# RegTech AI Financing

*Proving Compliance Outcomes and Durable Buyer Demand*

**Authored by Chennakeshav Adya, Independent Researcher**

September 2026

## Abstract

*Regulatory-technology companies use machine learning, natural-language processing, graph analytics, workflow software and rules engines to support customer due diligence, transaction monitoring, sanctions screening, fraud prevention, regulatory reporting, surveillance, policy management and operational resilience. The commercial claim often emphasises faster review, fewer alerts or continuous rule mapping. These measures do not establish compliance effectiveness or equity value on their own. A system can reduce alerts while missing relevant risk, automate work while creating validation and oversight burdens, win a pilot without surviving enterprise procurement, or depend on regulatory change that buyers cannot safely outsource. This paper develops an evidence-led framework connecting compliance outcomes, workflow economics, buyer procurement, governance and durable cash value in a RegTech financing or transaction process. It constructs a compliance workflow, outcome scorecard, procurement funnel, regulation-dependency map and financing-milestone plan. Forty modules cover legal perimeter, obligation lineage, alert quality, false negatives, human decisions, data provenance, model governance, regulatory change, integration, security, third parties, buyer demand, contracts, implementation, unit economics, forecasting, valuation and diligence. Five figures, five tables, eight frequently asked questions and twenty-six authoritative references support fact-specific review. Management claims, sales forecasts and illustrative scenarios require independent validation. The framework does not substitute for legal, accounting, tax, regulatory, cybersecurity, valuation or investment advice.*

JEL Classification: G21, G23, G24, G28, G32, O31

Keywords: regulatory technology, artificial intelligence, compliance, AML, transaction monitoring, regulatory reporting, procurement, growth capital, valuation, model governance

## 1. Define the financing decision

The work should begin with the board decision. A primary equity raise, strategic investment, acquisition or secondary sale requires an explicit amount, use of proceeds, runway, valuation range, operating milestone and decision date. RegTech evidence should support that decision and distinguish deployed outcomes from pilots, roadmap features and unsupported market opportunity.

The central investment question is whether the company can repeatedly convert regulatory and compliance problems into controlled software deployments, measurable outcomes, durable contracts and cash. The financing model should include product development, regulatory content, data, security, integration, validation, implementation, customer support and procurement time. Future benefits should enter the base case only when they have evidence, accountable ownership and a credible scaling path.

## 2. Define the RegTech problem precisely

RegTech covers different activities with different objectives. Transaction monitoring seeks potentially suspicious activity; sanctions screening identifies relevant parties or transactions; regulatory reporting produces required data; surveillance identifies conduct concerns; policy tools map obligations; and resilience platforms manage incidents and dependencies. A broad label cannot substitute for a defined decision and user.

The product thesis should state the regulated activity, customer, jurisdiction, obligation, workflow, decision right and output. It should identify whether the tool recommends, prioritises, drafts, validates, files or makes a constrained automated decision. This purpose determines required data, acceptable error, human review, evidence retention and commercial buyer. Adjacent use cases should remain separate until transfer is demonstrated.

## 3. Establish the legal and economic perimeter

The perimeter should identify the software provider, regulated institution, outsourced service provider, data processor, cloud provider, content source and professional adviser. It should show who owns the regulated obligation, makes the final decision, reports to authorities, bears remediation and controls customer or transaction data. Institutions generally remain accountable for compliance when they use technology or third parties.

The economic perimeter should map subscription, usage, implementation, content, support and professional-service revenue. It should also identify service credits, indemnities, audit obligations, cybersecurity exposure, minimum commitments and change-of-control restrictions. A platform may appear high margin while relying on intensive implementation or unpriced regulatory maintenance. Contracts, accounting and observed delivery effort should be reconciled before recurring revenue or margin is valued.

## 4. Build the obligation-to-evidence ledger

The evidence base should connect an authoritative obligation to policy, control, data, model or rule, workflow action, accountable decision and retained evidence. Each item should have jurisdiction, entity, product, effective date, owner, version and source link. Changes should preserve prior versions and their applicability periods.

**Table 1. Obligation-to-evidence ledger**

| Element | Primary evidence | Control question |
|---|---|---|
| obligation | authoritative rule, guidance or licence | what requirement applies and when? |
| control | approved policy and procedure | how does the institution respond? |
| system logic | versioned rule, model or workflow | can the operation be reproduced? |
| decision | alert, case, approval or filing | who exercised accountability? |
| outcome | quality review, issue or supervisory result | did the control operate effectively? |
| economics | labour, vendor, remediation and cash | what value and cost changed? |

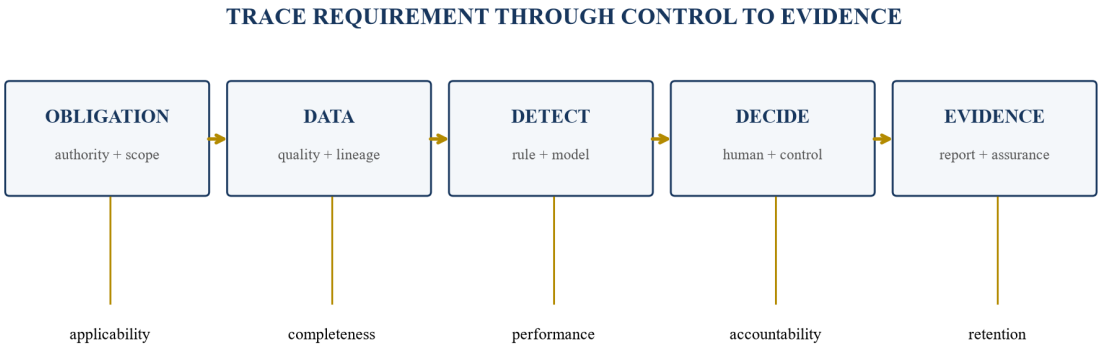
*Fields should be adapted to the activity, jurisdiction, institution and legal advice.*

The ledger should support two-way traceability. Reviewers should move from an obligation to the operating evidence that addresses it and from a system output back to its authority and control purpose. Gaps, conflicts and interpretive judgement should remain visible. A generated summary without authoritative source, applicability and decision ownership cannot support transaction-grade diligence.

## 5. Map the compliance workflow

The workflow should show intake, data validation, risk detection, prioritisation, investigation, decision, reporting, quality assurance and feedback. It should separate activities performed by the RegTech product, the institution and external parties. Counts, values, time and decision outcomes should reconcile at each stage.

