Reimagining KYC: From legacy friction to the pKYC triad

Intelligent, compliant, and scalable – the future of KYC is here

Capgemini

Foreword

We're at a defining moment for financial crime compliance. The traditional Know Your Customer (KYC) model – built on periodic reviews, manual processes, and fragmented systems – is no longer fit for purpose.

Regulatory expectations are rising, financial crime typologies are evolving at pace, and today's digital-first customers demand superior, friction-free experiences. Institutions that cling to static, time-bound models will face spiraling costs, widening control gaps, and reputational risk. The time for incremental change has passed. What's needed now is transformation.

Perpetual KYC (pKYC) represents this revolution. By shifting from calendar-driven refresh cycles to event-driven monitoring – supported by automation and explainable analytics – pKYC delivers a live, always-on view of customer risk. This isn't just a compliance upgrade: it's a structural redesign that strengthens resilience, accelerates onboarding, and improves customer experience.

At the heart of this transformation lies an integrated capability stack: modern data foundations, intelligent automation, and AI-driven analytics. GenAI is the accelerator, enabling the shift from ad-hoc assessments to a dynamic, real-time understanding of risk. The result? A fundamental shift in how institutions detect, understand, and respond to financial crime.

Early adopters are already seeing measurable impact: onboarding times cut by up to 60%, false positives reduced by 40%, and periodic review workloads slashed by as much as 90%. These outcomes translate into sharper risk insight, lower friction, and greater commercial agility – positioning compliance as a business enabler rather than a cost center.

The imperative is clear. Regulators across jurisdictions now require ongoing monitoring and risk-based approaches. Customers expect immediacy and transparency. Institutions that embrace pKYC won't just meet these expectations – they'll lead the pack. By modernizing data foundations, orchestrating workflows, and embedding intelligent analytics, firms can turn compliance from a reactive burden into a proactive, strategic capability.

This report sets out the blueprint: the capabilities that make pKYC real, the regulatory context that demands it, and the roadmap to deliver it. The message is simple: perpetual, intelligence-led KYC is no longer optional. It's the standard by which resilience, trust, and competitiveness will be judged.

The question isn't whether KYC must change – it's whether your organization is ready to lead.

Kartik Ramakrishnan

CEO of Capgemini's Financial Services Strategic Business Unit

Member of the Group Executive Board

Executive summary

Know Your Customer (KYC) is critical when it comes to meeting firms' anti-money laundering (AML) compliance needs and enabling customers to move through their onboarding journeys. The problem? As it stands, the KYC process is no longer fit for purpose.

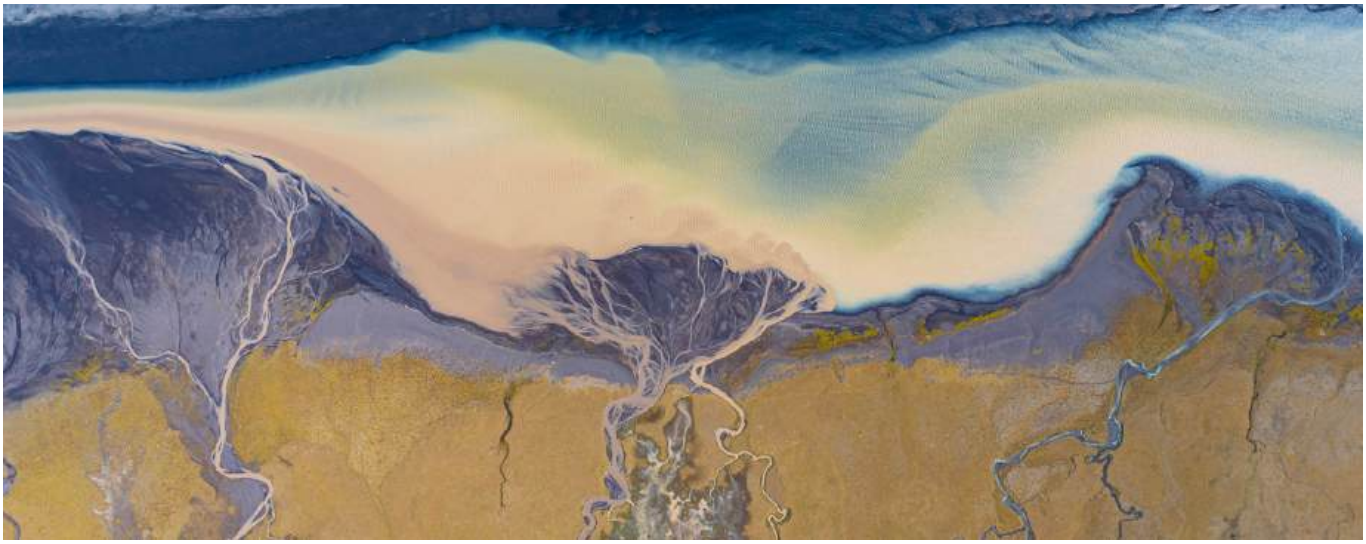
The traditional model, characterized by fragmented systems, manual reviews, and periodic refresh cycles, has become a structural bottleneck. It can't keep pace with growing regulatory expectations, the rising velocity and complexity of financial crime (FinCrime), digital customer demands for ease and immediacy, as well as the sheer volume and complexity of the data now required to manage FinCrime risk. Internally, this results in spiraling costs, stale risk profiles, missed revenue, and inconsistent decisions.

