The Cyber Liability Deal Team: Turning Technology Risk into Price and Protection

A Board Framework for Connecting Cyber Evidence to Value, Transaction Terms and Ownership Control

Authored by Chennakeshav Adya, Independent Researcher

August 2026

Abstract

Cyber risk in a transaction is an economic and control question. A target may carry a known incident, an undetected compromise, weak identity controls, unsupported systems, fragile recovery, exposed personal data, inadequate supplier contracts or insurance that will not respond after a change of control. Each condition can affect customer continuity, regulatory duties, remediation cost, working capital, financing, valuation and the allocation of loss between buyer and seller. A technical finding becomes decision-useful only when the deal team can connect it to an affected service, cash-flow mechanism, legal obligation and transaction response.

This paper develops a board framework for a cyber liability deal team. It defines the diligence perimeter, assembles an evidence-led cross-functional team, maps incidents and critical services, tests identity, vulnerabilities, data, software supply chains, cloud and operational technology, measures recovery, quantifies loss pathways, reviews insurance and converts findings into valuation, purchase-price mechanics, representations, indemnities, escrow, conditions, covenants and ownership actions. Six original figures and six tables translate the framework into practical decision tools.

The research draws on current primary and authoritative materials from the United Arab Emirates, European Union, United Kingdom, United States, India, Singapore and Australia. NIST Cybersecurity Framework 2.0 provides a governance and risk structure. The United Kingdom Information Commissioner's Office specifically addresses data-sharing diligence in mergers and acquisitions. The European Union's NIS2 regime, United States securities disclosure rules, UAE data-protection requirements, India's cyber-incident directions, Singapore's updated Cybersecurity Act and Australia's prudential and privacy regimes demonstrate why notification clocks, supply chains and board accountability must enter the transaction model.

All amounts, probabilities, scores, prices, time periods, loss estimates and transaction outcomes in this paper are hypothetical management assumptions used to demonstrate the framework. They do not describe a client, current market quotation, forecast, legal conclusion, insurance coverage opinion, transaction recommendation or assured outcome. This paper does not provide legal, regulatory, cybersecurity, technical, accounting, tax, insurance, valuation or investment advice. Qualified advisers should assess the target, transaction documents, systems, incidents, policies and applicable jurisdictions.

JEL Classification: G24, G32, G34, K22, K24, L86, M15

Keywords: cyber due diligence, cyber liability, technology risk, mergers and acquisitions, purchase price, indemnity, cyber insurance, data breach, operational resilience, transaction protection

1. Convert cyber findings into transaction decisions

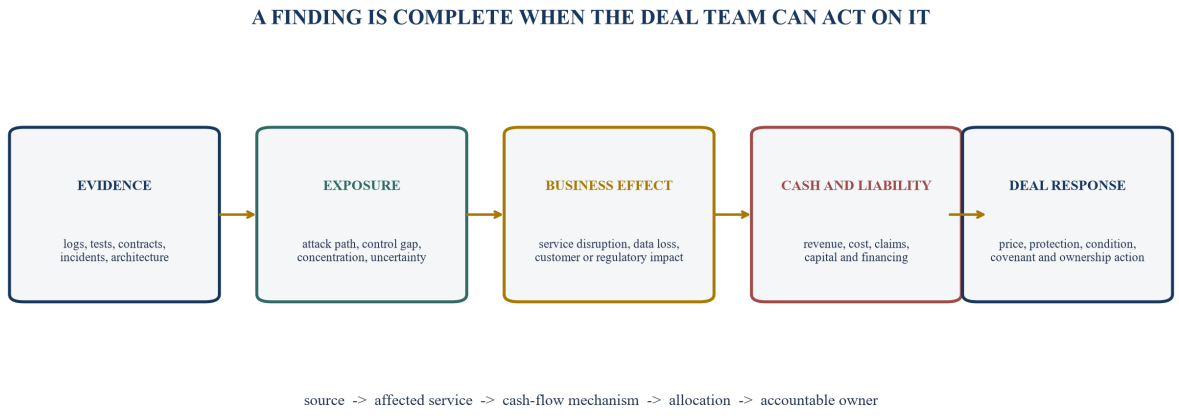
A cyber diligence report should support decisions about value, allocation and control. A list of vulnerabilities cannot do that on its own. The deal team needs to know which business service is exposed, how a failure could affect customers or cash, whether an incident has already occurred, which duties or contracts may be triggered, how quickly the condition can be corrected and who bears the cost and residual risk.

The analytical chain begins with evidence. A finding should identify its source, date, scope, owner and reliability. The team then maps it to an attack or failure path, an affected critical service and a financial or legal consequence. The final step assigns a transaction response: remediation before signing, a closing condition, a price adjustment, an escrow, a specific indemnity, a covenant, insurance treatment, Day One containment or an accepted ownership risk.

This chain prevents two common errors. First, it prevents technical severity from becoming an automatic valuation adjustment. A critical vulnerability on an isolated test system can be less economically important than a moderate weakness in the identity service supporting every customer environment. Second, it prevents commercial optimism from suppressing structural exposure. A fast-growing platform can carry a latent compromise, irrecoverable data, uninsurable representations or a supplier dependency that threatens the investment thesis.

The board needs visibility of uncertainty. Limited access, incomplete logs, restricted testing, unavailable personnel and unresolved forensic questions should be recorded as evidence limitations. The response to uncertainty may be additional work, a conservative model, stronger protection, delayed integration or a decision to stop. Describing a limitation without assigning a consequence leaves the transaction exposed.

Figure 1. Cyber evidence to transaction-decision chain



Every material finding should reach a documented economic, legal or operating response.

2. Define the transaction and technology perimeter

The diligence perimeter should follow the ability to deliver the acquired proposition. It should include legal entities, products, customer environments, critical services, applications, infrastructure, cloud accounts, operational technology, identities, data stores, code repositories, suppliers, licences, insurance and people. The share purchase perimeter may differ from the operating perimeter when technology is held by an affiliate, founder, joint venture, university, outsourced provider or shared group function.

The team should identify what changes at signing and closing. A change-of-control clause can affect cloud, software, managed-security, incident-response or insurance arrangements. A carve-out may require new domains, certificates, networks, licences and monitoring before the business can operate independently. A merger may connect two estates with incompatible identity, logging and recovery systems. The cyber review should therefore examine both the target's present state and the planned transition state.

Product claims should be connected to technical components and customer commitments. A target can describe its platform as resilient while relying on one cloud region, one identity provider or a small engineering team with privileged access. Customer contracts may promise notification, audit, recovery or security standards that exceed the target's current controls. The perimeter should map each obligation to the actual service and supporting assets.

The team should distinguish acquired liabilities from future integration choices. Historical incidents, inadequate disclosures and existing control gaps enter the transaction risk. A buyer's plan to consolidate systems, migrate data or change suppliers creates a separate execution risk. Combining the two can lead to duplicated cost or misplaced protection. The valuation bridge should show the stand-alone condition, mandatory remediation, chosen integration and expected synergy separately.

Perimeter changes during diligence should be controlled. New products, acquisitions, incidents, customer commitments, cloud migrations or regulatory designations can alter the exposure. A dated perimeter register and change log allow the deal team to identify when prior testing must be refreshed.

