Combining Data and AI Estates: Consent, Access, Model Risk and Competitive Information

A Pre-Close Control and Integration Framework

Authored by Chennakeshav Adya, Independent Researcher

September 2026

Abstract

Data and artificial-intelligence assets can drive a merger thesis while creating some of its most difficult pre-close and integration risks. Data that appears transferable may have been collected for a different purpose, licensed under restrictive terms, derived from third parties, embedded in models without reliable lineage or exposed to competitors through an uncontrolled integration channel. This paper develops a pre-close control and integration framework for combining data and AI estates. It maps legal entities, controllers, processors, datasets, licences, consent, provenance, quality, access paths, models, vendors and downstream decisions; separates clean-team analysis from operational integration; tests purpose compatibility, competitive sensitivity, security, interoperability, model validity, bias, resilience and exit rights; and sequences Day-One containment, migration and decommissioning. Five figures and five tables present the rights-to-value chain, clean-team access funnel, model-dependency map, migration-risk curve and retained data and AI integration certificate. The framework draws on current data-protection law, AI regulation, competition guidance, cybersecurity frameworks, model-risk guidance, cloud-switching rules and filed acquisition disclosures. Eight frequently asked questions and twenty-six primary or authoritative sources support application. Numerical values are illustrative analytical scenarios. Transaction-specific conclusions require verified contracts, data records, technical architecture, model documentation, security evidence and regulatory analysis together with independent legal, privacy, competition, cybersecurity, technology, financial and specialist advice.

JEL Classification: G34, K21, K24, L41, O33

Keywords: data integration, artificial intelligence, merger control, clean team, consent, data access, model risk, privacy, cybersecurity, M&A

1. Set the board's data and AI mandate

The transaction team should define the value thesis, legal boundary, risk appetite, decision rights and evidence required to combine the estates. The required output is a board-approved data and AI integration mandate. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [1][2].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that technology work can begin before lawful use and value objectives are agreed. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

2. Separate diligence, planning and integration

The transaction team should distinguish pre-signing review, clean-team analysis, pre-close planning, Day-One control and post-close migration. The required output is a phase-gated access protocol. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [3][4].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that commercial teams can receive information or influence operations before the transaction permits it. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

3. Map legal entities and accountability

The transaction team should identify controllers, processors, joint controllers, model owners, system owners and regulated entities across both groups. The required output is an accountability and entity map. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [5][6].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that data and model ownership can be assumed from system location rather than legal responsibility. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

4. Inventory the combined estate

The transaction team should catalogue datasets, models, prompts, features, interfaces, decision uses, vendors, locations, users and dependencies. The required output is a reconciled data and AI asset register. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [2][7].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that material shadow datasets and models can remain outside diligence and control. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

5. Build the rights-to-value chain

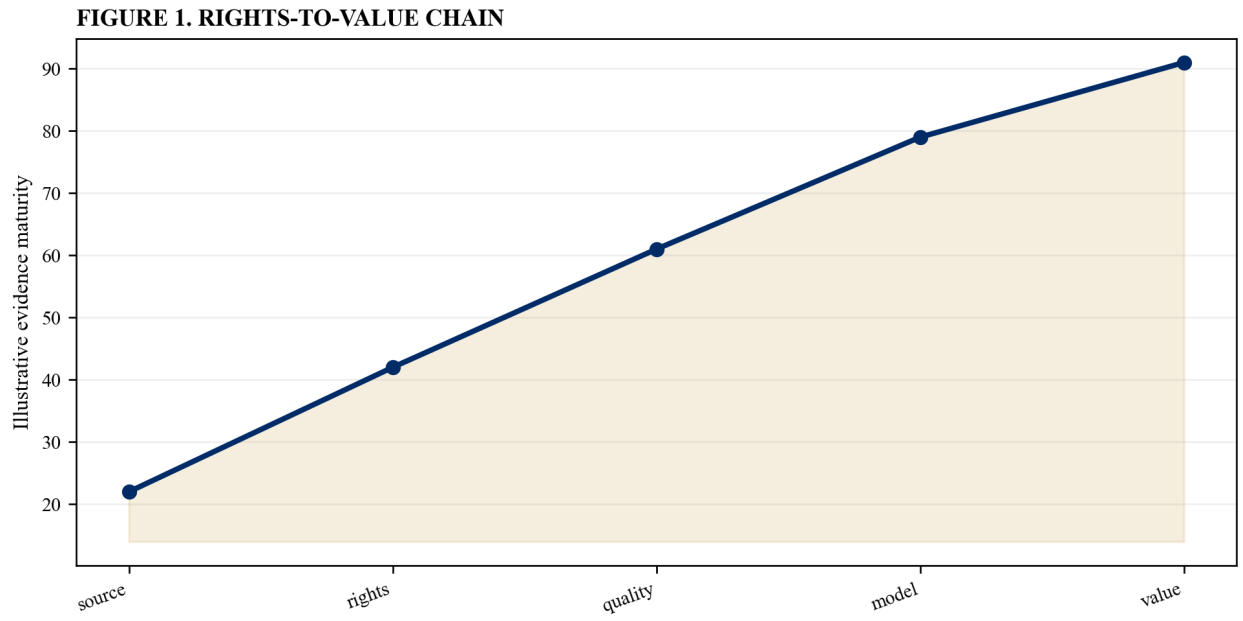
The transaction team should connect source, right, permitted purpose, transformation, model, decision, outcome and merger value. The required output is a testable rights-to-value chain. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [1][5].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that revenue or synergy can depend on data use that the combined company cannot lawfully or practically sustain. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