**Figure 1. Compliance workflow**




*Populate the workflow with institution-specific obligations, systems, roles and evidence.*

The workflow should retain exceptions, rework and hand-offs. Automation that moves work into another team is not a complete saving. Quality assurance and remediation should remain inside the population. The same map becomes the denominator for product validation, staffing analysis, implementation scope, contract pricing and investor reporting.

## 6. Build the authoritative obligations inventory

The obligations inventory should capture legislation, regulation, binding standards, licence conditions, supervisory rules, formal guidance and institution-approved interpretations. It should distinguish current, future, superseded and consultation material. Professional commentary can support understanding and should not replace authoritative sources.

Applicability should be determined by entity, permission, product, customer, geography and effective date. One paragraph can impose several requirements, and one control can address several obligations. The data model should support many-to-many relationships and record interpretive decisions. Regulatory content operations should have accountable legal or compliance review, service levels and escalation for ambiguous change.

## 7. Define compliance outcomes

Compliance outcomes should reflect the purpose of the control. Examples include relevant risk identified, prohibited activity prevented, complete and timely report, accurate regulatory data, resolved customer issue, controlled incident or evidenced policy implementation. Activity measures such as alerts processed or pages mapped describe workload and do not prove effectiveness.

The outcome definition should state population, horizon, evidence and error. Confirmed supervisory findings may be rare and lagged, so intermediate quality measures can support monitoring. Those measures should have demonstrated relationship to the final objective where possible. The company should avoid claiming that absence of enforcement establishes product effectiveness.

## 8. Establish the pre-product baseline

The baseline should measure the prior process under consistent definitions: population, alert volume, handling time, backlog, escalation, filing, error, quality review, staffing, incidents and remediation. It should identify manual tools, legacy systems, outsourced work and existing vendors. Historical weakness should not be exaggerated to make the new product appear stronger.

Baseline periods should cover seasonality and regulatory cycles. Changes in customer mix, business volume, risk appetite, typologies, data or staffing should be recorded. If no reliable baseline exists, the institution can run a parallel or shadow period. Equity value should use benefits observed against a credible comparison rather than management recollection.

## 9. Measure compliance effectiveness

Effectiveness combines coverage, detection, decision quality, timeliness, reporting and remediation. For transaction monitoring, the CBUAE identifies risk-based monitoring, alert prioritisation, decision making, filing and continuing activity as components. FATF technology guidance emphasises responsible use to improve AML/CFT effectiveness, including understanding and mitigating risk.

Metrics should be segmented by material risk, product, geography and model version. A portfolio average can hide a weak high-risk segment. Independent testing should assess design and operating effectiveness. Findings should be linked to exposure, remediation, customer effect and cost. A software output remains evidence for an accountable control, not a substitute for institutional responsibility.

## 10. Build the compliance-outcome scorecard

**Table 2. Compliance-outcome scorecard**

| Domain | Outcome evidence | Economic relevance |
|---|---|---|
| coverage | population completeness and applicable risk | defines addressable controlled work |
| detection | relevant cases and missed-event testing | informs effectiveness and liability |
| decision | consistent, evidenced and timely disposition | supports accountable operation |
| reporting | accurate, complete and timely submission | reduces correction and remediation |
| customer | complaints, delays and restrictions | identifies conduct and service cost |
| assurance | independent tests and finding closure | supports procurement and renewal |

*Measures require institution-specific risk appetite, legal review and validation.*

The scorecard should show baseline, current result, target, tolerance, source, owner and maturity. It should include negative indicators such as missed cases, rework, data exceptions and overdue remediation. Green averages should not offset a critical control failure. The board and buyer should see which outcomes are validated and which remain leading indicators.

## 11. Test false negatives

A false negative is relevant risk or non-compliance that the system fails to identify. It is difficult to measure because the missed event may remain unknown. Testing can use retrospective cases, seeded scenarios, independent samples, typology reviews, supervisory findings and comparison with complementary controls. Each method has coverage limitations.

The company should state the tested population, detection window and ground-truth method. A lower alert count can improve efficiency and increase missed risk. Material false-negative findings should trigger limits, remediation and valuation sensitivity. Investors should inspect how the product learns from newly identified cases without leaking post-event knowledge into historical validation.

## 12. Quantify false positives and unnecessary work

False positives consume investigator time, delay customers, create repeated requests and can weaken attention to relevant risk. The analysis should distinguish an alert that is correctly generated under policy from one that lacks useful risk. Disposition codes and quality review should remain consistent across teams and periods.

Alert reduction creates value when coverage and effectiveness remain controlled. Savings should include review, escalation, customer contact, documentation and assurance. Time released should convert into cash, capacity or improved outcomes before entering the valuation. A vendor-reported reduction without a stable baseline, equivalent risk population and independent testing is an experiment result.

## 13. Measure precision, recall and economic utility

Precision measures the share of flagged cases that meet the approved relevant-outcome definition. Recall measures the share of relevant cases that the system identifies, subject to the ability to observe the full population. These measures can support model assessment and should be interpreted alongside severity, customer effect and workload.

Economic utility can weight relevant detection, missed risk, unnecessary review, customer delay and remediation. The weights should reflect risk appetite and cannot convert prohibited outcomes into acceptable trade-offs. Threshold curves should show how metrics and workload change. The selected operating point should have accountable approval and segment-level limits.

## 14. Preserve workflow traceability

Every automated recommendation should retain source data, rule or model version, output, explanation, user action, override, evidence and timestamp. The system should distinguish machine-generated content from approved institutional decisions. Changes and corrections should preserve the original record.

Traceability supports internal audit, regulatory inquiry, customer response and model validation. It also reduces implementation risk during acquisition or migration. A product that cannot export complete evidence may create lock-in and operational liability. Data-room testing should replay selected cases from raw input through final decision and report.

## 15. Govern data provenance and quality

Data provenance should record origin, legal basis, observation time, transformation, completeness, ownership and permitted use. Compliance models can depend on customer, transaction, identity, communications, market and regulatory data. Missing or delayed feeds can change performance without visible software failure.

Quality controls should cover schema, reconciliation, duplication, identity resolution, reference data and lineage. The company should show how production data differs across customers and jurisdictions. Features derived after the relevant decision must not leak into validation. Vendor data rights, retention and transfer should be reviewed before growth assumptions rely on them.

## 16. Operate regulatory-change management

Regulatory change begins with authoritative publication and ends when affected policy, control, system, training, customer communication and evidence are updated. The workflow should record identification, applicability, interpretation, impact, owner, approval, implementation and assurance. Deadlines and dependencies should be visible.

The FCA's 2026 Handbook API illustrates how authoritative, versioned regulatory data can support rule mapping and AI tools. Access to an API does not determine applicability or legal interpretation. RegTech companies should show source freshness, change detection, quality controls and accountable review. Product claims should distinguish retrieval, mapping, interpretation and implementation.