3. Build a deal team with explicit decision rights

Cyber liability crosses functions. The chief information security officer or technical adviser can assess controls and threat paths. Legal advisers interpret duties, privilege, representations and liability. Privacy specialists assess personal-data obligations. Finance converts exposures into cash flows. Insurance advisers examine policy response. Commercial diligence tests customer consequences. Integration leaders determine feasibility and timing. The transaction lead and board decide allocation and residual risk.

The team should agree decision rights before high-pressure findings emerge. One owner should maintain the exception ledger. Each finding should have a technical assessment, legal or regulatory route where relevant, economic treatment, proposed deal response and integration owner. The transaction committee should resolve conflicts, such as whether a remediation belongs in price, seller protection or the ownership plan.

Legal privilege and clean-team arrangements require deliberate design. Sensitive forensic material, personal data, customer information, export-controlled technology and competitively sensitive systems may need restricted review. The team should define who may receive which evidence, how conclusions are summarised and how access is logged. The arrangement should preserve useful evidence while respecting applicable law and transaction constraints.

The team also needs escalation thresholds. Examples include evidence of active compromise, unreliable management statements, unreported incidents, unavailable backups, material customer notification duties, a regulatory deadline, a critical uninsured exposure or an essential system that cannot transfer. An escalation should trigger a specified decision forum and timetable.

Table 1. Cyber liability deal-team operating model

role	primary evidence responsibility	decision contribution	escalation trigger	output
transaction lead	perimeter, timetable and data-room completeness	coordinates price, protection and approvals	finding threatens signing, financing or thesis	integrated exception ledger
cyber specialist	architecture, controls, incidents and testing	assesses attack path, severity and remediation	active compromise or unreliable technical evidence	technical risk and remediation plan
legal and privacy	laws, contracts, privilege and notification	defines liability, disclosure and drafting route	notification duty, claim, order or missing consent	legal issue map and proposed clauses
finance and valuation	budgets, forecasts, losses and commitments	converts exposure into cash-flow and value effects	unbounded cost or double-counted adjustment	quantified value bridge
insurance adviser	policies, applications, notices and exclusions	assesses existing and transactional coverage	coverage gap, change-of-control issue or late notice	coverage and claims memorandum
integration leader	Day One access, continuity and remediation	tests deliverability, owners and sequence	critical action cannot be completed safely	100-day control plan
board or investment committee	complete evidence and residual-risk view	approves value, protection, conditions and acceptance	unresolved thesis-critical exposure	recorded decision and conditions

Actual roles and privilege arrangements depend on the transaction and applicable professional advice.

4. Use an evidence architecture that survives restricted access

Cyber diligence rarely provides unrestricted production access. Sellers must protect systems, personal data, customer confidentiality and transaction secrecy. The buyer still needs decision-grade evidence. A tiered architecture can begin with governance records and management interviews, progress to redacted artefacts and sampled evidence, and reserve targeted technical validation for the highest-risk questions.

The initial request should seek critical-service maps, security governance, risk registers, material incidents, regulatory correspondence, customer security obligations, insurance, asset and identity records, vulnerability management, logging, recovery tests, supplier access and security expenditure. The team should test internal consistency. An incident register should reconcile with insurance notices, customer communications, legal matters, service tickets, regulator contacts and

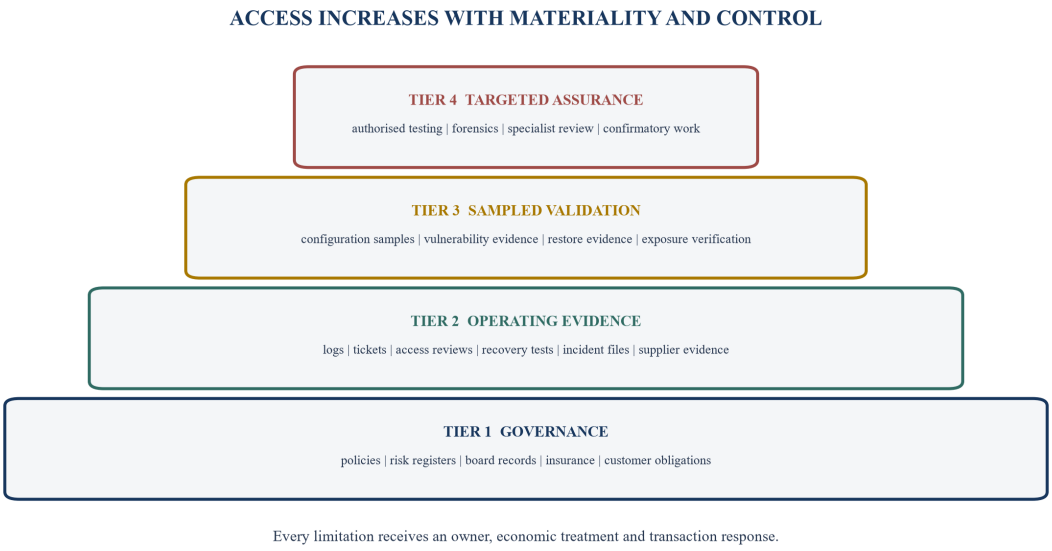
board minutes.

Technical validation should be risk-led. External attack-surface review, configuration evidence, vulnerability samples, access reviews, backup restoration evidence and log-coverage maps can reveal operating quality without intrusive testing. Penetration testing requires explicit authority, scope and coordination. A buyer should never treat unauthorised probing as diligence.

Evidence should be graded. Direct system output and independently reproduced tests provide stronger support than a policy document or verbal statement. Certification can inform the review while scope, date, exceptions and reliance need examination. A security report covering one product does not establish control across the estate. The ledger should state what the evidence proves and what remains unknown.

Where access remains limited, the deal response should reflect the untested condition. Options include a seller-led independent assessment, confirmatory work before close, a specific condition, restricted Day One connectivity, escrow, a covenant, enhanced warranty or a conservative valuation case. The limitation should never disappear from the committee paper simply because the transaction has progressed.

Figure 2. Tiered cyber evidence architecture for transaction diligence



Higher access should follow materiality, authority and controlled handling.

5. Reconstruct incident history and disclosure quality

Incident history is more than a count. The team should reconstruct detection, scope, containment, root cause, affected systems, data, customer impact, regulatory analysis, notifications, insurance, remediation and lessons. Near misses and control failures matter because they can reveal exposure that did not yet produce a reported loss. The absence of recorded incidents can indicate strong control, limited visibility or incomplete reporting.

The review should reconcile several sources. Security operations records, service-desk tickets, legal matters, privacy logs, customer notices, insurance claims, forensic reports, regulator correspondence and board materials may describe the same event differently. Differences should be investigated. A management statement that an incident was immaterial should be supported by

the contemporaneous assessment and available evidence.

Notification clocks vary by jurisdiction and sector. United States public-company rules require disclosure after a materiality determination. European regimes can require early warnings and later reports. Data-protection regimes may use risk or harm thresholds. India's CERT-In directions use a short reporting period for specified incidents. Singapore's critical-information-infrastructure regime includes rapid notification and supply-chain coverage. The deal team should identify the applicable clock, awareness point, threshold, recipient and evidence of compliance.

