Post-Merger Model Governance: One AI Control System across Two Companies

An acquisition framework for accountable operation and staged integration

Authored by Chennakeshav Adya

Independent Researcher

10 September 2026

Abstract

An acquisition committee needs a specific operating decision for every material AI deployment inherited at completion. This paper proposes a common governance system connecting deployment inventories, approval authority, evaluation evidence, vendor dependencies, data access and incident response across two companies. Separate technical environments may continue under that system while integration proceeds through documented acceptance conditions. Primary publications from NIST, the European Union, SDAIA and the UAE inform the analysis. Their different legal and institutional purposes require transaction-specific interpretation. A wholly hypothetical reconciliation starts with 180 inventory records and identifies 152 active deployments after duplicate removal, retirement evidence and additional discovery. A separate illustrative implementation budget totals USD 668,000; an assumed three-month extension and eight repeat evaluations increase it to USD 805,000. These figures demonstrate the calculation structure and provide no market benchmark, quoted advisory fee or return forecast. The proposed investment-committee package links expenditure to operating permissions, accountable decision makers and evidence of service continuity. It also identifies the conditions requiring restricted use, further evaluation or suspension before a shared platform can be approved.

JEL Classification: G34, M15, O33, K24

Keywords: post-merger integration, AI governance, model inventory, acquisition diligence, model validation, vendor risk, GCC acquisitions

1. Define the operating decision at completion

The acquisition committee should approve a documented operating basis for the AI systems that the combined business intends to use. The decision should identify permitted purposes, responsible entities, material limitations and the person authorised to suspend each service. For a revenue-critical application, the committee also needs evidence about the service available if the model is withdrawn. This paper proposes a post-completion framework for assembling that information and deciding which integrations can proceed.

A transaction can bring together applications that use the same underlying model through different contracts, data sources and customer interfaces. A shared supplier name provides an initial point of comparison. The integration team still needs to examine the deployed configuration and its actual use in each company. This includes conventional predictive models, third-party AI features within business software and generative systems that retrieve information or execute actions. The proposed scope follows operational exposure and decision authority.

The phrase one control system describes shared governance records and accountable decisions. It permits separate production environments where contractual conditions, technical dependencies or evaluation results support that arrangement. A common register can link those environments to the same approval

policy and incident procedure. Technical consolidation becomes a separately approved change with its own test evidence, budget and recovery arrangements. Continued operation depends on the conditions applicable to the individual service.

NIST's AI Risk Management Framework supplies a voluntary, cross-sector reference for organising governance, context mapping, measurement and risk treatment. Its inventory, monitoring and accountability outcomes are relevant to this proposed integration design. The framework does not establish that an acquisition is compliant or that an inherited system is safe. This paper uses its published outcomes to formulate diligence questions and operating records. The investment committee remains responsible for obtaining the professional advice and evidence needed for its actual decision. [1]

2. Establish the perimeter before changing access

Begin with the legal entities, business processes and environments included in the transaction. Record what transfers at completion and what remains dependent on the seller or a third party. Identify the intended operator of each service, the customers receiving its outputs and the staff who can alter its configuration. Before completion, any information sharing or integration preparation should follow the transaction's approved confidentiality and competition-law arrangements. The paper assumes no authority to combine systems ahead of legal completion.

The scope should extend to AI functionality embedded in purchased software. Ask each process owner to identify where recommendations or automated actions influence pricing, customer communications, production schedules, hiring or access to services. Reconcile those statements with authorised technical and procurement records. Keep discovery methods proportionate and approved. The objective is a traceable inventory of relevant uses; employees' personal accounts and unrelated confidential material remain outside an authorised review unless a lawful, specific process includes them.

For each deployment, define the operational unit being counted. A useful proposed unit is a versioned application in a specified environment, used by an identified entity for an approved purpose. Two applications using the same model family can remain two deployments because their data, permissions and consequences differ. Several registry entries may describe one deployment if they are duplicate administrative records. Preserve the evidence supporting each reconciliation decision so later counts can be reproduced.

Include dependencies that sit outside the acquired perimeter. Examples to investigate include a seller-managed identity service, a shared evaluation dataset and vendor support provided through the seller's contract. Record the dependency's owner, access arrangement, planned duration and replacement acceptance condition. A transition agreement should be reviewed for the assistance actually required. The integration plan can then connect dependency expiry to the date on which an alternative must have been tested and approved.

