Claims-Ready from Signing: Preserving Evidence under a W&I Policy

A transaction operating system for notice, evidence, loss quantification and recovery after completion

Authored by Chennakeshav Adya
Independent Researcher
September 2026

Abstract

Warranty and indemnity insurance can protect a buyer against specified breaches of warranty, subject to the executed policy. Recovery still depends on operating discipline after signing. A potential breach may first appear in an integration report, customer dispute, tax assessment, cyber investigation, accounting reconciliation or regulatory enquiry. If ownership is unclear, notice is delayed, source records change or loss is modelled without an evidential bridge, the buyer can weaken a claim before the insurer evaluates coverage.

This paper develops a claims-readiness system that begins at signing. It assigns claim ownership, freezes the underwriting and transaction record, defines notification and escalation protocols, preserves digital and physical evidence, reconciles insurer and seller conduct rights, separates breach from causation and loss, and creates a controlled quantum model. The framework also connects the policy owner with integration, finance, tax, legal, cyber, operations and external advisers. It gives the acquisition committee decision gates for potential circumstances, formal notification, investigation spend, claim submission, settlement and recovery.

The worked case is wholly hypothetical. It concerns a cross-border acquisition of a business-services and software group with enterprise value of USD 465.0 million and equity purchase price of USD 350.0 million. The W&I policy limit is USD 45.0 million, retention is USD 3.5 million and assumed premium, insurance tax and underwriting cost is USD 1.1 million. A potential claim is discovered in month seven. An initial gross loss hypothesis of USD 21.0 million becomes USD 15.5 million after evidence reconciliation. Retention and uninsured items total USD 4.0 million, producing a hypothetical policy claim of USD 11.5 million. The model assumes 14 months from discovery to recovery. Every company, event, amount, duration and outcome is hypothetical. A live claim requires current policy-specific and jurisdiction-specific legal, insurance, tax, accounting, forensic, cyber and regulatory advice.

JEL Classification: G34, G22, G32, K12, K22

Keywords: warranty and indemnity insurance, representations and warranties insurance, claims readiness, evidence preservation, claim notification, loss quantification, M&A, transaction risk, chain of custody, insurance recovery

1. Define claim readiness before signing

The board decision is whether the buyer can sign with an operating system capable of preserving and presenting a claim after completion. The existence of a policy does not establish that the buyer can identify a covered breach, comply with notice, preserve evidence, prove causation, quantify loss or coordinate recovery. Those capabilities require owners, procedures, records and authority before the transaction team disperses.

Claim readiness should begin with the executed policy and acquisition agreement. The buyer should identify insured parties, warranties, exclusions, retention, limits, policy period, knowledge provisions, notification requirements, conduct obligations, subrogation, mitigation, other insurance and dispute procedures. Counsel and the broker should explain how the documents interact. The policy wording remains controlling.

The committee should approve a claim-readiness objective at signing. It should state who can classify a matter as a potential circumstance, who can notify, which records must be frozen, who can instruct advisers, how investigation spend is approved, who owns the loss model and which decisions return to the committee. It should also specify the escalation period for facts that could engage the policy.

The system should accommodate uncertainty. A team may discover a discrepancy before it knows whether a warranty was breached or whether loss exceeds retention. The protocol should preserve facts and rights without asserting conclusions that have not been established. Early classification, protected investigation and policy-specific advice allow the buyer to act while the evidence develops.

2. Read the executed policy as an operating document

The claims team should convert the executed policy into an operational matrix. The matrix should list every notice address, delivery method, time requirement, information obligation, consent right, cooperation duty, mitigation requirement, defence-cost provision and dispute route. It should identify differences between the policy and acquisition agreement.

Under the UK Insurance Act 2015, the duties and remedies applying to a business insurance contract depend on the statute, policy terms and facts. [1] The Enterprise Act 2016 inserted an implied term concerning payment of sums due within a reasonable time, subject to the statutory framework and contracting-out rules. [2] The buyer requires legal advice on application to the particular policy.

The FCA's ICOBS claims-handling rules state, within their scope, that an insurer must handle claims promptly and fairly, provide reasonable guidance, avoid unreasonable rejection and settle promptly once settlement terms are agreed. [3] These obligations do not replace the insured's need to comply with the policy and substantiate the claim.

The operating matrix should distinguish notification of a circumstance from submission of a quantified claim. It should also distinguish a policy condition from an information request. The team should never assume that informal discussion with a broker satisfies formal notice. Delivery, receipt and acknowledgement should be preserved.

3. Establish the claim governance model

One executive should own the consolidated claim process. Supporting owners should cover legal analysis, insurance, finance and quantum, tax, operations, cyber, records, communications and integration. The governance model should identify who speaks to the insurer and seller, who approves disclosures and who controls privileged work.

Table 1. Proposed claim ownership and responsibility matrix

Workstream	Accountable owner	Core responsibility	Decision evidence
Policy and notice	General counsel or transaction legal lead	Interpret notice requirements, preserve rights and coordinate formal communications	Executed policy, notice log and acknowledgement
Evidence	Records custodian with specialist leads	Freeze, collect, authenticate and control the claim record	Preservation notice, inventory, access log and chain of custody
Breach and causation	Counsel and subject-matter adviser	Test warranty language, facts, disclosure and causal pathway	Legal analysis linked to source records
Loss and recovery	Finance lead with forensic accountant	Build the loss bridge, track mitigation and prevent double recovery	Controlled model, ledger support and recovery schedule

Workstream	Accountable owner	Core responsibility	Decision evidence
Operations and remediation	Business owner	Limit continuing loss while protecting evidence and approvals	Action log, spend approval and outcome evidence
Committee reporting	Deal sponsor or claims executive	Present decisions, residual exposure, liquidity and settlement authority	Decision paper and approved minutes

Roles are illustrative and require transaction-specific adjustment.

