Who Signs the Audit? Professional Liability in AI-Audit Firms

A diligence, valuation and integration framework for separating software leverage from accountable assurance

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

AI-audit and assurance firms combine software, technical testing and professional judgement. Their acquisition appeal is clear. Automated evidence collection, repeatable test libraries and continuous monitoring can increase capacity and recurring revenue. The difficult question is who accepts responsibility for the conclusion when a client, regulator or affected party relies on the work.

This paper develops the Accountable Assurance Valuation Framework for acquirers of AI-audit, certification, conformity-assessment and testing businesses. It separates five activities: software tooling; test execution; evidence evaluation; assurance conclusion; and certification or regulatory sign-off. Each activity has a different competence requirement, margin profile and liability exposure. The framework applies ISO/IEC 42006:2025, ISO/IEC 42001, ISO/IEC 17021-1, the European Union AI Act, the NIST AI Risk Management Framework, current NIST work on test, evaluation, verification and validation, and the United Kingdom's third-party AI assurance roadmap.

The central conclusion is that software leverage creates value only when the firm preserves a defensible boundary around human judgement, independence, competence, evidence and sign-off. Automated testing can expand coverage and consistency. It cannot establish that an assurance conclusion is appropriate without a defined engagement scope, acceptance criteria, review and accountable approval. The buyer should therefore value collected recurring revenue, reusable technical assets and demonstrated review capacity while funding professional indemnity, quality management, specialist competence and claims resilience.

Four tables and three figures convert this principle into a diligence and valuation method. A hypothetical transaction case illustrates capacity, margin and liability adjustments. All numerical values are illustrative management assumptions prepared solely to demonstrate the framework; they are not market observations, forecasts or valuation advice.

JEL Classification: G24, G32, G34, K13, K22, L84, L86, O32

Keywords: AI audit, AI assurance, professional liability, conformity assessment, certification body, software leverage, M&A due diligence, valuation

This paper is an educational and structural analysis prepared for research purposes. It is not investment advice, an offer, or a solicitation. It contains no client information.

1. DEFINE THE ACQUISITION DECISION

The investment committee must determine what the target sells and who stands behind the result. An AI-audit business may provide advisory reviews, technical testing, internal-audit support,

independent assurance, management-system certification or regulated conformity assessment. These services differ in scope, reliance, independence and liability.

The transaction thesis should identify the engagements that can use common software, the conclusions that require professional judgement and the signatories authorised to issue them. It should also state which revenue can scale without a matching increase in qualified reviewers. A broad label such as AI assurance cannot support a price.

2. MAP THE ASSURANCE MARKET

The UK government describes third-party AI assurance as an emerging profession and has committed to a consortium, competence framework and innovation fund. ISO published ISO/IEC 42006 in July 2025 to specify additional requirements for bodies auditing and certifying AI management systems under ISO/IEC 42001. The EU AI Act establishes conformity-assessment and notified-body roles for specified high-risk systems.

These developments create demand for evidence, testing and qualified review. They do not create one uniform service. Buyers should map the target's contracts to the exact engagement type, standard, regulatory basis, intended users and permitted claims. Market growth should remain separate from target-specific revenue evidence.

3. CLASSIFY THE ENGAGEMENT

Engagement classification begins with the conclusion. Advisory work gives findings or recommendations to management. Testing reports methods and results. Assurance expresses a conclusion against criteria. Certification attests that a management system conforms to a standard. Regulated conformity assessment follows a legal scheme and may require a designated body.

The same software may support every category, yet the duty, review and permitted language differ. Diligence should inspect proposals, contracts, reports and marketing for consistency. A target that sells advisory work using audit language can create reliance and claims risk without the quality controls associated with formal assurance.

Table 1. AI-assurance engagement types and transaction implications

Engagement type	Reader-facing output	Accountable decision	Core evidence	Principal transaction issue
Advisory assessment	Findings and recommendations	Client management retains the decision	Interviews, documents, selected tests and analysis	Marketing may imply independence or assurance beyond the contract
Technical testing	Test method, population, results and limitations	Testing lead approves the technical report	Reproducible test data, code, environment and results	Automation may obscure coverage gaps or unstable evaluation methods
Independent assurance	Conclusion against stated criteria	Authorised assurance signatory	Sufficient appropriate evidence and documented review	Professional judgement, reliance and claims exposure drive capacity
Management-system certification	Certification decision under a defined scheme	Competent certification body and authorised decision-maker	Audit programme, findings, corrective actions and certification record	Accreditation, impartiality, competence and surveillance obligations
Regulated conformity assessment	Statutory assessment and certificate where applicable	Designated or notified body acting within approved scope	Scheme-specific technical file, tests, quality system and review	Legal status, liability insurance, subcontracting and regulator oversight

Legal duties and liability vary by jurisdiction and contract; the buyer should obtain qualified advice for each engagement.

4. DEFINE ACCOUNTABLE ASSURANCE

Accountable assurance links a stated scope and criteria to evidence, evaluation, review and an authorised conclusion. The record should identify the entity responsible for the report, the engagement leader, technical specialists, reviewer and final signatory. It should also record limitations and intended users.

The buyer should distinguish responsibility from workflow completion. A software user can complete every task while lacking authority or competence to issue the conclusion. The product should prevent an automated status from being presented as a signed assurance opinion unless the required review and approval are complete.