## 17. Build the rule-to-control map

Rules should map to the institution's products, activities, customer journeys, entities and controls. The map should support effective dates and exceptions. It should identify conflicts, duplication and local overlays. A generic rule library becomes valuable when it can be adapted and evidenced without losing source authority.

Natural-language systems can assist extraction, comparison and drafting. Deterministic controls should manage identifiers, dates, versions and approved relationships. Human reviewers should resolve material ambiguity. Accuracy tests should use representative obligations and score omissions, unsupported mappings and stale sources, not only fluent summaries.

## 18. Govern AI models and language systems

The model inventory should state purpose, owner, developer, data, version, validation, limitation, monitoring and retirement. It should include embedded third-party models and retrieval systems. Intended use, prohibited use and human review should be explicit. NIST AI RMF and ISO/IEC 42001 provide general governance structures that can be adapted to the specific regulated activity.

Language-system testing should address source grounding, completeness, factuality, citation, instruction hierarchy, sensitive data, security and reproducibility. The company should preserve prompts, retrieval corpus, model version and output where needed for evidence. Model changes should trigger impact assessment and proportionate revalidation before the result enters a compliance process.

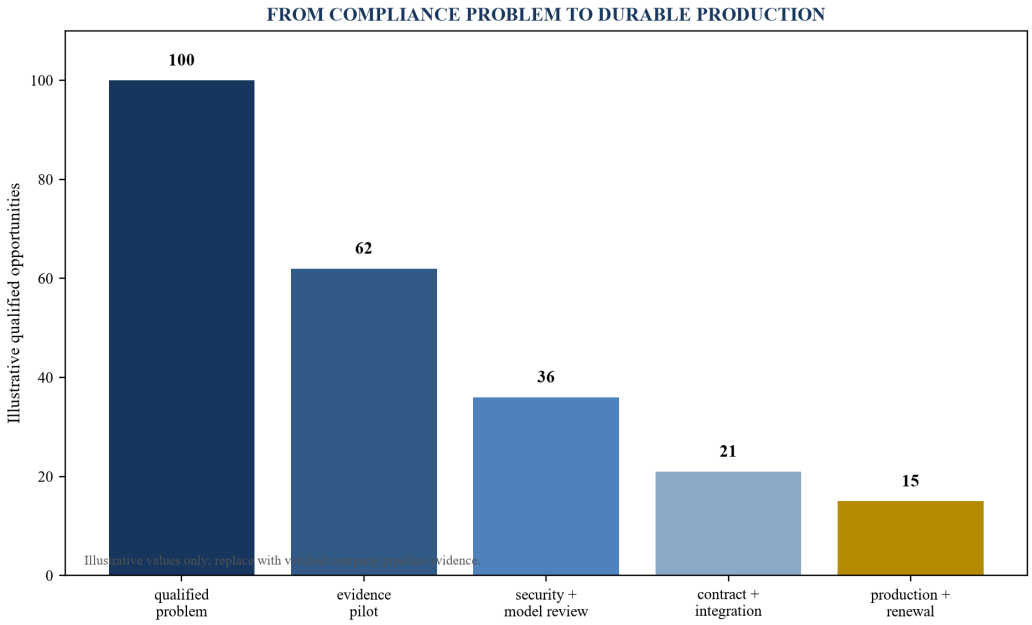
## 19. Design accountable human decisions

Human review should have defined authority, competence, information and time. An approval click does not establish meaningful oversight if the reviewer cannot understand or challenge the output. Interfaces should present source evidence, uncertainty, policy and available action. Escalation should be accessible for high-risk or ambiguous cases.

Overrides should record reason, direction, user, evidence and outcome. Concentrated overrides can reveal model weakness, policy conflict or poor implementation. Quality assurance should assess both machine and human decisions. Staffing models should include training, supervision and accountability rather than assume AI removes regulated judgement.

## 20. Construct the enterprise procurement funnel

**Figure 2. RegTech enterprise procurement funnel**




*Conversion and timing should be measured from controlled CRM, security and contracting records.*

The funnel should begin with a budgeted compliance problem and identified buyer, not a marketing lead. It should track pilot approval, data access, information security, model risk, legal, procurement, integration, production acceptance and renewal. Stage entry and exit criteria should be defined.

Pipeline value should be probability-weighted using observed conversion and time. A successful technical pilot can fail commercial procurement because of security, data residency, audit rights, liability or internal ownership. Financing plans should include the cash required to carry long enterprise cycles and implementation capacity.

## 21. Navigate enterprise buyer governance

RegTech purchases usually cross several control functions. Compliance owns the problem, technology owns architecture and operations, information security owns access and resilience, model risk may own validation, procurement owns commercial process, legal owns contractual allocation and finance owns budget. A credible commercial plan identifies each decision right, the evidence required and the sequence in which approvals occur.

The vendor should document a buyer-side responsibility matrix before a pilot begins. The matrix should identify the executive sponsor, operational owner, data owner, integration owner, control approver and contracting authority. This discipline reduces stalled pilots and distinguishes genuine demand from innovation theatre. It also provides investors with a testable explanation for sales-cycle duration and conversion.

Governance evidence should include signed pilot charters, decision calendars, security questionnaires, validation packs, procurement milestones and executive steering records. Management forecasts should use completed stages and observed cycle time. Verbal enthusiasm and conference interest are weak evidence of a budgeted purchase.

A practical diligence exercise should reconstruct three completed purchasing journeys: one converted customer, one stalled opportunity and one lost opportunity. Reviewers should compare

CRM timestamps with email approvals, pilot documents, security submissions, legal mark-ups and invoices. The comparison can reveal optimistic stage definitions, missing decision-makers and delays hidden by aggregate pipeline reporting. It also establishes whether improvement initiatives address observed constraints. For example, a standard security pack may reduce review time when questionnaires are the bottleneck, while additional product features may have little effect. The board should receive a funnel that separates buyer action from vendor action and records the next verifiable decision. This gives management a credible basis for capacity, runway and financing plans.

## 22. Integrate with legacy architecture

Financial institutions operate heterogeneous ledgers, case-management systems, customer records, data warehouses and regulatory-reporting stacks. A RegTech product creates value only when it receives reliable inputs, produces usable outputs and fits existing control ownership. Integration design should state source systems, schemas, latency, reconciliation, exception handling, identity, access and recovery.

The commercial model should distinguish product configuration from bespoke engineering. Reusable connectors, documented APIs, canonical data models and automated testing can shorten implementation and improve gross margin. Customer-specific transformations and manual remediation can create hidden services cost. Investors should inspect implementation hours, third-party dependencies, defect rates, time to production and support effort by customer cohort.

