

Operating Model Integration: Centralise, Federate or Preserve Autonomy?

A Domain-Level Decision Framework for Scale, Speed, Accountability and Local Advantage

Authored by Chennakeshav Adya, Independent Researcher

September 2026

Abstract

Acquirers frequently describe the combined operating model with one enterprise-wide label. The real design problem is more granular. Customer propositions, pricing, procurement, finance, people, data, technology, cybersecurity, risk and regulated activities can each have different sources of advantage, constraints and failure costs. This paper develops a domain-level framework for choosing among centralisation, federation and preserved autonomy after an acquisition. It tests strategic fit, scale economics, responsiveness, capability distinctiveness, regulation, information boundaries, control maturity, resilience, transition cost and reversibility. It then converts the selected model into decision rights, service interfaces, funding, metrics, migration gates and exception governance. Five figures and five tables present the domain-choice logic, weighted decision score, decision-rights architecture, transition-risk profile and operating-model certificate. The framework draws on current corporate-governance, merger-control, accounting, data-protection, cybersecurity, operational-resilience, workforce and sourcing sources. Eight frequently asked questions and thirty-eight primary or authoritative references support application. Numerical values are illustrative analytical scenarios. Transaction-specific conclusions require verified transaction terms, regulatory status, customer and supplier obligations, workforce arrangements, operating data, technology architecture, control evidence, tax, financing and legal advice in each relevant jurisdiction.

JEL Classification: G34, L22, M10, M14, D23

Keywords: operating model integration, centralisation, federation, autonomy, post-merger integration, decision rights, shared services, governance, M&A

1. Define the unit of design

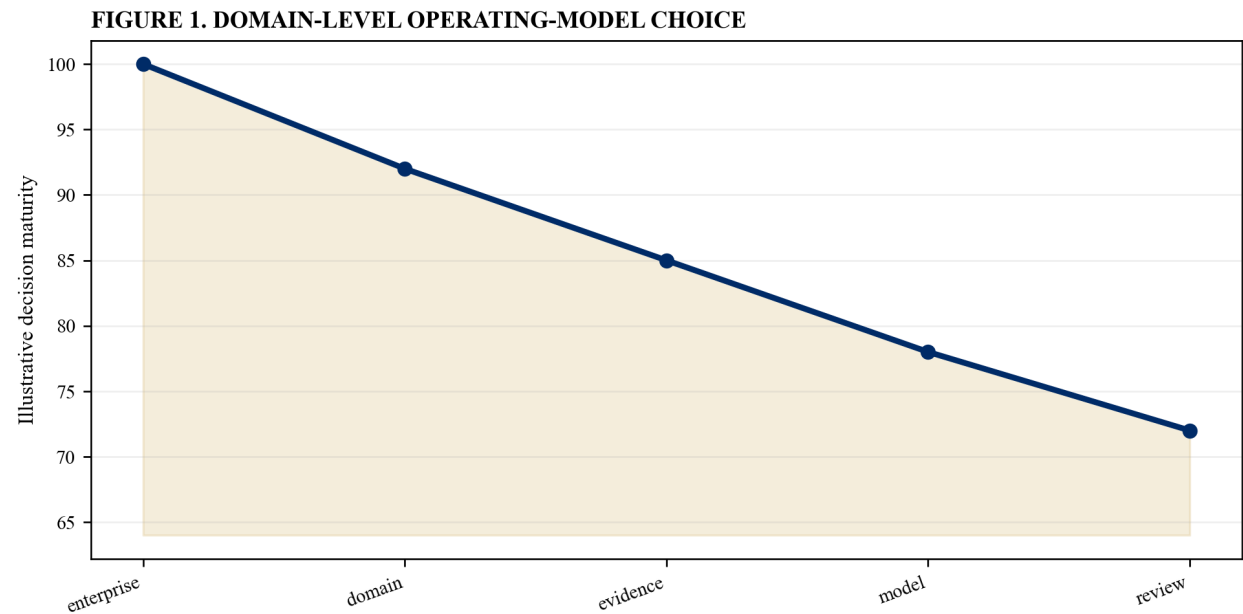
The integration leadership should separate the enterprise into customer, product, geography, function, process, data, technology, control and legal-entity domains. The required output is a domain inventory. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [1][2].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that an enterprise label can conceal incompatible operating requirements. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

Figure 1. Domain-level operating-model choice



Illustrative analytical scenario; verified transaction evidence should replace index values.

