Cyber Due Diligence for Deal Teams: Translating Exposure into Price and Closing Conditions

An Evidence-Led Framework for Valuation, SPA Protection, Day 1 Resilience and Post-Close Remediation

Authored by Chennakeshav Adya, Independent Researcher

August 2026

Abstract

Cyber due diligence often produces a catalogue of vulnerabilities, maturity ratings and remediation recommendations without a controlled translation into the transaction. Deal teams then struggle to determine whether a finding changes price, structure, financing, contractual protection, closing conditions, Day 1 readiness or the first 100 days. A technical observation can be material even when its immediate repair cost is modest: compromised identity can enable payment fraud; weak recovery can interrupt a critical service; undocumented data use can constrain integration; an untested supplier dependency can defeat a continuity plan; and an incident can create notification, litigation, customer and regulatory consequences.

This paper develops an evidence-led cyber diligence framework for deal teams. It begins with the target's critical business services and transaction perimeter, then maps attack surface, identity, data, applications, infrastructure, software supply chain, third parties, resilience and incident history. Findings are classified as active compromise, control failure, regulatory exposure, technical debt or integration risk. Each material finding is translated through a loss-scenario model into valuation, SPA, closing, Day 1 and remediation decisions. Five original figures and five implementation tables provide an attack-surface map, control maturity heat map, loss-scenario table, SPA protection matrix and 100-day remediation roadmap.

The framework is anchored in current primary and authoritative sources. NIST Cybersecurity Framework 2.0 adds Govern to the established Identify, Protect, Detect, Respond and Recover functions and includes supply-chain due-diligence outcomes.[1] NIST guidance also addresses security controls, cyber supply-chain risk and incident response.[2][3][4] The US Securities and Exchange Commission requires public-company disclosure of material cybersecurity incidents and annual disclosure about risk management, strategy and governance under its 2023 final rule.[5] UK financial-services operational-resilience rules require in-scope firms to identify important business services, set impact tolerances, map dependencies and test severe but plausible disruption; the FCA's current material-incident and third-party reporting rules take effect in March 2027.[6][7] The EU Digital Operational Resilience Act, NIS2 Directive, General Data Protection Regulation and Cyber Resilience Act create relevant sector, incident, data and product obligations.[8][9][10][11] The UAE's federal data-protection framework and 2025 National Cybersecurity Strategy add jurisdiction-specific governance, security and resilience considerations.[12][13] ISO/IEC 27001, IFRS 3 and IFRS 13 provide further control, business-combination and fair-value context.[14][15][16]

Every amount, probability, score, duration and valuation effect in the worked examples is a hypothetical modelling assumption used solely to demonstrate the method. The examples are not transaction forecasts, loss benchmarks, valuations, legal opinions, regulatory conclusions, accounting conclusions, insurance advice or investment recommendations. A live transaction requires

authorised testing, transaction-specific evidence and advice from qualified legal, cyber, privacy, regulatory, accounting, tax, insurance, financing and sector specialists in each relevant jurisdiction.

JEL Classification: G34, G32, K22, K24, L86, M15

Keywords: mergers and acquisitions, cyber due diligence, valuation, purchase price, closing conditions, operational resilience, data protection, incident response, third-party risk, post-merger integration

1. Define the cyber diligence decision

Cyber diligence is a transaction decision process supported by technical evidence. Its purpose is to determine how digital exposure changes the economics, protections, readiness and operating plan of a proposed transaction. A high-quality review therefore starts with the acquisition thesis, critical services, legal perimeter, integration intent and deal timetable. It does not start with a generic control checklist.

The central question is whether the target can protect and operate the assets, services, data and relationships that support the transaction case within an acceptable risk and investment envelope. The answer requires evidence about how the business earns revenue, collects cash, serves customers, meets regulation, develops products, manages suppliers, recovers from disruption and controls privileged authority. A technically weak control becomes transaction-critical when it connects to a concentrated revenue stream, payment pathway, regulated service, safety function, irreplaceable dataset or delayed separation dependency.

The diligence mandate should state the transaction perimeter, authorised testing methods, evidence access, legal privilege, clean-team restrictions, data-handling protocol, escalation path and decision dates. Intrusive testing can disrupt operations or breach law and contract. The buyer and its advisers should obtain explicit authority and use proportionate techniques. Evidence supplied by management should be distinguished from independently observed configuration, tested operation and third-party assurance.

The output is a transaction cyber register. Every material finding records the source, affected asset and service, threat pathway, control state, evidence confidence, loss scenario, regulatory relevance, valuation path, contractual response, closing requirement, Day 1 control, remediation owner and residual risk. The register maintains traceability from technical observation to board decision.

Table 1. Evidence states for transaction cyber findings

Evidence state	Minimum record	Transaction use	Control requirement
management assertion	owner, date, scope and supporting record	scope further work	label source and limitation
observed configuration	system, sample, method and timestamp	identify control design	preserve authorised evidence
tested operation	test procedure, population, exception and reviewer	assess operating effectiveness	reproducible test and access log
supported finding	threat pathway, affected service and consequence	quantify transaction exposure	independent challenge and confidence
approved response	valuation, SPA, condition, Day 1 or remediation decision	execute deal treatment	authority, rationale and residual risk
verified closure	remediation evidence and retest	close or reduce exposure	accountable owner and audit trail

A finding advances only when its source, business consequence and decision treatment are explicit.