Data lineage is especially important. Each material output should be traceable to authoritative source data, transformation logic, model version and reviewer action. Reconciliation should confirm completeness as well as accuracy. An elegant dashboard cannot compensate for missing transactions, stale customer attributes or broken interfaces.

Architecture diligence should follow representative records end to end. The reviewer should select normal, incomplete, duplicated, late and corrected records, then inspect ingestion, validation, transformation, scoring, case creation, decision, reporting and retention. Control totals should reconcile volumes and monetary values where relevant. Interface failures should create visible exceptions with ownership and ageing. Batch reprocessing and model reruns should preserve the relationship between original and amended results. These tests reveal whether implementation evidence supports the advertised platform model. They also help quantify the engineering and customer-success resources required for a new institution, which affects pricing, gross margin, delivery capacity and the amount of capital required to scale.

## 23. Secure data, privacy and residency

RegTech systems can process identity, transaction, communications, sanctions, fraud and employee data. The security design should apply least privilege, encryption, segregation, logging, vulnerability management, secure development and incident response. Data inventories should state purpose, location, retention, access, transfer and deletion. Sensitive inputs should be minimised where an outcome can be achieved with fewer fields.

Privacy assessment should connect legal basis, purpose limitation, transparency, individual rights and automated decision safeguards to actual product workflows. Cross-border architecture should reflect applicable localisation and transfer requirements. Customer contracts should identify

controller and processor roles, approved subprocessors, breach duties, audit rights and exit assistance.

Security evidence should include independent testing, remediation records, access reviews, continuity exercises and customer due-diligence responses. Certifications can support assurance, although scope and exclusions matter. A financing diligence team should test whether security capability scales with customer count and regulatory criticality.

The review should connect security claims to the deployed product boundary. It should identify environments, code repositories, cloud accounts, service identities, secrets, encryption keys, logging destinations and subprocessors. Open high-severity findings require owners, mitigations and dates. Customer-specific deviations should be visible because they can expand support cost and liability. Incident exercises should involve executives, engineering, compliance, legal and communications, with evidence that lessons were implemented. Cyber insurance terms should be reconciled with contractual commitments and known exclusions. These records allow investors to assess whether security is an operating capability that protects enterprise revenue or a collection of documents assembled for procurement.

## 24. Control third-party and operational resilience risk

DORA establishes detailed requirements for ICT risk management, incident handling, resilience testing and third-party risk for in-scope European financial entities. Similar expectations appear through operational-resilience and outsourcing regimes in other markets. RegTech vendors should expect customers to assess concentration, subcontracting, location, recovery, audit access and termination.

The vendor inventory should include cloud, data, model, identity, communications and specialist-service dependencies. Each dependency should have an owner, service commitment, continuity plan, substitutability assessment and exit route. Material incidents should be classified, investigated and used to strengthen controls. Recovery claims should be demonstrated through tests rather than policy text.

Contract design should align obligations with technical reality. Unlimited audit promises, impractical notification windows or unsupported recovery commitments create latent liability. Durable companies integrate legal, security and engineering review before accepting enterprise terms.

Concentration analysis should extend beyond revenue. A company may have diversified customers yet depend on one cloud region, model provider, data feed, screening list, integration partner or specialist employee. The reviewer should map dependency to affected products, customers, contractual promises and recovery paths. Exit tests should estimate time, data portability, revalidation and customer consent. Where substitution is impractical, the forecast should fund resilience and the valuation should reflect correlated downside. Customer audit findings can be analysed as a forward indicator: recurring findings in access, change, continuity or subcontracting suggest systemic cost and renewal risk. Closing findings with independently supportable evidence strengthens both operational resilience and financing credibility.

## 25. Prove durable buyer demand

Durable demand begins with a recurring obligation, risk or operating burden that senior management funds. Evidence should connect regulation or control need to a named workflow, current cost, adverse outcome, buyer, budget and decision timetable. The strongest proof is paid production use with measured outcomes, renewal and expansion.

Management should segment demand by problem, institution type, geography, deployment model and regulatory intensity. A product that succeeds in transaction monitoring may not transfer directly to prudential reporting or conduct surveillance. The sales thesis should identify which parts of the product, data model and evidence pack are reusable.

Independent customer interviews should test urgency, alternatives, implementation barriers, willingness to pay, procurement authority and renewal logic. Interview design should avoid leading questions. Responses should be reconciled with contracts, usage data, support records and observed purchasing behaviour.

Demand research should distinguish mandated activity from vendor-specific demand. A financial institution may need to perform a control while choosing an internal build, incumbent module, consultancy or manual process. The addressable market therefore depends on switching conditions, data access, implementation economics and buyer confidence. Management should build a bottom-up account universe with named institution types, relevant workflows, likely owners and observable triggers. Each account should have a reasoned contract range and adoption probability. Market reports can provide context; they should not substitute for account evidence. Sensitivity should test slower displacement, lower price, partner margin and longer local validation. This approach produces a financing narrative linked to executable sales work.

**Table 3. Durable-demand evidence ladder**

| Evidence level | Typical evidence | Financing interpretation | Required diligence |
|---|---|---|---|
| Interest | event engagement, inbound enquiry or non-binding discussion | early signal only | confirm buyer, problem and budget |
| Evaluated need | documented workflow and quantified baseline | problem appears material | validate baseline and alternatives |
| Controlled pilot | agreed success measures, data access and sponsor | product can be tested | inspect cohort, governance and completion |
| Paid production | signed contract, acceptance and live use | commercial proof exists | reconcile revenue, usage and outcomes |
| Renewal and expansion | renewed term, additional users or workflows | durability is emerging | assess retention, pricing and concentration |
| Referenceable outcome | independently supportable operational improvement | stronger repeatability evidence | test attribution and transferability |

*Evidence strength should be tested against underlying customer, contract, product and accounting records.*

## 26. Analyse customer cohorts and renewal

Cohort analysis should follow customers from qualified opportunity through pilot, production, renewal, expansion and churn. Measures should include contract value, implementation duration, time to first value, active use, support effort, gross margin, renewal timing and expansion. Results should be segmented by product, institution size, geography and deployment architecture.

Renewal quality matters more than a headline retention rate. Automatic renewals, short extensions, price concessions and unresolved remediation should be visible. Gross revenue retention should exclude expansion; net revenue retention should reconcile expansion and contraction. Customer concentration and correlated regulatory exposure should be reported separately.

Churn analysis should classify product failure, implementation failure, budget change, regulatory change, consolidation, insourcing and competitive loss. Each category implies a different corrective action and forecast assumption. A small cohort should be presented with appropriate caution and underlying records.