5. ESTABLISH THE LEGAL PERIMETER

The legal perimeter depends on jurisdiction, engagement and client. Contract, negligence, misrepresentation, product rules, professional regulation and statutory conformity-assessment requirements may apply. This paper does not determine those duties for a specific firm.

Diligence should obtain a jurisdictional matrix prepared by qualified counsel. It should cover entity licensing or designation, scope of authorised work, report users, limitation language, insurance, record retention, subcontracting and dispute provisions. The transaction structure should preserve the legal entity and approvals needed for outstanding engagements.

6. APPLY THE EU NOTIFIED-BODY REQUIREMENTS

The EU AI Act provides that notifying authorities designate and supervise notified bodies carrying out independent pre-market conformity assessment. The Act requires relevant bodies to

operate with professional integrity and competence. It also requires appropriate liability insurance unless a Member State assumes liability or is directly responsible.

The buyer should confirm the target's notification status, approved scope, conditions and oversight. A general AI-audit capability does not confer notified-body authority. Revenue associated with a future designation should remain outside the base case until the designation and operating capacity are verified.

7. APPLY ISO CERTIFICATION-BODY REQUIREMENTS

ISO/IEC 42006:2025 supplements ISO/IEC 17021-1 for bodies auditing and certifying AI management systems under ISO/IEC 42001. ISO describes specialised competence and rigorous, credible assessment as central to the standard. ISO/IEC 17021-1 also addresses legal and contractual matters, impartiality, liability and financing, competence, outsourcing and confidentiality.

Diligence should test whether the target operates a certification body, supports another body or merely prepares clients for certification. These positions have different independence requirements and economics. The acquirer should not attribute certification revenue or authority to a consultancy that lacks the relevant accreditation or contractual role.

8. SEPARATE SOFTWARE FROM OPINION

Software can collect evidence, execute tests, compare configurations, monitor changes and assemble workpapers. The opinion requires a judgement about scope, criteria, evidence, exceptions and limitations. The buyer should map every automated output to the person who reviews it and the conclusion it can support.

The product should label preliminary, machine-generated and approved outputs. It should preserve the underlying evidence and reviewer actions. A dashboard status should not become an assurance conclusion through formatting or marketing. This boundary is essential to professional-liability control.

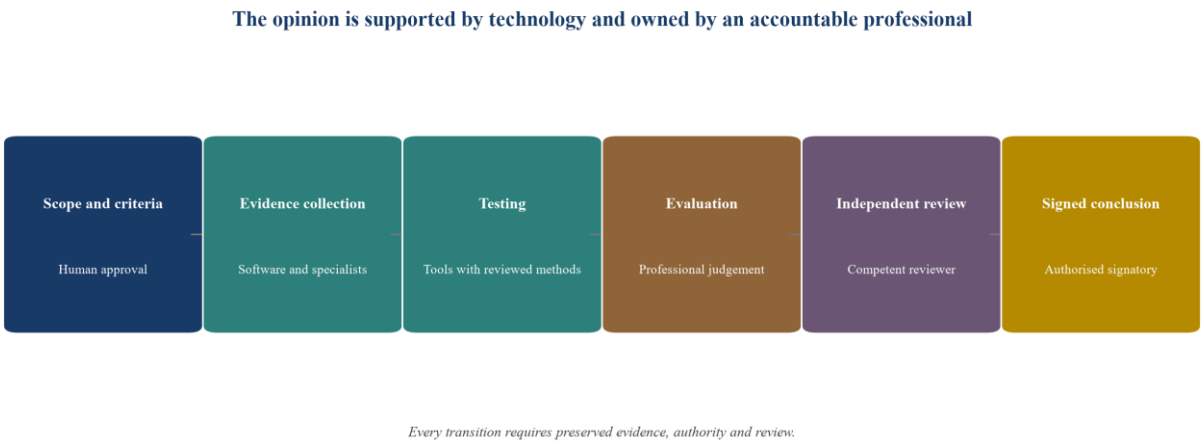

Figure 1. The accountable assurance chain

Software can increase coverage and consistency; an authorised person remains responsible for the final conclusion.

9. EXAMINE REPORT LANGUAGE

Report language determines what a reader may believe was performed. Diligence should compare engagement letters, methods, workpapers, conclusions and marketing. Terms such as audit, certified, independent, compliant and verified should have a defined basis.

The firm should state criteria, scope, period, evidence limitations and intended users. It should distinguish a point-in-time review from continuous monitoring. Material exclusions should appear near the conclusion. Standard language cannot correct a process that lacks evidence or competence.

10. TEST SIGNATORY AUTHORITY

The target should maintain an authority matrix showing which people can sign which reports, standards, sectors and jurisdictions. Authority should depend on competence, experience, independence and current approval. Departures should require documented escalation.

The buyer should sample signed reports and trace the signatory's authority at the issue date. It should inspect delegation, electronic signatures, report locks and later amendments. Shared accounts, pasted signatures or post-dated approval are critical failures.

11. VERIFY COMPETENCE

AI assurance draws on technical evaluation, risk management, audit, law, security, data governance and sector knowledge. No single credential establishes competence for every engagement. The firm should define competence requirements by role and service.

Personnel files should record education, experience, training, supervised work, observed performance and authorisation. Continuing development should address changing technologies and standards. Diligence should compare these records with actual staffing and report scope.