2. Reconstruct the acquisition logic

The integration leadership should connect each domain to the transaction thesis, ownership advantage and value mechanism. The required output is a thesis-to-domain map. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [1][3].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that integration choices can drift away from the reason the asset was acquired. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

3. Set the three model archetypes

The integration leadership should define centralised ownership, federated standards with local execution and preserved operating autonomy. The required output is an archetype dictionary. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [4][5].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that participants can use the same label for materially different authority and service arrangements. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

Table 1. Operating-model archetypes

Archetype	Authority	Primary strength	Principal control
centralise	enterprise centre	scale and consistency	service accountability
federate	shared standards and local execution	balance and adaptability	explicit interfaces
preserve autonomy	business or entity	distinctiveness and speed	group minimums

Illustrative structure; verified transaction evidence and specialist review govern.

4. Identify non-negotiable boundaries

The integration leadership should record merger-control, licensing, ring-fencing, customer, confidentiality, workforce and contractual restrictions. The required output is a boundary register. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [6][7].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that integration can breach a legal or commercial constraint before the target model is approved. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

5. Measure scale economics

The integration leadership should quantify volume leverage, fixed-cost absorption, scarce expertise, platform utilisation and purchasing power. The required output is a scale-value case. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [8][9].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that centralisation can be justified by headline savings that disappear after transition and service costs. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

6. Measure local responsiveness

The integration leadership should test decision latency, market knowledge, customer proximity, regulatory access and operational variability. The required output is a responsiveness score. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [10][11].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that a distant centre can reduce the speed and quality of local decisions. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

7. Protect differentiated capability

The integration leadership should identify talent, routines, data, relationships, intellectual property and culture that create distinctive performance. The required output is a capability-preservation map. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [1][12].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that standardisation can erase the capabilities that supported the purchase price. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

8. Define control consistency

The integration leadership should set group minimums for financial, operational, reporting, compliance, cyber and conduct controls. The required output is a minimum-control baseline. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [4][13].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that autonomy can leave material risk outside effective group oversight. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

9. Assess concentration risk

The integration leadership should model the failure impact of shared platforms, centres, suppliers, leaders and data dependencies. The required output is a concentration-risk view. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [14][15].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that scale benefits can create a single point of enterprise failure. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

10. Test resilience and recoverability

The integration leadership should compare recovery objectives, alternate capacity, manual workarounds, data restoration and crisis authority. The required output is a resilience design. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [14][16].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that the target model can improve efficiency while weakening recovery capability. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

11. Allocate board and executive accountability

The integration leadership should retain clear oversight for strategy, risk appetite, material controls and operating-model performance. The required output is an accountability charter. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [4][17].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that distributed execution can diffuse ultimate accountability. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

12. Design decision rights

The integration leadership should assign propose, challenge, approve, execute, assure and escalate rights for each material decision. The required output is a decision-rights matrix. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [17][18].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