Cohort quality should also reflect use. Login counts may be irrelevant when systems operate through automated interfaces. Product teams should identify workflow-specific adoption measures such as transactions assessed, cases reviewed, reports generated, obligations mapped, exceptions resolved and evidence retrieved. Measures require denominators and expected frequency. Low use can signal process change, poor integration, weak adoption or a valid reduction in activity. Customer-success records should explain the cause. Renewal forecasting should combine contract date, usage, outcome, sponsor status, open incidents, remediation and procurement progress. A documented renewal health process gives the board earlier warning than aggregate annual recurring revenue and supports a more defensible cash forecast.

## 27. Price for outcome and contract durability

Pricing may use subscription, institution tier, transaction volume, monitored entity, user, module, implementation or outcome-linked components. The metric should align value, cost and buyer budgeting without creating unstable bills. Minimum commitments can fund capacity; transparent overage rules can support expansion.

Contracts should define scope, data, acceptance, service levels, change control, support, security, intellectual property, regulatory cooperation, liability, termination and exit. Regulatory-change clauses should distinguish ordinary product maintenance from customer-specific work. Price escalation and renewal windows should be operationally manageable.

Outcome pricing requires a defensible baseline and attribution. Avoided losses and prevented fines are difficult to prove. Measured analyst time, case throughput, false-positive reduction and reporting cycle time are more auditable when controls remain effective. Hybrid pricing can combine platform access with bounded implementation or performance components.

Price diligence should reconstruct realised economics from order form to cash. Reviewers should capture contracted recurring fees, implementation, usage, credits, discounts, free periods, partner share, foreign exchange, invoicing, acceptance and collection. The analysis should identify side letters and customer-specific obligations. Annualised recurring revenue definitions should exclude non-recurring items and reflect cancellations or material concessions. Renewal increases

should be compared with delivered value and procurement tolerance. A product can show strong booked revenue while weak acceptance or extended payment terms consume cash. The financing model should therefore link price, delivery milestone, invoice date and expected receipt at customer level.

## 28. Build RegTech unit economics

Unit economics should include implementation labour, cloud and model cost, data licences, customer support, security assurance, validation and partner fees. Gross margin should be shown before and after capitalised development policies where relevant. Contribution margin should reflect the real resources required to acquire, implement and serve an enterprise account.

**Table 4. RegTech unit-economics bridge**

| Measure | Formula | Evidence source | Investor question |
|---|---|---|---|
| Acquisition cost | sales and marketing cost divided by new production customers | general ledger and CRM | does long procurement create excessive payback? |
| Implementation contribution | implementation revenue less delivery labour and external cost | project ledger | is deployment repeatable or bespoke? |
| Product gross margin | recurring revenue less hosting, data and direct support | billing and cost allocation | does scale improve economics? |
| Gross retention | retained recurring revenue divided by opening recurring revenue | contract and invoice records | is the compliance need durable? |
| Expansion rate | cohort expansion divided by opening cohort revenue | contract history | does value grow across workflows? |
| Cash payback | acquisition and implementation cash cost divided by contribution | reconciled cash model | can the company finance growth? |

*Definitions and allocations should reconcile to customer-level and accounting evidence.*

Management should reconcile each metric to accounting records and customer-level data. Allocation methods should be consistent and disclosed. Sensitivity should cover lower conversion, delayed go-live, higher model cost, security remediation and slower collection.

Unit-economics interpretation should consider maturity. Early customers may require deliberate learning investment, yet management should show which work becomes reusable and when. Engineering effort should be classified between core product, reusable integration and customer-specific delivery. Support tickets should be mapped to cause and customer cohort. Cloud and model costs should be measured per relevant workload and stress-tested for growth, retention and provider pricing. Customer acquisition cost should include enterprise subject-matter participation, pilots and partner commissions. Payback should begin when cash is spent and use collected contribution. These definitions provide a conservative view of financing need and allow future performance to be compared with the investment case.

## 29. Measure procurement conversion

The pipeline should record dates for qualification, pilot approval, data readiness, security clearance, model review, commercial approval, signature, implementation, acceptance and production. Stage conversion and time should be calculated by cohort. Forecasts should distinguish committed backlog, contracted implementation and probability-weighted pipeline.

Loss reasons should be recorded consistently. Common categories include no budget, no sponsor, integration burden, security concern, model-governance concern, competing priority, incumbent extension and failed outcome. Management should review whether losses concentrate in a product, geography or buyer type.

Cash planning should incorporate legal and procurement delay, milestone billing, acceptance conditions and payment terms. Revenue recognition and cash collection can differ materially. Financing runway should use downside cycle times and delivery capacity.

Pipeline governance should include periodic back-testing. Opportunities predicted to close in a prior quarter should be traced to signature, loss or continued delay, with reasons. Stage probabilities should be updated from the company's evidence rather than inherited software defaults. Large opportunities should receive individual scenarios because a single delay can affect runway. Partner-sourced pipeline requires confirmation of customer access and commercial rights. The board should see coverage by expected close period, implementation capacity and cash receipt, as well as total nominal value. This creates a direct link between selling activity, delivery constraints and financing risk.

## 30. Prove implementation and time to value

Implementation should begin with a jointly approved plan covering data, controls, configuration, testing, training, acceptance and go-live. The baseline should be measured before intervention. Success measures should include control quality and operating outcome. A faster process with weaker detection or incomplete reporting is not a successful implementation.