12. MEASURE REVIEWER CAPACITY

Reviewer capacity can constrain growth even when software scales. The buyer should identify engagement leaders, technical reviewers, independent reviewers and signatories. It should calculate available hours after management, quality and business-development duties.

Capacity should be measured by engagement complexity. A high-risk system, novel evaluation or regulated scheme may require more senior time than a standard readiness review. The operating model should reflect the mix rather than applying one utilisation assumption.

13. TEST INDEPENDENCE AND IMPARTIALITY

Independence and impartiality support credible assurance. A firm may advise a client, configure its system and later assess the same work. The conflict can be structural even when different people participate.

Diligence should inspect client acceptance, conflict checks, service combinations, fees, incentives and safeguards. Certification bodies need formal impartiality controls appropriate to their scheme. The combined company should not introduce cross-selling incentives that weaken reviewer judgement.

14. MAP CONFLICTS OF INTEREST

Conflicts can arise from ownership, referral fees, software licensing, contingent pricing, prior employment, investments and relationships with model vendors. The firm should maintain a register and a process for identification, assessment, mitigation and withdrawal.

The acquirer should test a sample from proposal to completion. It should verify that commercial teams cannot override a conflict decision without appropriate authority. Undisclosed conflicts can undermine both the opinion and the firm's market position.

15. DEFINE THE EVIDENCE STANDARD

The engagement should define what evidence is required and how sufficiency is judged. Evidence can include documents, configuration, logs, data, test results, observations, interviews and third-party reports. Reliability depends on source, completeness, relevance and reproducibility.

The firm should distinguish client assertion from independently examined evidence. Automated collection improves scale only when source integrity and coverage are known. Workpapers should explain why the evidence supports the conclusion and how conflicting evidence was resolved.

16. REVIEW SAMPLING

Sampling affects coverage and detection risk. The method should define the population, selection, sample size, period and treatment of exceptions. Convenience samples and client-selected examples require explicit limitation.

Software can increase population testing, yet data access and test design may still limit coverage. The buyer should inspect whether reported percentages use valid denominators and whether excluded records could change the conclusion. Sampling judgement should be reviewable.

17. EVALUATE TECHNICAL TESTING

NIST's AI RMF identifies test, evaluation, verification and validation as part of AI risk management. NIST's 2026 draft TEVV-Athlon framework emphasises adaptable evaluation across varied systems and use cases. Technical tests should therefore be tied to the system context and stated claim.

Diligence should inspect datasets, environments, metrics, thresholds, repeatability and change control. A benchmark score does not establish safety or compliance outside its design. The report should state what the test supports and what remains untested.

18. GOVERN TEST LIBRARIES

Test libraries create software leverage when methods are versioned, validated and linked to applicable claims. Each test should have an owner, purpose, input requirements, expected behaviour, limitations and review history.

The buyer should inspect deprecated tests, threshold changes and false-result investigations. It should identify methods licensed from third parties and verify transfer rights. A large library with weak governance can increase liability by scaling an incorrect method.

19. CONTROL GENERATED WORKPAPERS

AI tools can draft procedures, summarise evidence and identify anomalies. Generated workpapers need provenance, review and protection from silent change. The engagement file should retain the source evidence and the approved final wording.

The buyer should test hallucination, omission, prompt changes and access to confidential data. Generated conclusions should not bypass professional review. Productivity benefits should be measured after review and correction time.

20. ADDRESS BLACK-BOX SYSTEMS

Assurance may cover systems whose provider does not disclose model details, training data or evaluation methods. The firm should define the alternative evidence it can obtain and the limitations that follow. Contractual access and vendor cooperation affect engagement acceptance.

A limited-access engagement may still produce useful assurance if the scope and criteria fit the evidence. The report should avoid a broader conclusion than the work supports. Diligence should identify revenue dependent on unavailable vendor information.

21. REVIEW SUBCONTRACTING

AI-audit firms may use external technical experts, laboratories, certification partners or regional affiliates. The contracting firm can retain responsibility for their work. The EU AI Act requires notified bodies using subcontractors or subsidiaries to ensure relevant requirements are met and to inform the notifying authority.

The buyer should inspect approval, competence, independence, confidentiality, work review and insurance for each material provider. Contracts should permit transaction-related continuation or transfer. Concentration in one specialist can constrain capacity and resilience.

22. BUILD THE RESPONSIBILITY MATRIX

The responsibility matrix assigns each engagement decision to a named role. It should cover acceptance, scope, method, test approval, evidence evaluation, findings, remediation, review, sign-off, report release and later withdrawal or amendment.

Table 2. Responsibility matrix for an AI-assurance engagement

Decision	Software role	Technical specialist	Engagement leader	Independent reviewer	Authorised signatory
Client and scope acceptance	Conflict and risk prompts	Technical feasibility input	Recommends acceptance	Reviews high-risk acceptance	Approves where required
Test execution	Runs controlled procedures and records output	Owns method and investigates exceptions	Confirms engagement relevance	Challenges material judgements	Relies on approved record
Evidence sufficiency	Tracks requested and received evidence	Assesses technical reliability	Concludes on sufficiency	Reviews basis and unresolved gaps	Accepts conclusion basis
Finding and rating	Applies governed rules	Drafts technical finding	Determines engagement finding	Reviews material findings	Approves report conclusion
Report issue	Locks approved version and signature workflow	Confirms technical accuracy	Completes engagement file	Completes independent review	Signs and authorises release
Later correction or withdrawal	Preserves versions and notifications	Assesses technical effect	Coordinates response	Reviews revised conclusion	Approves correction or withdrawal

The authorised roles and legal consequences should be confirmed for the relevant jurisdiction and scheme.