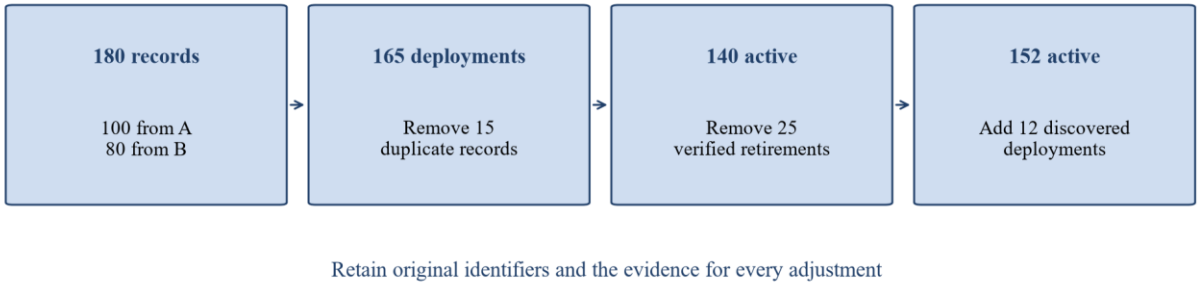
Separate discovery confidence from operational approval. An owner-confirmed inventory entry may still lack a validated monitoring threshold or a usable recovery process. Conversely, a well-controlled service may be absent from the initial transaction register. Track both conditions explicitly. This gives the committee a view of what has been found and a separate view of what evidence supports its continued use.

3. Reconcile the model inventory without losing deployments

Retain both companies' original identifiers and add a group identifier linked to them. The record should contain the model or service version, application purpose, operating entity, production location and responsible business owner. Link supporting documents through controlled references. Preserve historical versions so that a later incident can be connected to the configuration operating at the time. Changes to the inventory should identify the editor, reason and effective date.

The following reconciliation is wholly hypothetical. Company A supplies 100 records and Company B supplies 80. Review identifies 15 duplicate administrative records describing deployments already counted. Evidence then confirms that 25 of the remaining deployments have been retired. An approved discovery exercise finds 12 additional active deployments absent from the initial registers. The resulting active population is 180 less 15, less 25, plus 12, or 152. Every number is an illustrative assumption.

Figure 1. Hypothetical reconciliation to 152 active deployments



Author's illustrative inventory arithmetic. Shared model families are not removed merely because they have the same supplier.

Retirement requires a defined evidence standard. The proposed record should show that the production route is disabled, relevant credentials have been addressed and any continuing retention obligation has an owner. A project marked closed in a development tool may still leave an active scheduled process. The inventory owner should reconcile the administrative status with authorised operational evidence. Historical assets requiring retention can remain in an archive category separate from active deployments.

After reconciliation, classify the 152 illustrative deployments by operating evidence. Assume 82 have complete evidence for their present approved use, 50 have time-limited conditional approval and 20 require an unresolved operating decision. The first two categories total 132, or 86.8% of the inventory. That percentage describes recorded approval status under the assumed criteria. It says nothing by itself about the severity of remaining risks or the adequacy of the criteria used.

4. Connect each deployment to a permitted use

Write the intended purpose in operational language. A service that drafts a response for a trained employee has a different workflow from a service authorised to issue that response directly to customers. Record the output, recipient, permitted action and required review. Describe prohibited extensions and the route for requesting a change. The approved use statement should be specific enough that a process owner can identify when actual practice has departed from it.

Attach a data-access map to that statement. Identify the source systems, data categories, retrieval permissions and destinations for logs or outputs. The map should show the relevant legal entity and environment for each connection. Counsel and privacy specialists should assess the applicable rights and restrictions. Technical staff should demonstrate that the approved access can be implemented. A group-level ownership change provides no evidence that every dataset can be made available to every application.

Review the permissions of systems capable of taking actions. An application that can search a document store, update a customer record and initiate a payment-related workflow needs a separate description of each capability. Ask which permissions are necessary for the approved purpose and who can grant additional access. Test rejected actions and escalation paths as well as successful requests. The proposed acceptance record should identify which actions remain subject to human approval.

For generative systems, record the retrieval sources, prompts or configuration instructions, connected tools and relevant model version alongside the application code. NIST's Generative AI Profile addresses third-party dependencies and recommends inventorying entities with access to organisational content. Its discussion of value-chain and component integration supports a dependency review extending beyond the model supplier. The proposed transaction inventory uses that guidance to request version-specific evidence about access and service dependencies. [2]

Make access changes individually reviewable during integration. A proposed shared identity group should list the people and applications that gain access, the business purpose and the expected expiry of temporary permissions. Retain the test used to verify those boundaries. Where access remains unresolved, document the service configuration that is currently permitted and the work needed to reach a broader operating arrangement.

