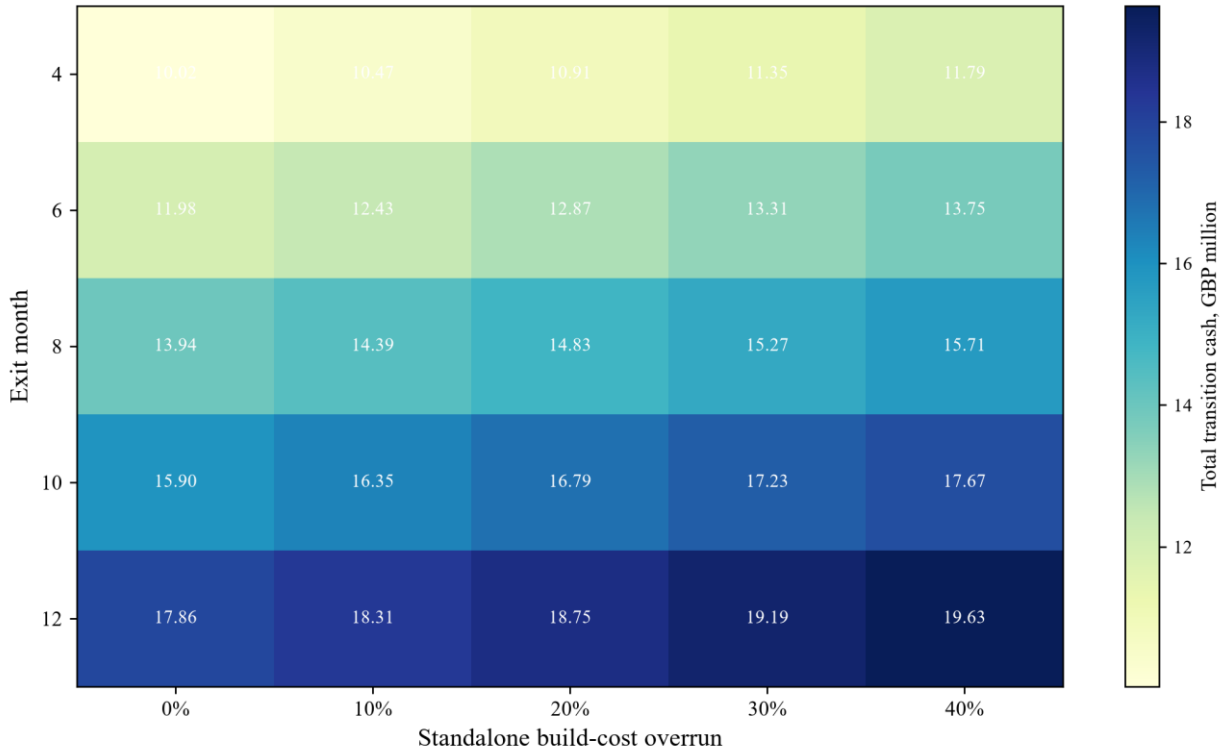
23. Read the three transition cases

The compressed case exits at month four. It carries the lowest transition charges and dependency-months, but the timetable may require more execution capacity than a buyer can safely mobilise. The model does not assign an acceleration premium or failure probability. The case is viable only if the critical path, vendor lead times, data availability and testing plan support it.

The base case exits at month seven. It creates three additional months of provider charges and dependency exposure compared with the compressed case. The buyer should test whether the extra period reduces implementation risk through proper procurement, migration and parallel operation. Time has value only when it is converted into accepted standalone capability.

The delayed case exits at month ten. It may arise from vendor delays, unresolved data, scarce specialists or failed testing. The model shows the cash effect mechanically. The operational decision must also consider provider deterioration, employee attrition, cyber exposure and a cutover moving into an unsuitable operating window. These consequences require transaction-specific evidence.

Figure 3. Hypothetical total cash sensitivity



Author assumptions. Each cell combines the stated exit month and build overrun; no likelihood is assigned.