Incremental improvements won't deliver the required impact. Modernizing KYC is a compliance necessity and a strategic differentiator.

In the age of Artificial Intelligence (AI), KYC transformation is no longer constrained by manual review capacity or static rulesets. Advances in machine learning (ML), entity resolution (ER), natural language processing (NLP), and generative AI (GenAI) fundamentally change how customer risk can be understood, maintained, and acted upon. AI lets institutions continuously ingest and reconcile vast internal and external data sets, detect material risk changes as they occur, generate explainable risk narratives, and route actions dynamically – without expanding headcount or sacrificing control. In this model, AI doesn't replace human judgment: it repositions it. This lets analysts focus on interpretation, escalation, and decision making, rather than data gathering and reconciliation.

The bottom line is that AI enables financial institutions to implement a fundamental, needed redesign, namely, a shift to the future of KYC: perpetual KYC (pKYC). This transformation moves the institution from time-based review cycles to an operating model that assesses customer risk in near real time using event-driven data ingestion, automated decisioning, and understandable analytics. Without AI-enabled analytics and automation, pKYC isn't operationally achievable at scale, making AI a prerequisite for modern, risk-based compliance rather than an optional enhancement.

As Dheeraj Maken, Practice Director at Everest Group, notes: "Perpetual KYC is quickly becoming the anchor of modern due diligence as institutions shift from periodic reviews to real-time visibility of customer risk. Early adopters are already demonstrating how continuous monitoring, stronger data foundations, and AI-driven insight can reduce blind spots, remove unnecessary re-papering, and elevate both regulatory confidence and customer experience. pKYC has moved well beyond early experimentation. It is now setting the pace for how institutions will manage financial crime risk in the years ahead."



Early adopters of pKYC are already seeing benefits across the value chain, for example, reducing:

- False positives by 20–40%.[1]
- Onboarding Turnaround Time (TAT) by 40–60%.[2]
- Case backlogs by 50–70%, depending on baseline maturity.[3]

The reduction in TAT is driven not only by compliance efficiencies, but also by materially lower front-office rework, fewer client follow-ups, and improved client experience. Also, Net Promoter Scores (NPS) show increases of 10–15 points within the first year of implementation.

The cumulative benefits of pKYC have the powerful operational impact of removing 70–90% of periodic review work.[4]

As KYC underpins the transaction monitoring, Suspicious Activity Report (SAR) filing, and sanctions screening processes, this transformation also directly affects, in a positive way, the entire AML system.

So, how can organizations move towards this?

Introducing the pKYC triad: the integrated capability stack required to make it real.