Figure 1. Rights-to-value chain



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

6. Classify data and model criticality

The transaction team should rank assets by customer, revenue, safety, regulatory, operational, competitive and recovery impact. The required output is a criticality tiering model. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [8][9].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that integration effort can be allocated by storage size rather than decision consequence. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

7. Trace collection purpose and consent

The transaction team should establish why personal data was collected, the lawful basis, notices, choices and evidence of consent where relied upon. The required output is a purpose and consent ledger. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [5][10].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that a change of controller or intended use can exceed the original basis or reasonable expectation. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

8. Test purpose compatibility

The transaction team should compare proposed combined-company uses with original context, relationship, data nature, consequences and safeguards. The required output is a purpose-compatibility assessment. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [5][10].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that a technically feasible cross-sell or training use can remain legally unavailable. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

Table 1. Purpose and rights matrix

Asset	Required evidence	Decision
customer data	notice and lawful basis	use or restrict
partner data	licence and transfer	use or segregate
training data	provenance and rights	retrain or retain
derived data	method and ownership	verify or quarantine

Illustrative structure; verified transaction evidence and specialist review govern.

9. Map contractual data rights

The transaction team should review customer, supplier, partner, employee, public-source and open-source terms for transfer, use, training and sublicensing. The required output is a data-rights contract matrix. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [11][12].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that ownership language can fail to cover derived data, embeddings, outputs or post-control-change use. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

10. Verify provenance and lineage

The transaction team should trace source, collection, transformations, labels, joins, features, training, validation and downstream reuse. The required output is an evidence-backed lineage graph. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [1][13].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that models can inherit rights, quality or bias problems that are invisible in the final dataset. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

11. Assess data quality and fitness

The transaction team should test completeness, accuracy, timeliness, representativeness, duplication, drift and reconciliation for each intended use. The required output is a use-specific data-quality file. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [1][14].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that headline record counts can overstate the data's usefulness for combined decisions. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

12. Identify sensitive and regulated data

The transaction team should classify special-category, financial, health, children's, biometric, location, communications and export-controlled information. The required output is a sensitivity and jurisdiction matrix. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [5][15].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that high-impact data can pass through general integration channels without the required controls. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

13. Design the clean-team perimeter

The transaction team should limit membership, datasets, fields, purpose, tools, outputs, duration and onward disclosure according to necessity. The required output is a clean-team operating charter. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [3][4].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that the clean team can become a broad information bridge between continuing competitors. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