Historical compromise can persist. Credentials, tokens, remote-access tools, scheduled tasks, backdoors or copied data may survive apparent containment. The team should test whether the target validated eradication and whether later monitoring supports that conclusion. A closed incident with incomplete forensic evidence may require a clean-environment plan, additional monitoring or specific transaction protection.

Disclosure quality is itself an indicator. Delayed escalation, missing root-cause analysis, inconsistent customer accounts or unsupported closure can reveal governance weakness. Strong incident records show authority, facts, decisions, communications, recovery and corrective action. The buyer should value that operating discipline independently from whether the target has experienced an attack.

Table 2. Minimum cyber-incident reconstruction ledger

field	evidence	diligence question	unresolved-risk treatment	ownership destination
detection and awareness	alerts, tickets, emails and chronology	when did the organisation first know enough to act?	test reporting clocks and governance	disclosure and notification workstream
scope and affected service	forensics, architecture and customer records	which systems, data and services were affected?	model wider plausible scope	valuation and continuity plan
containment and eradication	response records, credential resets and scans	was attacker access removed and validated?	require confirmatory work or clean build	closing or Day One condition
legal and regulatory analysis	advice, notices and correspondence	were all applicable duties assessed and completed?	quantify claims, penalties and remediation	legal protection and covenant
customer and contractual impact	notices, credits, disputes and renewals	did the event affect revenue or future obligations?	adjust cohorts and contingent value	commercial and valuation bridge
insurance response	policy, notice, reservation and payments	is the claim preserved and transferable?	exclude uncertain recovery from base case	insurance and purchase-price treatment
lessons and remediation	root-cause review, plan and closure evidence	did controls improve in operation?	fund and verify unfinished work	100-day programme

Legal privilege, confidentiality and reporting rules determine access and handling.

6. Map critical services and plausible attack paths

Business impact should be assessed through critical services. A target can remain technically online while producing corrupted transactions, exposing confidential data or operating an unsafe process. The service map should therefore cover availability, integrity, confidentiality and control. It should identify customers, operational tolerances, revenue, contractual commitments, regulated outcomes and dependencies.

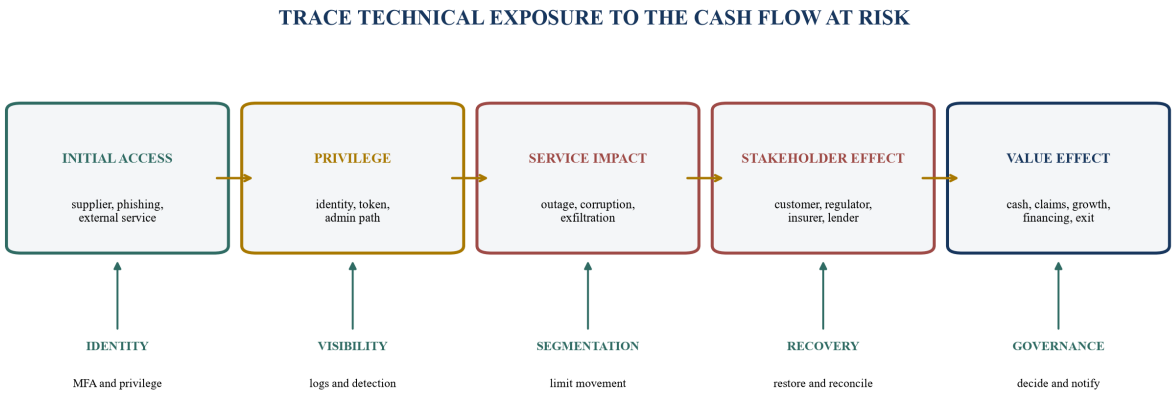
The team should select severe but plausible attack paths that reflect the target's architecture and threat environment. Examples include privileged-identity compromise, ransomware, destructive cloud control-plane access, software supply-chain compromise, business-email fraud, data exfiltration, denial of service and operational-technology manipulation. Each path should trace initial access, privilege, movement, affected service, detection, response and recovery.

This mapping changes prioritisation. An unpatched external system supporting a critical service can create an immediate exposure. A shared identity platform can connect otherwise separate products. A managed service provider can create correlated risk across environments. A backup platform using the same credentials and network can fail with production. The economic model should reflect these dependencies rather than average control scores.

Service tolerances provide a decision standard. The board can ask how long the service can be unavailable, how much data can be lost or corrupted, what manual capacity exists and which harm becomes unacceptable. Recovery objectives and service levels support those tolerances. A stated target without exercised recovery remains an assumption.

The attack-path review should also identify control breakpoints. Multi-factor authentication, privileged-access separation, endpoint visibility, network segmentation, immutable backup, supplier notification and practiced incident authority can interrupt different stages. The deal team should evaluate whether these controls operate across the relevant service, including inherited and third-party components.

Figure 3. Attack path to enterprise-value consequence



The path is illustrative; target-specific evidence determines the actual sequence and impact.

7. Test identity, privilege and ownership transition

Identity is often the shortest route from a single compromised account to enterprise-wide control. The review should map workforce identities, privileged accounts, service accounts, machine identities, application keys, cloud roles, emergency access and external administrators. It should identify authoritative directories, authentication methods, access-review processes and the ability to revoke access promptly.

The team should sample joiner, mover and leaver events; privileged grants; dormant accounts; shared credentials; emergency access; multi-factor enrolment; conditional access; password and key rotation; and logging. Evidence should cover subsidiaries, acquired systems, cloud platforms and operational technology. A policy applied to the corporate directory may omit product infrastructure or engineering environments.

Change of control creates specific risks. Founders or contractors may own domains, repositories, certificates, cloud subscriptions or password vaults. Service accounts may depend on personal email or unmanaged devices. The buyer should confirm ownership and transferability before closing. Critical secrets should have a controlled rotation plan, with rollback and service-continuity testing.

Privileged access should be assessed through reach and consequence. One account that can alter production, disable logging and delete backups has a different exposure from a local administrator on an isolated device. The team should identify toxic combinations and whether approval, session recording, time limits or separate recovery credentials constrain them.

Day One access should follow minimum necessary authority. The buyer may need visibility before broad federation or network connection. Staged trust, separate monitoring and verified revocation can reduce the risk of importing an undetected compromise. The integration plan should state the sequence and evidence required for each connection.

8. Assess external exposure, vulnerabilities and technical debt

Vulnerability counts require context. The team should identify internet-facing services, unsupported technology, known exploited vulnerabilities, exposed credentials, weak remote access, insecure configurations, missing endpoint visibility and patch-management failures. It should then map each condition to reachability, privilege, compensating controls, affected services and credible attacker use.

The target should provide asset and vulnerability evidence with dates, scope, exclusions and remediation performance. The buyer should test whether inventories reconcile across discovery, cloud, endpoint, network and service-management sources. Unknown assets and stale records can be more important than the average age of known vulnerabilities. External exposure review can help validate the perimeter, subject to explicit authority and passive or otherwise approved methods.