Governance should address conflicts. The integration team wants rapid remediation. Counsel may need to preserve a system state. The insurer may require consent before costs are incurred. The seller may have conduct rights under a tax covenant or specific indemnity. The executive owner should have a route to resolve these tensions within the relevant deadline.

The buyer should maintain a claim decision register. Each entry should record the fact, source, policy provision, required action, deadline, owner, approval and evidence of completion. The register should separate verified fact, adviser conclusion, management assumption and open question.

4. Freeze the underwriting and transaction record

The claim file begins with the record on which the transaction and policy were underwritten. It should include the final acquisition agreement, disclosure letter, policy, underwriting submission, diligence reports, management Q&A, data-room index, material source documents, broker communications, insurer questions and responses, signing and completion deliverables, and bring-down materials.

The archive should preserve version and provenance. A later reviewer should be able to identify the exact document available at the relevant time, the person who supplied it and the diligence treatment. The buyer should prevent routine retention policies from deleting material required for a potential claim, subject to applicable law and proportionality.

Digital evidence requires additional care. NIST SP 800-61 Revision 3 recommends preserving the integrity and provenance of incident records and collected data in accordance with evidence-preservation procedures and retention policies. [9] The principle is useful beyond cyber claims: collection should be documented, access controlled and transformations recorded.

The archive should remain usable. Encryption keys, proprietary formats, cloud accounts and specialist applications can become unavailable after integration. The custodian should test access and maintain authorised tools needed to read the evidence. Privacy, confidentiality, privilege, competition and cross-border restrictions should be addressed with counsel.

5. Design the notice protocol

Notice should be treated as a controlled transaction event. The protocol should identify the trigger for escalation, the people authorised to assess it, every contractual recipient, the permitted delivery method and the evidence required to prove delivery. It should cover the W&I policy, acquisition agreement, specific indemnities, escrow arrangements, other insurance and material third-party contracts.

The protocol should distinguish awareness from legal knowledge. An operating employee may discover a fact before the policyholder's designated knowledge group evaluates it. The policy wording and applicable law determine the significance. The buyer should establish a rapid route from operational discovery to policy-specific advice without asking employees to make coverage conclusions.

A notice should be accurate, timely and proportionate to the information available. It should identify the policy, insured, relevant facts, possible warranty or provision, known loss and continuing investigation. It should avoid unsupported certainty. Counsel should determine the content, privilege position and whether separate notices are required.

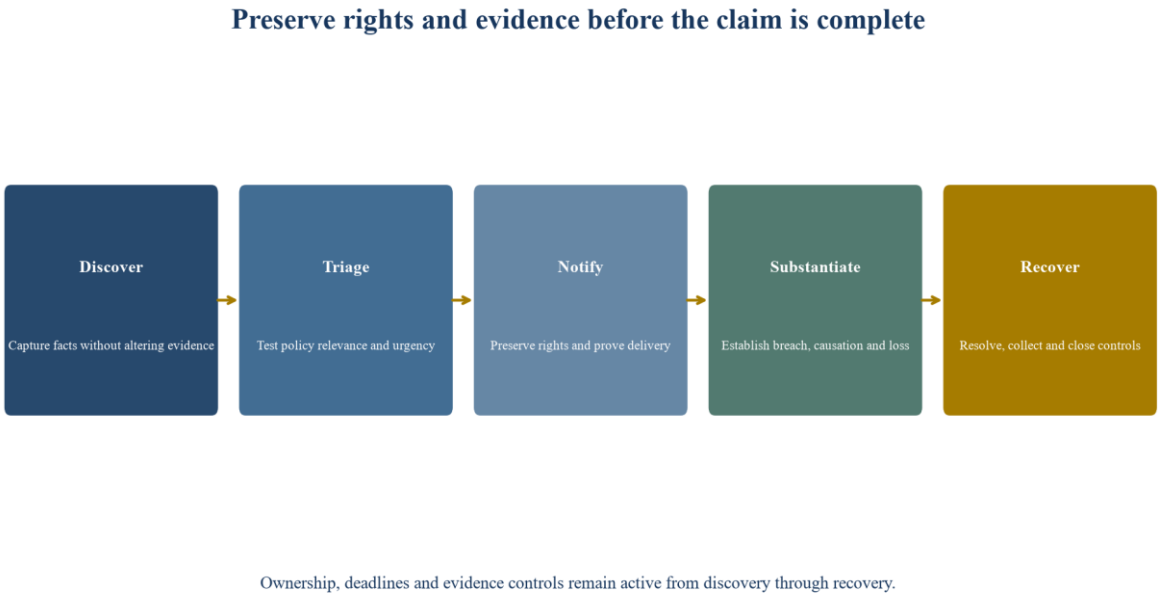
Delivery evidence should include the final notice, attachments, sender, recipient, channel, timestamp and acknowledgement. If a broker receives notice, the team should confirm whether the broker is authorised to receive it for the insurer. FCA guidance within ICOBS notes that an intermediary without claims-handling authority should promptly forward a notification or tell the policyholder that it cannot deal with it. [3]

6. Separate suspicion, circumstance and quantified claim

A claim can develop through several states. A suspicion is an observation requiring triage. A potential circumstance is a fact pattern capable of engaging the policy. A notified matter is one communicated under the relevant provision. A quantified claim includes an asserted breach, causation and loss supported by evidence. These states should have separate criteria and owners.

The buyer should avoid waiting for complete quantum before preserving rights. It should also avoid flooding the insurer with unanalysed operating noise. The triage matrix should consider materiality, warranty relevance, evidence reliability, possible loss, limitation periods and continuing harm. Legal advice is required on the notice threshold.

Figure 1. Proposed claim-readiness architecture



Original framework. Each stage requires policy-specific legal and insurance review.