5. Allocate decision authority across the combined business

The board or delegated executive should establish the risk appetite and appoint an accountable integration sponsor. The sponsor needs authority to resolve conflicts over resources, deadlines and business priorities. A named business owner should remain accountable for each service's approved use and consequences. Engineering should maintain the implementation and technical evidence. Independent challenge should be allocated to suitably competent people with sufficient separation from the delivery decision.

The following responsibility matrix is a proposed allocation for adaptation to the actual organisation. R means responsible for performing the work, A means accountable for the stated decision, C means consulted and I means informed. Each row assigns one accountable role. Professional review responsibilities remain subject to the organisation's legal and regulatory requirements. The matrix does not delegate statutory responsibilities away from the person or entity that holds them.

Table 1. Proposed governance responsibility matrix

Decision or work item	Sponsor	Business owner	Technical lead	Independent reviewer
Inventory and purpose record	I	A	R	C
Evaluation evidence and challenge	I	C	R	A
Ordinary release within approved limits	I	A	R	C
Material integration exception	A	R	C	C
Emergency technical containment	I	A	R	C
Resumption after material incident	A	R	R	C

Illustrative allocation. Sponsor, owner, technical lead and independent reviewer must be identified by name before use. Legal and compliance specialists are consulted on applicable requirements throughout.

The matrix should be accompanied by explicit delegations and response arrangements. Name alternates for absences and define how urgent decisions reach them. A governance committee meeting every month cannot serve as the sole mechanism for a service requiring immediate containment. Pre-authorise specific emergency actions within defined conditions, retain an audit trail and require subsequent review. The accountable owner should know the operational consequence of each authorised action.

Independent review should produce a conclusion that the decision maker can use. It should state what was tested, the important limitations and the changes requiring another review. An unresolved disagreement should remain in the approval record with the decision and rationale. Staff who evaluate a system need access to relevant evidence and an escalation channel when that evidence is missing. NIST identifies explicit roles and executive responsibility within its governance outcomes. [1]

Avoid making one individual the permanent owner of every deployment merely to complete the register. Allocate ownership to the function capable of understanding the service and acting on its consequences. Group governance can define common requirements and challenge exceptions while operational accountability remains identifiable. Review the allocation when organisational restructuring changes reporting lines or removes a role.

6. Harmonise approval thresholds through evidence

Compare the two companies' existing approval rules using actual changes that their systems undergo. Relevant examples include introducing a new data source, changing a model version, expanding to a new customer population or granting an application a new action capability. Record the evidence each company currently requires and the authority that signs the decision. This comparison should identify gaps and useful controls that need to survive the integration.

Create a common change taxonomy with thresholds tied to consequences and uncertainty. Routine maintenance may qualify for an established technical release procedure when it remains within an evaluated operating range. A change in purpose, affected population, autonomy or legal role should prompt additional review. Define the evidence required to establish that a change falls within an existing approval. A developer's description of a change as minor should be supported by the recorded assessment.

The approval record should specify measurable acceptance conditions where measurement is appropriate. Include relevant performance metrics, test populations, observation periods and limits on interpretation. Document qualitative requirements such as verified contractual permission or a trained human reviewer separately. A composite score can conceal a missing mandatory condition. The proposed process records each required condition and the evidence supporting its conclusion before a release decision is made.

Use time-limited exceptions for a defined operating arrangement where the authorised decision maker considers that arrangement permissible. State the unresolved issue, interim control, responsible owner and expiry condition. Identify events that cancel the exception early, such as a vendor version change or a monitoring breach. Continued operation after expiry requires a fresh decision with current evidence. The paper gives no basis for using an exception to override an applicable prohibition or mandatory obligation.

Retain a change history through the transition. When two release calendars overlap, record which version was evaluated and which version was deployed. Establish an agreed point at which an approval must be reassessed because intervening changes have affected its evidence. A shared ticket identifier can connect engineering records, business approval and independent review. The acceptance test should confirm that these references lead to the actual documents and deployed configuration.

7. Evaluate performance in the combined operating context

The evaluation plan should reflect the use proposed after completion. Identify the users, languages, data sources, transaction volumes and decision consequences in scope. A test performed for the seller's original workflow may require extension if the acquirer introduces a different customer population or action. Preserve the original results and document what remains applicable. The reviewer should state which additional observations are required before approving the changed use.

Use an evaluation dataset whose provenance and permitted use have been reviewed. Separate development material from the evidence used for independent challenge where the evaluation design

requires that distinction. Record sampling methods, relevant subgroups and known limitations. Quantitative results should include the denominator and test conditions. A percentage without a description of the cases assessed cannot support a reliable comparison between the two companies' evaluation records.