Technical debt becomes a transaction issue when it changes cash, timing or executability. Unsupported operating systems may require replacement. A monolithic application may make segmentation difficult. An unmaintained library can create repeated exposure. A product with no secure-development evidence may require a sustained engineering programme. The team should separate immediate containment, mandatory remediation and elective modernisation.

Severity should therefore combine exploitability, exposure, privilege, service criticality, detection, recovery and persistence. A scoring model can support consistency while the committee should retain judgement. The output should describe the loss pathway and treatment, not merely a colour.

Remediation estimates should include testing, downtime, supplier effort, customer coordination, licence cost, engineering opportunity cost and the risk of change. A fast patch may be inexpensive. Replacing an unsupported core platform can affect the investment case and integration sequence. The budget should show confidence and dependencies.

9. Build a jurisdiction and notification matrix

Cyber liability follows people, data, services, listings, sectors and infrastructure. The target's place of incorporation is only one factor. The team should identify where affected individuals are located, where systems and providers operate, which customers impose notification duties, whether the target is regulated, whether a listed parent or issuer is involved and which incident-reporting regimes apply.

The European Union's NIS2 framework requires risk-management measures that include supply-chain security and multi-stage reporting for significant incidents. The United States Securities and Exchange Commission requires public-company disclosure of material cybersecurity incidents after the materiality determination. UAE federal data-protection law requires security measures and breach processes, while ADGM and sector regimes can impose their own notification requirements. India's CERT-In directions require rapid reporting for specified incidents. Singapore's Cybersecurity Act extends attention to critical infrastructure, foundational digital infrastructure and supply chains. Australia's APRA and privacy regimes add board, third-party and notification duties.

The matrix should record the legal trigger, awareness point, timetable, information required, responsible decision maker, regulator or recipient, contractual overlay and evidence. A single event can activate several clocks. The team should prepare an integrated chronology and avoid assuming that one filing satisfies every duty.

Cross-border investigations also raise access and transfer questions. Forensic images, logs, personal data and employee information may be moved to advisers or response providers in other jurisdictions. The incident plan should identify lawful routes and minimum necessary access. Qualified advisers should decide the legal position from the facts.

Regulatory uncertainty should be explicit. A rule may be implemented differently across member states or sectors. A target may be approaching a designation threshold. The deal team should state current advice, assumptions and sensitivity rather than creating a false global standard.

Table 3. Illustrative cross-border cyber notification matrix

jurisdiction or regime	transaction diligence focus	incident trigger or clock	evidence to request	deal implication
United States public issuer	materiality process, governance and prior filings	Form 8-K within four business days after materiality determination	incident chronology, materiality record and disclosures	disclosure readiness, warranty and issuer integration
European Union NIS2	entity scope, supply chain and management oversight	staged reporting can include 24-hour warning and 72-hour notification	sector analysis, incident route and supplier obligations	covenant, governance remediation and reporting plan
European or UK personal data	controller role, risk and M&A data sharing	risk-based authority and individual notification duties	breach register, assessment, notices and data map	privacy indemnity, remediation and integration controls
UAE federal or financial centre	security measures, controller duties and local overlays	applicable federal, ADGM, DIFC or sector process	jurisdiction map, incident records and regulator contacts	condition, local advice and Day One authority
India CERT-In and data protection	specified cyber events and personal-data safeguards	specified incidents can require reporting within six hours	logs, reporting process, processor contracts and notices	rapid escalation design and compliance remediation
Singapore Cybersecurity Act and PDPA	CII, FDI, supply chains and personal-data impact	regulated cyber and notifiable data-breach processes	designation, supplier map, incident forms and assessments	supplier covenant, reporting plan and continuity test
Australia APRA and privacy	critical information assets, third parties and serious harm	APRA and NDB duties depend on scope and impact	CPS 234 evidence, incident assessment and notices	board assurance, control budget and customer response

This is a research summary. Qualified advisers should confirm current rules, scope, triggers and deadlines.

10. Trace personal data, confidentiality and customer obligations

Data diligence should map material information from collection through use, storage, sharing, backup, archive and deletion. The team should identify the controller or equivalent decision maker, processors, purposes, legal bases, sensitive categories, locations, transfers, retention and security controls. A high-level privacy policy cannot replace operational lineage.

M&A creates specific data-sharing questions. The UK Information Commissioner's Office states that organisations should consider data sharing as part of due diligence when a merger or acquisition changes the controller or adds one. The team should establish the original purpose, lawful basis, changes after the transaction, transparency, governance and security. Similar fact-specific analysis may be required elsewhere.

Customer contracts can create duties beyond data-protection law. Notification periods, audit rights, security standards, data-location commitments, subcontractor approvals, deletion obligations and liability caps should be extracted and mapped to the services involved. The target should demonstrate operating compliance and disclose exceptions. A single strategic customer can change the financial importance of a control gap.

The team should test whether the target can determine what data was affected during an incident. Asset inventories, classification, logging, encryption, key management and lineage support that decision. Weak evidence can expand the plausible breach population and response cost. It can

also delay notifications and customer communication.

Data deletion and separation matter at closing and integration. A carve-out may contain seller data that must be removed. The buyer may lack rights to combine datasets across businesses. Backups and logs can retain information after production deletion. The separation plan should define verified deletion, retained legal records, transition access and responsibilities.

11. Test software supply chains, suppliers and shared responsibility

Software products and digital services depend on code, packages, build systems, cloud platforms, managed service providers, identity services, data processors and specialist support. A target's control environment can therefore fail through a supplier. The diligence team should map direct providers, critical fourth parties, administrative access, data flows, incident duties, audit rights, continuity and exit.

NIST Cybersecurity Framework 2.0 includes governance outcomes for due diligence, contractual requirements, supplier monitoring, incident coordination and end-of-relationship actions. European NIS2 materials and Singapore's updated framework also emphasise supply-chain security and reporting. Australian guidance calls for supplier risk assessment, shared responsibility and transparency. These principles support a transaction-level supplier register.

Contracts should be compared with technical reality. A cloud shared-responsibility model can leave the target responsible for identity, configuration, data and applications. A managed provider may have broad privilege while the contract lacks rapid notification or evidence rights. A software vendor may disclaim consequential loss while supporting a critical service. The buyer should identify which responsibilities are controlled, transferred, insured or retained.

For software targets, the review should examine development environments, repositories, build pipelines, signing, dependencies, secrets, vulnerability handling and release approval. A software bill of materials can improve transparency when it is current and connected to deployed versions. Build provenance and reproducibility can support assurance that released code came from the controlled process.

Concentration should be modelled. Several suppliers may rely on one cloud, identity platform, network or open-source component. The team should identify realistic alternatives, transition time, data portability, contractual exit and tested continuity. A nominal right to terminate provides little protection when replacement takes a year.

12. Verify recovery, forensics and continuity evidence

Recovery is a financial control. The ability to restore critical services determines business interruption, customer harm, liquidity and the duration of crisis management. The diligence team should review backup scope, isolation, immutability, credentials, retention, monitoring, restoration testing and reconciliation. It should confirm that backups cover configuration, code, keys, dependencies and data required to deliver the service.