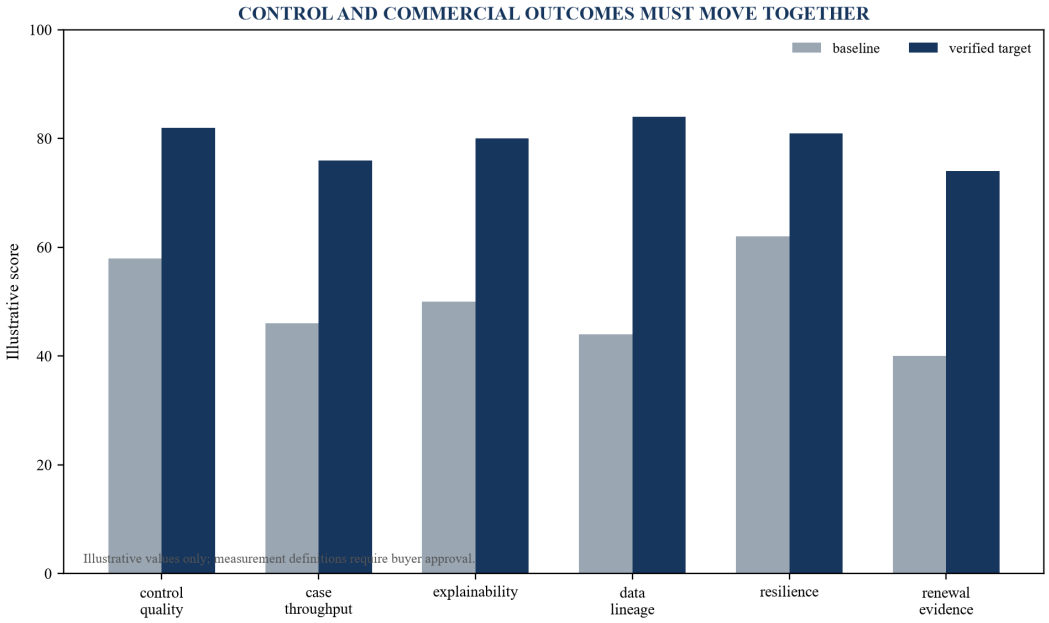
Time to value should be measured from contract, data availability and implementation start, since each reveals a different delay. Product readiness and customer readiness should be separated. Post-go-live review should confirm adoption, defects, override patterns, control performance and realised benefit.

Reusable playbooks, prebuilt connectors, test data, evidence templates and role-based training can reduce variation. Investors should inspect the distribution of implementation duration and cost rather than a selected showcase.

Acceptance design should identify who approves each deliverable and what evidence constitutes completion. Ambiguous acceptance can defer invoicing and create disputes. The implementation plan should include data-quality remediation responsibilities, since vendor schedules often depend on customer data and access. Change requests should record scope, cost and timetable. After go-live, a stabilisation period should track defects, workflow exceptions, user competence and control performance. Management can then compare estimated and actual effort, improve pricing and update capacity assumptions. Investors should sample both successful and difficult deployments because dispersion reveals the scalability of the operating model.

## 31. Build a product outcome scorecard

**Figure 3. RegTech product outcome scorecard**



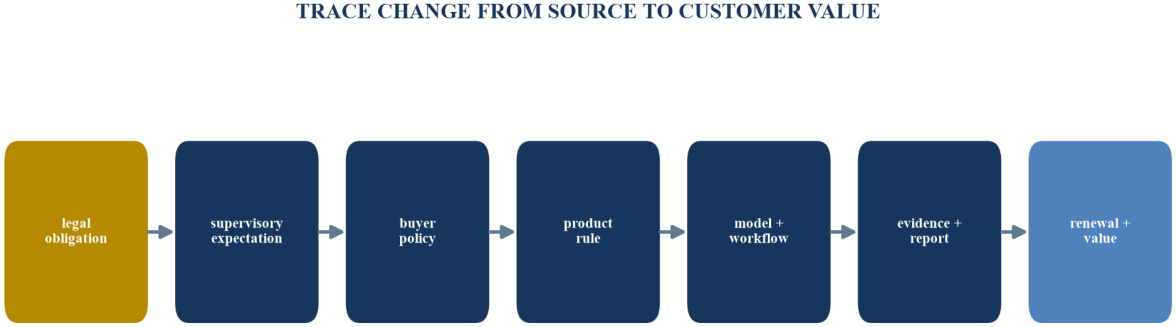

*Illustrative scores; replace with controlled customer evidence and approved thresholds.*

The scorecard should combine control effectiveness, operational performance, governance, resilience and commercial durability. Each measure needs an owner, definition, source, frequency, threshold and exception process. Composite scores should retain access to underlying measures.

Outcome governance should prevent selective reporting. Baselines, exclusions and changes should be documented. Customer attestations and independent review can strengthen evidence where permitted. The scorecard should feed product priorities, customer reviews and financing diligence.

## 32. Map regulatory dependency

**Figure 4. Regulation dependency map**




*Illustrative structure for assessing product exposure to regulatory and buyer-control change.*

The dependency map should show which obligations, interpretations, policies, rules, data and evidence support each product capability. Change impact should be traceable through this chain.

A regulatory amendment can create demand, require product investment, reduce relevance or alter liability.

Revenue concentration should be tested against common dependencies. Customers in different countries can remain exposed to the same cloud provider, model, regulatory concept or workflow. Scenario analysis should include delayed implementation, divergent rules, withdrawn guidance and buyer insourcing.

## 33. Assess competition, differentiation and intellectual property

Competition includes software vendors, consulting firms, data providers, incumbent platforms, internal teams and manual processes. Comparison should cover control outcome, data access, implementation effort, evidence quality, governance, resilience, total cost and switching. Feature lists alone do not demonstrate advantage.

Differentiation may arise from trusted data, domain workflow, validated models, integration assets, customer evidence, regulatory knowledge, distribution or operating execution. Each claim should be tied to a measurable result and tested for replicability. Proprietary terminology has limited value without protected capability or accumulated evidence.

Intellectual-property diligence should cover ownership, employee and contractor assignments, open-source obligations, licences, training data, third-party models and customer-specific developments. Freedom-to-operate analysis should focus on the product's actual markets and technical implementation.

## 34. Test transfer across products and geographies

Expansion should begin with an adjacency map. A new country may require different source law, supervisory practice, language, data residency, customer process and certification. A new workflow may require different labels, outcomes and buyers. Management should identify reusable platform components and localised components.

Transfer evidence should come from completed implementations, not assumed market size. Pilot cohorts should measure configuration effort, validation performance, procurement time, support burden and willingness to pay. The forecast should fund local expertise and regulatory maintenance.

Partnerships can accelerate distribution and implementation, although incentives, control ownership and margin sharing require diligence. The company should retain enough direct customer evidence to understand product value and avoid dependence on a single channel.

## 35. Build the operating forecast

The forecast should connect opportunity cohorts to procurement timing, implementation capacity, acceptance, billing, revenue recognition, collection, renewal and expansion. Headcount should follow delivery and governance requirements. Cloud, data, security, insurance and regulatory-maintenance costs should scale transparently.

Scenarios should include base, delayed-procurement and control-remediation cases. Drivers should be explicit: qualified opportunities, stage conversion, cycle time, contract value, implementation duration, gross retention, expansion, direct cost and collection days. Historical

actuals should reconcile to the ledger.

Cash runway should include working capital and restricted commitments. Growth can consume cash when enterprise sales and implementation precede collection. A funding request should state the milestones the capital is expected to achieve and the downside actions management can execute.

## 36. Construct the valuation bridge

Valuation should begin with verified revenue quality and cash economics. Recurring contract value should be adjusted for implementation dependence, concentration, cancellation rights, unresolved acceptance, price concessions and collection. Growth should be assessed alongside retention, margin and acquisition payback.