2. Start with critical business services and the transaction perimeter

An asset inventory alone cannot show transaction materiality. Deal teams should first identify the services whose disruption, manipulation or disclosure could materially affect customers, cash, safety, regulation or the deal thesis. Examples include order fulfilment, payment processing, clinical service, trading, grid operation, customer authentication, product release, treasury, financial reporting and regulatory submission. Each service is mapped to people, processes, technology, facilities, information and third parties.

The FCA's operational-resilience approach provides a useful discipline for relevant financial firms: identify important business services, define impact tolerances, map dependencies and test severe but plausible scenarios.[6][7] The underlying method has broader transaction value. A target can report good infrastructure uptime while a critical service remains unrecoverable because a specialist employee, supplier credential, encryption key, data feed or manual workaround is missing.

The transaction perimeter should capture legal entities, businesses, countries, products, customer groups, systems, networks, cloud tenants, development environments, operational technology, data stores, joint ventures and outsourced services. Carve-outs require special attention because the seller may retain identity, network, security monitoring, software licences, encryption keys, data platforms or response capabilities under transitional arrangements. The buyer must understand which controls move, which remain and which need replacement.

Integration intent changes exposure. A buyer planning rapid network connectivity inherits a different pathway from a buyer operating a ring-fenced platform. A transaction involving sensitive government, health, financial, defence or critical-infrastructure data can face ownership, localisation, access and national-security constraints. The diligence map should therefore show the current environment and the proposed post-close architecture.

3. Build the attack-surface and dependency map

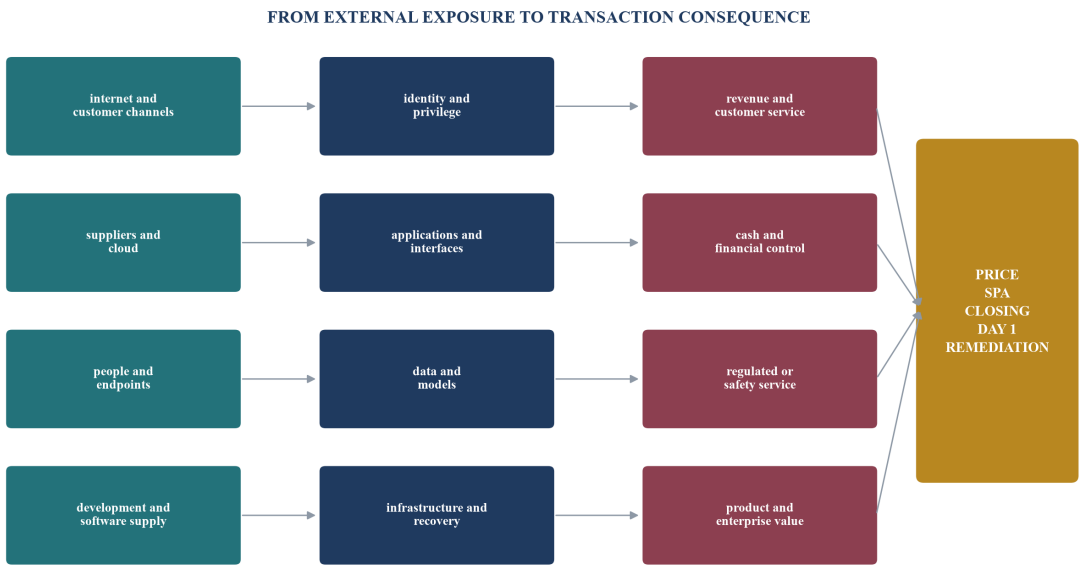
The attack-surface map connects externally reachable services, identity systems, endpoints, applications, data, cloud, operational technology, development pipelines and third parties to critical business services. It should identify trust boundaries and concentrated control points. The goal is a decision model, not an exhaustive network diagram.

Identity deserves priority because valid credentials can bypass many perimeter controls. The review covers authoritative directories, single sign-on, multifactor authentication, privileged access, service accounts, dormant users, contractors, emergency access, secrets, keys and joiner-mover-leaver processes. The team should test representative populations and critical roles. A policy statement without configuration or operating evidence provides limited assurance.

Data mapping should classify sensitive and transaction-critical information; record location, ownership, purpose, retention, transfer, encryption, access, deletion and backup; and connect datasets to customer promises and legal bases. Unknown data flows can constrain consolidation, analytics, AI use, cross-border integration and divestment. The map should also show repositories used for source code, models, product telemetry, customer content, employee data and regulated records.

Third-party mapping includes cloud, managed service, payment, telecoms, software, security, data, development and operational suppliers. NIST CSF 2.0 identifies due diligence, contractual requirements, monitoring, incident planning and end-of-relationship provisions within cyber supply-chain governance.[1][3] The deal review should examine concentration, subcontracting, access, audit rights, incident notice, recovery commitments, portability, termination and exit evidence.

Figure 1. Transaction attack-surface and dependency map



The map connects technical exposure to critical services and transaction decisions.