Test the whole application path. A correct model response can be transformed incorrectly by a downstream workflow, delivered to an unauthorised recipient or accepted without the intended review. Include input handling, retrieval, user interface, approvals and final actions in the test design. For systems using tools, assess whether the application respects permission boundaries under adverse inputs. The permitted level of testing should be authorised and isolated from production actions where necessary.

Document failure cases that matter to the business decision. A customer-support application may require separate assessment of unsupported commitments, disclosure of restricted information and incorrect routing of complaints. A production-planning application may require assessment of infeasible schedules and the consequences of late human intervention. These are proposed examples for use-case design. The actual test suite should follow the service's purpose, contractual obligations and relevant professional requirements.

NIST's measurement function includes testing before deployment and during operation, with attention to uncertainty and the appropriateness of methods. The integration committee should receive the evaluator's limitations alongside the results. A successful test supports the specific conclusion warranted by that test. Broader operating approval requires the remaining evidence identified in the evaluation plan. Review frequency should reflect the application and the changes that can affect its performance. [1]

8. Establish monitoring that leads to a decision

Each monitoring measure should have a defined response. Record the data source, calculation, reporting frequency and person who investigates a breach. Identify how missing observations are detected and what happens when monitoring itself becomes unavailable. The business owner should understand whether a measure describes service availability, output quality, access behaviour or an outcome affecting customers. These dimensions require separate interpretation even when they appear on one dashboard.

Preserve company-specific measures until the team has demonstrated a valid common definition. Two applications can report accuracy using different samples, labels or review methods. Combining those percentages may produce an uninterpretable result. A harmonisation record should explain the old definition, the proposed definition and any period of parallel measurement. Retain the information required to interpret historical results after a reporting measure changes.

Choose thresholds by reference to the approved purpose, evaluation evidence and applicable obligations. The paper proposes no universal accuracy threshold or acceptable error rate. Some conditions require immediate restriction even if aggregate performance remains within a numerical limit. Examples to assess include unauthorised access, a materially changed purpose and the loss of a required human-review step. Document those conditions alongside statistical alerts so the incident team can act on either type.

Measure human oversight as an operational activity. Establish who reviews outputs, the workload assigned to them and the evidence retained when they intervene. Test whether reviewers receive sufficient context to recognise a problematic result. Examine whether they can pause the workflow and obtain assistance. A requirement for review should be accompanied by staffing and service-capacity assumptions that can be checked against the actual operating schedule.

Review incidents, complaints and near misses together with numerical performance. A customer report can identify an issue outside the current test set. Link the report to the deployment and version concerned, investigate it and record any change to the evaluation plan. Maintain access controls over complaint

details and incident evidence. Monitoring should support a documented decision about continued operation, additional controls, re-evaluation or suspension.

9. Integrate vendors and contracts into governance

The vendor register should identify which entity contracts for each service and which entity uses it after completion. Examine assignment, change-of-control, authorised-user and processing provisions with the appropriate advisers. Record the evidence supporting continued access, including any required consent or revised order form. A supplier's technical ability to provide access should be considered separately from the contractual permission to use that access.

Document the changes the supplier can make without a customer-controlled release. These may concern the model, hosting arrangement, retention settings or application features, depending on the actual service. Obtain the applicable notification and version-management terms. The technical owner should explain how a supplier change is detected and how its effect on the approved use is assessed. Keep an alternative operating plan for dependencies whose relevant configuration cannot be held constant.

Agree how incident information reaches both the supplier and the combined business. Identify support channels, authorised contacts and the information each party can share. Review the assistance available for investigation, containment and recovery. NIST's incident-response guidance treats third parties as participants in a shared-responsibility model and includes them in planning and exercises. The proposed integration process uses a joint exercise to test the arrangements described in the actual contract. [3]

Assess concentration by dependency and consequence. Several business applications may rely on one service endpoint or identity provider even where they use different model names. A dependency map should show which customer processes would be affected by the failure or withdrawal of that service. Test alternatives against the relevant data permissions, capacity and quality requirements. An untested second vendor remains a candidate contingency with outstanding acceptance work.