23. TEST ENGAGEMENT ACCEPTANCE

Engagement acceptance should consider competence, independence, criteria, evidence access, timeframe, intended users and client integrity. A commercial opportunity should be declined when the firm cannot perform sufficient work or issue an appropriate conclusion.

The buyer should inspect rejected and modified engagements. A target with no declined work may have weak acceptance controls. Pricing should account for the work required to satisfy the criteria rather than the client's preferred budget.

24. INSPECT THE QUALITY-MANAGEMENT SYSTEM

The quality system should govern methodology, personnel, engagement performance, review, consultation, incidents, complaints and improvement. It should identify the owner and the records supporting operation.

Diligence should test whether policies match current practice. Quality reviews should select files independently and record findings, root causes and remediation. Repeated exceptions indicate an operating issue that belongs in the valuation and integration plan.

25. REVIEW ENGAGEMENT FILES

The buyer should sample complete files across services, sectors, offices and signatories. Each file should reconcile the contract, plan, work performed, evidence, findings, review and issued report. Later changes should remain traceable.

The sample should include an adverse engagement with significant findings, scope restriction or report amendment. Clean files alone do not test response under pressure. Missing evidence, undocumented consultation or unresolved review points are material concerns.

26. EXAMINE COMPLAINTS AND CLAIMS

Complaints, threatened claims, insurer notifications, regulator enquiries and report withdrawals provide direct evidence of liability exposure. The buyer should obtain complete registers, correspondence and financial treatment subject to legal privilege and applicable restrictions.

The analysis should distinguish service failure, client disagreement and broader reliance. Recurring causes should be connected to methodology, staffing, sales language or technology. The transaction should allocate known matters and preserve access to records after close.

27. ASSESS PROFESSIONAL INDEMNITY

Insurance should be reviewed by qualified brokers and counsel. Diligence should examine named insureds, covered services, jurisdictions, limits, deductibles, exclusions, aggregation, defence costs, retroactive dates, claims-made terms, notifications and change-of-control effects.

Policy limits do not establish adequate protection. Exposure depends on engagement volume, client concentration, statutory obligations and possible affected parties. The integration plan should avoid coverage gaps when entities, services or signatories change.

28. TEST CONTRACTUAL PROTECTIONS

Engagement contracts may address scope, criteria, client responsibilities, intended users, reliance, confidentiality, intellectual property, limitation of liability, indemnity and dispute resolution. Enforceability varies, so legal review is required.

The buyer should compare templates with executed contracts and report wording. Side letters, procurement terms and statements of work can alter protection. Revenue should be segmented by contract risk as well as service type.

29. RECONSTRUCT RECURRING REVENUE

Revenue should be rebuilt from contracts, invoices, credits, collections and the general ledger. Certification surveillance, monitoring subscriptions, software licences, one-time audits, remediation support and training should be separated.

Recurring labels require recurring obligations and collected revenue. An annual programme may include substantial senior review each cycle. The buyer should calculate contribution after reviewer, specialist, insurance and quality costs.

30. BUILD REVENUE COHORTS

Cohorts should be organised by service, client sector, signatory, first engagement date and framework. Measures should include repeat work, renewal, expansion, collection, claims and contribution. Software-assisted and manual engagements should be separated.

Table 3. Illustrative AI-assurance revenue cohorts

Cohort	Opening revenue USDm	Repeat or renewal	Software revenue share	Senior review hours per USD100k	Contribution margin	Liability observation
Readiness and advisory	5.0	62%	12%	24	38%	Lower formal reliance; marketing language remains important
Technical testing	7.0	78%	34%	18	52%	Method validity and coverage drive exposure
Independent assurance	8.0	86%	19%	31	43%	Signatory and review capacity constrain growth
Certification support and surveillance	6.0	91%	28%	27	47%	Scheme authority, impartiality and continuing obligations matter
Continuous monitoring	4.0	94%	63%	10	66%	Higher software leverage; alerts and conclusion boundaries need control

All values are hypothetical management assumptions included only to demonstrate the analysis.

31. MEASURE UTILISATION CORRECTLY

Utilisation should distinguish technical execution, engagement leadership, independent review, sign-off, quality work and rework. High billable utilisation can weaken supervision and increase claims risk. The operating model should reserve time for consultation, training and quality.

The buyer should reconcile timesheets to files and revenue. Fixed-fee engagements may hide overruns. Automation savings should appear as lower execution time without an unexplained reduction in review or evidence quality.

32. PRICE THE ENGAGEMENT

Pricing should reflect complexity, evidence access, reliance, specialist skills, review and liability. Software may lower execution cost while allowing broader coverage. The price should still fund the professional process required for the conclusion.

Contingent fees and success-based pricing can threaten independence for some services. The firm should define prohibited or restricted fee structures. Discount authority should consider delivery and claims exposure rather than sales targets alone.

33. VALUE SOFTWARE LEVERAGE

Software leverage can increase capacity through reusable workflows, evidence connectors, controlled tests, workpaper assembly and monitoring. Value depends on repeatability, adoption and net contribution. The buyer should verify that software is used in paid engagements and that clients accept its outputs.