4. Test control operation across the six cyber functions

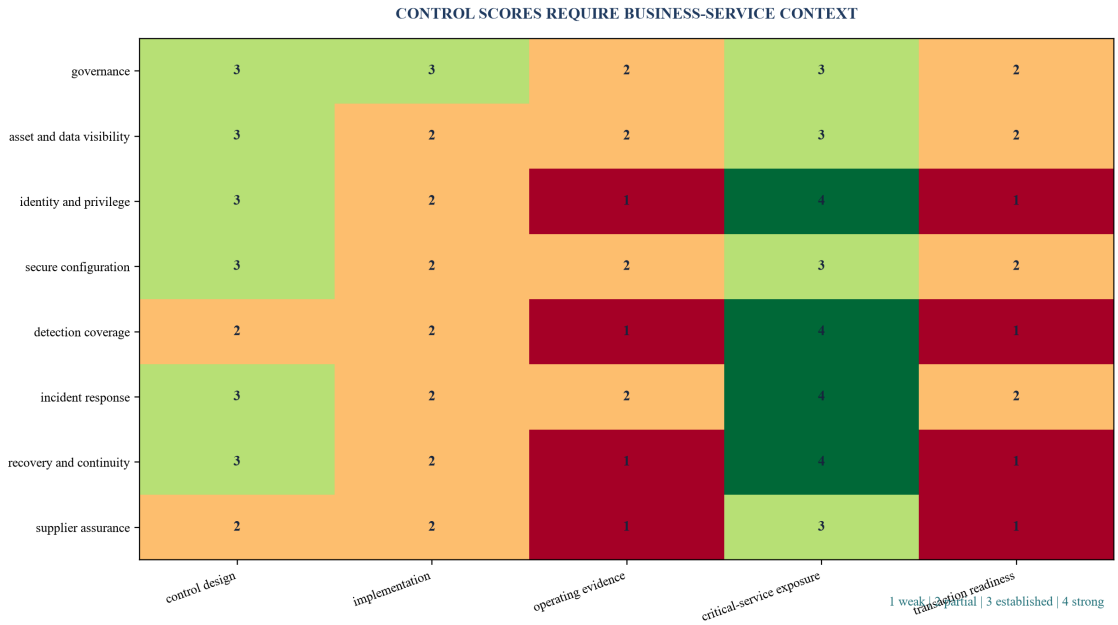
NIST CSF 2.0 organises outcomes through Govern, Identify, Protect, Detect, Respond and Recover.[1] A transaction review can use these functions as a common language while selecting evidence based on the target's services and risks. A framework mapping supports completeness; it does not substitute for testing.

Govern covers decision rights, risk appetite, policy, roles, oversight, supply chain and legal obligations. Evidence includes board reporting, risk acceptance, resource decisions, exceptions and accountability. Identify covers assets, services, data, dependencies, vulnerabilities and risk assessment. Protect covers identity, access, awareness, data security, platform configuration and technology resilience. Detect covers telemetry, coverage, alert logic, tuning and investigation. Respond covers incident command, analysis, containment, communication and reporting. Recover covers restoration, validation, customer service, lessons and resilience improvement.

The deal team should assess design, implementation, operation and outcome separately. A control can be well designed and partially deployed. A tool can be deployed without representative coverage. A process can operate without meeting the recovery outcome. Evidence confidence should reflect population coverage, sample selection, recency, independence and the target's ability to reproduce the result.

Maturity scores should remain subordinate to findings. An average score can hide a critical weakness in privileged access or recovery. The heat map should therefore show both control state and critical-service exposure. A low-maturity process attached to a non-critical environment may be a manageable technical-debt item. The same weakness in the only payment or clinical platform may require a closing gate.

Figure 2. Illustrative control-state and service-exposure heat map



Scores are hypothetical; live conclusions require representative evidence and deal-specific materiality.

5. Separate active compromise, control weakness and technical debt

Not every cyber finding has the same transaction meaning. The first category is active or recent compromise: unauthorised access, persistence, exfiltration, fraud, destructive activity or unresolved incident. This can require immediate containment, forensic preservation, legal assessment, notification, customer action, insurer engagement and a decision about signing or closing.

The second category is a control weakness that creates a credible loss pathway. Examples include unrestricted privileged access, incomplete multifactor authentication, exposed services, unmonitored critical assets, weak development controls, untested restoration or unsupported software. The transaction response depends on exploitability, affected service, compensating controls, evidence and remediation timing.

The third category is legal or regulatory exposure. Data may lack an adequate processing basis, incident reporting may be incomplete, security commitments may be unmet, regulated services may exceed tolerance or product obligations may be unclear. Counsel determines legal conclusions. The diligence record supplies facts, systems, data, jurisdictions, dates and operating evidence.

The fourth category is technical debt. Remediation may be required to reach the buyer's operating standard even where no present breach or material control failure is established. Technical debt should be costed, sequenced and separated from incident loss. The fifth category is integration-created risk: combining identity, networks, data, development tools or suppliers can create exposure that neither stand-alone business had. The buyer owns this risk and should not attribute it automatically to the seller.

Clear classification prevents the same finding from becoming an undifferentiated red flag. It also supports fair negotiation. Active compromise may justify a closing condition. A finite technical-debt programme may influence price or the integration budget. Buyer-created integration exposure belongs in the buyer's plan.