The register should show movement between states and the decision supporting each move. A matter can be closed if evidence demonstrates that it is unrelated to an insured warranty. The closure should be recorded so that the same issue is not repeatedly reopened without new facts.

7. Preserve digital and physical evidence

The preservation plan should identify systems, custodians, locations, devices, documents and physical assets capable of proving the fact pattern. It should suspend ordinary destruction where required, secure access and record collection. The scope should be proportionate and advised by counsel.

Digital evidence can include email, messaging, transaction systems, logs, backups, source code, cloud records, mobile devices, identity data and audit trails. Physical evidence can include signed originals, product samples, site records, equipment, correspondence and notebooks. The plan should account for third-party platforms and former employees.

NIST SP 800-61 Revision 3 recommends recording investigation actions and preserving the integrity and provenance of incident records and collected data. [9] The United States Department of Justice has also emphasised policies governing business communications, personal devices and ephemeral messaging, including preservation settings and document-retention guidance. [11][12] These sources address different regulatory contexts, yet both demonstrate why evidence systems need ownership and traceability.

The custodian should record the source, collector, date, method, hash where appropriate, storage location, access and transfer. Collection should avoid changing metadata or system state unnecessarily. Specialists should determine the forensic method. The buyer should preserve the original and use controlled working copies.

8. Protect privilege and manage investigation scope

The buyer should involve counsel when a matter may engage legal advice, litigation, regulatory exposure or policy notification. Privilege depends on jurisdiction, purpose and process. Labelling a document privileged does not establish privilege. Counsel should define the investigation mandate, reporting lines, interview process and sharing protocol.

The insurer may require information to evaluate cover and quantum. The seller may have contractual rights. Regulators, auditors and lenders may also require disclosure. The claims team should map these demands before circulating investigation material. It should distinguish underlying facts from legal advice and work product.

The investigation plan should state the questions, source population, custodians, time period, reviewers, quality controls and escalation criteria. It should avoid collecting irrelevant personal data. The ICO advises organisations involved in mergers and acquisitions to establish purpose, lawful basis, security and documented governance for data sharing. [13]

The team should keep one controlled chronology of verified events. Adviser hypotheses should be recorded separately. Interview notes should identify the interviewer, participant, date and status. Conclusions should link to source evidence and disclose material limitations.

9. Reconcile insurer, seller and third-party conduct rights

The policy and acquisition agreement can allocate control differently. The insurer may require consent before settlement or material costs. A tax covenant may give the seller conduct rights. A third-party contract may restrict disclosure. Regulators may control timing. The buyer should create one conduct matrix before an event occurs.

The matrix should cover notification, investigation, appointment of advisers, admission, defence, settlement, remediation, communications, access to records and cost approval. It should identify whose consent is required, the response period and the fallback if consent is withheld or delayed. Counsel should resolve inconsistent obligations.

Business continuity remains a decision factor. A theoretically strong claim should not prevent urgent action needed to contain cyber compromise, protect safety, comply with law or preserve customers. The policy owner should know how to seek emergency consent and document the necessity and proportionality of action.

The buyer should also control external communications. Statements to customers, regulators, employees or markets can affect the evidence and coverage analysis. Communications should be accurate, approved and consistent with legal obligations. The team should preserve final versions and the facts supporting them.

10. Build the loss bridge

Loss quantification should begin with the warranty and causal pathway. The model should show the represented state, actual state, breach, consequence, mitigation, third-party recovery, tax effect and policy

treatment. It should separate cash cost, lost profit, diminution in value, remediation, defence cost and other categories.

The bridge should reconcile to accounting records while preserving differences between accounting recognition and policy loss. Each input needs a source, owner, date and status. Management estimates should be identified and supported by methodology. The model should retain versions and change explanations.

Double recovery must be controlled. The buyer may have seller recourse, escrow, specific insurance, tax relief, customer payment, litigation recovery or operational benefit. The claim model should show gross loss, mitigation and each recovery route. Applicable wording and law determine treatment.

The model should include timing. Investigation and remediation can create cash demands before insurance recovery. The board should see peak liquidity, debt headroom and covenant effects. A nominally covered amount can still create material financing pressure if collection is delayed.

11. Establish the hypothetical case

The hypothetical buyer acquires a business-services and software group for enterprise value of USD 465.0 million and equity purchase price of USD 350.0 million. The W&I policy limit is USD 45.0 million. Retention is USD 3.5 million. Assumed premium, insurance tax and underwriting cost is USD 1.1 million. These amounts are scenario assumptions and do not represent market pricing.

In month seven, integration identifies inconsistencies between represented customer economics and underlying contract and billing records. The initial gross loss hypothesis is USD 21.0 million. The matter is preserved and notified while financial, contractual and operational evidence is reconciled.

The reconciliation removes USD 2.5 million of unsupported forecast loss and USD 3.0 million of effects attributable to post-completion decisions, leaving supported loss of USD 15.5 million. Retention and uninsured items total USD 4.0 million. The hypothetical claim submitted under the policy is USD 11.5 million. The model assumes 14 months from discovery to recovery.

The scenario does not predict coverage or recovery. The executed policy, acquisition agreement, evidence, legal analysis and loss method would determine a live outcome. The case demonstrates the governance and liquidity questions created by delay and evidential challenge.

