

ERP and Data Migration after M&A: Business Continuity before Standardisation

A Process-Criticality, Data-Quality and Customer-Impact Framework

Authored by Chennakeshav Adya, Independent Researcher

September 2026

Abstract

Post-merger ERP and data programmes can interrupt order capture, billing, cash, payroll, procurement, service, regulatory reporting and customer access when standardisation outruns operational evidence. This paper develops a continuity-first framework for sequencing systems and data migration after M&A. It begins with the deal thesis and a business-process criticality map, then establishes data ownership, lawful purpose, quality rules, lineage, interface dependencies, separation constraints and control requirements. It compares preservation, coexistence, consolidation and replacement by domain; designs transitional service, security, access, reconciliation and fallback controls; and gates each wave through rehearsals, business acceptance, rollback readiness and stabilisation evidence. Five figures and five tables present the continuity chain, migration-wave matrix, data-quality profile, cutover bridge and migration certificate. Eight frequently asked questions and thirty-eight primary or authoritative references support application. Numerical values are illustrative analytical scenarios. Transaction-specific conclusions require verified system inventories, contracts, licences, data maps, privacy obligations, cyber controls, financial reconciliations, customer commitments, regulatory duties, separation terms, capacity, cost and jurisdiction-specific legal, tax, accounting, technology and data-protection advice.

JEL Classification: G34, L86, M15, O32, C81

Keywords: ERP integration, data migration, post-merger integration, business continuity, data quality, systems separation, cutover, M&A

1. Start with the deal thesis

The integration leadership should link systems change to value drivers, control obligations and separation milestones. The required output is a technology-value map. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [1][2].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that migration can become a generic harmonisation exercise. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

2. Map critical business processes

The integration leadership should identify order-to-cash, procure-to-pay, record-to-report, payroll and service dependencies. The required output is a process-criticality inventory. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [3][4].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that application inventories can conceal operational consequence. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

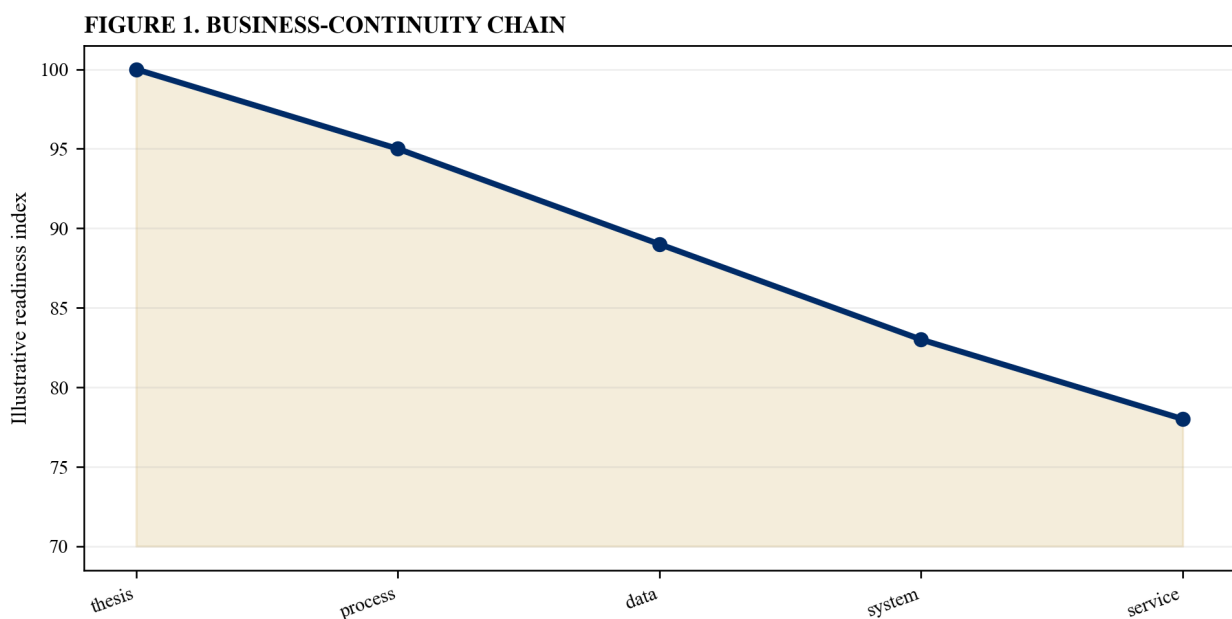
Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

Table 1. Process-continuity score

Process	Tolerance	Migration implication
order to cash	minutes to hours	protect first
record to report	close calendar	reconcile
payroll	statutory deadline	dual control
analytics	bounded delay	later wave

Illustrative structure; verified transaction evidence and specialist review govern.