14. Build the access funnel

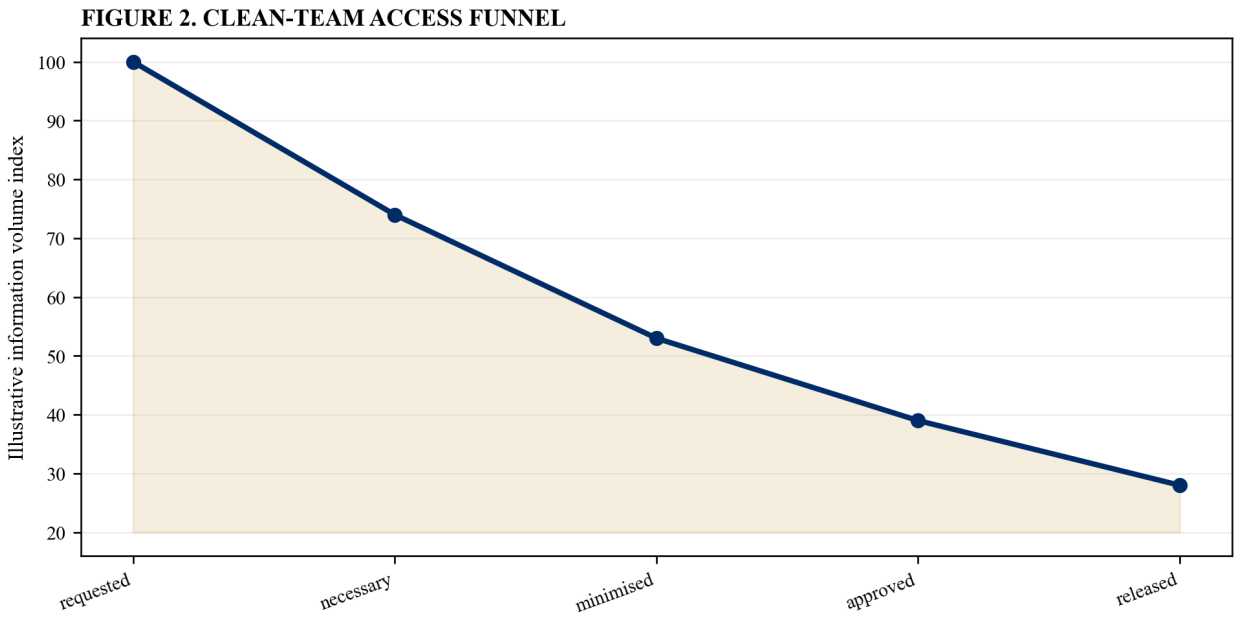
The transaction team should move from request to necessity test, minimisation, masking, approval, controlled access, output review and deletion. The required output is a governed access workflow. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [3][16].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that access can expand through convenience, copied files or unreviewed analytical outputs. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

Figure 2. Clean-team access funnel



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

15. Protect competitive information

The transaction team should identify prices, costs, customers, pipeline, strategy, capacity, innovation, bids and rival data requiring enhanced restriction. The required output is a competition-sensitivity map. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [4][17].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that shared information can influence pre-close conduct or weaken post-merger competition. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

16. Control clean-team tools and outputs

The transaction team should use approved environments, logging, download restrictions, aggregation, counsel review and recipient controls. The required output is an auditable clean-team evidence room. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [3][18].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that sensitive information can escape through screenshots, prompts, model memory or derived tables. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

Table 2. Clean-team control matrix

Control	Evidence	Release test
necessity	approved purpose	minimum fields
access	named roles and logs	authorised only
output	aggregation and review	safe disclosure
closure	return and deletion	certified

Illustrative structure; verified transaction evidence and specialist review govern.

17. Map identity and privileged access

The transaction team should reconcile users, service accounts, administrators, tokens, keys, roles, segregation and dormant access. The required output is a combined identity-control map. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [8][19].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that inherited privilege can create immediate unauthorised access after close. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

18. Assess cybersecurity posture

The transaction team should compare governance, asset protection, detection, response and recovery across critical data and AI systems. The required output is a cyber-control baseline. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [8][20].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that integration connectivity can join two attack surfaces before controls are aligned. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

19. Protect secrets and model artefacts

The transaction team should locate source code, weights, prompts, embeddings, keys, notebooks, feature stores and proprietary methods. The required output is an AI intellectual-property control file. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [11][21].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that the most valuable model assets can sit in unmanaged repositories or vendor environments. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

20. Inventory model uses and decisions

The transaction team should record intended purpose, users, affected parties, inputs, outputs, automation, human oversight and materiality. The required output is a model-use register. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [1][2].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that the same model can carry different risk when deployed in a new combined-company context. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

