Cyber and AI Vendor Due Diligence: From Policies to Control Evidence

A Transaction-Assurance Architecture for Security, Privacy, Model Governance and Operational Resilience

Authored by Chennakeshav Adya, Independent Researcher

September 2026

Abstract

Cyber and artificial-intelligence diligence frequently begins with polished policies, certifications and management presentations. Those materials establish useful context, yet a buyer must determine whether controls actually operated across the systems, people, data, models and third parties on which value depends. This paper develops a transaction-assurance architecture that converts governance claims into testable evidence for businesses preparing for sale, investment, carve-out or strategic partnership. It begins by reconciling legal entities, technology assets, data flows, AI systems and vendor dependencies to the deal perimeter. A materiality model then ranks systems and suppliers by revenue, safety, confidentiality, availability, substitutability, customer promise, regulatory exposure and closing dependency. The method distinguishes policy design from operating effectiveness and records evidence provenance through native exports, controlled samples, reperformance, logs, tickets, configurations, assurance reports and incident records. Cyber review covers identity, privileged access, secure configuration, vulnerability management, software development, open-source supply chains, monitoring, incident response, backup, recovery and resilience. AI review covers system inventory, model lineage, data rights and provenance, evaluation design, performance limitations, drift, human oversight, generative-AI attack paths, tool permissions and third-party model risk. Contractual and regulatory analysis connects customer commitments, service levels, audit rights, privacy obligations, AI requirements, subcontracting, portability, exit and insurance to observed control performance. Findings are translated into quantified remediation, continuity, customer, regulatory and transaction consequences. The framework links those consequences to forecast confidence, investment needs, valuation, separation or integration plans, closing conditions, covenants, warranties, indemnities, escrow, insurance and disclosure. Five figures, five tables, eight frequently asked questions and twenty-six primary or authoritative sources support company-specific assessment. Figures present illustrative readiness indices and do not represent measured company results. Legal, regulatory, accounting, insurance, security, technical and valuation conclusions remain dependent on the relevant facts, jurisdictions and authorised professional advice.

JEL Classification: G34, L86, M15, O33, K24

Keywords: cyber due diligence, AI governance, control evidence, vendor diligence, transaction assurance, M&A

1. Set the transaction assurance objective

Define the deal perimeter, buyer reliance standard and risk appetite before evidence collection begins.

The review should reconcile board mandate, deal route, critical systems and decision thresholds. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is an approved cyber and AI diligence charter.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

2. Map entities, systems and data flows

Reconcile legal entities, business units, hosting regions, networks, applications, models, datasets and processors.

The review should reconcile architecture diagrams, asset registers, data maps and entity records. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a transaction technology perimeter.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

3. Build the vendor and dependency universe

Identify cloud, software, managed services, model, data, security and critical subcontractor dependencies.

The review should reconcile procurement, accounts payable, SSO, network, API and contract populations. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a reconciled third-party dependency register.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

4. Separate policy from operating evidence

Test whether written requirements are implemented, monitored and enforced in practice.

The review should reconcile policies, configurations, tickets, alerts, logs, samples and interviews. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a policy-to-control evidence bridge.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

5. Establish evidence provenance

Record source, owner, extraction date, system of record, completeness and alteration controls.

The review should reconcile native exports, hashes, access histories, screenshots and reviewer workpapers. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is an evidence chain-of-custody register.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

6. Design materiality tiers

Rank systems and vendors by revenue, safety, confidentiality, availability, substitutability and closing dependency.

The review should reconcile financial, operational, customer, regulatory and transaction exposure. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a risk-based review plan.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

7. Assess cyber governance

Evaluate accountability, board oversight, management forums, risk acceptance and reporting cadence.

The review should reconcile charters, minutes, dashboards, exceptions and remediation decisions. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a cyber governance fact book.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

8. Assess AI governance

Evaluate model ownership, intended use, prohibited use, human oversight and lifecycle accountability.