Figure 1. Business-continuity chain



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

3. Set continuity tolerances

The integration leadership should define acceptable outage, data loss, backlog, manual work and recovery time by process. The required output is a continuity tolerance register. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [5][6].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that one enterprise target can misstate domain risk. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

4. Inventory the application estate

The integration leadership should record systems, versions, customisations, integrations, owners, licences and support status. The required output is an application register. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [7][8].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that shadow systems and spreadsheets can be omitted. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

5. Map data domains and ownership

The integration leadership should assign accountable owners to customer, supplier, product, employee, finance and operational data. The required output is a data-accountability map. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [9][10].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that technical custody can be mistaken for business ownership. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

6. Establish lawful data boundaries

The integration leadership should document controller roles, purpose, lawful basis, transparency, transfer and retention duties. The required output is a data-boundary register. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [11][12].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that a change of ownership can alter lawful processing conditions. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

7. Protect pre-close restrictions

The integration leadership should separate competitively sensitive information and limit integration action before lawful closing. The required output is a clean-team data protocol. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [13][14].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that system access can create premature coordination. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

8. Profile source-data quality

The integration leadership should measure completeness, validity, consistency, timeliness, uniqueness and referential integrity. The required output is a source-quality baseline. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [15][16].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that averages can conceal critical-record defects. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

9. Preserve lineage and provenance

The integration leadership should trace source, transformation, approval, destination and downstream use for material fields. The required output is a field-lineage map. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [9][17].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that converted values can lose their evidential history. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

10. Define the system-of-record model

The integration leadership should assign authoritative sources during coexistence and after each migration wave. The required output is a golden-source register. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [18][19].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that multiple masters can create silent divergence. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

11. Choose by domain

The integration leadership should compare preserve, coexist, consolidate and replace choices for each business capability. The required output is a domain disposition matrix. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [2][20].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that an enterprise-wide platform decision can ignore local economics. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

12. Separate integration from transformation

The integration leadership should distinguish continuity-critical migration from process redesign and feature expansion. The required output is a scope-boundary schedule. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [3][21].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that ambition can overload the critical path. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

13. Design transitional architecture

The integration leadership should use controlled interfaces, replication, identity federation and reporting bridges. The required output is a coexistence architecture. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [7][22].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that temporary interfaces can become unmanaged permanent infrastructure. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

14. Control identity and access

The integration leadership should reconcile users, roles, privileged access, segregation of duties and joiner-mover-leaver processes. The required output is an access-control matrix. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [23][24].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that legacy privileges can propagate into the combined estate. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

15. Secure the migration pipeline

The integration leadership should protect extraction, staging, transformation, transport, loading, logs and credentials. The required output is a migration security plan. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [24][25].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that staging environments can expose production data. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

16. Design the wave sequence

The integration leadership should rank domains by criticality, dependency, readiness, reversibility and learning value. The required output is a migration-wave matrix. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [5][20].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that easy technical migrations can precede essential dependencies. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