21. Map model dependencies

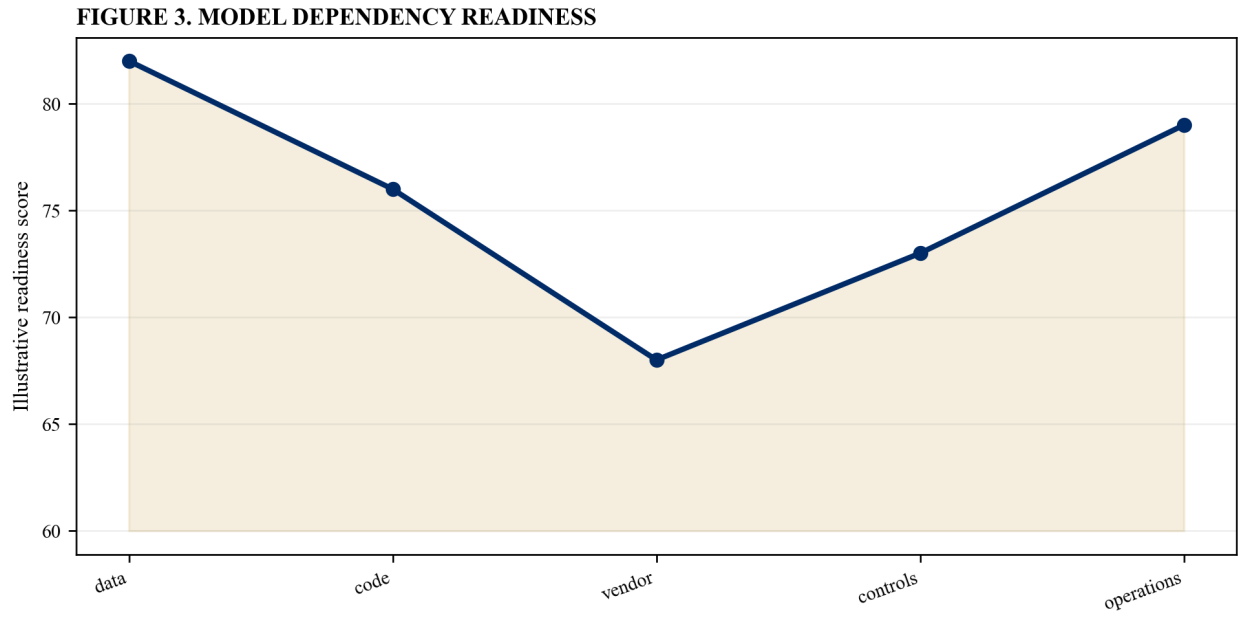
The transaction team should trace data, code, libraries, infrastructure, vendors, interfaces, human steps and downstream controls. The required output is a model-dependency graph. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [2][22].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that a migration can preserve the model file while breaking the system that makes it reliable. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

Figure 3. Model dependency readiness



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

22. Assess model validity

The transaction team should review conceptual soundness, testing, limitations, performance thresholds, stability and independent challenge. The required output is a model validation dossier. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [23][24].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that acquisition urgency can substitute inherited performance claims for current validation. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

23. Test bias and affected-party risk

The transaction team should evaluate population coverage, proxies, error distribution, feedback loops, accessibility and appeal. The required output is an impact and fairness assessment. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [1][15].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that combined datasets can change outcomes for groups even when each legacy model appeared stable. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

24. Map AI regulatory classification

The transaction team should determine provider, deployer, importer and distributor roles together with prohibited, high-risk and transparency obligations. The required output is an AI Act role and obligation map. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [1][25].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that transaction structure can change regulatory roles and compliance duties. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

Table 3. Model-risk assessment

Dimension	Test	Control
validity	performance and limits	independent review
data	quality and lineage	use approval
fairness	error distribution	impact review
operations	monitoring and rollback	named owner

Illustrative structure; verified transaction evidence and specialist review govern.