The bridge should then consider governance and liability. Strong evidence lineage, model control, security, resilience and regulatory maintenance can reduce execution risk. Control weaknesses, unbounded contractual exposure and dependency concentration can reduce value or defer financing.

Market multiples can inform a range when comparability is documented. Discounted cash flow and scenario methods can expose driver sensitivity. The conclusion should present a range with explicit assumptions rather than a single precise number unsupported by evidence.

**Table 5. RegTech valuation and financing bridge**

| Driver | Value-supporting evidence | Downside evidence | Diligence response |
|---|---|---|---|
| Recurring demand | paid production, renewal and expansion | pilot dependence or budget uncertainty | cohort and contract review |
| Control outcome | repeatable quality and efficiency improvement | selective or unaudited claims | baseline and outcome testing |
| Product economics | improving margin and cash payback | bespoke implementation burden | customer-level contribution analysis |
| Governance | traceable rules, models and decisions | weak lineage or unsupported automation | control walkthrough and sample testing |
| Resilience | tested continuity and manageable dependencies | concentration and untested exit | architecture and third-party review |
| Liability | bounded, insurable and operationally supported terms | uncapped or impractical commitments | legal and claims diligence |

*Valuation conclusions require explicit assumptions, reconciled evidence and scenario sensitivity.*

## 37. Structure financing scenarios

Equity can fund product development, governance, enterprise sales and expansion when milestone timing is uncertain. Venture debt can extend runway where recurring revenue, retention and cash visibility support repayment. Receivables or contract-backed facilities may fit strong counterparties and enforceable payment claims. The instrument should match cash generation and downside risk.

Financing scenarios should test amount, timing, dilution, interest, amortisation, covenants, security and follow-on need. Debt capacity should use downside collections and operating cash,

not only annualised recurring revenue. Equity scenarios should show milestone-based value creation and capital required to reach the next credible financing point.

Investors should receive a use-of-funds bridge from opening cash through hiring, implementation, control investment, working capital and contingency. The plan should preserve resources for regulatory and security obligations that cannot be deferred safely.

## 38. Prepare the financing data room

The data room should contain corporate records, capitalisation, intellectual property, product architecture, source and model governance, security, resilience, regulatory analysis, contracts, customer cohorts, pipeline, implementation records, outcome evidence, financials, tax, employment and disputes. Each claim in the investment narrative should link to supporting evidence.

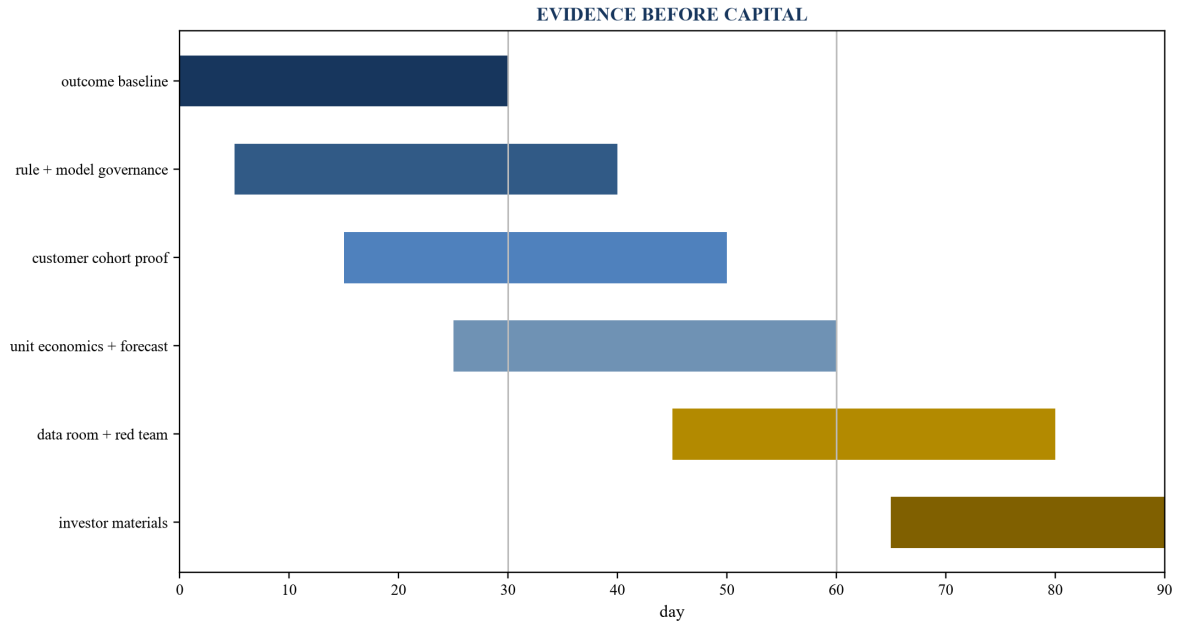
Customer data should be minimised and access-controlled. Sample evidence can be anonymised where appropriate while preserving auditability. A disclosure log should identify limitations, open remediation and management assumptions. Consistent filenames, dates, owners and version control reduce diligence friction.

Management should run a red-team review before launch. The team should test revenue reconciliation, pipeline probability, model ownership, open-source use, data rights, contractual liability, security remediation, regulatory dependencies and forecast sensitivities.

The data room index should state document owner, period, status and relationship to the investment case. Management explanations should be separated from primary records. Open questions should be logged with response date and supporting document. Historical versions may be needed to explain changes in metrics, contracts or models. Customer confidentiality should be protected through redaction and controlled access without removing information required for diligence. The company should prepare reconciliations for recurring revenue, bookings, pipeline, cash, headcount and capitalisation before investor review. These controls reduce avoidable delay and help all parties focus on material commercial, technical and governance decisions.

## 39. Run a ninety-day readiness sprint

**Figure 5. Ninety-day RegTech financing-readiness milestones**




*Illustrative sequencing; timing depends on company evidence, governance and transaction scope.*

Days 1–30 establish the baseline, obligation map, model inventory, customer cohorts and evidence gaps. Days 31–60 complete outcome testing, unit economics, forecast scenarios, contract review and remediation priorities. Days 61–90 assemble the data room, conduct red-team diligence and prepare decision-useful financing materials.

The sprint should have an accountable executive, weekly evidence review and explicit completion criteria. Material defects should remain visible with owners and dates. Readiness means the company can support its claims and manage identified risks through the financing process.