6. Reconstruct incident history and latent exposure

Incident diligence should examine known events, suspected events, alerts, investigations, insurance notifications, customer communications, regulator engagement, litigation, law-enforcement contact, restoration, root cause and lessons. The absence of a recorded incident does not establish the absence of compromise. Detection coverage, log retention and investigation quality determine how much confidence can be placed in history.

The team should test whether the target can produce an incident chronology and evidence of decisions. It should reconcile security records with legal, privacy, customer-support, fraud, finance, insurance and operational-resilience records. Discrepancies can indicate fragmented reporting or incomplete escalation. A material customer outage recorded as an operational problem may have had a cyber cause; a fraud case may have involved compromised identity.

The SEC's 2023 final rule requires registrants to disclose material cybersecurity incidents on Form 8-K and provide annual disclosures about processes for assessing, identifying and managing material cyber risks, together with governance disclosures.[5] The exact applicability, materiality and reporting path require issuer-specific legal advice. Transaction teams should nevertheless

preserve the evidence used for materiality decisions and reconcile public statements with diligence findings.

Incident evidence should be handled carefully. Premature system changes can destroy forensic artefacts. Broad circulation can affect privilege, confidentiality and response. The diligence protocol should define who receives details, who has authority to contain, how evidence is preserved and how the transaction timetable responds. If active compromise is suspected, the response team should take control through an agreed incident process.

7. Model credible cyber loss scenarios

A cyber loss scenario connects threat, vulnerability, asset, service, control, event and consequence. It avoids applying a generic breach cost to every finding. The scenario should specify the initiating event, access pathway, affected environment, detection and response assumptions, disruption duration, data impact, fraud exposure, regulatory pathway, customer effect, restoration work and residual uncertainty.

Financial consequences can include response and forensic cost, restoration, customer remedy, business interruption, lost gross profit, contractual credits, fraud, legal cost, regulatory penalty, insurance retention, higher premiums, accelerated capital expenditure, delayed integration, revenue churn and management diversion. Some are one-time cash items; others affect recurring earnings, growth, working capital or cost of capital. The model should identify tax, accounting and insurance treatment for professional review.

Probability estimates require humility. Sparse incident data, changing attackers and unknown control coverage make precise point estimates unreliable. The team can use ranges, scenarios and decision thresholds. Expected value may support negotiation, while tail severity may still justify a closing condition or risk limit. A low-probability event that can prevent safe operation of a critical service remains relevant.

Loss scenarios should distinguish target stand-alone exposure, transaction-triggered exposure and buyer integration exposure. A change-of-control clause, supplier termination, employee departure or accelerated attacker activity can alter risk around announcement and closing. The plan should account for heightened monitoring and privileged-access control during the transaction period.

Table 2. Illustrative cyber loss-scenario decision table

Scenario	Stand-alone cash range	Recurring earnings effect	Transaction response	Key uncertainty
compromised privileged identity	USD 0.5m-4.0m	possible customer and control effect	containment, forensic gate and specific protection	persistence and data access
critical-service ransomware	USD 2.0m-15.0m	interruption and customer attrition	recovery test, liquidity and Day 1 command	restoration integrity and duration
unsupported product component	USD 0.8m-6.0m	margin or roadmap effect	remediation budget and product covenant	replacement scope and customer commitments
unlawful or uncontrolled data use	USD 0.3m-8.0m	analytics, AI or cross-sell constraint	legal review, data condition and integration ring-fence	jurisdiction and remediation feasibility
concentrated cloud or supplier failure	USD 0.5m-10.0m	service-level and revenue effect	contract, exit plan and resilience investment	subcontracting and portability
integration-created identity exposure	buyer-funded	execution and delay effect	staged connectivity and buyer control	target-to-buyer dependency sequence

Amounts and probabilities are hypothetical modelling inputs, not benchmarks or forecasts.

Figure 3. Cyber exposure-to-value bridge

The bridge prevents repair cost, loss exposure and valuation effects from being combined without a defined economic path.

8. Translate exposure into valuation and financing

The valuation bridge starts with the nature of the economic effect. Immediate response, restoration and remediation are generally cash requirements. Sustained security staffing, licences, hosting changes, product support or customer concessions can affect recurring earnings. Lost or constrained revenue can affect forecasts and terminal value. Delayed integration can defer synergies and increase one-time cost. A severe uncertainty can affect financing capacity, insurance availability or the required return.

Repair cost alone can understate exposure because a technically simple control may sit on a severe loss pathway. It can also overstate seller responsibility where the buyer's standard exceeds the target's stand-alone need. The model should show the target requirement, buyer integration requirement and optional transformation separately. This allows the deal team to negotiate supported adjustments while budgeting buyer-led change honestly.

The team should define the valuation mechanism. A recurring earnings adjustment may flow through maintainable EBITDA and the selected multiple. A one-time cash item may affect equity value or a specific reserve. A contingent exposure may be addressed through probability-weighted scenarios, escrow, holdback, indemnity or insurance. The transaction model should prevent duplicate treatment across forecast, price adjustment, provision and synergy case.

IFRS 3 requires an acquirer to recognise identifiable acquired assets and assumed liabilities under the business-combination framework, while IFRS 13 defines fair-value measurement principles.[15][16] Cyber findings can influence information used in purchase-price allocation, asset valuation, contingent consideration, useful lives, provisions and impairment assessment, subject to professional accounting judgement. The diligence model should preserve source evidence and avoid presenting a transaction negotiation adjustment as an accounting conclusion.