The review should reconcile AI inventories, approvals, model cards, monitoring and incident records. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is an AI governance fact book.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

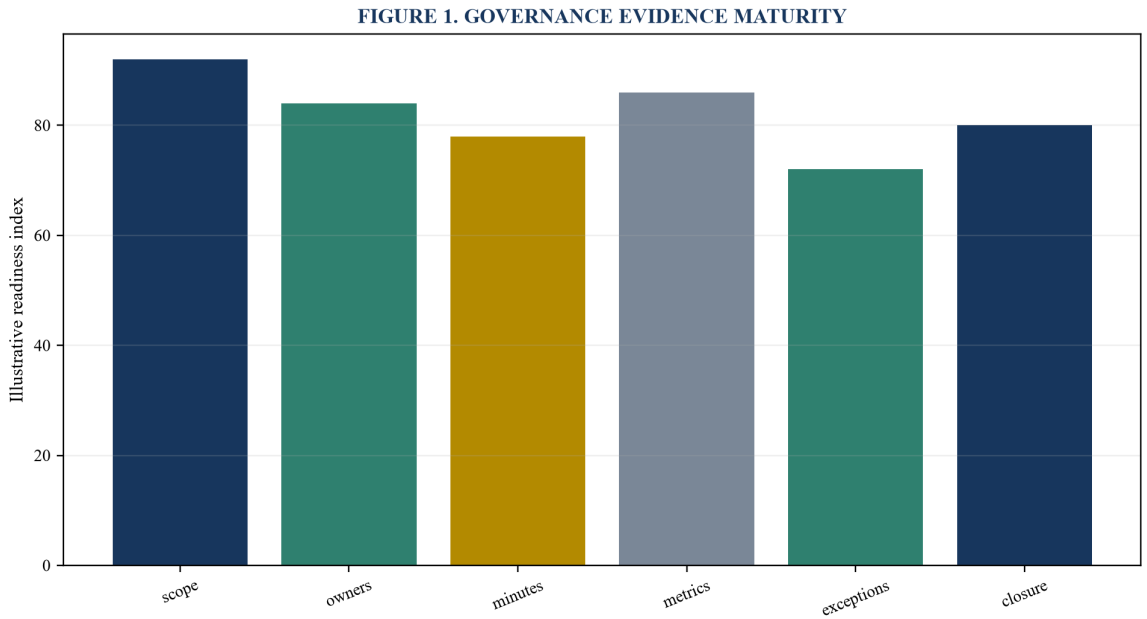
The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

Table 1. Policy-to-evidence test

Claim	Operating evidence	Decision
governance	minutes and exceptions	accountability
access	native logs and samples	effectiveness
resilience	restore and failover tests	continuity
AI oversight	evaluations and approvals	trust

Illustrative analytical design; company-specific scope, evidence and authorised advice govern.

Figure 1. Governance evidence maturity



Values are illustrative readiness indices and require company-specific testing.

9. Inventory identities and privileged access

Reconcile employees, contractors, service accounts, administrators, keys and emergency access.

The review should reconcile identity provider, HR, PAM, cloud and application records. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a privileged-access assurance map.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

10. Test joiner, mover and leaver controls

Sample provisioning, role changes, termination, recertification and dormant-account handling.

The review should reconcile HR events, workflow tickets, approval records and access logs. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is an identity lifecycle test pack.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

11. Test security configuration

Compare production settings with approved baselines across cloud, endpoints, networks, applications and databases.

The review should reconcile configuration exports, policies, drift reports and exception registers. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a configuration assurance matrix.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

12. Test vulnerability and patch management

Measure discovery, prioritisation, remediation, exception and verification across assets and dependencies.

The review should reconcile scanner results, patch records, KEV exposure, penetration tests and retests. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a vulnerability closure analysis.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

13. Test secure software development

Trace security requirements, code review, dependency control, secrets handling, testing and release approval.

The review should reconcile repositories, pipelines, artefact stores, SBOMs, findings and deployment records. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a software assurance evidence pack.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

14. Assess open-source and software supply-chain risk

Map component provenance, licences, vulnerabilities, maintainers, build integrity and update exposure.

The review should reconcile SBOMs, lockfiles, attestations, advisories and supplier controls. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a software supply-chain risk map.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

15. Assess data governance and privacy

Trace lawful purpose, minimisation, quality, retention, access, localisation, transfer and deletion.