The valuation should deduct maintenance, cloud cost, security, testing and human review. A feature that accelerates execution while increasing correction work may not improve contribution. Usage telemetry should reconcile with engagement files and billing.

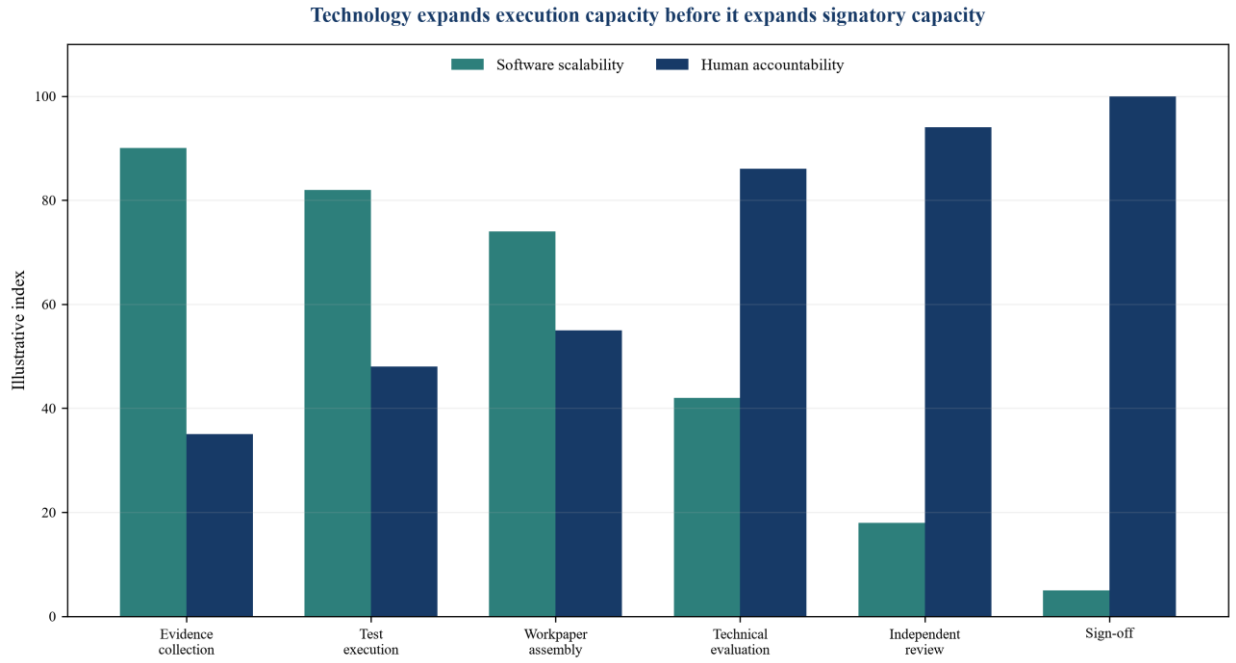

Figure 2. Illustrative assurance capacity by activity

Values are hypothetical management assumptions; they show that software scales execution faster than accountable review.

34. REVIEW INTELLECTUAL PROPERTY AND DATA RIGHTS

The buyer should verify ownership and licence rights for methods, test code, datasets, standards content, report templates and training materials. Contractor and academic contributions require particular attention. Transaction transfer and derivative-use rights should be explicit.

Client data should be governed by contract, confidentiality, retention and permitted use. Benchmarking or model improvement needs a documented basis. A dataset assembled from confidential engagements may have limited reuse value.

35. TEST CYBERSECURITY AND CONFIDENTIALITY

Assurance firms hold sensitive model details, vulnerabilities, personal data and regulatory records. Diligence should assess identity, privileged access, encryption, tenant isolation, secure development, incident response and recovery.

The engagement file should restrict access by role and client. External experts need equivalent controls. A breach can cause direct cost, client claims and loss of accreditation or designation, so cyber risk belongs in the transaction model.

36. EVALUATE TECHNOLOGY RESILIENCE

The platform should preserve evidence when connectors fail, tests change or services become unavailable. It should identify incomplete collections and stale results. A green status based on missing data is a critical design failure.

The buyer should test backup, recovery, export and vendor substitution. Technical dependencies should have owners, contracts and exit plans. Continuous-monitoring commitments require capacity and incident processes outside normal project hours.

37. REVIEW CUSTOMER CONCENTRATION

Large regulated or technology clients can provide reference value and concentrated exposure. The buyer should measure revenue, receivables, contribution, reviewer demand and potential claim severity for each major client.

Several clients may use the same test library, platform connector or signatory. A single method failure can therefore create correlated exposure. Concentration analysis should include common dependencies and report users.

38. TEST CROSS-SELLING

An acquirer may expect to sell software, testing and assurance to the same client. The independence matrix should determine which combinations are permitted and which require safeguards or separate teams. Commercial plans should respect that boundary.

Cross-selling evidence includes contracted multi-service clients, qualified demand, approved service combinations and available reviewers. Pipeline should remain outside the base case until these conditions are met.

39. PLAN INTEGRATION

Integration should protect active engagements, signatory authority, accreditation, insurance, evidence and client obligations. Product consolidation should follow a tested migration plan. Methodologies should not be combined through informal document merging.