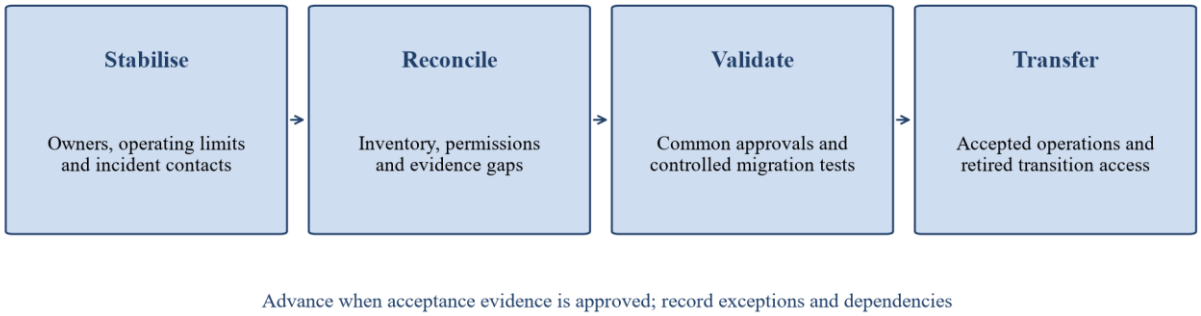
Keep procurement savings conditional on verified scope and exit costs. Consolidating contracts can change minimum commitments, usage rights and support arrangements. Ask finance to reconcile proposed savings with the cost of migration, remaining obligations and additional evaluation. The governance record should identify which supplier decision has been approved and the evidence required before recognising its effect in the integration budget.

10. Sequence control harmonisation through acceptance conditions

The proposed integration sequence begins with a stable operating record at completion. Establish accountable owners, preserve existing approved configurations and identify urgent decisions. Introduce shared incident contacts and a controlled change log before undertaking broad technical migration. Any known issue requiring immediate action should enter the appropriate response process. The sequence provides an organising framework; transaction-specific obligations and incident conditions can require earlier intervention.

The next phase reconciles inventories and compares control evidence. Confirm the purpose and dependencies of material deployments, review gaps and assign time-bound remediation. Introduce common record definitions and approval routes. This work can take place while separate production environments continue under their approved arrangements. A phase is complete when the required evidence and decisions exist, regardless of the date originally printed in the integration plan.

Figure 2. Proposed control harmonisation waves



An illustrative sequence with evidence-based acceptance conditions. No fixed completion time is assumed.

Migration should follow a tested design with an explicit recovery decision. Compare outputs and workflow behaviour in the proposed environment under approved test conditions. Determine which differences are expected and which require investigation. Agree the person who can stop migration, the latest point at which rollback remains possible and the evidence required to resume. A technical rollback should address data written or actions taken during the attempted cutover.

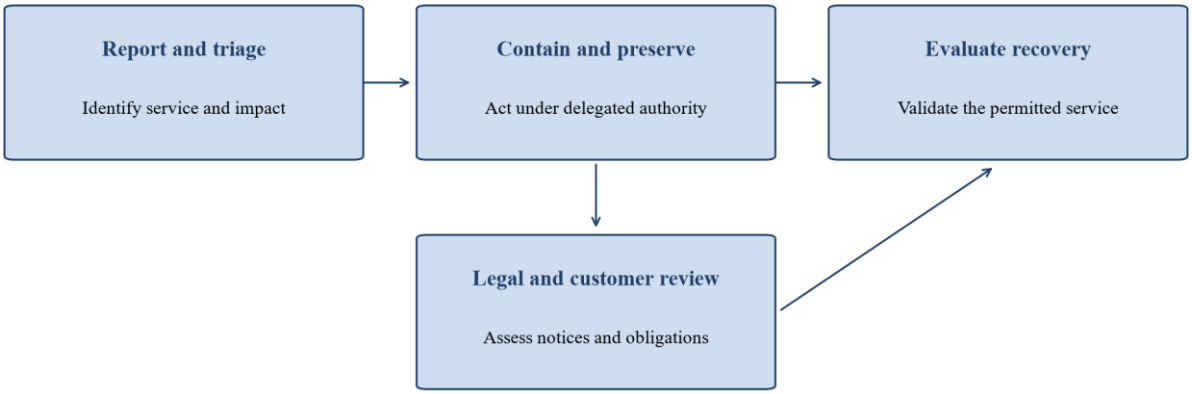
Transfer ownership to the permanent operating organisation only after its staff have accepted the documentation, access and support responsibilities. Record open exceptions, remaining supplier dependencies and review dates. Retire temporary accounts and transition arrangements through an authorised process. Preserve evidence subject to applicable retention requirements. The integration sponsor should receive a closeout statement identifying what has been accepted and what remains an operating obligation.

11. Map incidents from detection to authorised recovery

Use a shared incident route that can accept reports from either company, customers and relevant suppliers. The initial record should identify the affected service, observed behaviour, time and source of the report. Preserve evidence through authorised procedures. The responder should assess the potential impact and decide whether immediate containment is needed. Classification should be revisited as information improves; an early description may omit important consequences.