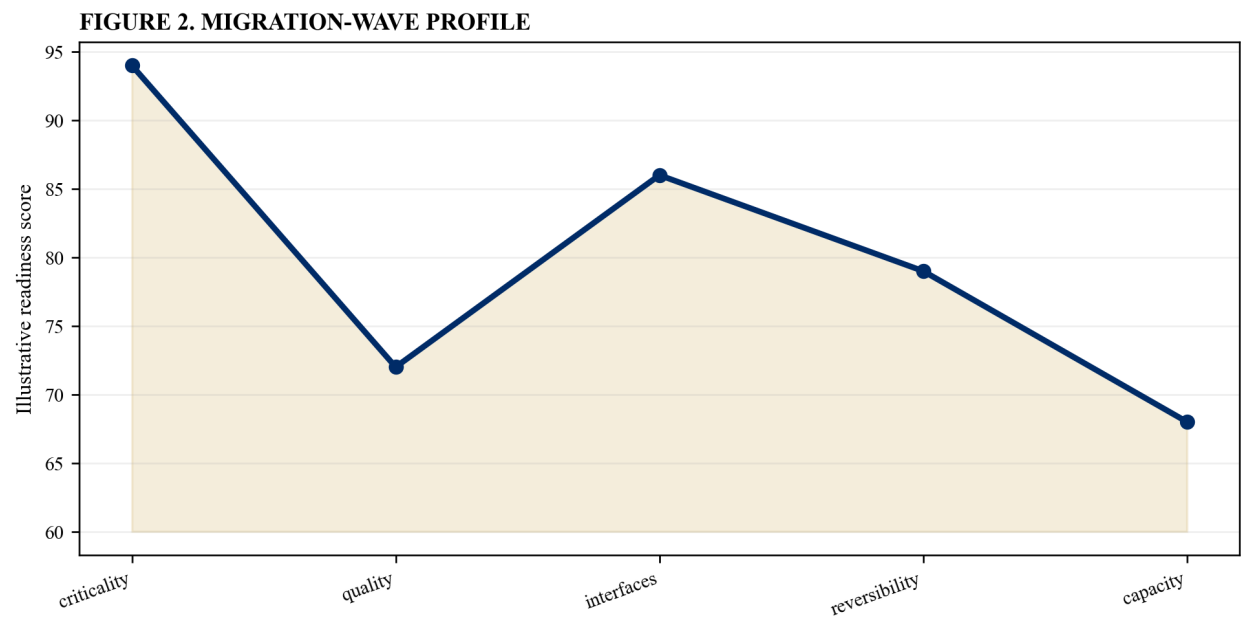
Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

Table 2. Migration-wave matrix

Readiness	Criticality	Treatment
high	high	controlled early wave
low	high	coexist and remediate
high	low	learning wave
low	low	defer

Illustrative structure; verified transaction evidence and specialist review govern.

Figure 2. Migration-wave profile



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

17. Quantify interface dependencies

The integration leadership should map upstream and downstream systems, timing, formats, volumes, errors and owners. The required output is an interface dependency graph. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [7][26].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that a successful load can still break downstream operations. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

18. Control master-data convergence

The integration leadership should govern identity resolution, duplicates, hierarchies, codes, units and survivorship rules. The required output is a master-data rulebook. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [15][18].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that forced matching can merge distinct legal or commercial records. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

19. Design transformation rules

The integration leadership should specify field mapping, cleansing, enrichment, defaults, rounding and exception treatment. The required output is a transformation catalogue. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [16][17].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that undocumented rules can change economics and reporting. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

20. Reconcile financial data

The integration leadership should prove opening balances, subledger totals, dimensions, tax, currency and consolidation mappings. The required output is a financial reconciliation pack. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [27][28].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that balanced totals can conceal account-level misclassification. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

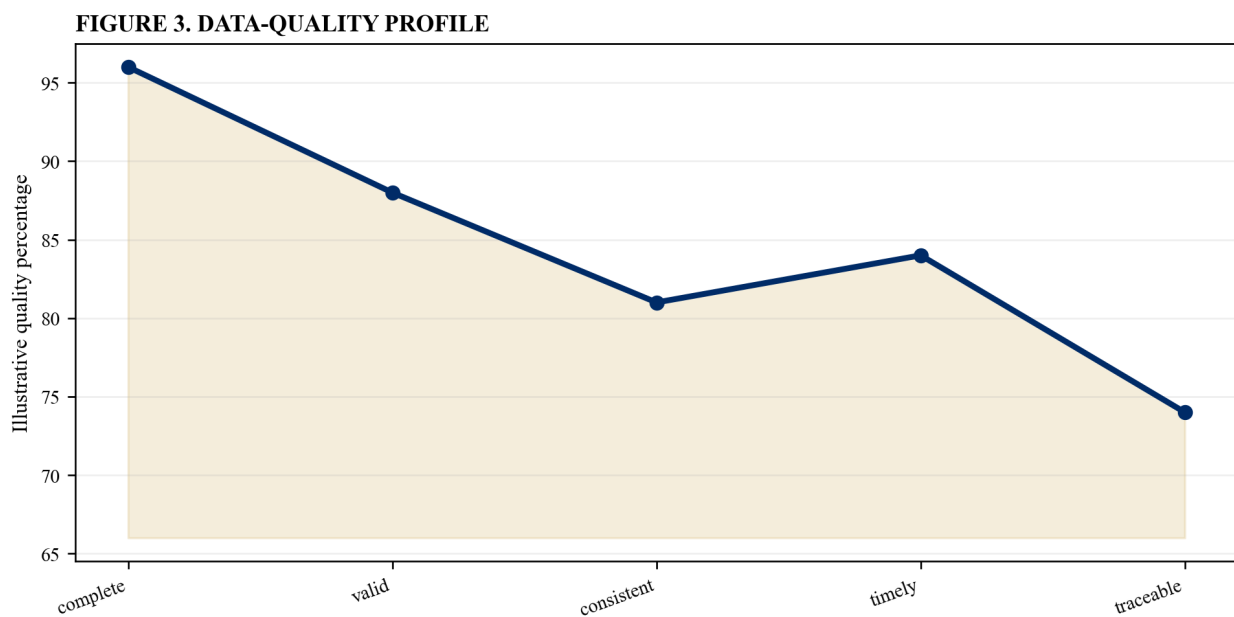
Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