The review should reconcile records of processing, inventories, contracts, consent, DPIAs and deletion evidence. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a data lifecycle assurance map.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

16. Map AI systems and model lineage

Identify internally built, fine-tuned, embedded and externally supplied models and their dependencies.

The review should reconcile registries, APIs, model cards, training records, evaluation reports and licences. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is an AI system and lineage register.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

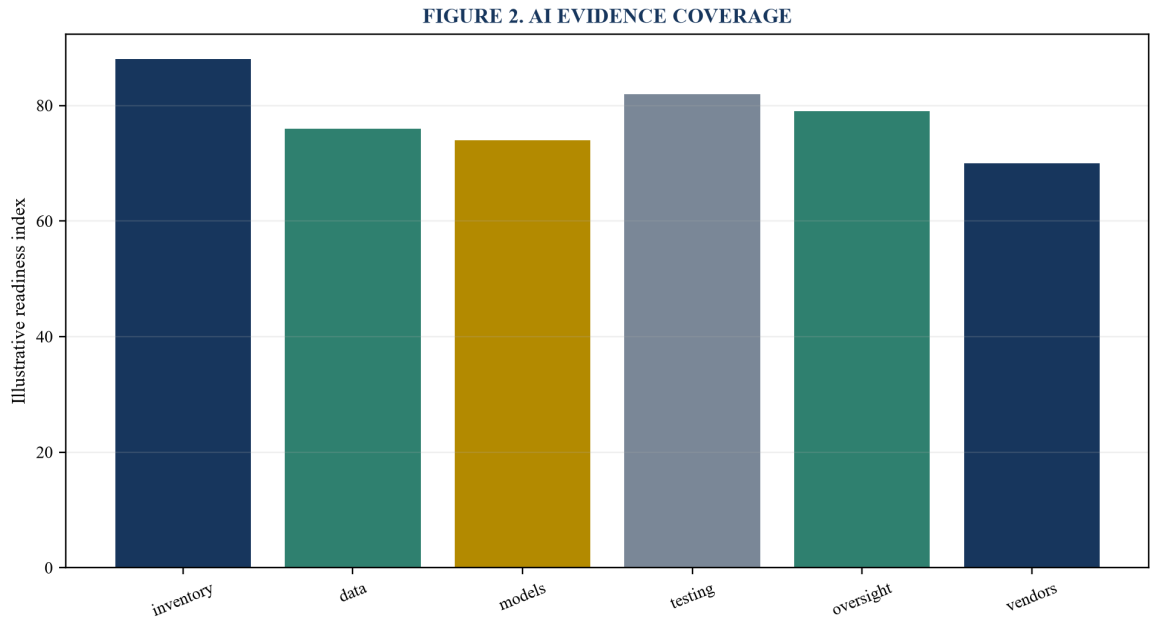
The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

Table 2. AI system diligence map

Layer	Key evidence	Primary risk
data	provenance and rights	leakage or misuse
model	evaluation and monitoring	performance drift
application	permissions and logs	unsafe action
vendor	contract and assurance	dependency

Illustrative analytical design; company-specific scope, evidence and authorised advice govern.

Figure 2. AI evidence coverage



Values are illustrative readiness indices and require company-specific testing.

17. Test training and evaluation data

Assess provenance, rights, representativeness, leakage, poisoning, privacy and quality controls.

The review should reconcile dataset cards, licences, sampling, deduplication and test results. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a data suitability assessment.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

18. Test model performance and limitations

Verify accuracy, robustness, calibration, drift, subgroup behaviour and conditions of use.

The review should reconcile benchmark design, test sets, evaluation logs, acceptance thresholds and monitoring. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a model performance assurance pack.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

19. Test generative AI security

Evaluate prompt injection, sensitive-information disclosure, tool misuse, excessive agency and unsafe output paths.

The review should reconcile red-team cases, guardrails, permissions, retrieval controls and execution logs. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a generative AI attack-path map.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

20. Test human oversight and contestability

Determine where people review, override, escalate and communicate AI-assisted decisions.

The review should reconcile workflow design, approval logs, user guidance, complaints and remediation. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a human-control effectiveness assessment.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

21. Assess incident preparedness

Test classification, escalation, containment, evidence preservation, notification and recovery for cyber and AI events.