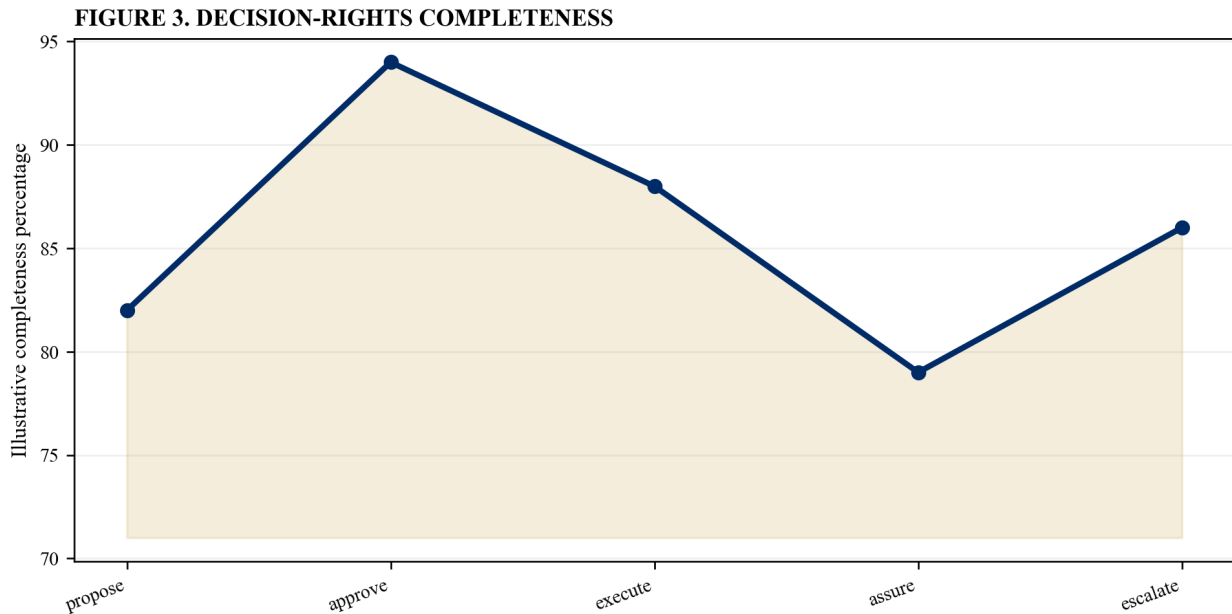
The principal risk is that unclear authority can produce delay, duplicate work or unauthorised commitments. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

Table 3. Decision-rights architecture

Right	Required clarity	Evidence
approve	named authority	decision record
execute	accountable owner	service measure
assure	independent challenge	control testing
escalate	threshold and route	exception log

Illustrative structure; verified transaction evidence and specialist review govern.

Figure 3. Decision-rights completeness

Illustrative analytical scenario; verified transaction evidence should replace index values.

13. Separate standards from execution

The integration leadership should decide which policies, architectures, data definitions and controls are common while execution remains local. The required output is a standards-and-execution map. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [13][19].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that federation can become unmanaged variation when common standards lack owners. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

14. Design the commercial model

The integration leadership should allocate proposition, pricing, sales, account ownership, channels and customer-service authority. The required output is a commercial operating model. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [6][20].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that premature account or pricing integration can harm customers and competition compliance. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

15. Design the product model

The integration leadership should balance common portfolio governance with product-level ownership, experimentation and lifecycle accountability. The required output is a product governance map. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [10][21].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that central portfolio control can slow innovation while autonomous products can duplicate investment. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

16. Design the geographic model

The integration leadership should allocate country, regional and global authority according to market variation, regulation and scale. The required output is a geographic authority map. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [7][22].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that global consistency can conflict with local licences, customers and operating conditions. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

17. Design shared services

The integration leadership should define eligible services, service owner, catalogue, service levels, charging, controls and exit rights. The required output is a shared-services contract. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [8][23].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that mandatory migration can transfer cost and failure without transferring accountability. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

18. Design procurement authority

The integration leadership should separate category strategy, supplier selection, contracting, demand approval and local continuity decisions. The required output is a procurement authority model. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [9][15].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that aggregated sourcing can increase dependency or weaken specialist supply. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