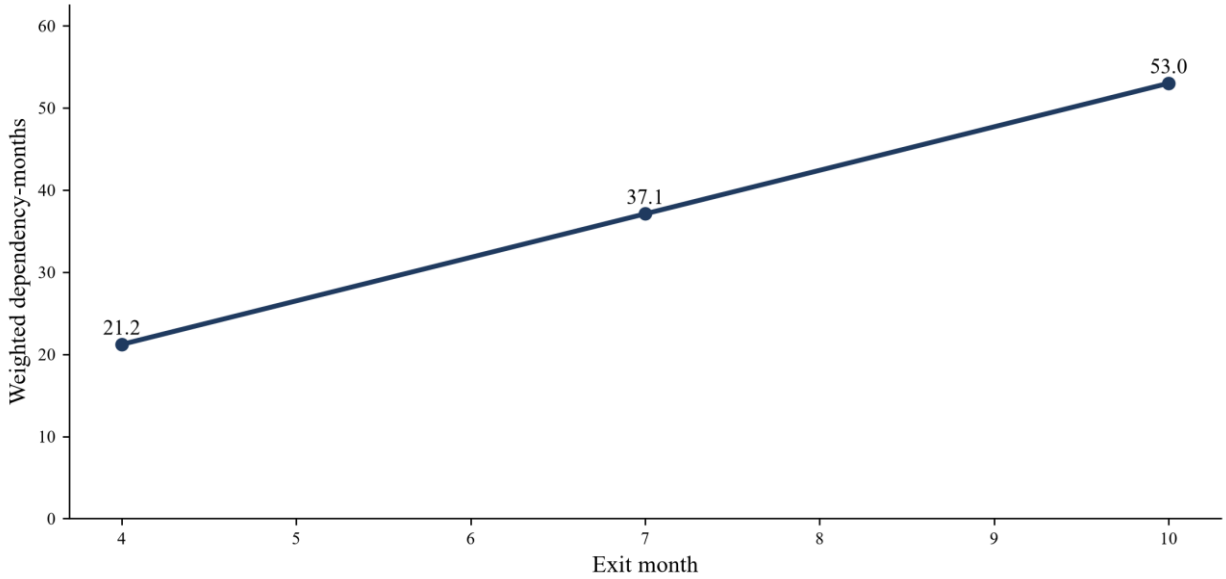
24. Use sensitivity as a decision tool

The two-dimensional sensitivity highlights interaction between schedule and build cost. A longer transition raises monthly charges while a build overrun increases the standalone and contingency components. The result helps the buyer distinguish a funding problem from an operating dependency. A plan can remain affordable while relying too long on a failing provider; another can reduce dependency quickly while requiring more opening cash.

The team should add scenarios that match verified risks. A vendor may require an upfront annual payment, a data migration may need specialist remediation, or the seller may cease a service earlier than contracted. Each scenario needs a stated trigger and response. The model should preserve the base assumptions and show the change rather than overwrite them.

Sensitivity does not establish a recommended exit date. The investment committee needs service criticality, execution evidence, contractual rights, provider capacity and liquidity. The grid is one input to that decision. Its value lies in exposing which assumptions change cash materially and where further evidence is worth obtaining.

Figure 4. Hypothetical weighted dependency-months



Author-assigned workstream weights multiplied by service duration. The measure is comparative and has no calibrated loss interpretation.

25. Govern the programme through evidence

The transition steering committee should receive an integrated view of business-service continuity, contract position, access, standalone milestones, cash and exceptions. Each item needs a source date and owner. The committee should distinguish verified completion, accepted risk and unresolved evidence. A colour status unsupported by a test or signed record does not demonstrate readiness.

Decision rights should reflect the consequence. Workstream leads can resolve routine actions within approved scope. Material service reductions, access exceptions, funding changes and cutover approvals belong with named executives or the board under the transaction governance. Legal, regulatory and insolvency questions should go to qualified advisers. The programme office maintains the record; it does not replace accountable judgement.

The evidence pack should survive a change in personnel or provider control. It includes executed agreements, service schedules, contacts, access registers, data maps, test results, reconciliations, vendor confirmations, decisions and closure evidence. Storing the only copy in the seller's environment defeats the purpose. The buyer should maintain a secure repository under its control.