Table 2. Hypothetical loss bridge

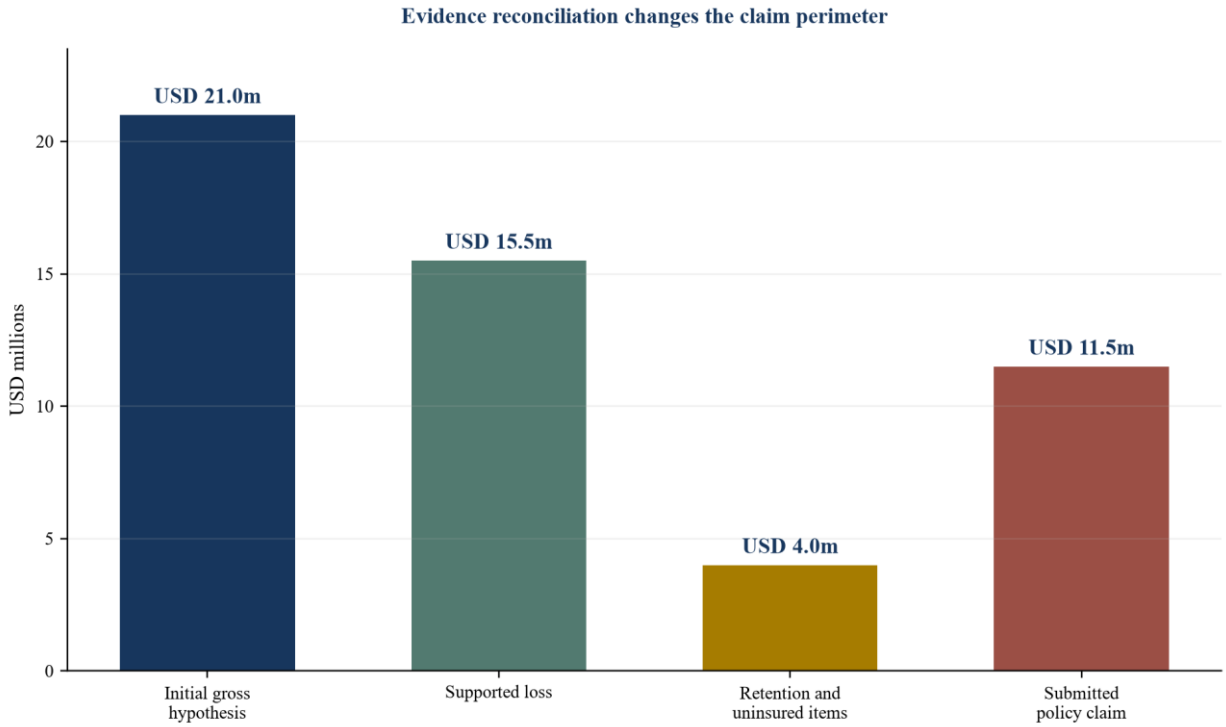
Component	Amount	Evidential treatment	Claim-model treatment
Initial gross loss hypothesis	21.0	Preliminary management and adviser model	Starting perimeter only
Unsupported forecast element	(2.5)	Insufficient causal and source support	Removed from supported loss
Post-completion decision effects	(3.0)	Attributed to buyer-controlled actions	Removed from supported loss
Supported loss	15.5	Reconciled to contracts, records and causation analysis	Subject to policy analysis
Retention and uninsured items	(4.0)	Policy and claim-specific treatment	Buyer-funded in the scenario
Hypothetical submitted claim	11.5	Controlled claim file and quantum model	Recovery remains unverified

All values are scenario assumptions in USD millions and do not represent expected recovery or market experience.

12. Model the claim and liquidity waterfall

The waterfall should distinguish economic loss from cash recovery. The buyer may fund investigation, remediation and operating continuity before claim resolution. It should model the month of each cash flow and test delay.

Figure 2. Hypothetical loss reconciliation and claim waterfall



Values are scenario assumptions and do not represent market claims outcomes.

The model should show investigation cost, legal cost, forensic cost, remediation and any continuing operating loss separately. Coverage of these amounts depends on wording. The buyer should obtain consent where required and preserve invoices, engagement terms, time records and work products.

The 14-month delay in the scenario requires a liquidity reserve. The board should test shorter and longer periods. The Enterprise Act framework concerning payment within a reasonable time does not create a fixed timetable for the hypothetical claim. [2] The facts, complexity and insurer's grounds for investigation matter.

13. Separate breach, causation and loss

A warranty can be inaccurate without causing the full loss asserted. The claim file should prove the warranty, represented fact, actual fact, timing, reliance where relevant, causal pathway and recoverable measure. Each element should link to evidence.

The team should test alternative causes. Market deterioration, buyer decisions, integration failure, customer behaviour and unrelated operational events can affect the same outcome. The model should quantify material alternatives rather than hide them. Counsel and experts should determine the applicable legal test.

The disclosure record is central. The buyer should identify whether the relevant fact was disclosed, diligenced, known or excluded and how the policy treats those matters. The underwriting record should show what was presented to the insurer.

The causation analysis should be updated as evidence develops. Changes should be logged with rationale and approval. A reduced claim can reflect stronger evidence and improve credibility. An increased claim requires the same controlled support.

14. Track mitigation and recoveries

The buyer should take reasonable and lawful steps to limit continuing loss while respecting policy conditions and conduct rights. The action log should record the problem, decision, consent, cost, owner, timing and effect. It should connect each action to the claim model.

Mitigation can include system containment, customer engagement, contract enforcement, tax appeal, remediation, replacement sourcing or operational control. The team should distinguish loss avoided from cash recovered. It should avoid claiming both the original loss and the benefit created by mitigation where that would duplicate recovery.

Third-party and seller recoveries should enter one schedule. The schedule should show notices, claims, security, collection probability, timing, costs and interaction with subrogation. The insurer may have rights after payment. Counsel should advise on preserving those rights.

The buyer should report net exposure and peak cash separately. A recovery expected in year two does not fund a payment due in month one. The finance team should integrate the claim model with liquidity forecasting and acquisition financing.