Financing analysis should examine liquidity for response and remediation, covenant headroom, business interruption, delayed synergy, insurance retention, committed facilities and lender conditions. A lender may care about service continuity, regulatory standing, cash concentration and control over collateral or data. The cyber register should link these consequences to treasury and financing workstreams.

9. Select the transaction response without double counting

A supported finding can change price, structure, financing, SPA protection, closing conditions, Day 1 controls, remediation or risk acceptance. The selected response should address both economic allocation and operating cure. A price adjustment transfers value; it does not secure the environment. An indemnity may allocate specified loss; it does not restore a critical service. A remediation covenant may require action; it may provide limited recovery if the action fails.

The disposition paper should show evidence, uncertainty, economic path, available responses, residual risk and recommended authority. It should also show which treatments are mutually reinforcing and which would duplicate recovery. If remediation cost reduces price, is placed in escrow and is already reflected in the forecast, the model needs explicit reconciliation.

The deal team should preserve optionality. A suspected compromise may require forensic work before the appropriate economic response is known. The transaction can use a signing condition, closing condition, price mechanism, specific indemnity, information right or termination right as advised by counsel. Long-stop dates, materiality thresholds and waiver authority should align with the technical investigation timetable.

Risk acceptance should be written. The record identifies the decision maker, exposure, rationale, compensating controls, monitor, trigger and review date. The accepted finding remains in the Day 1 and 100-day register until the operating owner and risk authority approve closure.

10. Convert findings into SPA protection and closing conditions

Legal counsel determines drafting, enforceability and remedies. The cyber team provides the factual chain that allows provisions to be specific and operable. The SPA protection matrix links each finding to the relevant representation, warranty, indemnity, covenant, condition, price mechanism, escrow, insurance or information right. It records the protected exposure, evidence owner, survival period, cap, threshold, notice requirement, claim owner and remediation dependency.

Cyber representations may address incidents, compliance, security measures, data handling, contracts, business continuity, investigations and notices. Specific indemnities can allocate identified exposures. Pre-close covenants can preserve controls, require notification of new events, restrict material technology changes and support access for agreed remediation. Conditions can require containment, independent testing, regulator or customer action, restoration evidence, separation capability or delivery of critical records.

A closing condition should be objective and verifiable. “Improve cybersecurity” is not a controlled gate. A condition can identify a defined environment, control outcome, authorised test, evidence package, reviewer and acceptance authority. The target should know what completion means; the buyer should know which residual exposure remains.

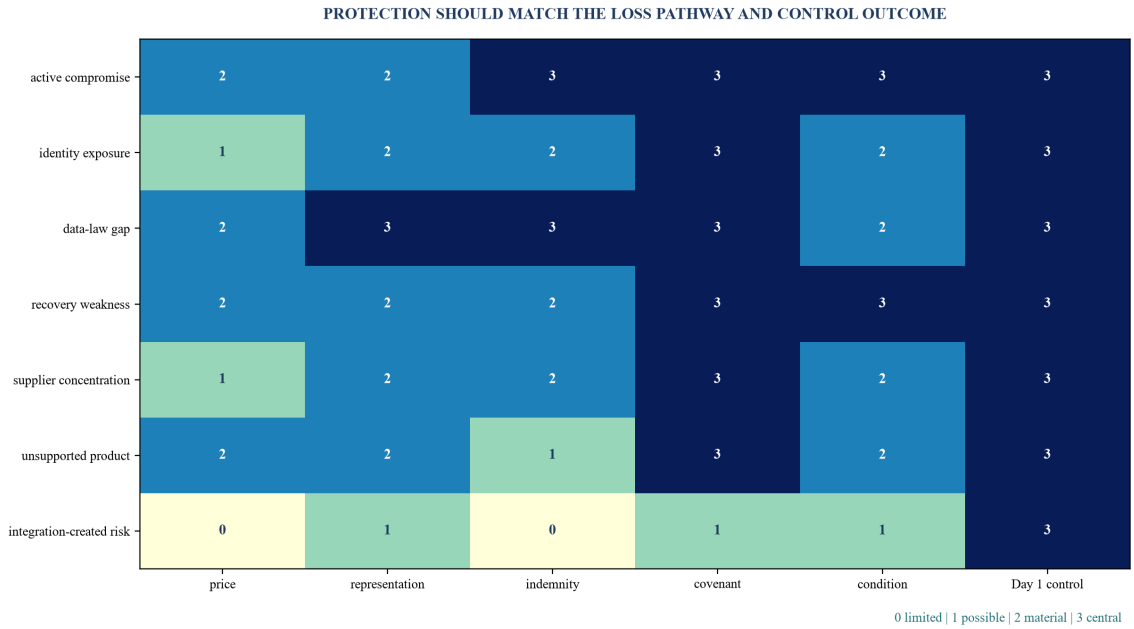
The matrix should distinguish confidentiality and privilege. Sensitive technical details may sit in a restricted schedule or evidence room rather than broad transaction documents. Access should be proportionate. The operating team still needs enough information after closing to execute remediation and meet reporting obligations.