- **Data modernization:** a unified, high-integrity data foundation that eliminates re-keying, reconciles identity attributes across systems, and ensures risk signals are accurate, connected, and explainable.
- **Intelligent automation:** workflow orchestration and event-driven processing that compress onboarding cycles, reduce manual touchpoints, and turn previously episodic tasks into streamlined, rules-aligned processes.
- **Intelligent analytics:** AI tools used as controlled co-pilots that accelerate analyst judgment, surface material risks early, and strengthen defensibility.

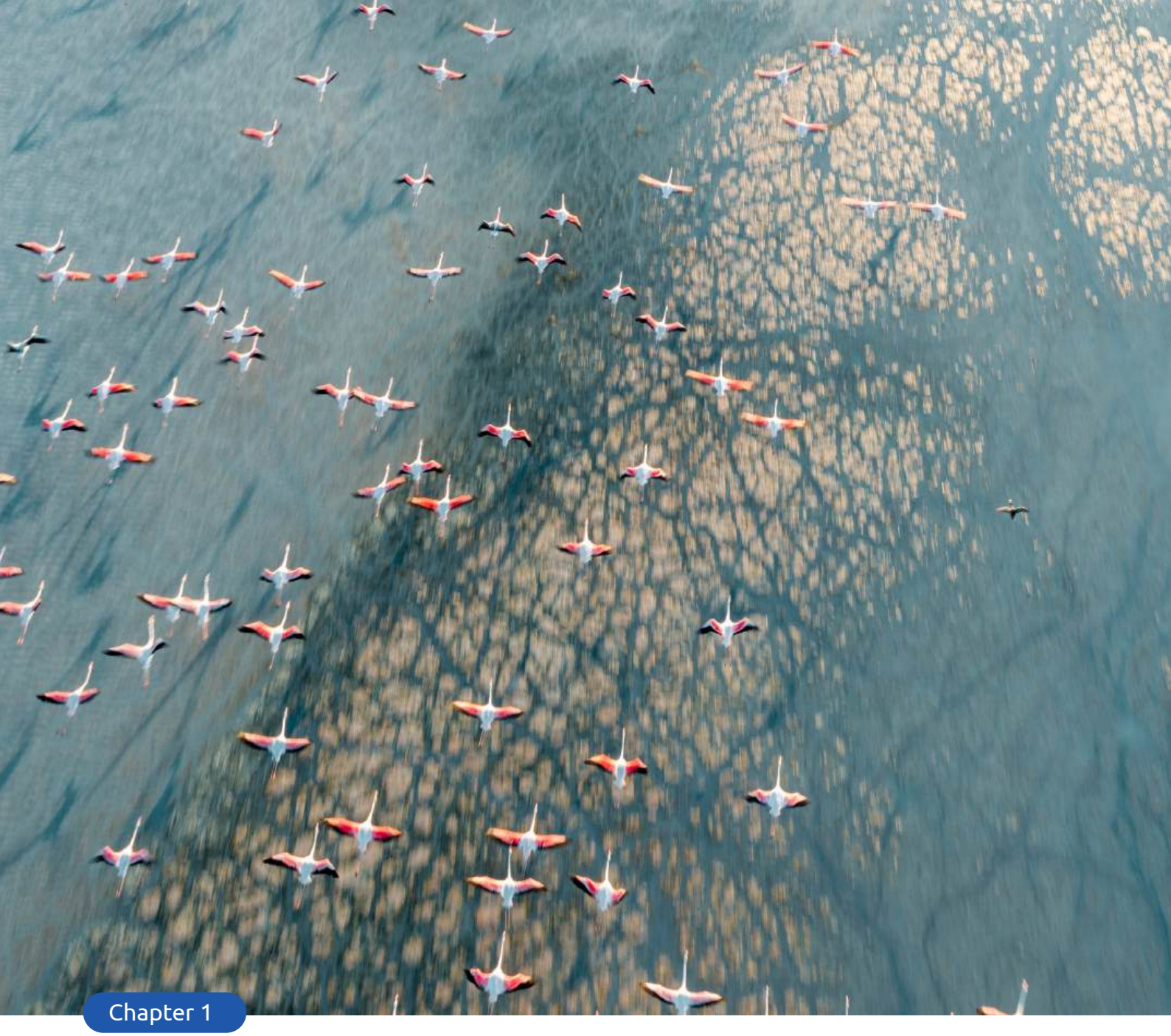
pKYC is a continuous-monitoring operating model that ingests internal and external risk indicators – like beneficial-ownership changes, sanctions updates, adverse-media events, and behavioral anomalies – and routes them through automated workflows supported by explainable analytics. Instead of reassessing a customer every 1–5 years, pKYC maintains a live, always-current view of customer risk.