The review should reconcile plans, exercises, incidents, communications, lessons and corrective actions. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is an incident readiness report.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

22. Assess backup, recovery and resilience

Verify backup scope, immutability, restoration, failover, capacity and recovery objectives.

The review should reconcile backup consoles, restore tests, DR exercises, dependencies and exceptions. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a resilience evidence pack.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

23. Assess security monitoring and detection

Evaluate telemetry coverage, alert logic, investigation, retention, tuning and management oversight.

The review should reconcile SIEM, EDR, cloud, identity, model and application monitoring records. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a detection coverage and efficacy map.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

24. Assess customer-facing security commitments

Reconcile contractual obligations, questionnaires, certifications, SLAs and actual control performance.

The review should reconcile customer contracts, trust portals, audit reports, exceptions and claims. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a commitments-to-controls matrix.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

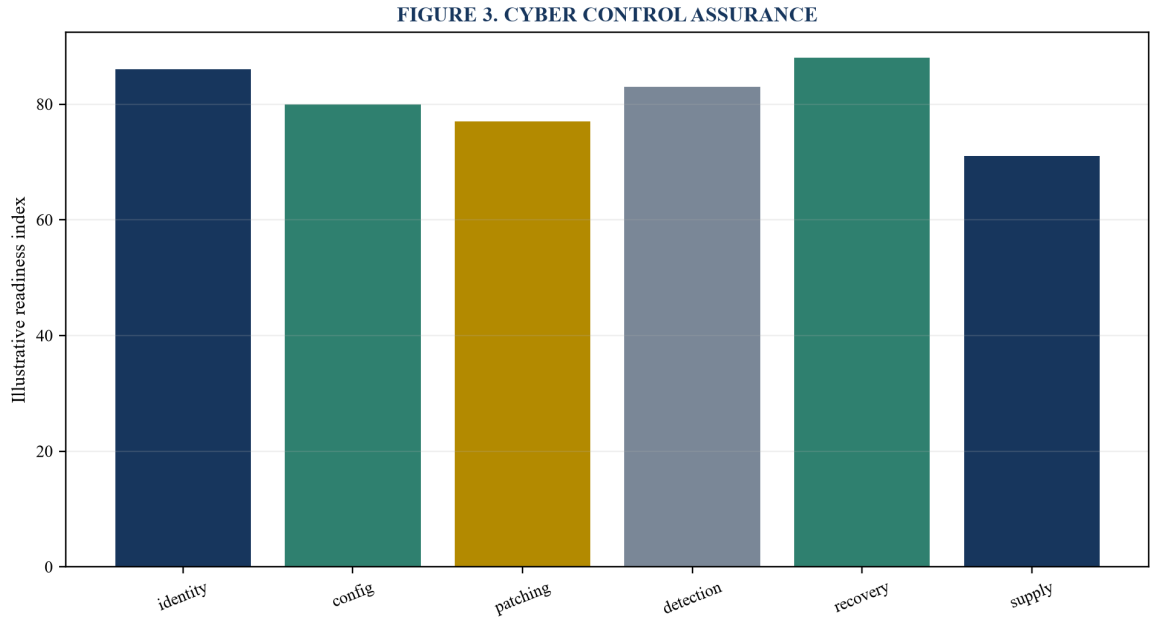
The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

Table 3. Control evidence hierarchy

Evidence	Strength	Use
native export	high	configuration or event
reperformed test	high	control operation
assurance report	conditional	scoped reliance
policy or interview	supporting	design and context

Illustrative analytical design; company-specific scope, evidence and authorised advice govern.

Figure 3. Cyber control assurance



Values are illustrative readiness indices and require company-specific testing.

25. Assess regulatory exposure

Map applicable cyber, privacy, AI, sector, securities and resilience requirements by entity and geography.

The review should reconcile legal analyses, registrations, filings, regulator correspondence and control mappings. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a regulatory applicability register.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

26. Assess certifications and assurance reports

Determine scope, period, exclusions, reliance limits, exceptions and bridge coverage.