15. Control experts, advisers and costs

Claims can require counsel, forensic accountants, tax advisers, cyber specialists, engineers, valuers and industry experts. The claims executive should establish scope, authority, reporting line, confidentiality, budget and deliverables before work begins, subject to urgent action.

The engagement should identify whether insurer consent is required and whether cost is potentially recoverable. Invoices should separate workstreams and time. The team should prevent overlapping mandates and unsupported expert assumptions.

Expert independence and methodology matter. A loss model should state source data, counterfactual, period, discounting, tax and sensitivity. A technical report should preserve observations and limitations. A legal opinion should remain within its jurisdiction and instructions.

The buyer should maintain an adviser-decision log. It should record recommendations, management decisions and departures. This protects governance while preserving management responsibility for commercial choices.

16. Govern cyber and ephemeral-message evidence

Cyber events can change evidence quickly. Logs rotate, cloud instances are rebuilt and compromised systems are remediated. The incident-response and claim teams should coordinate collection before altering material evidence, subject to the overriding need to contain harm.

NIST recommends preserving incident-record integrity and provenance and collecting evidence under established procedures. [9] The DOJ's compliance guidance asks how organisations preserve information across electronic channels and manage ephemeral messages and personal devices. [11][12] The buyer should map these channels during integration.

The protocol should cover legal hold, backup preservation, identity logs, endpoint data, security alerts, ticketing, messaging, mobile devices and third-party platforms. It should document unavailable data and the reason. Specialists should validate forensic images and chain of custody where required.

Privacy and security remain important. Claim evidence can contain credentials, vulnerabilities and personal data. Access should be restricted and monitored. Transfer to advisers or insurers should use authorised channels and documented purpose.

17. Prepare for insurer information requests

The buyer should expect iterative questions. A controlled request register should record the request, date, owner, source, review, response, privilege treatment and delivery evidence. It should identify any limitation or unresolved inconsistency.

Responses should reconcile with prior underwriting submissions, management Q&A, disclosure and other claim materials. A changed explanation should state why. The team should avoid sending multiple uncontrolled versions.

Table 3. Proposed evidence and notice control register

Control	Required record	Owner	Escalation trigger
Potential circumstance	Fact summary, source, time discovered and possible policy relevance	Legal and policy owner	Material fact or deadline uncertainty
Preservation	Custodians, systems, hold, collection method and access	Records custodian	Missing, altered or expiring evidence
Notice	Final notice, attachments, delivery and acknowledgement	Counsel or authorised policyholder	No acknowledgement or disputed receipt
Information request	Request, response, supporting sources and limitations	Request coordinator	Conflict, privilege or unavailable source
Quantum	Versioned model, ledger support, assumptions and approvals	Finance and forensic lead	Material change or unsupported input
Conduct and settlement	Consents, authority, offers, decisions and releases	Claims executive and counsel	Consent delay or authority threshold

Controls require adaptation to the executed policy and applicable law.

The response process should be prompt and accurate. FCA ICOBS requires prompt and fair claims handling within its scope and appropriate information on progress. [3] The buyer should also maintain its own timetable, overdue list and escalation route.

18. Use technology with accountable review

Technology can index records, detect duplicates, preserve hashes, compare policy versions, search communications, reconcile ledgers and maintain the claim chronology. It can also omit sources or generate unsupported conclusions. Material outputs require human review.

The system should preserve the source population, query or configuration, tool version, reviewer, validation sample, exceptions and final approval. It should separate machine-generated suggestions from verified findings. Confidential transaction data should remain in authorised environments.

Automated clause comparison can identify wording differences. Counsel should interpret them. Data analysis can identify revenue changes. Finance and forensic advisers should validate causation and quantum. Language models can assist retrieval and organisation, while users remain responsible for accuracy and disclosure.

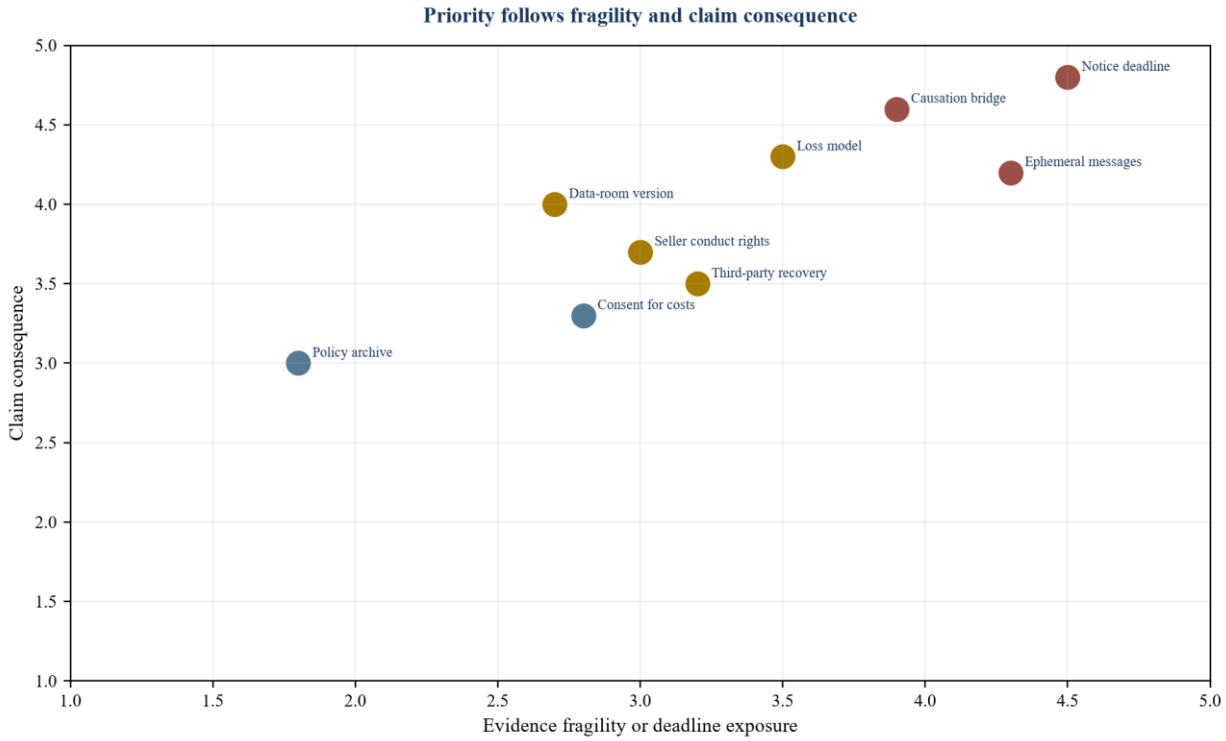
The best use of technology is traceability. A reviewer should be able to move from each claim assertion to the policy, warranty, evidence, chronology, causal analysis, loss model and approval. Access and change logs should show who altered the record.