With these capabilities in place, KYC is transformed from a reactive compliance burden into a proactive, intelligence-led function that detects risk sooner, improves customer experience (CX), and reduces unit cost, all while strengthening regulatory alignment.

Modernizing KYC is a compliance necessity and a strategic differentiator. Institutions that don't embark on this journey will struggle with rising costs and customer friction, widening control gaps, unhappy regulators – who are increasingly vocal that static review models are inadequate – and an operating model that simply can't scale.

Currently, end-to-end pKYC adoption remains limited across the industry. This paper describes the target operating model that financial institutions are converging toward. Later sections delineate how sandbox environments let institutions test pKYC capabilities safely before production rollout.

Table of contents



Chapter 1

The need for KYC transformation

The legacy KYC operating model has reached its functional limits. Structural, regulatory, and customer-driven pressures mean the time for change is now.

Legacy systems are holding organizations back

Each year, tens of billions of dollars are spent on KYC globally. Costs continue to rise as data, screening, and regulatory demands expand. Yet traditional KYC systems are typically siloed, heavily manual, and built on outdated technologies.

Customer onboarding often requires re-entering the same data across multiple systems, which creates multiple, redundant customer touchpoints, inefficiencies, and makes mistakes more likely. Another constant pain point is having to ask customers directly for information – like their ID, source of income, and how they'll use the account – as opposed to being able to gather the data from what can be reasonably derived from external or internal sources and have the customer verify it.

Periodic reviews – the costliest manual AML control – rely on static data and arbitrary time intervals, rather than dynamic risk indicators. The result? Inefficiency and structural fragility. Risks are identified late, resources are misallocated, remediation becomes cyclical, and institutions lose credibility with both customers and supervisors.

10 frictions of legacy AML

Friction	Description
1. Redundant data entry across systems	Customer information is collected, re-keyed, and reconciled across multiple platforms, creating avoidable touchpoints, inconsistencies, and operational load.
2. Periodic refreshes that ignore real risk timing	Reviews happen on fixed annual cycles rather than when risk changes come up. This produces stale profiles, missed red flags, and unnecessary work on low-risk customers.
3. Fragmented data and lack of an authoritative identity record	Disconnected systems force analysts to search, compare, and reconcile attributes manually, undermining accuracy, auditability, and regulatory robustness.
4. Heavy reliance on manual investigation and judgment	Analysts spend most of their time gathering information instead of interpreting it – slowing throughput, inflating costs, and increasing error rates.
5. Inconsistent case handling and decision logic	Variations in analyst experience, local procedures, and undocumented judgment calls produce unpredictable outcomes and weaken supervisory confidence.
6. Excessive, repetitive outreach to customers	Organizations keep asking customers for documents and information they already have or could find themselves, creating friction, abandonment risk, and reputational damage.
7. Slow, siloed escalation paths	Risks surface but fail to trigger timely action because of unclear ownership, fragmented workflows, and reliance on email chains rather than structured orchestration.
8. Static screening and monitoring rules	Rules are often outdated, too broad, or insufficiently calibrated, leading to high false-positive rates and backlogs that hide real risk.
9. Weak data lineage and limited explainability	AML decisions can't be reconstructed cleanly because of poor documentation, hard-to-trace input data, and opaque technology steps – problems amplified under regulatory scrutiny.
10. Expensive remediation cycles	Organizations repeatedly resort to large-scale clean-ups to satisfy regulators, which diverts resources, inflates operational budgets, and reinforces a perpetual state of catch-up.