19. Design the finance model

The integration leadership should allocate policy, controllership, planning, treasury, tax, transaction processing and business-partner roles. The required output is a finance accountability model. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [24][25].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that central processing can obscure local economics or delay statutory obligations. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

20. Design the people model

The integration leadership should allocate workforce policy, organisation design, hiring, reward, performance, consultation and employee-relations authority. The required output is a people decision map. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [26][27].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that uniform change can disregard lawful consultation and scarce local capability. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

21. Design data governance

The integration leadership should assign controller roles, lawful purpose, stewardship, quality, access, retention and cross-border transfer decisions. The required output is a data-accountability architecture. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [28][29].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that shared data can exceed lawful purpose or create unclear accountability. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

22. Design technology ownership

The integration leadership should allocate enterprise architecture, platforms, applications, infrastructure, integration and technical-debt decisions. The required output is a technology ownership map. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [19][30].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that local freedom can multiply interfaces while central mandates can force unsuitable migrations. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

23. Design cybersecurity governance

The integration leadership should set risk tolerances, roles, policies, supply-chain oversight, incident authority and target profiles. The required output is a cyber governance profile. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [13][31].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that fragmented governance can leave material exposures between organisations and suppliers. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

24. Design AI governance

The integration leadership should allocate model purpose, data, evaluation, human oversight, deployment, monitoring and retirement authority. The required output is an AI accountability model. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [32][33].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that rapid reuse of models can propagate unreliable or unlawful decisions across the group. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

25. Design risk and compliance

The integration leadership should separate group risk appetite and minimum standards from business-owned risk decisions and local obligations. The required output is a three-lines responsibility map. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [4][34].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that central oversight can become detached from operations while local control can become inconsistent. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

26. Design regulated-entity interfaces

The integration leadership should preserve statutory responsibilities, capital, liquidity, records, outsourcing oversight and regulator access. The required output is a regulated-boundary map. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [7][35].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that group integration can weaken an entity's ability to meet independent obligations. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

27. Quantify transition economics

The integration leadership should model one-time cost, stranded cost, dis-synergy, productivity dip, working capital, tax and time to benefit. The required output is a net transition-value bridge. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [3][24].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that steady-state savings can conceal negative cash and value during migration. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

28. Score each domain

The integration leadership should weight strategic fit, scale, responsiveness, capability, control, resilience, regulation, cost and reversibility. The required output is a domain decision score. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [5][18].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that a qualitative preference can masquerade as a transaction-specific decision. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

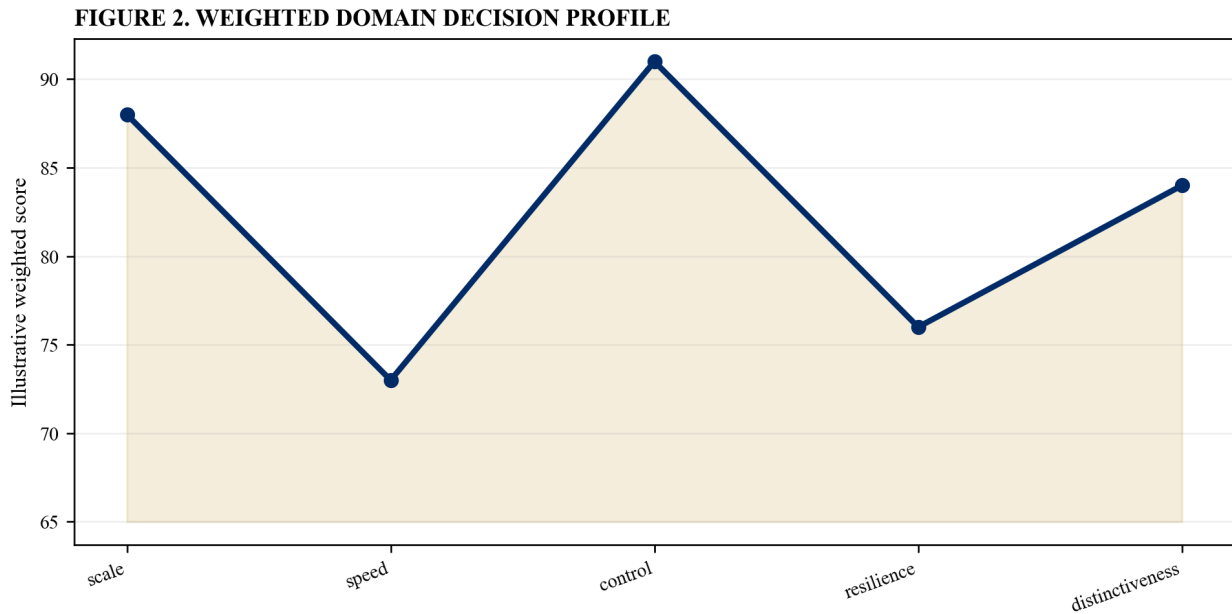
Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