The integration committee should include assurance, technical, legal, quality, insurance, security, finance and customer leaders. Each work package should state affected reports, required approvals and rollback. Historical files need continued access.

40. SET DAY ONE CONTROLS

Day One should govern report issue, signatures, conflicts, incidents, subcontractors, software releases and client communications. The buyer should confirm every authorised signatory and outstanding review. Unapproved branding or legal-entity changes should be blocked.

Open findings, claims, complaints and regulator correspondence need owners. The quality function should have authority independent of revenue leadership. Escalation routes should remain available across the combined group.

41. DEFINE ONE-HUNDRED-DAY DECISIONS

Within one hundred days, management should approve the service taxonomy, authority matrix, target platform, quality system, insurance programme and integration roadmap. It should validate recurring revenue and signatory capacity.

Management should also decide which advisory and assurance combinations are permitted. Revenue targets should reflect independence, competence and reviewer availability. Product investment should prioritise evidence quality and controlled methods.

42. BUILD THE VALUATION BRIDGE

Valuation begins with collected revenue and contribution by engagement type. The buyer can then credit reusable technology, retention and qualified capacity. It should deduct remediation, insurance, claims exposure, reviewer recruitment and integration cost.

The buyer should avoid applying software multiples to labour-intensive assurance revenue. It should also avoid treating professional services as low value when signatory authority, competence and client trust create scarcity. The bridge should show each element.

Table 4. Hypothetical transaction valuation bridge

Item	Illustrative value USDm	Evidence condition	Treatment
Indicative enterprise value	180	Initial offer based on reported revenue and category growth	Starting point only
Revenue-quality adjustment	-18	One-time advisory, uncollected fees and unsupported recurring labels	Deduct from base economics
Quality and security remediation	-10	Confirmed file, method and platform improvements	Deduct funded cost
Insurance and claims reserve	-12	Broker, counsel and actuarial review of exposure	Deduct or escrow as appropriate
Verified software leverage	+16	Paid use, controlled methods and net contribution	Credit after evidence
Signatory-capacity value	+11	Authorised, retained professionals with demonstrated delivery	Credit subject to retention
Integration and accreditation continuity	-14	Cost of preserving approvals, files and active engagements	Deduct funded cost
Evidence-adjusted value	153	Sum of hypothetical adjustments	Decision scenario only

All values are hypothetical management assumptions and do not represent a market observation, forecast or valuation opinion.

43. RUN LIABILITY SCENARIOS

Scenarios should include an incorrect clean conclusion, a missed material limitation, flawed test methods, independence failure, confidentiality breach and unauthorised report. The model should

estimate response cost, defence, insurance recovery, client loss and regulatory effects using qualified advice.

The scenarios should test correlation. One defective test can affect many reports. One signatory can cover several clients. Software scale can increase both efficiency and the number of engagements exposed to the same error.

44. USE TRANSACTION PROTECTIONS

Price adjustment, escrow, indemnity, warranty insurance and contingent consideration may address identified risks subject to legal and commercial advice. The mechanism should match the evidence gap and preserve access to files.

Retention arrangements can protect specialist and signatory capacity. They should not reward report volume at the expense of judgement. Milestones should include quality, retained revenue and collected contribution.

45. IDENTIFY CRITICAL RED FLAGS

Critical red flags include unclear engagement classification, unauthorised signatures, inconsistent report language, missing evidence, ungoverned tests, conflicted services, weak insurance, unreported claims and dependence on one reviewer. Each requires investigation and transaction treatment.

A critical issue may justify remediation, a condition, repricing or withdrawal. The investment committee should record the decision and evidence. Urgency should not convert an open liability question into an assumption.

46. SET APPROVAL GATES

The assurance gate tests scope, criteria, evidence and sign-off. The competence gate tests people and authority. The liability gate tests contracts, insurance and claims. The commercial gate tests revenue and capacity. The integration gate tests continuity.

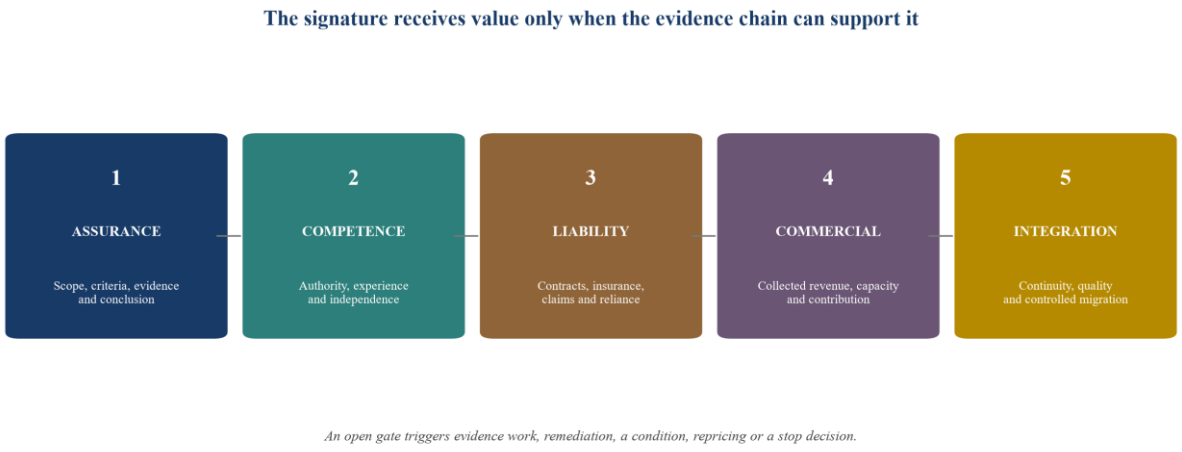

Figure 3. Approval gates for acquiring an AI-audit firm

47. MAINTAIN THE DECISION RECORD

The buyer should record every material decision, evidence source, owner, assumption and review trigger. Key entries include service classification, signatory authority, insurance, claims treatment, technology value and integration sequence.