The review should reconcile ISO certificates, SOC reports, penetration tests and management responses. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is an assurance reliance schedule.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

27. Review cyber insurance

Test insured entities, limits, exclusions, notifications, control warranties and change-of-control effects.

The review should reconcile policies, applications, claims, broker correspondence and incident facts. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a cyber insurance continuity analysis.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

28. Review critical technology contracts

Test audit, security, privacy, AI use, service levels, subcontracting, portability, exit and termination rights.

The review should reconcile master terms, orders, DPAs, AI addenda, amendments and performance records. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a technology contract risk register.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

29. Assess concentration and substitutability

Quantify reliance on cloud regions, models, data sources, specialists and single points of failure.

The review should reconcile architecture, spend, workloads, capacity, alternatives and migration tests. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a concentration downside model.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

30. Test separation and integration feasibility

Identify shared infrastructure, identities, data, licences, teams and transition dependencies.

The review should reconcile carve-out maps, TSA assumptions, migration plans, costs and critical paths. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a technology separation and integration plan.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

31. Connect control gaps to financial exposure

Translate incidents, downtime, remediation, churn, claims, fines and investment needs into cash and forecast effects.

The review should reconcile loss scenarios, historic costs, customer exposure and remediation estimates. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a cyber and AI value bridge.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

32. Connect findings to valuation

Adjust forecast confidence, maintenance investment, growth enablement, discount rates and scenario weightings.

The review should reconcile management plan, buyer case, capex, opex and sensitivity analysis. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a valuation impact schedule.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

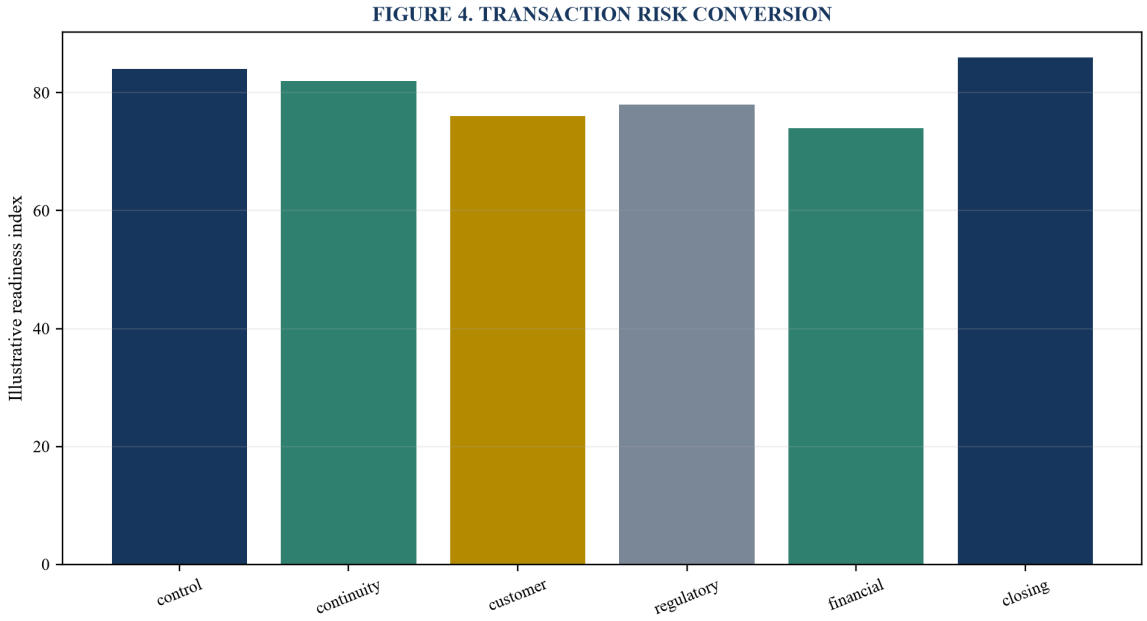
The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

Table 4. Transaction consequence map

Finding	Potential effect	Response
critical vulnerability	incident and delay	verified remediation
model limitation	forecast and conduct	guardrail or restriction
vendor concentration	continuity and leverage	fallback or protection
evidence gap	buyer uncertainty	test and disclosure

Illustrative analytical design; company-specific scope, evidence and authorised advice govern.