Table 2. Domain decision score

Dimension	Centralise signal	Autonomy signal
economics	material scale	low transferable benefit
market	common proposition	local differentiation
control	inconsistent weakness	strong local assurance
resilience	diversified centre	concentration exposure

Illustrative structure; verified transaction evidence and specialist review govern.

Figure 2. Weighted domain decision profile



Illustrative analytical scenario; verified transaction evidence should replace index values.

29. Test inter-domain dependencies

The integration leadership should map how decisions in organisation, process, data, technology, controls and legal entities constrain one another. The required output is a dependency network. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [19][30].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that locally rational domain choices can create an incoherent enterprise model. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

30. Choose the target state

The integration leadership should approve the model, evidence, economics, boundaries, accountabilities and residual risk for each domain. The required output is a board-approved domain portfolio. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [4][17].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that an unowned compromise can persist because no explicit decision was recorded. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

31. Set transition states

The integration leadership should define temporary authority, services, controls, data access and reporting between current and target models. The required output is a transition-state architecture. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [6][16].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that the organisation can operate for months in an undocumented interim model. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

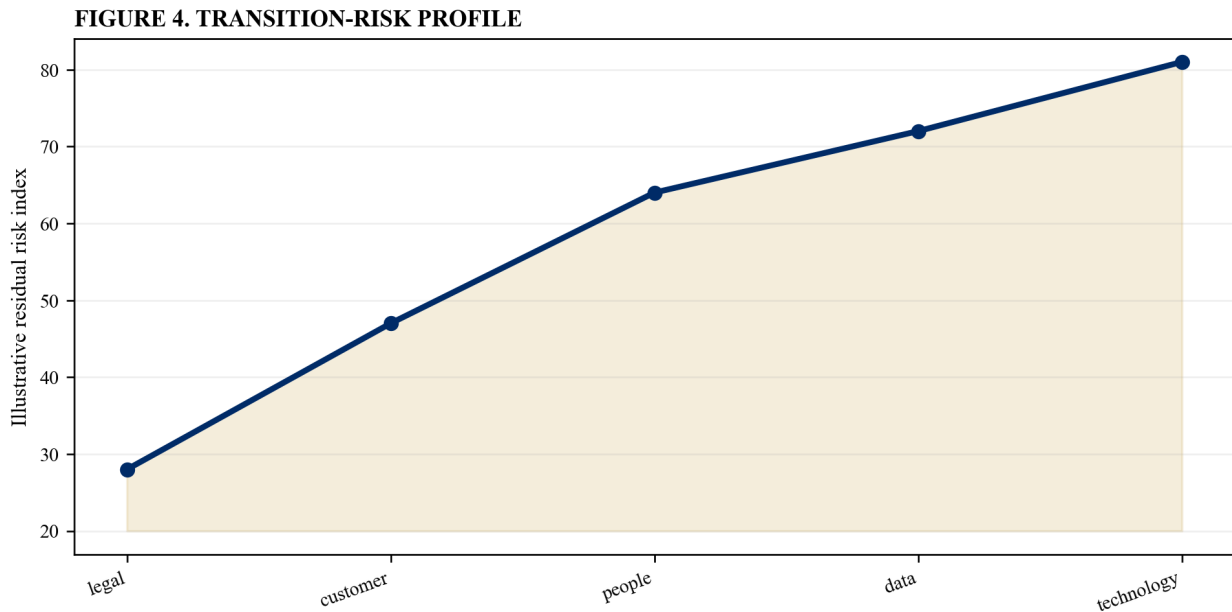
Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