A backup success report does not prove recoverability. The target should demonstrate restoration of representative services, including clean infrastructure, identity, applications, data and validation. The test should measure elapsed time, data loss, manual work, dependencies and unresolved errors. Recovery into a compromised environment can reintroduce the attacker or

corrupted configuration.

Forensic readiness supports both response and liability management. The team should assess logging scope, time synchronisation, retention, tamper resistance, endpoint and cloud visibility, evidence handling and access to specialist support. Missing evidence can prevent management from defining the affected population, validating eradication or supporting insurance and regulatory positions. The cash-flow model should recognise the wider plausible scope created by weak evidence.

Continuity plans should address customer delivery, manual alternatives, communications, legal decisions, liquidity, payroll, suppliers and critical personnel. A technical recovery plan can restore systems while leaving a commercial crisis unmanaged. The board and executive team should have explicit authority for containment, shutdown, disclosure, notification, ransom decisions, customer remedies and external communications.

The buyer should review exercises and actual outcomes. A tabletop can test decisions and coordination. A technical exercise can test detection and recovery. A supplier exercise can test external dependencies. Findings should have owners, budgets and closure evidence. Repeated unresolved actions indicate that the plan is not operating as intended.

13. Quantify cyber loss through cash-flow pathways

Cyber value adjustments should be based on cash-flow mechanisms rather than headline breach statistics. The model can separate immediate response, business interruption, customer remediation, contractual claims, regulatory and legal cost, capital expenditure, working-capital effects, insurance recovery, financing impact and delayed growth. Each line needs a scenario, probability or range, timing, tax treatment where advised, dependency and evidence source.

Immediate response can include forensics, legal advisers, notification, public relations, customer support and emergency technology. Business interruption should use the critical-service map, downtime, manual capacity, backlog, service credits, lost transactions and recovery curve. Customer effects can include churn, lower renewal, delayed sales, price concessions and audit requirements. Capital cost can include identity redesign, segmentation, platform replacement, logging, recovery and secure development.

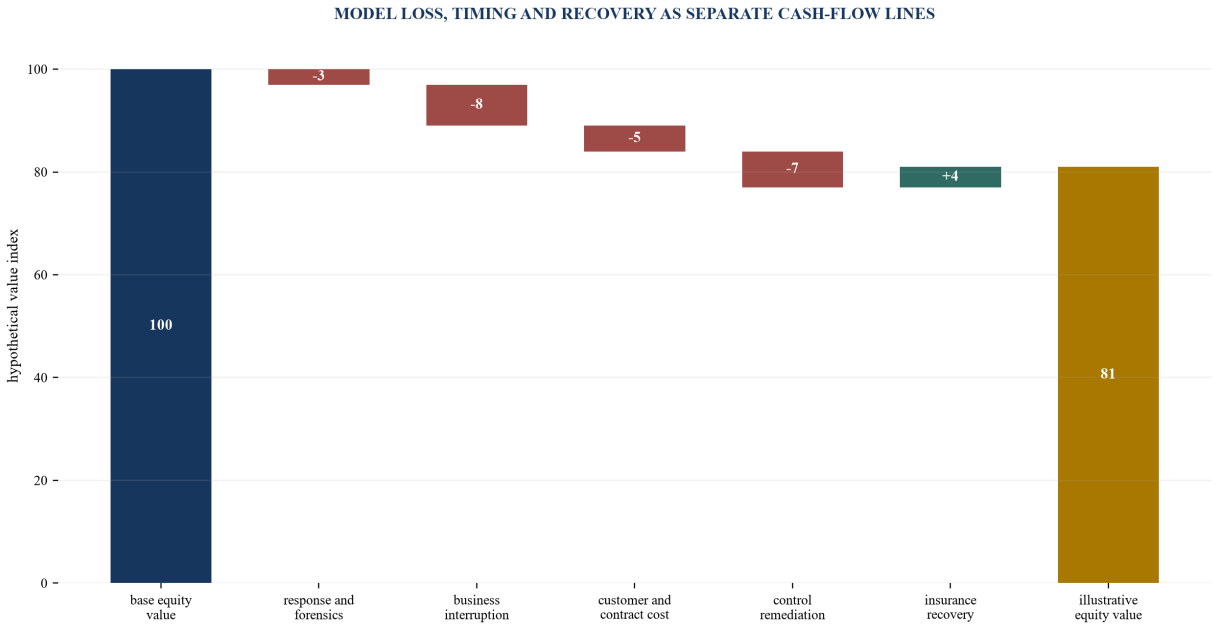
Regulatory penalties should not be treated as the only liability. Investigation, remediation, monitoring, customer communication and management distraction can be more significant. Fines and claims depend on facts, law, discretion, causation and mitigation. The model should state uncertainty and avoid presenting statutory maxima as expected loss.

Insurance recovery should remain separate. Coverage depends on policy terms, application accuracy, notice, exclusions, retentions, sublimits, consent, aggregation and change of control. A gross-loss case and a separately probability-weighted recovery case allow the committee to see the underlying exposure. Expected insurance proceeds should not erase the need for liquidity during response.

The model should also identify non-linear effects. A short outage during a low-volume period differs from the same outage at a regulatory deadline or peak sales event. A data incident involving sensitive records can have a different claims path from loss of ordinary contact information. A compromise of code signing can affect customers beyond the target. Scenarios

should therefore reflect business context.

Figure 4. Illustrative cyber loss bridge from technical event to equity effect



Values are hypothetical management assumptions and do not represent an actual company, claim or transaction.

Table 4. Cyber loss and value bridge

cash-flow pathway	evidence	modelling question	common error	transaction use
incident response	panel rates, retainers, prior events and scope	what specialist work begins immediately?	using a generic cost per record	liquidity reserve and escrow sizing
business interruption	service tolerance, revenue pattern and recovery test	how does disruption affect transactions, backlog and cash?	assuming full revenue loss for all downtime	downside case and covenant headroom
customers and contracts	credits, notification duties, concentration and cohorts	which customers can claim, leave or delay purchase?	treating reputation as an unquantified label	revenue bridge and earnout design
legal and regulatory	incident facts, jurisdictions, claims and advice	what investigation, defence, remediation and redress may occur?	using maximum fines as expected value	specific protection and disclosure
control remediation	architecture, estimate, sequence and downtime	which spend is mandatory to preserve the thesis?	blending mandatory work with integration choice	price, condition and 100-day budget
insurance recovery	policy, notice, exclusions, retention and consent	when and how much recovery is supportable?	netting assumed limits against gross exposure	separate recovery case and claims covenant
financing and exit	lender terms, disclosure and assurance gaps	can the exposure affect liquidity, covenants or later diligence?	omitting capital-market consequences	financing condition and exit evidence plan

The table provides a modelling structure. Actual amounts require target evidence and qualified advice.

14. Examine insurance as evidence, liquidity and allocation

Cyber insurance can provide response services and financial protection, while policy existence does not establish coverage for the transaction's exposure. The team should review policy periods, named insureds, limits, retentions, sublimits, waiting periods, exclusions, territorial scope, retroactive dates, prior knowledge, control warranties, applications, notices, claims, consent requirements and change-of-control provisions.