19. Operate decision gates and escalation

The system should have at least five gates: discovery triage, preservation, notice, quantified submission and settlement. Each gate should have required evidence and authority. Urgent preservation can occur before full analysis.

At triage, the team decides whether facts require protected investigation. At preservation, it confirms custodians and systems. At notice, it tests timing, content and recipients. At submission, it verifies breach, causation, quantum and recoveries. At settlement, it compares cash, timing, costs, precedent and residual rights.

Figure 3. Hypothetical claim-readiness risk heat map



Positions are scenario judgements and do not represent observed claims data.

The committee pack should show deadlines, claim amount, evidence gaps, adviser spend, mitigation, liquidity, policy and seller responses, and decisions required. Dissent should be recorded. A change above delegated authority should return to the committee.

20. Implement the system in five phases

Table 4. Proposed claims-readiness implementation roadmap

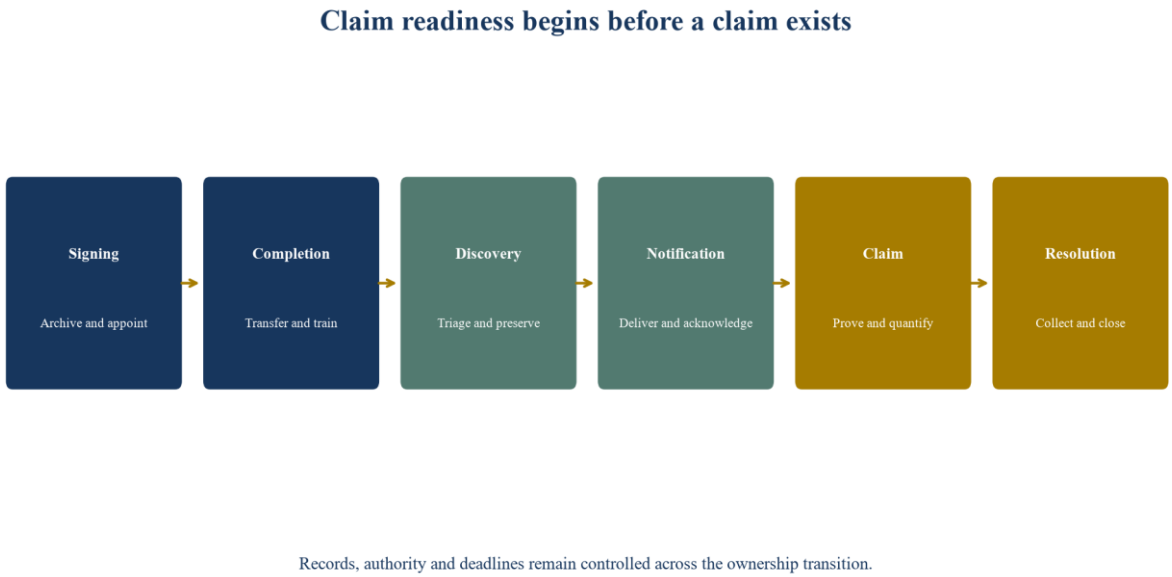
Phase	Core outputs	Decision test	Escalation if incomplete
Signing design	Policy matrix, owners, notice routes, archive and authority	Can the buyer preserve rights immediately after signing?	Preserve seller recourse and complete the operating design
Completion handover	Final archive, custodians, access, calendar and training	Has ownership moved from the deal team to operating leaders?	Retain deal-team oversight until transfer is evidenced
Discovery and notice	Triage, legal hold, evidence inventory, notice and acknowledgement	Are facts preserved and deadlines met?	Activate executive and counsel escalation

Phase	Core outputs	Decision test	Escalation if incomplete
Substantiation	Breach, causation, quantum, mitigation and recovery schedules	Is the claim supported and internally reconciled?	Expand work, correct the model or narrow the claim
Resolution and close	Settlement authority, collection, subrogation, release and lessons	Are cash, rights and residual actions controlled?	Maintain the claim office and reserve

Timing is indicative and should follow the transaction and executed policy.

The operating rhythm should include quarterly readiness checks before any claim and a daily or weekly cadence after discovery, depending on urgency. The readiness check should test contacts, archive access, notice routes, retention controls and decision authority.

Figure 4. Proposed signing-to-recovery operating timeline



Original framework. Timing and actions depend on the executed policy, facts and applicable law.

Measures should include potential matters without owners, preservation actions overdue, notices without acknowledgement, unresolved evidence gaps, quantum inputs without sources, adviser costs without consent, recoveries not reflected in the model and decisions approaching authority limits.