25. Assess generative-AI controls

The transaction team should review grounding, provenance, prompt injection, sensitive disclosure, content risks, evaluation and incident response. The required output is a generative-AI control baseline. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [2][26].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that general-purpose tools can expose protected information or create unsupported outputs inside material workflows. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

26. Test interoperability and portability

The transaction team should verify schemas, interfaces, metadata, identity, workload movement, functional equivalence and export completeness. The required output is a portability and interoperability test. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [12][22].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that nominal export rights can produce unusable data or materially degraded services. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

27. Review cloud and AI vendor concentration

The transaction team should map spend, dependency, sub-processors, service levels, audit rights, change control, insolvency and exit. The required output is a third-party concentration file. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [12][20].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that the combined estate can deepen dependence on one provider without credible substitution. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

28. Quantify integration economics

The transaction team should model migration, cleansing, revalidation, licences, egress, parallel run, remediation, delay and decommissioning. The required output is a data and AI integration cost case. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [9][12].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that headline synergies can exclude the cost of making data and models legally and operationally combinable. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

29. Design Day-One containment

The transaction team should preserve logical separation, monitoring, incident response, critical access and service continuity until controls are proven. The required output is a Day-One containment plan. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [8][19].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that close can trigger broad access before the combined control environment is ready. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

30. Sequence migration waves

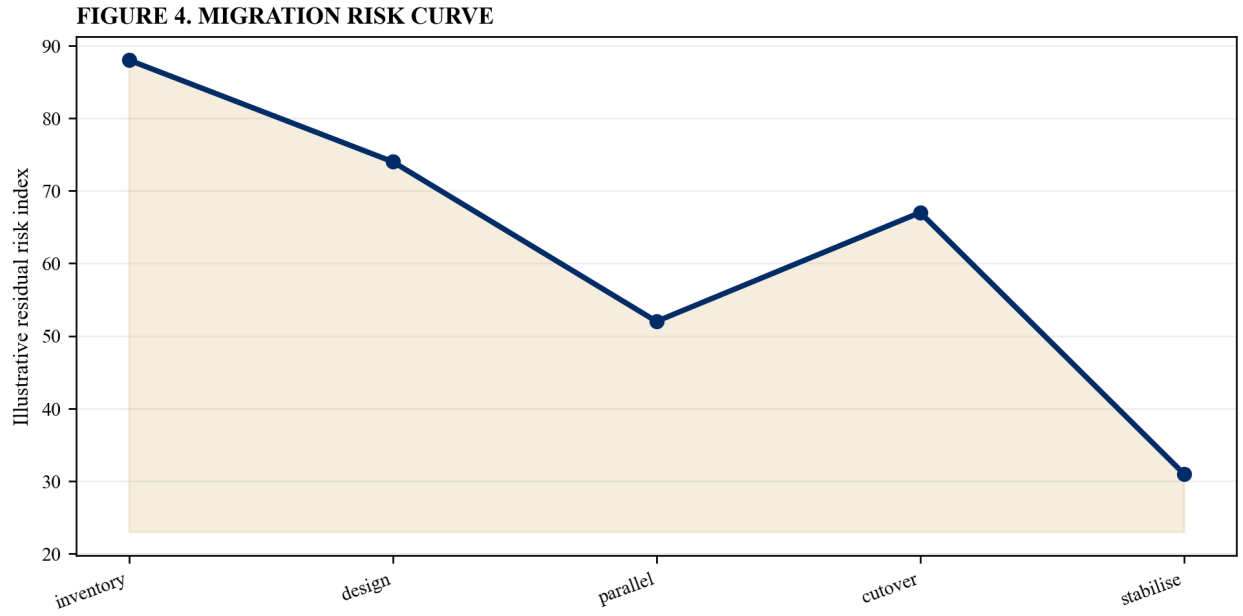
The transaction team should prioritise systems by criticality, dependency, legal readiness, technical readiness and rollback capacity. The required output is a risk-based migration roadmap. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [8][22].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that a calendar-led migration can move high-consequence systems before evidence is sufficient. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

Figure 4. Migration risk curve



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

31. Revalidate after context change

The transaction team should repeat performance, fairness, security and control testing against combined data, users and decisions. The required output is a post-change validation record. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [1][23].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that legacy validation can become stale when populations, processes or incentives change. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

32. Run parallel and rollback controls

The transaction team should define comparison windows, tolerances, exception treatment, authority and tested restoration for critical decisions. The required output is a controlled cutover file. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [8][24].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that migration failure can become irreversible before outcome differences are understood. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

Table 4. Migration gate

Gate	Required evidence	Failure action
rights	permitted purpose	segregate
technical	reconciled output	remediate
model	revalidation	parallel run
control	access and monitoring	hold cutover

Illustrative structure; verified transaction evidence and specialist review govern.