## 40. Conclusion

RegTech financing quality depends on the chain from obligation to controlled workflow, measurable outcome, durable contract and cash value. Products should demonstrate effective controls, reliable data, governed models, accountable decisions, secure integration and tested resilience. Commercial evidence should demonstrate buyer authority, procurement progression, paid production, renewal and contribution economics.

The framework in this paper gives founders, boards and investors a structured diligence path. It separates attractive demonstrations from financeable operating systems. A company that can reconcile its claims to customer, control, product and financial records is better prepared for equity or debt discussions and for the responsibilities that follow growth.

Board oversight should continue after a financing. Management should report control outcomes, customer cohorts, procurement conversion, implementation dispersion, security remediation, model changes, regulatory dependencies, contribution economics and cash against the approved case. Financing milestones should be defined as evidence-backed operating achievements rather than expenditure alone. Where performance diverges, the company should identify cause, corrective action, accountable owner and cash consequence. This discipline gives capital providers a clearer view of execution and helps management allocate scarce resources to product reliability, customer value and durable growth. It also supports responsible expansion because

commercial ambition remains connected to the compliance outcomes the product is designed to improve.

Evidence quality should remain central to every financing decision.

The board should also maintain an integrated evidence register. Each material commercial claim should identify its owner, definition, source record, measurement period, approval and known limitation. Claims about detection, productivity, renewal, gross margin, market demand and pipeline should be reproducible from controlled records. When a definition changes, management should preserve the prior basis and explain the effect. This prevents inconsistent investor materials and supports more reliable decision-making inside the company.

Financing diligence should test the complete value chain through samples. A customer sample should connect signed terms, implementation work, production acceptance, system use, control outcome, invoice, cash receipt and renewal. A product sample should connect authoritative obligation, configured rule, data, model version, decision, reviewer action and evidence output. A forecast sample should connect a named opportunity to stage evidence, expected implementation capacity, billing milestone and cash timing. Exceptions should be evaluated for frequency, materiality and systemic cause.

Management should translate the results into a prioritised action plan. Critical items include unsupported control claims, data-rights gaps, model ownership uncertainty, unresolved security findings, concentrated dependencies, unbounded contractual exposure and forecasts that do not reconcile to capacity or cash. Each item should have a decision, owner, funding requirement and completion evidence. Some issues may require remediation before financing; others can be disclosed and reflected in structure, valuation or use of funds.

This approach also improves strategic choice. Evidence may show that the best path is deeper penetration of a proven workflow, a partner-led geographic expansion, a narrower product perimeter or a delayed debt raise until collections mature. The financing decision should follow the operating evidence. A disciplined RegTech company can then present a coherent proposition: a material compliance problem, a controlled and repeatable solution, verified buyer outcomes, durable revenue, manageable risk and a credible path from invested capital to cash value.

Post-transaction reporting should preserve the same definitions and reconciliations used during diligence. Investors and management can then compare actual customer conversion, implementation, outcomes, retention, contribution and cash with the approved case. Variances should lead to timely operating decisions and transparent capital allocation. This continuity turns financing diligence into a durable management system rather than a temporary transaction exercise.

## References


[1] Central Bank of the UAE, Guidance Note on Consumer Protection and Responsible Adoption and Use of Artificial Intelligence. https://rulebook.centralbank.ae/en/rulebook/guidance-note-consumer-protection-and-responsible-adoption-and-use-artificial-intelligence

[2] Central Bank of the UAE, Transaction Monitoring. https://rulebook.centralbank.ae/en/rulebook/82-transaction-monitoring

[3] Central Bank of the UAE, Automated Transaction Monitoring Systems. https://rulebook.centralbank.ae/en/rulebook/82-automated-transaction-monitoring-systems

[4] Central Bank of the UAE, Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening. https://www.centralbank.ae/media/f0ofufub/guidance-for-licensed-financial-institutions-on-transaction-monitoring-and-sanctions-screening.pdf

[5] Dubai Financial Services Authority, New DFSA AI survey: generative AI adoption has nearly tripled within DIFC. https://www.dfsa.ae/news/new-dfsa-ai-survey-generative-ai-adoption-has-nearly-tripled-within-difc-last-12-months-governance-continues-develop

[6] European Banking Authority, Analysis of RegTech in the EU financial sector. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2021/1015484/EBA%20analysis%20of%20RegTech%20in%20the%20EU%20financial%20sector.pdf

[7] European Banking Authority, EBA assesses benefits, challenges and risks of RegTech use in the EU. https://www.eba.europa.eu/publications-and-media/press-releases/eba-assesses-benefits-challenges-and-risks-regtech-use-eu

[8] European Banking Authority, Opinion on money laundering and terrorist financing risks across the EU financial sector. https://www.eba.europa.eu/publications-and-media/press-releases/eba-identifies-new-types-money-laundering-and-terrorist-financing-risks-and-calls-swift-action

[9] Financial Action Task Force, Opportunities and Challenges of New Technologies for AML/CFT. https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-aml-cft.html

[10] Financial Conduct Authority, RegTech. https://www.fca.org.uk/firms/innovation/regtech

[11] Financial Conduct Authority, Introducing the FCA Handbook API. https://www.fca.org.uk/news/blogs/introducing-fca-handbook-api

[12] Financial Conduct Authority, Digital regulatory reporting. https://www.fca.org.uk/innovation/regtech/digital-regulatory-reporting

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

[14] European Union, Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[15] Information Commissioner's Office, Guidance on AI and data protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

[16] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework. https://www.nist.gov/itl/ai-risk-management-framework

[17] National Institute of Standards and Technology, AI RMF Playbook. https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook

[18] International Organization for Standardization, ISO/IEC 42001 Artificial intelligence management systems. https://www.iso.org/standard/81230.html

[19] Bank for International Settlements, Innovative technology in financial supervision. https://www.bis.org/fsi/publ/insights59.htm

[20] Bank for International Settlements, Generative artificial intelligence in financial supervision. https://www.bis.org/fsi/publ/insights69.htm

[21] Bank for International Settlements, G20 TechSprint 2024. https://www.bis.org/hub/2024_g20_techsprint.htm

[22] Basel Committee on Banking Supervision, Principles for operational resilience. https://www.bis.org/bcbs/publ/d516.htm

[23] Basel Committee on Banking Supervision, Principles for effective risk data aggregation and risk reporting. https://www.bis.org/publ/bcbs239.htm

[24] Financial Stability Board, The Financial Stability Implications of Artificial Intelligence. https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/

[25] Organisation for Economic Co-operation and Development, OECD AI Principles. https://oecd.ai/en/ai-principles

[26] International Valuation Standards Council, International Valuation Standards. https://www.ivsc.org/standards/

## About the Author

Authored by Chennakeshav Adya, Independent Researcher

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

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

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

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