The signing design should include a policy abstract written for operators. It should identify the covered transaction, insured entities, principal exclusions, retention, limit, policy period, key definitions, notice details and consent provisions. The abstract should link to the executed policy and state that it does not replace the wording. Integration leaders should receive role-specific instructions rather than a generic copy of the policy. Finance needs the loss and cost protocol. Technology needs the cyber-evidence protocol. Tax needs conduct and correspondence rules. Human resources needs escalation triggers for employment matters.

The completion handover should be evidenced through acceptance. The deal team should demonstrate archive access, test notice contacts, confirm the records custodian, transfer open diligence findings and identify known matters outside cover. The receiving owners should sign or otherwise record acceptance. Open actions should retain deal-team sponsorship until they are complete. A calendar should include limitation periods, escrow releases, policy notifications, tax-covenant dates, retention changes and any completion accounts or earn-out events that could interact with loss.

Training should use short scenarios. An operating manager should know what to do after receiving a customer allegation. A finance controller should know how to preserve the original ledger and model version. A cyber lead should know how to contain an incident while maintaining evidence. A legal manager should know the formal notice route. Exercises should identify uncertain ownership and inaccessible records. Results should enter the action register with deadlines and accountable owners.

The discovery process should protect the first account of events. The person reporting the matter should identify what was observed, when, where and through which source. The intake record should preserve the original language and attachments. Follow-up analysis should be separated from the initial report. This reduces the risk that later interpretation replaces the underlying observation. The triage team should also identify evidence that may disappear through system rotation, employee departure, physical change or routine deletion.

The preservation notice should be understandable to recipients. It should identify the subject, relevant period, record categories, systems, devices and suspension of deletion, subject to counsel's advice. Recipients should acknowledge it. The custodian should monitor compliance, new custodians and system migrations. Collection should be refreshed when the scope changes. Release from preservation should be authorised and documented after the matter and related obligations have concluded.

The claims file should include a master chronology. Each event should state date, time zone, source, actor, significance and evidential status. Corrections should remain visible. The chronology should link to documents rather than reproduce unsupported summaries. It should distinguish transaction events, discovery, mitigation, insurer communications, seller communications, adviser work, cost and approvals. A well-controlled chronology helps reconcile accounts from different workstreams and exposes periods where evidence is missing.

The finance workstream should maintain a source-data dictionary. It should define each metric, system, extraction date, currency, accounting treatment and transformation. Reconciliations should connect the claim model to ledgers, contracts, invoices and operating reports. Adjustments should have an owner and approval. Foreign-currency treatment, discounting, tax, inflation and allocation among entities should be explicit. Sensitivities should change one material assumption at a time and show the resulting claim and liquidity effects.

The loss bridge should also distinguish historical fact from counterfactual modelling. Historical fact includes actual invoices, payments, customer actions and remediation spend. Counterfactual modelling estimates what would have occurred absent the breach. The counterfactual should be commercially and legally supportable, consistent with information available at the relevant date and tested against alternative explanations. Advisers should disclose limitations, dependencies and data gaps. The committee should see the range rather than a single precise number when uncertainty remains material.

Claim correspondence should use one controlled channel and naming convention. The team should identify the authoritative version of each submission and retain delivery evidence. Internal drafts, comments and privileged advice should remain segregated. The request register should prevent conflicting responses from different advisers. A response should identify whether it is complete, partial or subject to further work. Material errors should be corrected promptly through an approved communication that explains the change.

Settlement evaluation should compare more than headline cash. The committee should consider timing, adviser cost, management time, uncertainty, confidentiality, tax, accounting, subrogation, seller rights, continuing remediation and precedent. The decision paper should show the modelled recovery under continued pursuit and the proposed settlement on consistent assumptions. Authority should be confirmed before any binding offer or acceptance. Executed settlement documents, receipts and releases should enter the final archive.

Reserving and reporting should follow applicable accounting and governance requirements. The claims model can inform management without determining the financial-statement result. Finance and auditors should assess recognition, measurement and disclosure. The board should see management's claim estimate, accounting treatment, liquidity forecast and insurer reserve communication as separate items. Differences should be explained and updated as evidence develops.

The programme should include independent quality review before a quantified submission. A reviewer who did not build the principal claim should sample the warranty analysis, notice evidence, chronology, source population, calculations, recoveries and policy reconciliation. The review should identify unsupported assertions, formula errors, double counting and missing approvals. Exceptions should be corrected or disclosed in the claim file. The independent check should remain proportionate to the amount and complexity.

Closure should include a control review. The buyer should determine which diligence, disclosure, integration or records weakness allowed the matter to develop or remain undetected. Actions should have owners and completion evidence. The review should avoid rewriting the historical claim record. It should create a separate lessons register linked to future transaction templates, adviser scopes, data-room standards and integration plans.

After resolution, the buyer should close the record deliberately. It should collect settlement amounts, comply with release and subrogation obligations, complete remediation, preserve the final archive and update acquisition controls. Lessons should improve future diligence, warranties, disclosure and integration.

The readiness protocol should also survive changes in personnel and advisers. Named individuals may leave the buyer, the target, the broker, the insurer or the external advisory team during a multi-year policy period. Each critical role should therefore have a designated deputy, a role-based mailbox where appropriate and a documented transfer process. Access rights should be reviewed after completion and after every material personnel change. A quarterly confirmation can test whether the buyer can still retrieve the executed policy, locate the underwriting archive, contact the correct notice recipient and identify the current internal decision-maker. These checks create evidence that the control remained active between signing and discovery.

Management information should focus on decisions and exceptions. A concise claims-readiness dashboard can show potential circumstances, notice status, preservation status, consent requests, evidence gaps, quantified ranges, adviser spend, key dates and unresolved governance decisions. It should avoid presenting preliminary estimates as settled outcomes. Each figure should carry an as-of date, source and accountable owner. Where a range changes, the dashboard should explain whether the movement arose from new evidence, a revised legal assessment, mitigation, another recovery source or a modelling correction. This discipline makes changes intelligible to the investment committee, board, finance function and auditors.