Assign an incident lead with access to the business owner, technical team and relevant legal specialists. The lead coordinates the response and records decisions. The proposed map separates technical containment from decisions about external notification and resumption. Applicable law, contracts and professional obligations determine notification requirements. The paper sets no universal reporting deadline and assumes no permission to disclose personal or confidential information to every participant.

Figure 3. Proposed incident decision map across the combined business



Notification requirements and recovery authority must be determined for the actual service and jurisdiction. Arrows show coordination, with concurrent specialist review where needed.

Consider an illustrative incident in which a newly connected retrieval source exposes information to an application outside its approved access scope. The proposed immediate response is to restrict the affected connection using authorised controls, preserve relevant evidence and identify the scope of exposure. The investigation should examine permissions, configuration changes and downstream recipients. The business owner should establish which service can continue within verified restrictions while the wider issue is assessed.

Recovery requires evidence that the approved service can operate under the revised conditions. Test the remediation and relevant failure path, confirm monitoring and record residual issues. Obtain the required authorisation before resuming affected functionality. A return to technical availability provides one observation in that decision. The incident review should also address customer consequences, evidence retention and changes needed to the integration process. NIST's response guidance includes recovery and lessons feeding back into risk management. [3]

12. Apply jurisdiction and sector requirements to specific uses

Create a legal applicability record for each material deployment. Identify the operating entities, affected people, markets served, purpose and role in the supply chain. Ask qualified advisers to determine the relevant obligations and application dates. Keep that record linked to the approved configuration. A change in geography, purpose or branding should prompt review where it could affect the legal analysis. The group policy can then incorporate the resulting requirements without obscuring local responsibilities.

The EU AI Act's consolidated text dated 27 July 2026 provides a specific example. Article 25 addresses circumstances in which an operator becomes a provider of a high-risk system, including certain changes involving branding, substantial modification or intended purpose. Article 26 addresses deployer obligations, including competent human oversight and monitoring. These provisions require assessment of scope, exceptions and the applicable transition rules before they are treated as a current duty for a particular system. [4]

The European Commission's current implementation page describes different application dates for different parts of the Act and reflects the 2026 amendments. The integration team should maintain a dated obligations register checked against the consolidated legislation and relevant advice. This paper makes no blanket assertion that every high-risk requirement applies to every deployment at completion. The transaction plan should record the specific requirement, applicable date, accountable entity and evidence needed for compliance. [5]

SDAIA's AI Ethics Principles discuss accountability, traceability, monitoring and third-party diligence across the system lifecycle. The UAE's July 2024 charter includes human oversight, governance, accountability and compliance with applicable laws. These primary publications provide relevant regional reference points for the proposed governance design. Their status and application to a particular entity require separate assessment. They provide no general approval for a cross-border data transfer, regulated financial activity or sector-specific deployment. [6,7]

For GCC operations serving international customers, maintain the contractual obligations alongside the legal register. A customer's security schedule or procurement requirement may impose evidence conditions relevant to continued delivery. Verify the executed terms and the party entitled to accept a change. Preserve the distinction between statutory requirements, contractual commitments and internally chosen controls. The investment committee needs a clear record of the basis for each condition and the consequence of failing to meet it.

13. Budget for evidence collection and parallel operation

The implementation budget should separate common programme costs from deployment-specific work and temporary operating costs. Use a documented inventory as the volume basis. Obtain estimates for the actual evaluation, remediation and migration tasks, together with the assumptions behind them. Record dependencies that can change the number of reviews or the duration of parallel operation. Finance should reconcile the budget to approved work packages and identify the owner of each material estimate.

The following budget is wholly hypothetical and uses US dollars. Assume USD 180,000 for common programme setup, including the register, policy reconciliation and initial operating procedures. The 152 illustrative deployments are allocated to three effort categories: 32 requiring intensive evaluation at USD 4,000 each, 60 requiring intermediate evaluation at USD 2,000 each and 60 requiring a limited review at USD 500 each. These are assumed workload categories, with no claim about legal risk classification.

Table 2. Hypothetical implementation expenditure

Work package	Calculation	Assumed expenditure
Common programme setup	Fixed assumed amount	180,000
Intensive evaluations	32 deployments at 4,000	128,000
Intermediate evaluations	60 deployments at 2,000	120,000
Limited reviews	60 deployments at 500	30,000
Temporary parallel operation	6 months at 35,000	210,000
Total base implementation	Sum of the five work packages	668,000

Author's assumptions in USD. No observed supplier prices, staffing rates, advisory quote or market benchmark. Evaluation categories are mutually exclusive for this calculation.