Table 3. Cyber finding transaction-response matrix

Finding class	Price or structure	SPA protection	Closing evidence	Post-close control
active compromise	contingent or fixed adjustment after investigation	specific indemnity, covenant and notice	containment, forensic scope and clean restoration	heightened monitoring and closure retest
critical access weakness	remediation reserve where material	security covenant and incident notice	privileged-account inventory and tested control	Day 1 identity command
untested recovery	liquidity and delayed-synergy treatment	resilience covenant or specific protection	representative restore and service test	recovery programme and board tolerance
data-law exposure	scenario-based value and integration constraint	representation, indemnity and data covenant	legal basis, inventory and restricted-use plan	ring-fence, remediation and audit
unsupported technology	cash, earnings and product-roadmap effect	disclosure and remediation covenant	funded plan and critical supplier support	staged replacement with customer controls
supplier concentration	financing and continuity effect	contract and change-of-control protection	consent, service commitment and exit evidence	portability and resilience programme

Live provisions require jurisdiction-specific legal advice and deal-specific evidence.

Figure 4. Illustrative SPA and closing-protection matrix



Scores indicate relative suitability in a hypothetical case; counsel selects live transaction treatment.

11. Define cyber closing readiness

Closing readiness protects the first hours and days of ownership. The buyer should know who has legal and technical authority, which critical services must remain available, how privileged access is controlled, how payments are protected, where incident evidence is reported and how recovery will work. Readiness should be tested rather than inferred from a completed checklist.

The closing gate can include confirmation of no unresolved active compromise within the agreed scope; controlled administrator and service-account access; multifactor authentication for critical pathways; secured transaction and payment communications; current backups with representative restoration evidence; active monitoring for critical environments; incident contacts; legal and regulator reporting routes; supplier and cloud access; cyber-insurance status; and a tested escalation bridge.

The deal period can heighten risk. Public announcement, employee uncertainty, adviser access, data-room activity and integration preparation create new pathways. The parties should agree enhanced monitoring, credential hygiene, phishing response, secure communication and notification of material events. Seller and buyer responsibilities remain distinct before control transfers.

Carve-outs need an explicit separation-security plan. It identifies shared directories, networks, monitoring, applications, data, keys, licences, certificates, suppliers and response processes. Transitional services should include access boundaries, incident responsibilities, service levels, evidence, audit, change control and exit. The buyer should test its replacement capability before dependency expiry.

12. Protect Day 1 and the first 100 days

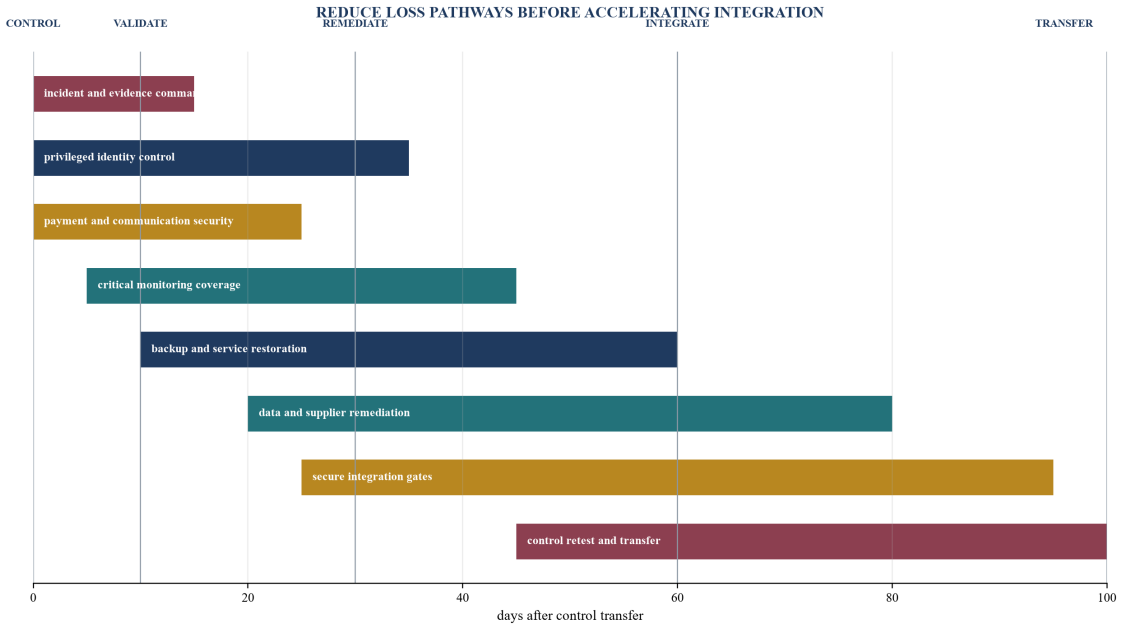
Day 1 should stabilise identity, payments, critical services, incident response, regulatory reporting, data boundaries and recovery. Rapid network integration can wait where evidence is incomplete. The buyer can use ring-fencing, monitored gateways, staged trust, restricted data movement and dedicated privileged access until control outcomes are verified.

The first ten days establish command: confirm accountable executives, reconcile privileged identities, preserve evidence, validate monitoring, test payment controls, inspect critical alerts, confirm backups and review open incidents. Days 11 to 30 complete high-confidence containment and validate the target baseline. Days 31 to 60 deliver critical remediation and test service resilience. Days 61 to 100 embed controls, complete priority integration and transfer residual risks into normal governance.