Figure 4. Transaction risk conversion



Values are illustrative readiness indices and require company-specific testing.

33. Design remediation before launch

Prioritise evidence gaps and control failures by closing, customer, regulator, continuity and value consequence.

The review should reconcile owners, milestones, proof requirements, dependencies and budgets. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a transaction remediation roadmap.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

34. Prepare the buyer evidence room

Organise governed evidence, summaries, samples, exceptions, remediation and authorised legal analysis.

The review should reconcile indexed documents, provenance records, redactions, access and Q&A controls. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a buyer-ready cyber and AI data room.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

35. Govern management representations

Separate verified facts, management assertions, legal conclusions, forecasts and unresolved matters.

The review should reconcile representation matrices, source links, approvals and uncertainty labels. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a controlled management fact book.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

36. Design transaction protections

Map findings to conditions, covenants, warranties, indemnities, escrows, retention, insurance and disclosure.

The review should reconcile risk ownership, quantification, duration, caps, exclusions and evidence. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a transaction protection options paper.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

37. Plan Day One cyber continuity

Protect identities, monitoring, incident response, access, connectivity and customer commitments at control transfer.

The review should reconcile cutover plans, command structures, contact trees and rollback options. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a Day One cyber control plan.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

38. Plan AI continuity and change control

Preserve model performance, data access, approvals, monitoring and vendor support through ownership change.

The review should reconcile model baselines, licences, interfaces, thresholds and release controls. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a Day One AI continuity plan.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

39. Govern buyer questions and new facts

Control responses, source verification, authorised review, concessions and downstream document changes.

The review should reconcile Q&A logs, evidence links, versioning, approvals and issue escalation. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a buyer challenge register.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

40. Issue the transaction assurance conclusion

Summarise scope, testing, exceptions, remediation, residual risk, reliance limits and next decisions.

The review should reconcile signed workpapers, exception schedules, open items and board approval. The workpaper records population, period, source system, owner, completeness, sample basis, exception logic, reviewer, authorised-advice dependency and transaction relevance. Its immediate output is a cyber and AI transaction assurance certificate.

Testing asks whether the evidence supports the stated control across the relevant period, including failures, overrides and changes. The conclusion should separate design, implementation and operating effectiveness; distinguish confirmed facts from management assertions; and connect exceptions to confidentiality, integrity, availability, privacy, safety, customer commitments, regulatory exposure, operational continuity and buyer reliance.

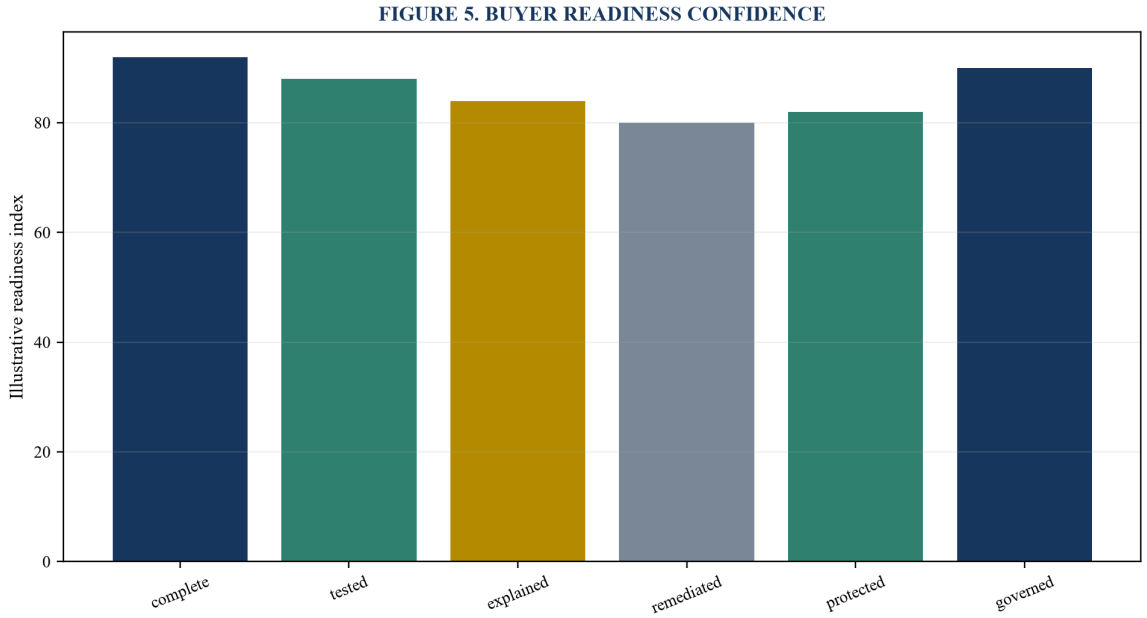
The transaction team should quantify realistic consequences, assign remediation ownership and preserve closure evidence. Material matters flow into the data room, management fact book, forecast, separation or integration plan, disclosure process, purchase agreement, financing case and board decisions. Residual uncertainty remains explicit until the required proof is obtained or the risk is contractually allocated.