The record supports later review when facts change. It also prevents management estimates from becoming embedded as historical fact. The combined firm can use the same discipline for new methods and services after close.

48. AUDIT THE THESIS AFTER CLOSE

The board should compare actual retained revenue, reviewer hours, claims, software use, contribution and integration cost with the transaction model. Variances should be supported by records. Cost savings should be measured after quality and review work.

Post-close file reviews should test whether the combined company preserved evidence and independence. A successful technology migration requires reliable assurance outcomes. The audit creates a stronger basis for future acquisitions.

49. RECONCILE THE AUDIT UNIVERSE

The target should maintain an audit universe covering every active engagement, report, certificate, client entity, applicable framework and responsible signatory. Diligence should reconcile this universe to contracts, billing, report repositories and the general ledger. Missing engagements can conceal unrecorded obligations, while duplicate records can overstate activity and recurring revenue.

The universe should identify the current status, period under review, reliance, surveillance or renewal date, subcontractors and unresolved findings. It should also record whether software monitoring continues after the report date. This allows the buyer to distinguish completed projects from continuing responsibilities.

The buyer should sample engagements from each source rather than relying on the management list alone. A contract without a report may reflect delayed delivery. A report without a contract may indicate informal scope or weak commercial control. A certificate without a current surveillance record can create customer and reputational risk. Reconciliation findings should become conditions, adjustments or integration work packages.

50. EXAMINE REPORT WITHDRAWAL AND CORRECTION

An assurance firm needs a controlled response when later evidence shows that a report may be incomplete or incorrect. The process should define technical investigation, legal consultation, signatory review, client notification, insurer notification and regulator or accreditation-body engagement where required. Every issued and revised version should remain preserved.

Diligence should inspect actual corrections, withdrawals and near misses. The time taken to identify affected reports matters when one test method or data source supports many engagements. The platform should enable the firm to locate every use of a method, rule or dataset and assess the impact of a defect.

Contracts and report terms should address later information and continuing duties. The precise obligation depends on the engagement and jurisdiction. The buyer should avoid assuming that completion of fieldwork ends all exposure. Post-report monitoring, complaints and new facts may require action.

51. PROTECT KEY-PERSON AND SUCCESSION CAPACITY

Signatory authority and specialist competence can be concentrated in a small number of people. The buyer should map revenue, frameworks, sectors and client relationships to each critical person. It should identify notice periods, restrictive covenants, authorisations, professional memberships and succession readiness.

Retention value should reflect the person's actual capacity and authority. A senior leader may originate work while another professional performs the review and signs. Diligence should trace the complete chain. Client consent or accreditation approval may be required when personnel change.

Succession planning should include supervised experience, observed engagements and formal authorisation. Hiring a qualified person does not immediately create familiarity with the firm's methods or clients. The integration schedule should allow for transition and parallel review. Retention arrangements should reward quality, knowledge transfer and sustainable capacity rather than report volume alone.

52. APPROVE NEW ASSURANCE SERVICES

New services should pass a formal approval process before marketing or delivery. The proposal should define users, criteria, scope, method, competence, independence, report language, insurance, data rights and quality review. Product and commercial teams should not launch an assurance claim solely because software can perform a new test.

The approval record should distinguish advisory, testing, assurance, certification and statutory activity. It should identify jurisdictions and sectors where the service is permitted. Pilot engagements should use controlled terms and additional review. Lessons should be documented before wider release.

Acquisition integration often creates pressure to combine capabilities quickly. The combined firm may have new datasets, tools and distribution without an approved methodology. The new-service gate protects the brand and prevents unpriced liability from entering the sales pipeline.

53. TEST GEOGRAPHIC EXPANSION

Geographic expansion requires a current view of legal duties, professional regulation, accreditation, data transfer, insurance and report enforceability. A method used in one jurisdiction may remain technically relevant while the assurance claim and responsible entity change.

The buyer should identify who contracts, performs, reviews and signs in each market. Local affiliates and subcontractors should be included in the responsibility and insurance analysis. Marketing should avoid suggesting regulated authority where the firm provides only advisory or technical support.

Commercial forecasts should separate translation and software localisation from professional and legal work. Repeatable platform features can scale efficiently. Jurisdictional analysis, local competence and approval may require continuing investment. Expansion value should enter the transaction model when the operating path and cost are supported.

54. STRESS-TEST THE INSURANCE PROGRAMME

The insurance programme should be tested against plausible engagement failures rather than reviewed only for headline limits. Scenarios can examine one large claim, multiple related claims arising from a shared method, cyber events, regulatory investigations and claims reported after a transaction. Brokers and counsel should confirm how aggregation, deductibles, defence costs and exclusions may operate.