The calculation assumes that evaluation charges cover the specified review work and that the temporary operating cost is additional to those charges. It excludes ordinary business operating costs, taxes, financing costs, revenue effects and remediation beyond the stated work packages. In an actual budget, scope definitions and time records would be needed to avoid counting the same staff cost twice. The illustrative total is expenditure under selected assumptions, with no probability attached.

Consider an extension of three months at the same assumed USD 35,000 monthly parallel-operation cost. This adds USD 105,000. Assume eight intensive evaluations must also be repeated after material configuration changes, each costing USD 4,000. The repeat work adds USD 32,000, bringing incremental expenditure to USD 137,000 and the extended total to USD 805,000. The repeat evaluations are additional work on existing deployments; they do not increase the inventory count.

The committee should examine the causes of that extension. Delayed supplier consent, unavailable evidence and failed migration tests require different responses. A budget reserve should have a documented purpose and approval rule. The model does not quantify avoided losses or suggest that this expenditure creates a particular investment return. Any savings or revenue assumption should be supported by separate evidence and reconciled with the cost of maintaining service during integration.

14. Test continuity before relying on the integration case

For each material service, establish what the business can deliver while an AI component is restricted or unavailable. Describe the alternative workflow, staffing requirement and customer consequences. Verify whether that alternative is permitted under relevant contracts and professional requirements. A manual process should be tested using representative work and authorised data. Record the volume it can handle, the review required and the backlog that accumulates under the chosen test conditions.

Separate technical uptime from completed customer service. An application may be reachable while producing outputs that require substantial correction or cannot be used within the approved process. Define a service measure connected to the actual customer obligation. The proposed continuity test should follow a transaction from input through review and delivery. Include the time needed to resolve exceptions and the capacity of downstream teams to absorb additional work.

Identify the point at which the fallback becomes insufficient. The owner should know which services receive priority and which commitments require escalation. The integration plan should specify who communicates changes to customers and who approves expenditure on temporary capacity. A proposed contingency remains conditional until the relevant people, access and operating procedures are available. Retain the test evidence and schedule revalidation when those conditions change.

The investment case should show the period during which both old and new arrangements operate. Record what costs continue and which benefits depend on migration acceptance. Finance should challenge any assumption that full savings begin at legal completion if the underlying service is still using the previous environment. The proposed model keeps temporary parallel operation visible so the committee can assess the cash required to support the agreed transition.

Review continuity evidence before each material cutover. Confirm that the fallback still matches current data, vendor access and staffing. A recovery plan written before a restructuring may name people who no longer hold the necessary authority. The test record should identify the actual participants and decision makers. The committee's acceptance statement should specify the evidence supporting the service arrangement approved for the next phase.

15. Commission a bounded integration mandate

A buyer commissioning external support should define the decisions it needs help to make and the evidence to be delivered. A proposed mandate can cover inventory reconciliation, control comparison, integration governance and coordination of the implementation plan. It should state which specialist assessments are performed by appropriately qualified advisers and which remain with the client's teams. The engagement should preserve management's responsibility for operating approvals and risk acceptance.

Tie deliverables to acceptance criteria. An inventory deliverable should reconcile the original records, identify unresolved scope and link material deployments to owners. An approval framework should be tested against representative changes. A vendor workstream should record executed terms and outstanding decisions. An incident procedure should be exercised with the relevant participants. The final report should state the limitations of the evidence and the actions still needed for the proposed operating model.

Agree information access, confidentiality, retention and conflict-management arrangements before sharing material. The adviser should receive access appropriate to the task and the authority granted. The scope

should explain how findings are reported and how urgent concerns reach management. Any additional work identified during discovery should have a documented change process. This allows the client to approve the cost and purpose of further investigation before it begins.

Commercial terms should distinguish a retainer for defined work from implementation expenditure, software charges and specialist fees. The hypothetical budget in this paper is not a Matchpoint Partners fee proposal. A client-specific proposal would require confirmed scope, jurisdictions, deployment complexity and access to evidence. Neither the paper nor a preliminary discussion establishes a promise of regulatory clearance, uninterrupted operation or a financial outcome.

For an investment committee, the useful closeout is a decision record showing the approved operating arrangement, remaining conditions and accountable owners. That record can support subsequent governance reviews and future acquisition integration. It should remain accessible to the operating organisation after the transaction team disbands. The mandate's completion criteria should reflect the agreed deliverables and the evidence actually provided.