Remediation sequencing should follow loss-pathway reduction. Disabling exposed or dormant access can reduce immediate risk before a broad platform replacement. Segregating critical assets can reduce blast radius while long-term architecture is designed. A roadmap should show dependency, service impact, change window, customer obligation, resource, evidence and rollback.

The buyer should avoid declaring closure based on tool deployment. Closure requires a defined outcome and retest. Privileged-access remediation means the population is known, access is justified, authentication is controlled, use is monitored and exceptions are governed. Recovery remediation means a representative service can be restored with verified data integrity, dependent resources and operating sign-off.

Figure 5. Illustrative 100-day cyber remediation roadmap



Timing is hypothetical; live sequencing depends on compromise status, legal duties and service constraints.

Table 4. Cyber remediation work-package standard

Field	Required content	Decision use
supported finding	source, affected service, pathway and confidence	preserve why the work exists
target outcome	specific control and service result	define completion
accountable owner	executive, delivery lead and independent reviewer	establish authority
dependencies	legal, people, supplier, technology and change windows	sequence delivery
economic record	cash, recurring cost, downtime and forecast effect	control transaction model
evidence and retest	population, test, exception and acceptance	verify closure
residual exposure	remaining pathway, tolerance and monitor	support risk acceptance

Each work package should produce evidence of an operating outcome.

13. Address data, privacy and cross-border integration

Data diligence connects inventory, purpose, legal basis, consent where relevant, contract, retention, security, sharing, localisation, transfer and data-subject rights. The team should identify which datasets support the transaction thesis and whether the buyer can lawfully and practically use them after closing. A large dataset can have limited transaction value if provenance, rights, quality or permitted purpose is unclear.

The EU General Data Protection Regulation governs personal-data processing within its scope and includes security, breach-notification, processor and transfer obligations.[10] NIS2 addresses cybersecurity risk-management and incident reporting for covered entities, while DORA creates a financial-sector digital operational-resilience regime.[8][9] The Cyber Resilience Act introduces horizontal cybersecurity requirements for products with digital elements, with phased application.[11] Applicability and transition require entity, product and jurisdiction analysis.

The UAE federal data-protection framework establishes obligations and rights for personal-data processing, security and cross-border transfers within its scope.[12] The UAE Cabinet approved a National Cybersecurity Strategy in February 2025 based on governance, protection, innovation, capacity building and partnership.[13] Free-zone and sector regimes can add requirements. The diligence map should identify each legal entity, processing role, jurisdiction, regulator and data flow for counsel review.

Integration should use a data-permission gate. Before migration, consolidation, analytics, cross-selling or AI use, the owner confirms purpose, authority, customer promise, retention, access, transfer, security and deletion. The buyer can ring-fence data while gaps are remediated. This protects value by preserving lawful use and reducing uncontrolled replication.

14. Govern third parties and the software supply chain

Third parties can concentrate service, data and access risk. Diligence should identify critical suppliers, subcontractors, shared-responsibility boundaries, privileged access, data locations, incident notification, resilience commitments, audit rights, change-of-control terms, termination, portability and exit. A strong cloud provider does not make the target's configuration, identity or recovery strong.

NIST SP 1305 explains how CSF 2.0 can support supply-chain risk management and communication of supplier requirements.[3] NIST SP 800-161 addresses cyber supply-chain risk-management practices.[2] The transaction team should use these sources as governance anchors while applying contract and service evidence to the live target.

Software-product diligence examines source control, build systems, dependencies, secrets, vulnerability management, signing, release authority, open-source obligations, support status and product incident response. A software bill of materials can support visibility while completeness, version accuracy and operating use still require testing. Unsupported components can affect product security, customer commitments, roadmap, gross margin and valuation.

Change-of-control analysis belongs in the critical-supplier register. Consent, termination, price reset, data transfer, licence scope and service support can change at closing. The team should obtain evidence, quantify alternatives and define Day 1 continuity. Portability claims should be tested against data volume, interfaces, skills, time and contractual exit support.

15. Set governance, escalation and board reporting

The cyber diligence lead owns technical integrity. The deal lead owns transaction decisions. Legal counsel owns legal advice and drafting. Finance owns the economic bridge. Business and technology executives own remediation and service outcomes. Risk and internal assurance provide challenge according to mandate. The board or authorised committee accepts exposure outside delegated tolerance.

Escalation should depend on consequence and timing. Immediate escalation applies to suspected active compromise, unsafe operation, material service disruption, possible legal reporting, payment fraud, critical evidence conflict or a closing condition at risk. Other findings follow the transaction cadence with clear decision dates. A late finding should not be diluted because the timetable is compressed.

The board dashboard should show critical services, active incidents, high-severity pathways, evidence confidence, transaction decisions, price and cash effects, closing conditions, Day 1 readiness, remediation spend, overdue decisions and residual risk. It should distinguish target exposure from buyer integration risk and show where professional conclusions remain pending.

Management should retain an evidence archive after closing. It includes authority, scope, source records, test results, finding decisions, SPA links, closing evidence, remediation, retest and acceptance. Access remains controlled. The archive supports integration, claims, audit, regulatory response, insurance and future divestment.