The application and renewal evidence matter because inaccurate statements about controls can affect coverage. The buyer should compare representations about multi-factor authentication, backups, endpoint detection, privileged access and incident history with diligence findings. A gap should be reviewed by qualified insurance and legal advisers. The deal team should also identify whether circumstances or claims require notice before closing.

Coverage should be mapped to loss pathways. Incident response, business interruption, dependent business interruption, data restoration, cyber extortion, privacy liability, regulatory defence, media liability and fraud may have different conditions and sublimits. Business-email compromise or infrastructure failure may be excluded or addressed elsewhere. The policy can also provide access to approved forensic, legal and communication providers.

Change of control can end or restrict cover for post-close events while preserving claims for pre-close acts under specific conditions. Run-off or tail arrangements may be relevant. The buyer's programme may begin at closing, subject to underwriting and disclosure. The team should coordinate placement, notices and continuity so that no assumption of coverage is left untested.

Insurance does not substitute for control or transaction protection. It can provide liquidity and expertise while claims can be delayed, disputed or capped. The valuation should show gross exposure and supportable recovery separately. The purchase agreement should address control of claims, cooperation, proceeds and the interaction between insurance and indemnity.

15. Translate findings into valuation without double counting

The valuation bridge should distinguish four mechanisms: sustainable cash-flow change, one-time remediation, contingent liability and transaction execution cost. A weak security programme can require recurring operating expense. Unsupported systems can require capital expenditure. A known incident can create contingent claims. A carve-out can require transition cost. Each item should appear once in the model.

Revenue adjustments should follow customer evidence. A cyber incident can affect retention, pricing, sales cycles or contractual credits. The team should avoid reducing revenue for a risk and then separately deducting the full enterprise-value effect of the same risk. A transparent bridge should state the affected forecast line, period, probability and any corresponding protection.

Gross margin can change when the target must add monitoring, secure infrastructure, support, insurance or supplier redundancy. Recurring control cost belongs in the operating case. One-time remediation should be separately budgeted. Integration choices that create broader buyer capability should not be charged entirely to the seller condition without a defined allocation.

Valuation may also reflect option loss. A target that cannot meet regulated-customer requirements may have a smaller addressable market. A weak software supply chain may delay product release.

An inability to demonstrate security can impair financing or exit. These effects need scenario evidence rather than a generic discount.

The board should see base, remediation and severe-event cases. The severe case should test liquidity, covenant headroom, customer concentration, recovery capacity and financing. The purpose is to understand resilience of the investment thesis. Scenario weights are management assumptions and should be shown explicitly.

16. Select a proportionate transaction-protection ladder

Transaction protection should match the nature of the exposure. A correctable control gap may be addressed through a closing action or funded remediation. A known historical incident may require a specific indemnity, escrow and claims cooperation. An uncertain latent exposure may affect price, representations, insurance and confirmatory diligence. A thesis-breaking condition may require stopping the transaction.

The team should begin with the desired operating state. What evidence must exist before control transfers? Which condition can be completed after closing without exposing customers or violating obligations? Which risk can be quantified and accepted? Which loss should remain with the seller because it arose before closing? These questions guide the legal mechanism.

Generic cybersecurity representations can cover policies, incidents, compliance, data, controls and notices. Specific drafting may be needed for known facts, material systems, customer obligations, software provenance, access, backups or regulatory correspondence. Disclosure schedules should identify exceptions clearly. A broad data-room reference can leave the commercial issue unresolved.

Escrow and holdback design should reflect plausible loss, duration, evidence and claim mechanics. A large escrow with a short period can fail to protect a slowly developing exposure. A long claim period with no accessible funds can provide limited practical recovery. Qualified advisers should align survival, caps, baskets, exclusions, insurance and control of defence.

Protection should remain linked to ownership action. Legal recovery does not restore a critical service or retain customers. Each protected exposure should have a remediation owner, budget, timetable and verification standard. The deal team should monitor both legal rights and operating closure.

Figure 5. Cyber transaction-protection decision ladder

Qualified advisers should design the final transaction terms from the facts and governing law.

Table 5. Cyber finding to transaction response

finding type	economic treatment	protection route	closing or ownership action	verification
active or suspected compromise	severe downside and interruption liquidity	condition, specific protection and claims cooperation	independent containment and clean-environment decision	forensic evidence and monitored period
known historical incident	contingent claims and remediation	specific indemnity, escrow, notice and defence terms	complete notices, preserve evidence and close actions	regulator, customer, insurer and technical records
unsupported critical platform	recurring risk plus replacement capital	price adjustment, covenant or condition	containment, funded replacement and continuity plan	migration, recovery and service test
weak identity or privileged access	remediation cost and elevated incident scenario	covenant, retention and representation	rotate secrets, control privilege and stage connectivity	sampled access and logging evidence
missing supplier rights or notification	interruption and claims sensitivity	consent condition, warranty or specific covenant	amend contract, create alternative and test exit	executed agreement and continuity evidence
incomplete diligence evidence	conservative case or unpriced uncertainty	confirmatory work, escrow or enhanced representation	restrict Day One trust until evidence is complete	independent report and committee sign-off
bounded control gap	one-time budget with contingency	ordinary covenant or accepted risk	assigned remediation with due date	closure evidence and board reporting

The response should be tailored to the evidence, loss mechanism and legal advice.

17. Align representations, indemnities and transactional insurance

Representations should be built from the diligence perimeter. Relevant subjects can include material systems, security policies, compliance, incidents, notices, claims, personal data, customer commitments, business continuity, suppliers, software components, access and insurance. Definitions and materiality qualifiers determine coverage. Qualified counsel should connect drafting to the actual evidence and disclosure schedule.

Known issues generally require explicit treatment. A representation can establish a factual baseline while a specific indemnity may allocate a defined pre-close exposure. The agreement should address loss definition, third-party claims, mitigation, defence control, cooperation, insurance proceeds and interaction with caps or baskets. The transaction team should understand practical recovery, not only drafting breadth.

Warranty and indemnity insurance can affect negotiation and recovery, subject to underwriting, exclusions and the diligence record. A cyber issue excluded from the policy remains with the negotiated parties. An incomplete diligence process can narrow coverage. The deal team should coordinate the technical report, legal analysis, disclosure and underwriting answers so they describe the same facts.

Cyber insurance and transactional insurance serve different purposes. Cyber insurance can respond to incidents and operational losses under its terms. Transactional insurance can respond to breach of covered representations. Neither should be assumed to cover a known matter without specific confirmation. The model should show each recovery path and avoid duplicate proceeds.

The disclosure process is an operational test. The seller should identify incidents, exceptions, notices and claims in a form the buyer can evaluate. Late or inconsistent disclosure may require fresh diligence and revised terms. The buyer should preserve the evidence supporting the final allocation because later claims depend on what was known, represented and disclosed.

18. Control the period from signing to closing

Cyber exposure can change between signing and closing. Attackers do not wait for regulatory clearance, financing or completion. The agreement and operating plan should address ordinary-course security, material architecture changes, supplier changes, incident notification, access, remediation, insurance and cooperation. The seller should retain operational control until permitted transfer.

The parties need a transaction-specific incident protocol. It should define what event triggers notice, to whom, how quickly, what information is provided, how privilege and confidentiality are managed and who controls response. The protocol should respect law, customer contracts, insurance and securities duties. It should also address whether a material event changes closing conditions, valuation or termination rights.