Table 4. Transition-state controls

Transition area	Release condition	Fallback
people	consultation and roles	temporary authority
data	lawful access and quality	segregated environment
technology	tested interfaces	rollback plan
service	capacity and recovery	dual run

Illustrative structure; verified transaction evidence and specialist review govern.

Figure 4. Transition-risk profile



Illustrative analytical scenario; verified transaction evidence should replace index values.

32. Sequence migrations

The integration leadership should order changes by legal clearance, continuity, dependency, readiness, value, risk and management capacity. The required output is a gated migration roadmap. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [6][14].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that simultaneous centralisation can overload common platforms and leaders. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

33. Protect customer continuity

The integration leadership should test service, contracting, communications, complaint handling, privacy and recovery before release. The required output is a customer migration gate. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [20][28].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that internal efficiency can be achieved at the expense of customer outcomes. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

34. Control information exchange

The integration leadership should classify clean-team, competitively sensitive, personal, privileged and operational information. The required output is an information-control protocol. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [6][28].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that integration planning can create prohibited access or irreversible competitive harm. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

35. Fund the operating model

The integration leadership should allocate investment, run cost, transfer pricing, service charges, contingency and stranded-cost ownership. The required output is a funded operating-model plan. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [23][25].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that accountability can fail when authority and budget sit in different places. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

36. Measure service and value

The integration leadership should pair cost and productivity with quality, speed, customer, control, resilience and innovation measures. The required output is a balanced service scorecard. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [8][17].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that cost-only measures can reward deterioration elsewhere in the system. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

37. Govern exceptions

The integration leadership should require a reason, owner, control, duration, economics, review date and exit path for every variance. The required output is an exception register. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [4][13].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that federation can accumulate permanent exceptions that defeat common standards. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

38. Revisit the model with evidence

The integration leadership should review domain choices after regulatory, customer, performance, technology and capability evidence changes. The required output is a periodic model review. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [4][31].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that the target state can remain fixed after its assumptions have failed. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

39. Prepare the operating-model certificate

The integration leadership should reconcile decisions, evidence, rights, interfaces, economics, controls, exceptions and residual risk. The required output is an auditable certificate. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [1][17].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