The buyer should review historical applications and representations to insurers. Inaccurate or incomplete disclosures can affect coverage. New services, jurisdictions, revenue and transaction changes should be notified where required. Tail or run-off arrangements may be necessary for legacy entities and reports.

Management assumptions about insurance recovery should remain separate from expected loss. Coverage may be disputed, delayed or exhausted. The transaction model should fund deductibles, uncovered response cost and operating disruption using evidence-based scenarios.

55. DEFINE THE BOARD DASHBOARD

The board dashboard should connect commercial growth with assurance quality. Measures should include collected revenue, contribution, engagement backlog, reviewer capacity, overdue files, significant findings, report amendments, complaints, claims, method changes and security incidents. Definitions and sources should be stable.

Metrics should be segmented by service, sector, geography and signatory. Aggregate growth can hide a strained practice or concentrated exposure. A fall in senior review hours may indicate genuine automation, a change in mix or weakened supervision; management should explain the source.

The dashboard should identify management estimates and unresolved evidence. It should show corrective actions and accountable owners. A concise set of reliable measures gives the board a better view than a large volume of platform activity without connection to issued opinions and economic results.

56. DISTINGUISH CERTIFICATION FROM IMPLEMENTATION SUPPORT

Certification preparation can improve a client's management system, but the organisation that later certifies the system may face impartiality restrictions on consultancy. The buyer should identify whether the target designs controls, implements workflows, performs internal audits, conducts pre-assessments or makes certification decisions. Contracts and marketing should describe each role consistently.

Revenue analysis should separate implementation support from accredited certification. The services have different sales cycles, staffing and margins. A referral or partner relationship may

create commercial value without giving the target authority to issue a certificate. The buyer should verify the contracting entity and certificate record before crediting that revenue stream.

Integration can create new conflicts when a consulting acquirer buys a certification or assurance unit. Governance may require legal separation, information barriers, independent leadership, restricted incentives and service prohibitions. The transaction model should include the cost and revenue effect of those safeguards. Commercial teams should receive clear rules before cross-selling begins.

57. EXAMINE RELIANCE AND DISTRIBUTION

An assurance report may be prepared for management, a board, customers, regulators, investors or the public. The intended users and distribution affect the engagement design and potential reliance. The buyer should examine how reports are delivered, quoted in marketing, published on websites or incorporated into procurement and financing decisions.

The firm should control use of its name, marks, certificates and extracts. A qualified conclusion can appear unqualified when a client publishes only favourable language. Monitoring and enforcement of permitted use may be part of the continuing obligation. Diligence should inspect misuse cases and response.

Report templates should state intended users and limitations in clear language. Distribution controls cannot substitute for sufficient work, yet they help prevent a conclusion from travelling beyond its design. The acquirer should assess whether existing contracts and reports align with actual distribution practice.

58. CONNECT AUDIT QUALITY TO ECONOMICS

Audit quality is an operating input rather than a separate compliance cost. Competent acceptance avoids engagements the firm cannot perform. Controlled methods reduce rework. Reliable evidence and review support defensible conclusions. Effective complaints and correction processes protect client relationships and limit escalation.

The buyer should connect these activities to economic measures. File-review findings can be compared with write-offs, delivery delays, claims and renewal. Reviewer capacity can be compared with backlog and pricing. Method changes can be compared with execution time and error rates. These relationships show where investment improves both quality and contribution.

Cost reduction should be assessed net of its quality effect. Removing review hours may raise short-term margin while weakening evidence and increasing tail risk. Automating evidence collection may improve both margin and coverage when source controls work. The valuation case should credit the second result and challenge the first.

59. RECONCILE WORK IN PROGRESS AND BACKLOG

Work in progress should be reconciled at engagement level. The buyer should compare contracted scope, milestones, time, costs, invoices, collections, review status and remaining obligations. Percentage-complete estimates should be supported by the engagement plan and file. A nearly complete technical test may still require substantial senior evaluation and review before report issue.

Backlog should include only enforceable contracted work with a defined service and delivery path. Framework agreements, preferred-supplier status and unsigned proposals should remain separate. The buyer should test whether capacity exists to deliver the backlog without weakening review or relying on unapproved subcontractors.

The analysis should identify loss-making or high-risk engagements. Fixed fees, evidence delays, expanded scope and repeated retesting can create negative contribution. Client pressure for rapid issue can increase liability at the same time. The transaction should preserve the firm's right to extend work, modify the conclusion or withdraw when evidence is insufficient.

Opening balance-sheet adjustments should reflect unbilled work, deferred revenue, client advances, provisions and collection risk. Revenue recognition requires accounting advice and contract-specific analysis. The valuation model should use cash and remaining delivery cost rather than treating backlog as equivalent to recurring revenue.

60. CONCLUSION

AI-audit firms can create valuable recurring services and scalable technical assets. Their value depends on a defensible chain from scope and criteria through evidence, evaluation, review and authorised conclusion. Software can expand coverage and consistency. Accountable professionals remain responsible for the opinion.

The buyer should value verified software leverage together with qualified signatory capacity, quality management and claims resilience. The Accountable Assurance Valuation Framework connects these elements to diligence, transaction terms and integration. It gives technology appropriate credit while preserving the professional boundary that makes the assurance credible.

REFERENCES

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 close.

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

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

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

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

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