Table 3. Data-quality controls

Dimension	Test	Evidence
completeness	required fields	exception count
validity	domain rules	reject log
consistency	cross-system	reconciliation
lineage	source to target	approved mapping

Illustrative structure; verified transaction evidence and specialist review govern.

Figure 3. Data-quality profile



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

21. Protect customer journeys

The integration leadership should test account access, orders, pricing, service entitlements, communications and consent. The required output is a customer-continuity plan. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [6][11].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that back-office success can coexist with customer harm. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

22. Protect supplier and cash flows

The integration leadership should test purchase orders, invoices, payments, bank details, approvals and fraud controls. The required output is a supplier-continuity plan. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [23][29].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that migration pressure can weaken payment controls. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

23. Protect regulated reporting

The integration leadership should map submissions, records, retention, evidence, accountability and reporting calendars. The required output is a regulatory reporting map. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [30][31].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that standardisation can remove jurisdiction-specific evidence. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

24. Govern third parties and licences

The integration leadership should review assignment, consent, capacity, support, data location, exit and audit rights. The required output is a vendor obligation register. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [8][32].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that a technically viable target can breach contract or licence terms. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

25. Design test coverage

The integration leadership should combine unit, integration, regression, performance, security, reconciliation and business acceptance testing. The required output is an evidence-based test plan. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [21][33].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that pass counts can obscure untested critical scenarios. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

26. Use production-like rehearsals

The integration leadership should simulate volumes, timings, failures, support handoffs and operational backlogs. The required output is a cutover rehearsal record. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [5][34].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that laboratory success can understate real operating conditions. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

27. Define cutover criteria

The integration leadership should require evidence on data, controls, users, interfaces, support, communications and fallback. The required output is a cutover gate. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [3][35].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that schedule pressure can substitute for readiness. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

28. Design rollback and recovery

The integration leadership should state restore points, reversal mechanics, decision deadlines, authority and customer treatment. The required output is a tested rollback plan. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [4][25].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that rollback can exist on paper without recoverability. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