Pre-close integration planning should avoid unauthorised control and unsafe connectivity. Teams can map dependencies, design Day One access, prepare monitoring, identify critical secrets and agree recovery priorities. Network connection, credential sharing or operational direction should wait until legally permitted and technically controlled.

Confirmatory diligence should refresh time-sensitive evidence. External exposure, critical vulnerabilities, incidents, insurance notices, privileged access, key suppliers and recovery status can change quickly. The committee should receive a dated update before close, with changes to the risk and protection map.

Day One should preserve service and evidence. Critical logs, forensic records, insurance documents, regulator correspondence, customer commitments and security architecture should be transferred to accountable owners. The buyer should avoid immediate changes that destroy evidence or weaken the target's existing controls.

19. Run a control-led first hundred days

The first hundred days should begin with authority, visibility and continuity. The buyer should confirm incident command, privileged access, monitoring, backup protection, critical suppliers, insurance contacts, notification routes and service owners. High-risk credentials and secrets should be rotated through a tested sequence. Connectivity should be staged according to evidence.

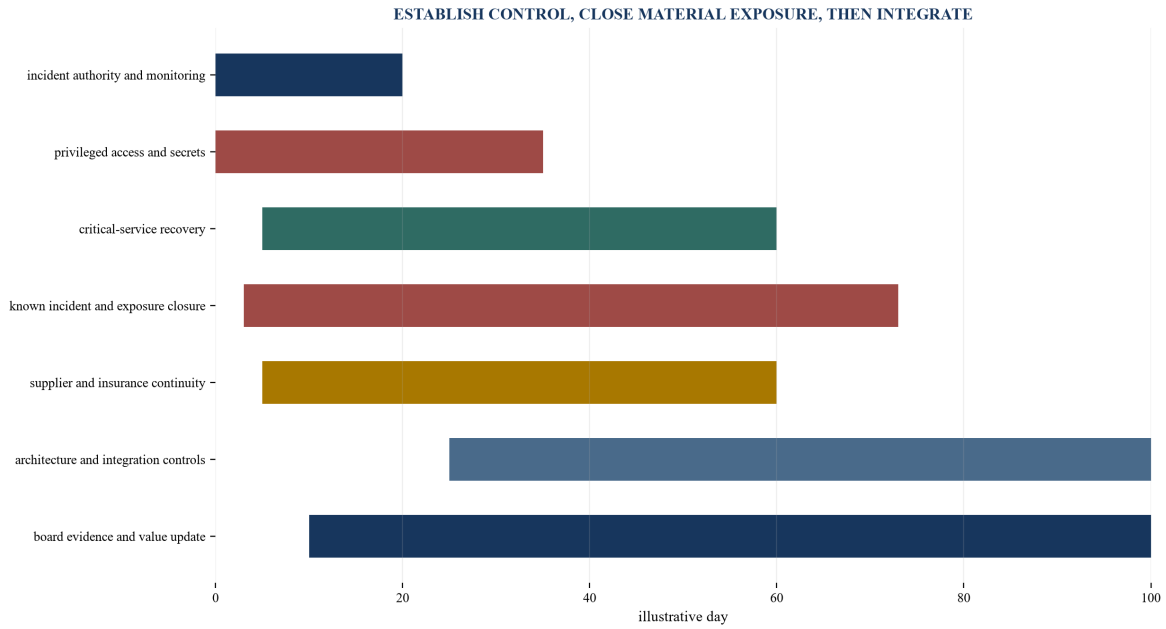
The next phase should close thesis-relevant gaps. Examples include removing exposed services, completing incident remediation, strengthening identity, expanding logs, isolating recovery, replacing unsupported platforms, improving supplier terms and testing critical-service restoration. Each action needs a service owner, technical owner, budget, due date, dependency and verification evidence.

Integration decisions should preserve resilience. Consolidating identity, cloud, networks or monitoring can create temporary concentration and migration risk. The team should compare current and target states, define rollback, test customer obligations and maintain detection during transition. Cost synergy should not depend on removing a control that supports the investment case.

Board reporting should focus on decisions and residual exposure. A dashboard can show critical services, material exceptions, incident readiness, recovery evidence, supplier concentration, insurance, regulatory actions and remediation. A completion percentage is insufficient when the remaining item is thesis-critical.

The hundred-day review should update valuation assumptions. Actual remediation cost, customer response, recovery tests and supplier negotiations provide evidence. Material deviations should enter the value-creation plan, covenant forecast and exit-readiness record. This closes the loop between diligence and ownership.

Figure 6. Illustrative 100-day cyber ownership programme



Timing is a hypothetical management assumption; actual sequencing depends on the target and transaction.

20. Apply the framework to a hypothetical acquisition

Consider a hypothetical acquisition of a business-to-business software company. Management reports USD 60 million of recurring revenue and states that no material cyber incident has affected customers. The company operates in several jurisdictions, uses two cloud providers and relies on a managed security provider. All figures and outcomes in this example are hypothetical management assumptions.

The service map identifies one identity platform and one deployment pipeline supporting every product. Evidence shows broad administrator access, incomplete service-account ownership and inconsistent log retention. An external review identifies an unsupported internet-facing component connected to a legacy customer portal. Management remediates the exposure during diligence and commissions targeted forensic work.

Incident reconstruction finds that a credential compromise eighteen months earlier was recorded as a minor service event. The target reset one account and found no evidence of customer-data access. Available logs cover only part of the relevant period, so complete scope cannot be established. Customer contracts include short notification periods for security events, while the contemporaneous legal assessment did not test every contract.

The recovery review demonstrates successful database restoration but no full-service recovery from clean infrastructure. Cloud backups use a separate account, while identity recovery depends on two individuals. The supplier review finds that the managed provider's contract lacks a rapid notification requirement and gives the target limited access to investigation evidence. Cyber insurance remains in force, subject to notice and change-of-control analysis.

The deal team builds three cases. The base case includes recurring identity, monitoring and supplier-assurance cost. The remediation case funds service-account ownership, log retention, clean recovery and portal replacement. The severe-event case models interruption, customer response, forensic cost and limited insurance recovery. It avoids using statutory maximum fines

as expected loss.

The transaction requires completion of targeted forensic work and insurance notice before closing. A specific escrow supports the historical incident and defined customer claims. Representations and disclosure identify the affected environment, incident and available evidence. Signing-to-closing covenants require rapid incident notice and preservation of security controls. Day One connectivity remains staged until privileged access and monitoring meet the agreed evidence gate.

The example demonstrates connected decision-making. The historical incident does not automatically determine the transaction outcome. Evidence limitations, customer duties, recovery and control concentration create specific cash-flow and execution consequences. The board can approve the transaction with an explicit value bridge, protection package and ownership plan.

21. Use a board gate that records value, protection and residual risk

The board paper should state the acquisition thesis, technology perimeter, critical services, material incidents, plausible attack paths, jurisdiction matrix, customer obligations, identity and vulnerability findings, supplier concentration, recovery evidence, insurance, cash-flow bridge, transaction terms and first-hundred-day plan. It should separate verified evidence, management assumptions and advice still required.