26. Prepare for provider failure

The buyer should assume that at least one critical transition service can become unavailable. The response plan identifies the detection signal, decision authority, manual fallback, alternative vendor, data source, communications and cash required. It should prioritise people safety, legal obligations, customer harm and preservation of assets. Severe scenarios should be tested at a level proportionate to the service.

The UK Government's distress guidance separates short-term service maintenance from the longer-term alternative commercial solution and emphasises contingency planning for critical outsourced services [1]. That distinction is central to a failing-group transition. Emergency continuity can keep the business operating while the standalone programme removes the underlying dependency.

The plan should address simultaneous failures. Loss of the seller's network may affect identity, ERP, telephony and data together. Testing each module in isolation can understate the exposure. The team should map common dependencies and rehearse at least the combinations that could stop critical business services.

27. Close each service with proof

Service closure should be treated as a controlled transaction. The buyer confirms that the replacement is operating, data is complete, users and vendors have moved, open incidents are allocated, charges are reconciled and provider access is revoked. Both parties record retained data, continuing obligations and dispute items. The closure pack supports audit and reduces later ambiguity.

The buyer should monitor the replacement through a stabilisation period. Error rates, throughput, reconciliations, user incidents and customer outcomes show whether the new capability is sustainable. A short period of read-only access or specialist support may be appropriate where agreed, but it should have narrow scope and an automatic end.

Financial closure requires final invoices, pass-through evidence, deposits, credits and asset transfers. The programme reconciles actual spend to the approved case and explains variances. This record improves later acquisition reviews and prevents temporary charges from becoming an unnoticed permanent cost base.

Table 5. Proposed acquisition decision gates

Gate	Required evidence	Decision
Signing	Service catalogue, authority and funding	Approve executable bridge
Completion	Day-one access, cash and contacts	Release funds or invoke condition
Build ready	End-to-end tests and reconciled data	Approve parallel operation
Cutover	Accepted defects, fallback and support	Move production service
Closure	Revoked access, final data and charges	Terminate module

Proposed workflow. The accountable transaction body and qualified advisers determine actual conditions and approvals.

28. Convert the framework into an acquisition decision

The investment committee should receive four conclusions. First, which business services must remain available and their interruption tolerances. Second, which dependencies remain with the failing group and the rights supporting them. Third, when and how each dependency will end. Fourth, how much cash is required under the approved base and downside cases. Each conclusion should identify evidence gaps and conditions.

The acquisition agreement, transition services agreement, funding plan and standalone programme must reconcile. A service shown as available in the operating case needs an executed right and funded delivery. A service shown as ending needs a tested replacement. A cost in the contract needs a corresponding source of funds. The integrated check is the main control proposed by this paper.

The final decision remains conditional on the actual company, process and jurisdiction. The framework does not determine whether an administrator can provide a service, whether a contract transfers, whether data can be shared, or whether a proposed payment is protected. It gives the buyer a structured way to obtain those answers, connect them to continuity and build an acquired business that can stand independently.

References

[1] UK Government. Corporate Financial Distress Guidance Note. Updated 2026; accessed 5 September 2026. https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks/corporate-financial-distress-guidance-note-html

[2] The Insolvency Service. Director information hub: Administration. Accessed 5 September 2026. https://www.gov.uk/guidance/director-information-hub-administration

[3] Competition and Markets Authority. Merger remedies guidance, CMA87, December 2025. Accessed 5 September 2026. https://www.gov.uk/government/publications/merger-remedies

[4] UK Government and Government Legal Department. Model Services Contract and guidance, version 2.2A. Updated September 2025; accessed 5 September 2026. https://www.gov.uk/government/collections/model-services-contract

[5] Financial Conduct Authority. Operational resilience: insights and observations for firms. Accessed 5 September 2026. https://www.fca.org.uk/firms/operational-resilience/insights-observations

[6] Information Commissioner's Office. Due diligence when sharing data following mergers and acquisitions. Accessed 5 September 2026. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/due-diligence/

[7] National Cyber Security Centre. Cyber Assessment Framework, Principle A4: Supply chain. Accessed 5 September 2026. https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-a-managing-security-risk/principle-a4-supply-chain

About the Author

Authored by Chennakeshav Adya, Independent Researcher

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds; bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.