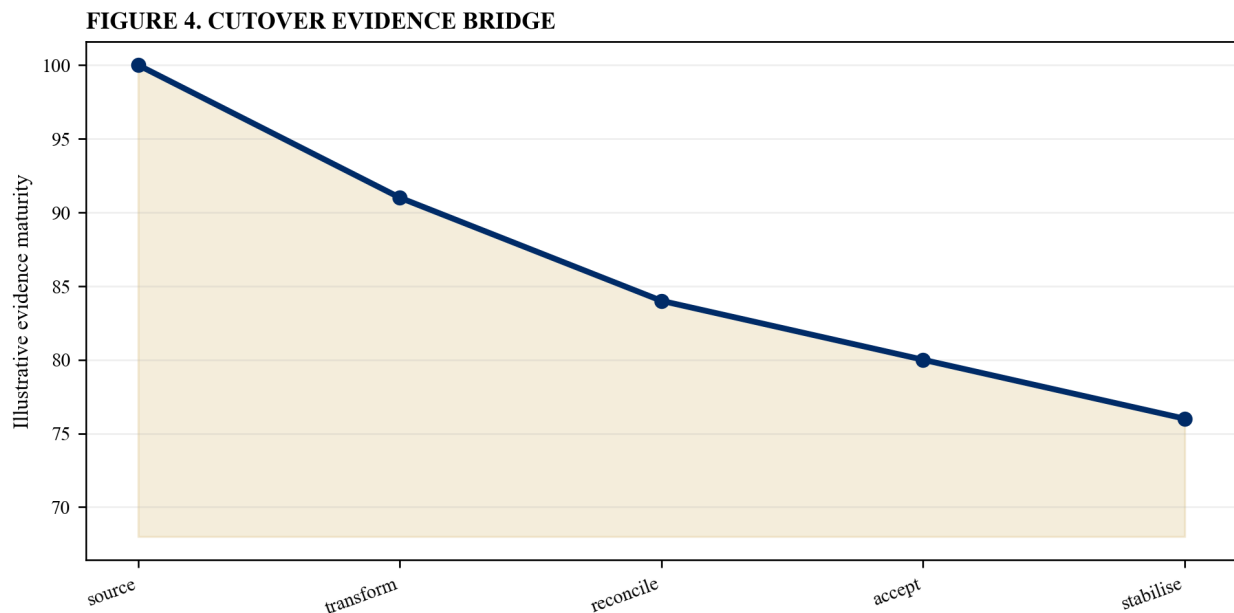
Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

Table 4. Cutover decision

Gate	Acceptance	Fallback
data	reconciled	restore point
process	rehearsed	manual continuity
control	approved	restricted mode
support	staffed	escalation

Illustrative structure; verified transaction evidence and specialist review govern.

Figure 4. Cutover evidence bridge



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

29. Control change and configuration

The integration leadership should freeze material changes, version mappings, approve exceptions and preserve deployable baselines. The required output is a configuration ledger. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [22][33].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that parallel releases can invalidate migration evidence. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

30. Prepare the operating organisation

The integration leadership should train users, service desks, control owners, data stewards and executive decision makers. The required output is an operational readiness pack. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [5][36].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that technical delivery can outrun human capability. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

31. Plan communications

The integration leadership should sequence messages for employees, customers, suppliers, regulators and support teams. The required output is a stakeholder communication plan. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [6][11].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that late or generic messages can amplify disruption. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

32. Run command and incident governance

The integration leadership should establish decisions, telemetry, thresholds, escalation, communications and authority during cutover. The required output is a cutover command model. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [25][35].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that distributed accountability can delay containment. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

33. Stabilise before the next wave

The integration leadership should clear defects, reconcile backlogs, validate controls and measure process performance. The required output is a stabilisation scorecard. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [4][37].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that success can be declared at technical go-live. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

34. Measure business outcomes

The integration leadership should track customer service, cash, close, payroll, control exceptions, adoption, cost and value. The required output is an outcome dashboard. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [2][38].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that system availability can conceal business deterioration. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

35. Govern data retention and deletion

The integration leadership should preserve required records and evidence while removing redundant copies through authorised controls. The required output is a retention and deletion schedule. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [11][12].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that duplicate estates can expand legal and cyber exposure. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

36. Retire legacy systems safely

The integration leadership should prove archive access, legal hold, record integrity, support exit, decommission and cost removal. The required output is a retirement certificate. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [17][32].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that premature shutdown can destroy evidence or continuity. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

37. Manage separation dependencies

The integration leadership should align transitional services, stranded systems, shared data, exit milestones and reverse dependencies. The required output is a TSA exit plan. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [8][20].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that integration and separation work can conflict. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

38. Reforecast economics

The integration leadership should update one-time cost, licences, interfaces, remediation, delay, stranded cost and expected value. The required output is a migration value case. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [1][28].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that original synergy estimates can survive contrary delivery evidence. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

39. Issue the migration certificate

The integration leadership should reconcile scope, lineage, controls, tests, acceptance, exceptions, residual risk and retirement evidence. The required output is an auditable migration certificate. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [3][9].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that leaders can declare completion without business proof. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