The buyer should test the protocol through a tabletop exercise within the first post-completion quarter. A realistic scenario can begin with a customer complaint, regulatory inquiry, tax assessment or cyber incident that may engage a warranty. Participants should locate the relevant wording, identify the notice route, preserve the first evidence, decide whether urgent mitigation requires consent and prepare a preliminary loss bridge. The exercise should record elapsed time, unavailable records, unclear authority and conflicting instructions. Remediation actions should enter the integration plan and remain open until tested. Repeating the exercise after a major system migration or management change helps confirm that the control still works in the operating environment.

Finally, claim readiness should be included in transaction retrospectives even when no claim arises. The buyer can assess whether disclosure was usable, diligence records were complete, the underwriting submission was reproducible, policy terms were translated into operating controls and integration teams understood escalation duties. This review produces practical improvements for the next acquisition. It also reinforces that a W&I policy is one component of transaction risk allocation. Contractual rights, diligence quality, disclosure, integration controls, seller recourse, insurance and operational resilience must operate as a connected system.

21. Conclusion

W&I claim recovery begins with transaction design. A buyer needs the executed policy, evidence archive, notice protocol, claims authority and loss methodology to remain operational after the deal team leaves.

The hypothetical case begins with a USD 21.0 million gross loss hypothesis. Evidence reconciliation produces USD 15.5 million of supported loss. Retention and uninsured items reduce the hypothetical submitted claim to

USD 11.5 million. The assumed 14-month recovery period creates a separate liquidity requirement. Every amount and outcome is hypothetical.

The reusable method is direct. Appoint owners. Read the policy as an operating document. Freeze the underwriting record. Preserve evidence and privilege. Notify through controlled channels. Reconcile conduct rights. Prove breach, causation and loss. Track mitigation and other recovery. Govern advisers and technology. Escalate decisions through defined gates.

Claim readiness protects optionality. It allows the buyer to investigate uncertain facts, preserve rights and present a coherent claim while continuing to operate the acquired business.

Frequently asked questions

When should W&I claim readiness begin?

It should begin before signing, when the buyer can still define owners, archive the underwriting record, map notice requirements and align the policy with transaction and integration governance.

Does a potential circumstance require a fully quantified loss?

The applicable threshold depends on the executed policy and law. A protocol should permit timely legal assessment and rights preservation while the evidence and quantum develop.

What records should be preserved?

The buyer should preserve the final policy, acquisition agreement, disclosure, underwriting submission, diligence, management answers, data-room index, source records, signing and completion materials, and post-completion evidence relevant to the matter.

Who should own a W&I claim?

One executive should own the consolidated process, supported by legal, insurance, finance, tax, cyber, operations, records and integration owners with documented authority.

How should loss be quantified?

The model should connect the warranty and actual facts to breach, causation, loss, mitigation and recoveries. Inputs should be sourced, versioned, reviewed and reconciled to records.

Can urgent remediation proceed before insurer consent?

The response depends on legal duties, operational urgency and policy wording. The buyer should use the emergency escalation and consent process defined for the transaction and document its decisions.

How should digital evidence be controlled?

Collection should preserve integrity and provenance, document source and custody, restrict access, retain authorised tools and comply with privacy, privilege and security requirements.

What happens after a claim is resolved?

The buyer should collect payment, comply with release and subrogation terms, close remediation, preserve the final archive and feed lessons into future diligence and transaction controls.

References

[1] United Kingdom, Insurance Act 2015, https://www.legislation.gov.uk/ukpga/2015/4/contents

[2] United Kingdom, Enterprise Act 2016 explanatory notes, Part 5 Late Payment of Insurance Claims, https://www.legislation.gov.uk/ukpga/2016/12/notes/division/6/index.htm

[3] Financial Conduct Authority, ICOBS 8 Claims handling, https://handbook.fca.org.uk/handbook/icobs8

[4] Financial Conduct Authority, Insurance Conduct of Business Sourcebook overview, https://www.fca.org.uk/firms/insurance-conduct-business-sourcebook-icobs

[5] Lloyd's, Principle 4 Claims Management, https://www.lloyds.com/market-resources/market-oversight/principles-for-doing-business-at-lloyds/claims-management

[6] Lloyd's, Transactional liability W&I, tax and contingent-risk codes, Market Bulletin dated 16 June 2025, https://assets.lloyds.com/media/7e1ff6f4-639b-4d05-9fde-81bd5de85fef/Market_bulletin_16.06.2025%20-%20FINAL.pdf

[7] AIG, M&A Claims Reports, https://www.aig.com/home/risk-solutions/business/management-and-professional-liability/mergers-and-acquisitions/mergers-and-acquisitions-claims-reports

[8] AIG, Representations and Warranties Insurance, https://www.aig.com/home/risk-solutions/business/management-and-professional-liability/mergers-and-acquisitions/representations-and-warranties

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

[10] United States Department of Justice, Evaluation of Corporate Compliance Programs, September 2024, https://www.justice.gov/criminal/criminal-fraud/page/file/937501

[11] United States Department of Justice Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, November 2024, https://www.justice.gov/d9/2024-11/DOJ%20Antitrust%20Division%20ECCP%20-%20November%202024%20Updates%20-%20FINAL.pdf

[12] United States Department of Justice, Justice Manual 9-28.000 Principles of Federal Prosecution of Business Organizations, https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations

[13] Information Commissioner's Office, Data sharing due diligence in mergers and acquisitions, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/due-diligence/

[14] United States Courts, Federal Rules of Civil Procedure, https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-civil-procedure

[15] European Union, Directive (EU) 2016/97 on insurance distribution, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016L0097

About the Author

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

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

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

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

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

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

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