33. Reconcile records and audit trails

The transaction team should preserve source records, decisions, model versions, approvals, access events, incidents and deletion evidence. The required output is a combined evidence-retention schedule. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [5][6].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that technical consolidation can destroy records needed for rights, disputes or regulatory review. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

34. Design monitoring and incident response

The transaction team should set drift, security, quality, fairness, service and access thresholds with owners and escalation clocks. The required output is a combined monitoring and response plan. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [2][20].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that emerging harm can sit between technology, privacy, risk and business teams. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

35. Decommission safely

The transaction team should verify dependency removal, export, archive, retention, deletion, licence termination and recovery before shutdown. The required output is a decommissioning certificate. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [6][12].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that retired systems can retain live data, credentials, obligations or hidden dependencies. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

36. Stress the unlawful-use case

The transaction team should model revenue, remediation, customer, litigation and regulatory consequences if a planned use lacks a valid basis. The required output is a rights-failure downside case. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [5][10].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that data-dependent value can disappear after signing when the use case is challenged. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

37. Stress the competitive-information case

The transaction team should model leakage, gun-jumping, behavioural influence, remedy and investigation scenarios. The required output is a competition-control downside case. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [3][17].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that one uncontrolled information path can impair closing certainty or market conduct. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

38. Stress the model-failure case

The transaction team should combine drift, bias, cyber compromise, vendor outage, weak oversight and migration error. The required output is a compounded model-risk scenario. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [2][23].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that several moderate weaknesses can create a material customer or financial event. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

39. Set board escalation triggers

The transaction team should define thresholds for rights gaps, sensitive access, incidents, failed validation, migration variance and value impairment. The required output is a board data and AI escalation protocol. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [1][8].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that material exceptions can be normalised inside a large technology programme. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

40. Issue the data and AI integration certificate

The transaction team should approve rights, provenance, access, model controls, migration evidence, residual risks and accountable handover. The required output is a retained board and integration-ready certificate. Each conclusion should identify the asset, entity, jurisdiction, original purpose, proposed use, right, dependency, control owner, evidence source and confidence attached to the result [1][2].

Translate the conclusion into a controlled decision. Specify data class, model use, users, access, vendor, dependency, legal basis, competition restriction, security, validation, migration gate and deadline. Reconcile legal, privacy, competition, cybersecurity, technology, model-risk, business and integration views.

The principal risk is that the estate can be declared integrated without proving lawful, secure and reliable use. Quantify records, critical decisions, access, concentration, remediation cost, delay, revenue exposure and residual risk across base, adverse and remediated cases.

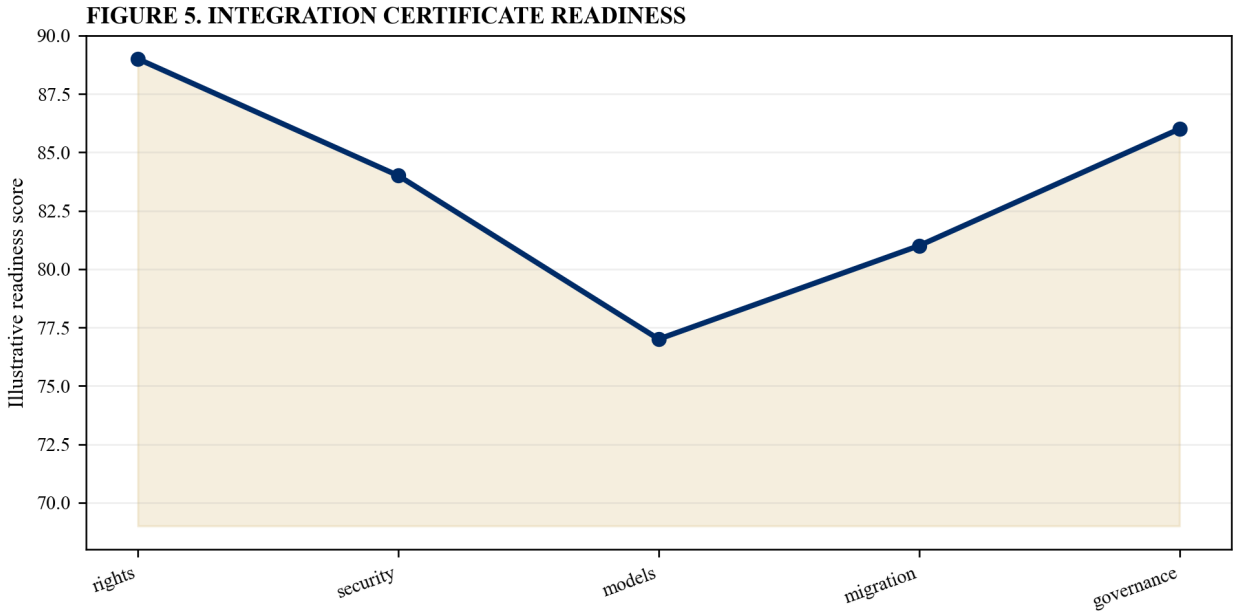
Retain contracts, notices, consent, lineage, architecture, model documentation, access logs, validation, incidents, approvals, limitations and advice. Refresh after changes to purpose, population, data, code, vendor, architecture, regulation or timing; assign exceptions owners and deadlines.