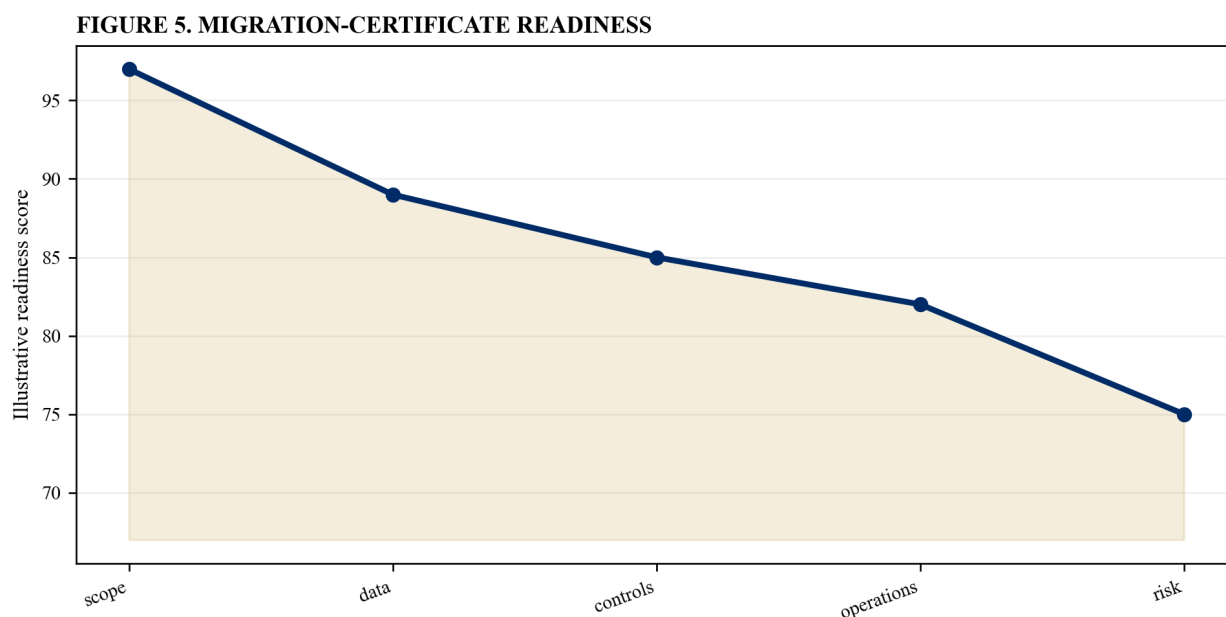
Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

Table 5. Migration certificate

Conclusion	Evidence	Acceptance
scope	domain inventory	approved
migration	lineage and testing	controlled
continuity	business outcomes	verified
risk	exceptions and rollback	accepted

Illustrative structure; verified transaction evidence and specialist review govern.

Figure 5. Migration-certificate readiness



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

40. Institutionalise data and platform governance

The integration leadership should embed ownership, quality measurement, architecture standards, continuity tests and lifecycle accountability. The required output is an enduring governance cycle. Record the business purpose, source and target state, process dependency, data owner, control owner, timing, acceptance evidence, decision rationale and review date [10][15].

Assess business continuity before standardisation. Test customer and supplier impact, cash and reporting exposure, data quality, interfaces, security, legal purpose, capacity, reversibility and the critical window. Apply documented business judgement to verified evidence.

The principal risk is that new fragmentation can reappear after programme closure. Compare preservation, coexistence, consolidation and replacement by domain, including transitional interfaces, manual continuity, remediation, rehearsal, rollback and staged retirement.

Retain source extracts, mappings, transformations, reconciliations, approvals, access logs, privacy controls, test results, acceptance, exceptions and outcomes. Reforecast when systems, data, dependencies, transaction timing, capacity or continuity needs change.