Table 5. Board cyber transaction dashboard

Dashboard item	Evidence	Escalation trigger	Decision owner
critical-service exposure	service and dependency map	outcome outside approved tolerance	accountable executive
active or suspected incident	incident command record	material impact or unresolved compromise	executive, legal and board forum
valuation effect	controlled cash and earnings bridge	price or financing case changes	investment committee or board
SPA and closing protection	provision and condition matrix	protection unavailable or evidence overdue	deal and legal authority
Day 1 readiness	tested controls and exceptions	critical control lacks evidence	executive sponsor
remediation delivery	outcome, spend, dependency and retest	milestone or risk tolerance missed	value and risk forum
residual risk	accepted pathway and monitor	trigger reached or assumption invalidated	designated risk authority

The board view should emphasise decisions and exceptions rather than tool activity.

16. Apply a worked transaction scenario

Consider a hypothetical acquisition of a business-to-business software provider with USD 90 million of annual revenue. The buyer plans to connect customer-support, identity and analytics environments within 60 days. Diligence identifies incomplete multifactor authentication for privileged cloud accounts, limited log retention, an untested customer-platform restoration process, uncertain rights for a legacy training dataset and a critical deployment supplier with a change-of-control consent requirement.

The team does not combine these findings into one maturity discount. It models separate pathways. Privileged access and limited logs create uncertainty about compromise and support a contained forensic review. Restoration weakness creates a critical-service scenario and a closing readiness test. The training dataset requires legal analysis and a restricted-use plan before integration. The supplier contract requires consent and a continuity alternative.

The hypothetical economic bridge includes USD 1.2 million of priority cash remediation, USD 0.6 million of recurring security and resilience cost, a range for customer-service interruption and a delay to the analytics synergy case until data rights are confirmed. The deal model excludes the delayed synergy until the permission gate is met. It prevents the same USD 1.2 million from reducing both cash consideration and recurring earnings.

Counsel then maps supported facts to representations, notification covenants, specific protections and objective closing evidence. The Day 1 plan ring-fences the target identity environment, establishes monitored administrator access, protects payment communications and creates a joint incident bridge. The first 100 days sequence forensic closure, recovery testing, supplier resilience, data remediation and staged integration. Each work package closes only after outcome evidence and retest.

This scenario is illustrative. A live decision could differ materially based on evidence, law, insurance, seller response, customer terms, financing and bargaining position. The value lies in

the controlled translation from evidence to decision.

17. Implementation sequence and conclusion

The framework can be implemented through ten gates. Define authority and perimeter. Identify critical business services and integration intent. Build the attack-surface and dependency map. Test representative control operation. Reconstruct incident history. Classify findings. Model credible loss scenarios. Translate supported exposure into valuation and transaction protection. Test closing and Day 1 readiness. Verify remediation and transfer residual risk into normal governance.

Quality depends on traceability. A board should be able to move from a proposed price or condition back to the loss scenario, technical finding and authorised evidence. An operating owner should be able to move from a remediation task back to the service and transaction rationale. Finance should be able to reconcile cash, earnings, reserve, insurance and valuation treatment without overlap.

Cyber diligence creates transaction value when it changes a decision in time. It can identify a reason to stop, improve price, secure protection, protect critical services, preserve lawful data use, sequence integration and direct investment to the pathways that matter. The discipline is an evidence-led operating system connecting technology, law, finance and execution through closing and the first verified control cycle.

References

[1] National Institute of Standards and Technology. The NIST Cybersecurity Framework 2.0. 26 February 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] National Institute of Standards and Technology. SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. May 2022, updates current. https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final

[3] National Institute of Standards and Technology. SP 1305, Cybersecurity Framework 2.0 Quick-Start Guide for Cybersecurity Supply Chain Risk Management. October 2024. https://csrc.nist.gov/pubs/sp/1305/final

[4] National Institute of Standards and Technology. SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management. April 2025. https://csrc.nist.gov/pubs/sp/800/61/r3/final

[5] United States Securities and Exchange Commission. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule 33-11216. 26 July 2023. https://www.sec.gov/files/rules/final/2023/33-11216.pdf

[6] Financial Conduct Authority. Operational resilience requirements and current implementation materials, updated 14 July 2026. https://www.fca.org.uk/firms/operational-resilience

[7] Financial Conduct Authority. Operational resilience: insights and observations one year on. 2026. https://www.fca.org.uk/publications/good-and-poor-practice/operational-resilience-insights-observations-one-year

[8] European Union. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[9] European Union. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

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

[11] European Union. Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements. https://eur-lex.europa.eu/eli/reg/2024/2847/oj

[12] United Arab Emirates Cabinet. UAE legislative reform and federal personal-data-protection framework. 27 November 2021. https://uaecabinet.ae/en/news/uae-adopts-largest-legislative-reform-in-its-history

[13] United Arab Emirates Cabinet. UAE Cabinet approves National Cybersecurity Strategy. 3 February 2025. https://uaecabinet.ae/en/news/uae-cabinet-approves-national-cybersecurity-strategy-api-first-policy

[14] International Organization for Standardization. ISO/IEC 27001:2022 Information security management systems. https://www.iso.org/standard/27001

[15] IFRS Foundation. IFRS 3 Business Combinations. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/

[16] IFRS Foundation. IFRS 13 Fair Value Measurement. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-13-fair-value-measurement/

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.