Table 5. Data and AI integration certificate

Conclusion	Record	Approval test
rights	purpose and licence	use permitted
access	identity and clean team	auditable
models	validation and monitoring	fit for context
migration	cutover and rollback	residual risk accepted

Illustrative structure; verified transaction evidence and specialist review govern.

Figure 5. Integration certificate readiness



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

References

[1] European Union, Regulation EU 2024/1689, Artificial Intelligence Act, https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[2] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework 1.0, https://doi.org/10.6028/NIST.AI.100-1

[3] UK Competition and Markets Authority, Interim Measures in Merger Investigations CMA108, https://www.gov.uk/government/publications/interim-measures-in-merger-investigations

[4] UK Competition and Markets Authority, Tell the CMA about your merger, https://www.gov.uk/guidance/tell-the-cma-about-your-merger

[5] European Union, General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[6] UK Information Commissioner's Office, Accountability framework, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/

[7] UK National Cyber Security Centre, Guidelines for secure AI system development, https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development

[8] National Institute of Standards and Technology, Cybersecurity Framework 2.0, https://doi.org/10.6028/NIST.CSWP.29

[9] US Securities and Exchange Commission, Regulation S-K Item 101 human capital and business resources, https://www.ecfr.gov/current/title-17/chapter-II/part-229/section-229.101

[10] 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/

[11] World Intellectual Property Organization, WIPO Intellectual Property Handbook, https://www.wipo.int/publications/en/details.jsp?id=275

[12] European Commission, Data Act explained, https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

[13] European Union Agency for Cybersecurity, Data protection engineering, https://www.enisa.europa.eu/publications/data-protection-engineering

[14] US Government Accountability Office, Assessing Data Reliability, https://www.gao.gov/products/gao-20-283g

[15] US Equal Employment Opportunity Commission, Artificial Intelligence and Algorithmic Fairness Initiative, https://www.eeoc.gov/ai

[16] UK Information Commissioner's Office, Data minimisation, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/data-minimisation/

[17] US Department of Justice and Federal Trade Commission, 2023 Merger Guidelines, https://www.justice.gov/atr/merger-guidelines/overview

[18] UK Competition and Markets Authority, Transparency and disclosure policy CMA6, https://www.gov.uk/government/publications/transparency-and-disclosure-statement-of-the-cmas-policy-and-approach-cma6

[19] National Institute of Standards and Technology, Digital Identity Guidelines SP 800-63, https://pages.nist.gov/800-63-4/

[20] National Institute of Standards and Technology, Cybersecurity Supply Chain Risk Management Practices SP 800-161 Revision 1, https://doi.org/10.6028/NIST.SP.800-161r1

[21] US Copyright Office, Copyright and Artificial Intelligence, https://www.copyright.gov/ai/

[22] European Union, Regulation EU 2023/2854 on harmonised rules on fair access to and use of data, https://eur-lex.europa.eu/eli/reg/2023/2854/oj

[23] Board of Governors of the Federal Reserve System, SR 26-2 Revised Guidance on Model Risk Management, https://www.federalreserve.gov/supervisionreg/srletters/SR2602.htm

[24] Office of the Comptroller of the Currency, Revised Guidance on Model Risk Management 2026, https://www.occ.gov/news-issuances/bulletins/2026/bulletin-2026-8.html

[25] European Commission, AI Act regulatory framework, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[26] National Institute of Standards and Technology, Generative Artificial Intelligence Profile NIST AI 600-1, https://doi.org/10.6028/NIST.AI.600-1

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.