16. Reach a documented operating conclusion

The committee should receive a reconciled inventory and a specific operating decision for every material deployment. It should see which systems can continue within approved limits, which require additional conditions and which await an unresolved decision. The report should identify the evidence behind those categories, the material dependencies and the date at which each conclusion was reached. Aggregate completion percentages should be accompanied by the consequences of the outstanding items.

Approve the integration sequence using acceptance conditions supported by tests and accountable sign-off. Preserve the ability to restrict a specific function when its conditions are no longer satisfied. Keep customer continuity, legal obligations and incident authority visible throughout the transition. Technical consolidation can proceed when the proposed environment has the required permissions, evaluation evidence and operating support. Any remaining separation should have a documented reason and review condition.

The hypothetical calculations illustrate two distinct management questions. The inventory reconciliation defines the population requiring governance, while the implementation budget identifies expenditure under selected scope and timing assumptions. Neither calculation establishes actual deployment readiness or commercial value. An acquisition committee should replace those assumptions with transaction evidence before using the method to approve resources or assess the integration case.

The proposed framework closes with a permanent owner for the combined governance process, a maintained record of approved uses and a working route for change and incident decisions. Its effectiveness requires evidence from operation and review. The next investment decision should therefore include the cost and responsibility for maintaining the system after the initial integration programme has ended.

Appendix A. Minimum evidence for a deployment decision

The proposed deployment record should identify the legal entity, business owner, approved purpose and production environment. Retain the original identifiers from each company and the group identifier used after reconciliation. Link the relevant model or service version, application configuration and dependencies. Record the date on which the operational facts were checked and the person who performed that check. Where discovery remains incomplete, describe the missing evidence and its consequence for the decision.

The approval section should identify the applicable internal policy and the legal or contractual conditions supplied by the relevant advisers. Attach evaluation results with test scope, denominators and limitations.

Describe the monitoring measures, response thresholds and human-review arrangements. Record the approved action capabilities and restrictions on data access. A decision should identify the authorising person, effective date, expiry or review condition and changes requiring reassessment.

The continuity section should describe the fallback, its tested capacity and the person authorised to activate it. Link the incident route, vendor support arrangement and evidence-preservation procedure. The recovery decision should specify the tests and approvals required before affected functions resume. Keep the operating record aligned with current staffing and contractual arrangements. A handover exercise should confirm that the permanent owner can locate the evidence and perform the required actions.

Appendix B. Reproducing the hypothetical calculations

The inventory starts with 100 records from Company A and 80 from Company B. Deduct 15 duplicate administrative records and 25 confirmed retired deployments, then add 12 newly discovered active deployments. The result is 152 active deployments. The three illustrative approval categories comprise 82 with complete evidence, 50 with conditional approval and 20 awaiting a decision. The first two categories total 132; dividing by 152 gives 86.8421%, displayed as 86.8%.

The evaluation workload categories are a separate classification of the same 152 deployments. Multiply 32 by USD 4,000, 60 by USD 2,000 and 60 by USD 500 to obtain USD 278,000 of assumed evaluation expenditure. Add USD 180,000 of common setup and six months at USD 35,000, producing USD 668,000. Three additional months and eight repeat intensive evaluations add USD 137,000. The extended expenditure is USD 805,000. No discounting, probability weighting, inflation adjustment or tax calculation is included.

References

[1] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework, AI RMF 1.0, NIST AI 100-1, January 2023. Voluntary framework; governance, mapping, measurement and management outcomes. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[2] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST AI 600-1, July 2024. Third-party dependencies, organisational content access and value-chain integration. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

[3] National Institute of Standards and Technology. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, SP 800-61r3, April 2025. Incident authority, third-party coordination, recovery and improvement. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

[4] European Union. Regulation (EU) 2024/1689, consolidated text dated 27 July 2026. Articles 25, 26 and 113; role-specific provisions and application rules require transaction-specific assessment. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02024R1689-20260727

[5] European Commission. AI Act implementation and application timeline. Current official overview, accessed 10 September 2026. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[6] Saudi Data and Artificial Intelligence Authority. AI Ethics Principles. Accountability, monitoring and third-party diligence; accessed 10 September 2026. https://dgp.sdaia.gov.sa/wps/wcm/connect/4c56ed1c-1b82-447d-ac29-638f5f99c12e/ai-principles-EN.pdf?MOD=AJPERES

[7] UAE Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications Office. The UAE Charter for the Development and Use of Artificial Intelligence, July 2024. https://ai.gov.ae/wp-content/uploads/2024/07/UAEAI-Methaq-EN2-3.pdf

About the Author

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

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

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

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

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.