Table 5. Buyer-ready assurance certificate

Gate	Required proof	Decision use
complete	reconciled scope	coverage
tested	operating evidence	effectiveness
remediated	closure evidence	residual risk
protected	continuity and documents	closing

Illustrative analytical design; company-specific scope, evidence and authorised advice govern.

Figure 5. Buyer readiness confidence



Values are illustrative readiness indices and require company-specific testing.

References

[1] NIST, Cybersecurity Framework 2.0, https://www.nist.gov/cyberframework

[2] NIST, Artificial Intelligence Risk Management Framework 1.0, https://www.nist.gov/itl/ai-risk-management-framework

[3] NIST, Generative Artificial Intelligence Profile NIST AI 600-1, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

[4] NIST, Cybersecurity Framework Profile for Artificial Intelligence, https://csrc.nist.gov/pubs/ir/8596/iprd

[5] NIST, Security and Privacy Controls for Information Systems and Organizations SP 800-53 Rev. 5, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[6] NIST, Secure Software Development Framework SP 800-218, https://csrc.nist.gov/pubs/sp/800/218/final

[7] NIST, Computer Security Incident Handling Guide SP 800-61 Rev. 2, https://csrc.nist.gov/pubs/sp/800/61/r2/final

[8] NIST, Cybersecurity Supply Chain Risk Management Practices SP 800-161 Rev. 1, https://csrc.nist.gov/pubs/sp/800/161/r1/final

[9] CISA, Secure by Design, https://www.cisa.gov/securebydesign

[10] CISA, Known Exploited Vulnerabilities Catalog, https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[11] CISA, Software Bill of Materials, https://www.cisa.gov/sbom

[12] International Organization for Standardization, ISO/IEC 27001 Information Security Management Systems, https://www.iso.org/standard/27001

[13] International Organization for Standardization, ISO/IEC 27017 Cloud Security Controls, https://www.iso.org/standard/43757.html

[14] International Organization for Standardization, ISO/IEC 27018 Protection of PII in Public Clouds, https://www.iso.org/standard/76559.html

[15] International Organization for Standardization, ISO/IEC 27701 Privacy Information Management, https://www.iso.org/standard/71670.html

[16] International Organization for Standardization, ISO/IEC 42001 Artificial Intelligence Management Systems, https://www.iso.org/standard/81230.html

[17] International Organization for Standardization, ISO/IEC 23894 Artificial Intelligence Risk Management, https://www.iso.org/standard/77304.html

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

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

[20] European Union, Digital Operational Resilience Act, https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[21] European Union, NIS 2 Directive, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[22] European Data Protection Board, Guidelines and Recommendations, https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

[23] UK Information Commissioner's Office, Guidance on AI and Data Protection, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/

[24] US Securities and Exchange Commission, Cybersecurity Risk Management Strategy Governance and Incident Disclosure, https://www.sec.gov/rule-release/33-11216

[25] US Federal Trade Commission, Safeguards Rule, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

[26] OWASP Foundation, Top 10 for Large Language Model Applications, https://owasp.org/www-project-top-10-for-large-language-model-applications/

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.