Every material finding should have one economic treatment and one accountable owner. If the same exposure reduces forecast revenue, creates a separate valuation deduction and is fully covered by escrow, the committee should understand whether the treatments overlap. If a finding receives legal protection without funded remediation, the service remains exposed after closing.

The board should challenge uncertainty. Which logs, systems, incidents or jurisdictions remain untested? What adverse condition is plausible? How does the proposed protection respond? What evidence will release escrow, permit network connection or close the remediation? A limitation should become a condition or accepted residual risk with clear reasoning.

Stop conditions should be approved before timetable pressure dominates. Examples include evidence of active compromise without credible containment, an essential service that cannot recover, unbounded customer or regulatory exposure, unavailable rights to operate the platform, insurance or seller protection that cannot be secured, or remediation cost that breaks the investment thesis.

The final decision should establish a continuous evidence system. Diligence records should transfer into risk, incident, supplier, insurance and board processes. Post-close reviews should compare assumptions with actual cost, recovery, customer response and control performance. This makes cyber diligence an ownership capability and improves the quality of future transactions.

Table 6. Board gate for cyber liability in a transaction

domain	minimum evidence	board challenge	pause or stop signal	post-close owner
perimeter and critical services	mapped entities, services, assets, suppliers and obligations	what must remain available and controlled at close?	essential operating asset or right is outside the perimeter	integration executive
incidents and exposure	reconciled history, current monitoring and targeted validation	can management define scope and validate eradication?	active compromise or irreducible evidence gap	incident executive and counsel
identity and technology	privileged-access map, vulnerability context and transition plan	which account or component can create enterprise control?	critical privilege cannot be transferred or constrained	chief information security officer
data and regulation	data map, jurisdictions, notices and customer duties	which clocks and claims can the transaction activate?	material unreported duty or missing lawful route	legal and privacy leads
recovery and suppliers	restoration evidence, shared responsibility and alternatives	can critical services recover within the approved tolerance?	no credible recovery or concentrated supplier exit	operations and technology leads
value and insurance	cash-flow pathways, remediation budget and policy analysis	is gross exposure separated from supportable recovery?	unbounded liquidity or financing requirement	chief financial officer
transaction protection	price, conditions, warranties, indemnities, escrow and covenants	does each term correspond to a defined exposure?	thesis-critical loss remains unallocated	transaction lead and counsel
ownership programme	Day One control, 100-day plan, budget and closure evidence	who will complete each action and how will closure be proved?	critical action lacks owner, funding or safe sequence	portfolio or integration committee

The board should approve explicit evidence requirements, conditions and residual-risk ownership.

References

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

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

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

[4] United States Securities and Exchange Commission, Small Entity Compliance Guide for Cybersecurity Disclosures https://www.sec.gov/resources-small-businesses/small-business-compliance-guides/cybersecurity-risk-management-strategy-governance-incident-disclosure

[5] United States Department of Justice, Evaluation of Corporate Compliance Programs https://www.justice.gov/criminal/criminal-fraud/page/file/937501

[6] United States Federal Trade Commission, Safeguards Rule Notification Requirement https://www.ftc.gov/business-guidance/blog/2024/05/safeguards-rule-notification-requirement-now-effect

[7] United States Federal Trade Commission, New and Improved Data Security Orders https://www.ftc.gov/business-guidance/blog/2020/01/new-improved-ftc-data-security-orders-better-guidance-companies-better-prote

ction-consumers

[8] UK Information Commissioner's Office, Due Diligence when Sharing Data Following Mergers and Acquisitions https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/due-diligence/

[9] UK Information Commissioner's Office, Marriott International Penalty Notice https://ico.org.uk/media2/migrated/2618524/marriott-international-inc-mpn-20201030.pdf

[10] UK National Cyber Security Centre, Cyber Insurance Guidance https://www.ncsc.gov.uk/guidance/cyber-insurance-guidance

[11] UK National Cyber Security Centre, Supplier Assurance Questions https://www.ncsc.gov.uk/guidance/supplier-assurance-questions

[12] UK National Cyber Security Centre, Cyber Assessment Framework Response and Recovery Planning https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-d/principle-d1-response-and-recovery-planning

[13] European Union, Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

[14] European Data Protection Board, Guidelines 9/2022 on Personal Data Breach Notification under GDPR https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en

[15] European Union, Implementing Regulation on NIS2 Cybersecurity Risk-Management Measures https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

[16] United Arab Emirates, Federal Decree by Law No. 45 of 2021 Concerning the Protection of Personal Data https://www.uaelegislation.gov.ae/en/legislations/1972/download

[17] Abu Dhabi Global Market, Data Protection Regulations 2021 https://assets.adgm.com/download/assets/Annex%2BA%2BData%2BProtection%2BRegulations%2B2020.pdf/42147be6799611efa8bd72a3b161ad77

[18] Abu Dhabi Global Market, Personal Data Breach Notifications https://www.adgm.com/operating-in-adgm/office-of-data-protection/data-breach-notifications

[19] Abu Dhabi Global Market Financial Services Regulatory Authority, IT Risk Management https://www.adgm.com/operating-in-adgm/it-risk-management

[20] Dubai Financial Services Authority, Cyber Risk Supervision Summary https://www.dfsa.ae/what-we-do/supervision/cyber-risk-supervision/summary

[21] Indian Computer Emergency Response Team, Directions under Section 70B of the Information Technology Act https://www.cert-in.org.in/Directions70B.jsp

[22] Indian Computer Emergency Response Team, Frequently Asked Questions on Cyber Security Directions https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

[23] Government of India, Digital Personal Data Protection Act 2023 https://www.meity.gov.in/static/uploads/2024/02/Digital-Personal-Data-Protection-Act-2023.pdf

[24] Government of India, Digital Personal Data Protection Rules 2025 https://www.meity.gov.in/documents/act-and-policies/digital-personal-dataprotection-rules-2025gDOxUjMtQWa?pageTitle=Digital-Personal-Data-ProtectionRules-2025

[25] Cyber Security Agency of Singapore, Cybersecurity Act https://www.csa.gov.sg/legislation/cybersecurity-act/

[26] Personal Data Protection Commission Singapore, Guide on Managing and Notifying Data Breaches under the PDPA https://www.pdpc.gov.sg/help-and-resources/2021/01/data-breach-management-guide

[27] Australian Prudential Regulation Authority, CPS 234 Information Security https://www.apra.gov.au/standards/cps-234

[28] Office of the Australian Information Commissioner, Notifiable Data Breaches Scheme https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme

[29] Australian Securities and Investments Commission, Key Questions for an Organisation's Board of Directors https://asic.gov.au/regulatory-resources/corporate-governance/cyber-resilience/key-questions-for-an-organisation-s-board-of-directors/

[30] Australian Signals Directorate, Guidelines for Procurement and Outsourcing https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-procurement-and-outsourcing

About the Author

Authored by Chennakeshav Adya, Independent Researcher

Chennakeshav Adya is an independent researcher and Managing Partner of Matchpoint Partners. His work focuses on corporate finance, capital strategy, transactions, operating transformation and the governance systems that convert strategic choices into measurable execution.