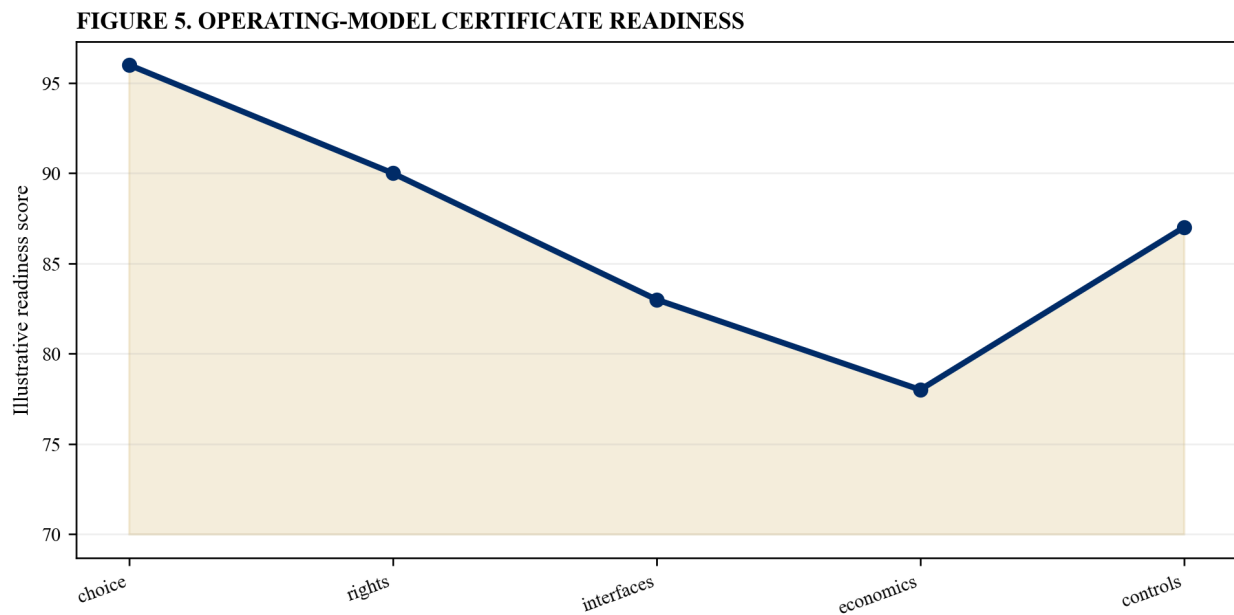
The principal risk is that leaders can declare integration complete without proving how the organisation now operates. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

Table 5. Operating-model certificate

Conclusion	Retained evidence	Acceptance
domain choice	weighted rationale	approved
authority	decision-rights map	understood
transition	gates and tests	verified
residual risk	exceptions and owners	accepted

Illustrative structure; verified transaction evidence and specialist review govern.

Figure 5. Operating-model certificate readiness

Illustrative analytical scenario; verified transaction evidence should replace index values.

40. Institutionalise accountable evolution

The integration leadership should embed model ownership, architecture governance, change control and post-implementation review. The required output is an enduring evolution cycle. Record the business purpose, evidence, decision owner, affected entities, legal and contractual boundaries, economics, interfaces, service expectations, controls, dependencies, transition state and review date [17][36].

Evaluate centralisation, federation and preserved autonomy separately. Test scale, decision speed, customer proximity, capability distinctiveness, regulatory obligations, information rights, resilience, transition cost, reversibility and management capacity. A domain may adopt a different model from the wider enterprise when the evidence supports it.

The principal risk is that future changes can recreate fragmentation or central bottlenecks. Quantify steady-state benefit, one-time cost, stranded cost, dis-synergy, service impact, control exposure, concentration risk, time to benefit and residual uncertainty across base, delayed, disrupted and remediated scenarios.

Retain source data, calculations, approvals, authority maps, interface specifications, tests, exceptions and post-implementation evidence. Release change only when continuity, customer, workforce, data, technology, control and regulatory gates are satisfied. Revisit the choice when underlying evidence changes.