References

- [1] IFRS Foundation, IFRS 3 Business Combinations, <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/>
- [2] UK Government, The Green Book: Appraisal and Evaluation in Central Government, <https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government>
- [3] UK Government Service Manual, Service Standard, <https://www.gov.uk/service-manual/service-standard>
- [4] National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, <https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final>
- [5] International Organization for Standardization, ISO 22301 Business Continuity Management Systems, <https://www.iso.org/standard/75106.html>

- [6] UK Financial Conduct Authority, Operational Resilience, <https://www.fca.org.uk/firms/operational-resilience>
- [7] National Institute of Standards and Technology, Enterprise Architecture, <https://www.nist.gov/topics/enterprise-architecture>
- [8] UK Government, Technology Code of Practice, <https://www.gov.uk/guidance/the-technology-code-of-practice>
- [9] International Organization for Standardization, ISO 8000-1 Data Quality Overview, <https://www.iso.org/standard/81745.html>
- [10] International Organization for Standardization, ISO 8000-150 Data Quality Management Roles and Responsibilities, <https://www.iso.org/standard/80753.html>
- [11] UK Information Commissioner's Office, Due Diligence when Sharing Data following Mergers and Acquisitions, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/due-diligence/>
- [12] European Union, General Data Protection Regulation, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [13] UK Competition and Markets Authority, Interim Measures in Merger Investigations, <https://www.gov.uk/government/publications/interim-measures-and-derogations-guidance-and-templates>
- [14] European Commission, EU Merger Control Procedures, https://competition-policy.ec.europa.eu/mergers/procedures_en
- [15] International Organization for Standardization, ISO 8000-8 Information and Data Quality Concepts and Measuring, <https://www.iso.org/obp/ui/#iso:std:iso:8000:-8:ed-1:v1:en>
- [16] UK Government, Government Data Quality Framework, <https://www.gov.uk/government/publications/the-government-data-quality-framework/the-government-data-quality-framework>
- [17] UK National Archives, Managing Information, <https://www.nationalarchives.gov.uk/information-management/manage-information/>
- [18] UK Government, Data Standards Authority, <https://www.gov.uk/government/groups/data-standards-authority>
- [19] UK Government Service Manual, Managing Data, <https://www.gov.uk/service-manual/technology/managing-data>
- [20] UK Government, Digital and Technology Spend Control, <https://www.gov.uk/government/publications/digital-and-technology-spend-control-version-6>
- [21] UK Government Service Manual, Testing Your Service, <https://www.gov.uk/service-manual/helping-people-to-use-your-service/testing-your-service>
- [22] National Institute of Standards and Technology, Secure Software Development Framework, <https://csrc.nist.gov/pubs/sp/800/218/final>
- [23] National Institute of Standards and Technology, Zero Trust Architecture, <https://csrc.nist.gov/pubs/sp/800/207/final>
- [24] National Institute of Standards and Technology, Cybersecurity Framework 2.0, <https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20>
- [25] National Institute of Standards and Technology, Data Integrity Recovery, <https://csrc.nist.gov/pubs/sp/1800/11/final>
- [26] The Open Group, ArchiMate Specification, <https://pubs.opengroup.org/architecture/archimate3-doc/>
- [27] IFRS Foundation, IFRS 18 Presentation and Disclosure in Financial Statements, <https://www.ifrs.org/issue-d-standards/list-of-standards/ifrs-18-presentation-and-disclosure-in-financial-statements/>

- [28] IFRS Foundation, Conceptual Framework for Financial Reporting, <https://www.ifrs.org/issued-standards/list-of-standards/conceptual-framework/>
- [29] UK Government, Procurement Act 2023 Guidance, <https://www.gov.uk/government/collections/procurement-act-2023-guidance-documents>
- [30] UK Financial Conduct Authority, Systems and Controls, <https://www.handbook.fca.org.uk/handbook/SYSC/>
- [31] European Banking Authority, ICT and Security Risk Management, <https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-ict-and-security-risk-management>
- [32] UK Government, Outsourcing Playbook, <https://www.gov.uk/government/publications/outsourcing-playbook>
- [33] National Institute of Standards and Technology, Security and Privacy Controls for Information Systems, <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
- [34] National Institute of Standards and Technology, Data Integrity Detection and Response, <https://csrc.nist.gov/pubs/sp/1800/26/final>
- [35] UK Government Service Manual, Deploying Software Regularly, <https://www.gov.uk/service-manual/technology/deploying-software-regularly>
- [36] UK Government Service Manual, Learning about Users and Their Needs, <https://www.gov.uk/service-manual/user-research/start-by-learning-user-needs>
- [37] UK Government Service Manual, Measuring Success, <https://www.gov.uk/service-manual/measuring-success>
- [38] OECD, Digital Security Risk Management, <https://www.oecd.org/digital/digital-security/>

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.