References

- [1] IFRS Foundation, IFRS 3 Business Combinations, <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/>
- [2] IFRS Foundation, Business Combinations Disclosures Goodwill and Impairment Project, <https://www.ifrs.org/projects/work-plan/goodwill-and-impairment/>
- [3] IFRS Foundation, IAS 36 Impairment of Assets, <https://www.ifrs.org/issued-standards/list-of-standards/ias-36-impairment-of-assets/>
- [4] UK Financial Reporting Council, UK Corporate Governance Code 2024, <https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/uk-corporate-governance-code/>
- [5] US Government Accountability Office, Business Process Reengineering Assessment Guide, <https://www.gao.gov/products/aimd-10.1.15>
- [6] UK Competition and Markets Authority, Interim Measures in Merger Investigations, <https://www.gov.uk/government/publications/interim-measures-and-derogations-guidance-and-templates>
- [7] European Commission, EU Merger Control Procedures, https://competition-policy.ec.europa.eu/mergers/procedures_en
- [8] UK Government, Shared Services Strategy for Government, <https://www.gov.uk/government/publications/shared-services-strategy-for-government>
- [9] UK Cabinet Office, Sourcing Playbook, <https://www.gov.uk/government/publications/the-sourcing-playbook>
- [10] OECD, Guidelines for Multinational Enterprises on Responsible Business Conduct, <https://mneguidelines.oecd.org/mneguidelines/>
- [11] UK Competition and Markets Authority, Consumer Protection from Unfair Trading Regulations Guidance, <https://www.gov.uk/government/publications/consumer-protection-from-unfair-trading-regulations-traders>
- [12] International Organization for Standardization, ISO 56002 Innovation Management System, <https://www.iso.org/standard/68221.html>
- [13] Committee of Sponsoring Organizations of the Treadway Commission, Internal Control Integrated Framework, <https://www.coso.org/internal-control>
- [14] UK Financial Conduct Authority, Operational Resilience, <https://www.fca.org.uk/firms/operational-resilience>
- [15] National Institute of Standards and Technology, SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management, <https://csrc.nist.gov/pubs/sp/800/161/r1/final>
- [16] UK Government, UK Government Resilience Framework, <https://www.gov.uk/government/publications/the-uk-government-resilience-framework>
- [17] UK Financial Reporting Council, Corporate Governance Code Guidance, <https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/corporate-governance-code-guidance/>
- [18] US Government Accountability Office, Cost Estimating and Assessment Guide, <https://www.gao.gov/products/gao-20-195g>
- [19] The Open Group, TOGAF Standard, <https://www.opengroup.org/togaf>
- [20] UK Competition and Markets Authority, Green Claims Code, <https://greenclaims.campaign.gov.uk/>

- [21] International Organization for Standardization, ISO 9001 Quality Management Systems, <https://www.iso.org/standard/62085.html>
- [22] IFRS Foundation, IFRS 8 Operating Segments, <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-8-operating-segments/>
- [23] UK Government, Government Functional Standard GovS 008 Commercial, <https://www.gov.uk/government/publications/government-functional-standard-govs-008-commercial>
- [24] IFRS Foundation, IAS 7 Statement of Cash Flows, <https://www.ifrs.org/issued-standards/list-of-standards/ias-7-statement-of-cash-flows/>
- [25] IFRS Foundation, IAS 12 Income Taxes, <https://www.ifrs.org/issued-standards/list-of-standards/ias-12-income-taxes/>
- [26] European Union, Directive 2002/14/EC on Informing and Consulting Employees, <https://eur-lex.europa.eu/eli/dir/2002/14/oj>
- [27] UK Government, Business Transfers Takeovers and TUPE, <https://www.gov.uk/transfers-takeovers>
- [28] European Union, General Data Protection Regulation, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [29] European Data Protection Board, Guidelines on Controllers and Processors, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en
- [30] National Institute of Standards and Technology, Enterprise Architecture Model, <https://www.nist.gov/publications/nist-enterprise-architecture-model>
- [31] National Institute of Standards and Technology, Cybersecurity Framework 2.0, <https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20>
- [32] National Institute of Standards and Technology, AI Risk Management Framework, <https://www.nist.gov/itl/ai-risk-management-framework>
- [33] European Commission, Regulatory Framework for Artificial Intelligence, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- [34] Institute of Internal Auditors, Three Lines Model, <https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/>
- [35] European Banking Authority, Guidelines on Outsourcing Arrangements, <https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements>
- [36] US Department of Justice, Evaluation of Corporate Compliance Programs, <https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl>
- [37] International Organization for Standardization, ISO 22301 Business Continuity Management Systems, <https://www.iso.org/standard/75106.html>
- [38] IFRS Foundation, IFRS 18 Presentation and Disclosure in Financial Statements, <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-18-presentation-and-disclosure-in-financial-statements/>

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.