Market and regulatory drivers

The demand for modern, intelligent KYC systems is rising, thanks to a confluence of market expectations, digital disruption, and compliance mandates.

One critical barrier to fulfilling rising regulatory expectations is the ability to notice and mitigate customer AML risk in a way that's reliable and scalable. Ben Hargreaves, Former General Manager of Financial Crime Compliance (FCC) Operations at Bank of Queensland says, "If a bank doesn't innovate or transform, not only will it be unable to refresh its whole customer base effectively within a timeframe that satisfies its regulators – but it'll never actually finish its KYC reviews. It'll fall into a never-ending cycle."

Meanwhile, institutions are under pressure to reduce cost, scale operations, and adapt to increasingly complex risk scenarios, including Environmental, Social, and Governance (ESG) risk, geopolitical sanctions, and emerging fraud typologies. As they strive to adapt to these complex risk scenarios, they face the parallel pressure of not compromising speed or CX.

Across jurisdictions, supervisors are increasingly explicit that static, time-bound KYC models are misaligned with a risk-based approach. Timeliness and escalation discipline are critical, so material changes in customer risk need to be identified and acted on straightaway.

Changing customer expectations

Customers now expect immediacy, transparency, and continuity – across retail, commercial, and institutional segments. Standards set by digital-first platforms have set a new bar. This means that prolonged onboarding, repeated document requests, and opaque review processes are no longer tolerated as unavoidable regulatory friction. Instead, they're seen as inefficient and frustrating.

As one industry expert notes: "Nowadays, the typical customer doesn't want to use a phone, text, or email to contact its bank – and banks understand that these sorts of interactions leave them vulnerable to fraud. So, institutions have moved rapidly toward non-intrusive, digitally enabled, end-to-end ways of gathering the information they need, and completing onboarding via an app, for example. And, ideally, they want to let the customer finish onboarding in one fell swoop instead of iteratively – which means performing the onboarding in an automated way, without human intervention."

This shift reflects a broader demand for efficiency and coherence in the customer journey. Retail customers accustomed to real-time payments and instant verification expect identity checks to be fast, intuitive, and minimally disruptive. Corporate and institutional customers – often operating under their own regulatory and commercial pressures – expect the same: single points of data entry, a clear onboarding status, and rapid clearance to transact. In both cases, static, periodic KYC models struggle to meet expectations shaped by constant digital interaction.

At the same time, a one-size-fits-all approach to digitization is neither realistic nor desirable. As noted by another industry expert, "In particular, less sophisticated customers, and ones who have been with an institution for a long time, may struggle to understand the new informational requirements. So, it's critical to constantly evolve the data-gathering process to smooth the customer experience, and for relationship managers to work to educate them on the institution's regulatory compliance requirements." Effective KYC transformation requires flexibility and keeping human-led engagement where it's needed, while reducing unnecessary friction elsewhere.

These expectations aren't limited to retail banking. Corporate and institutional clients demand the same efficiency and clarity in how financial institutions verify identity and establish trust. As observed by Alex Ford, Chief Revenue Officer at Encompass, "Seamlessly verifying who you're doing business with on the corporate or institutional side – and establishing trust with them – is a North Star objective for the industry."

pKYC in a nutshell

Although KYC and AML processes are rarely welcomed by customers, they sit at the heart of CX. When they're slow, repetitive, or inconsistent, the institution appears bureaucratic. On the flipside, when they're timely, intelligent, and explainable, they reinforce confidence and trust. pKYC enables this shift by embedding compliance into the natural flow of customer interactions – allowing identity confirmation and risk reassessment to occur contextually, rather than as disruptive, standalone exercises.

As institutions migrate customers away from legacy platforms toward unified digital environments, KYC becomes less of an interruption and more of an integrated capability. In this model, information is captured once, reused intelligently, and refreshed only when risk changes. The result is a compliance framework that supports regulatory obligations while aligning with modern expectations for speed, clarity, and continuity across the customer lifecycle.

Strategic benefits and an irrefutable business case

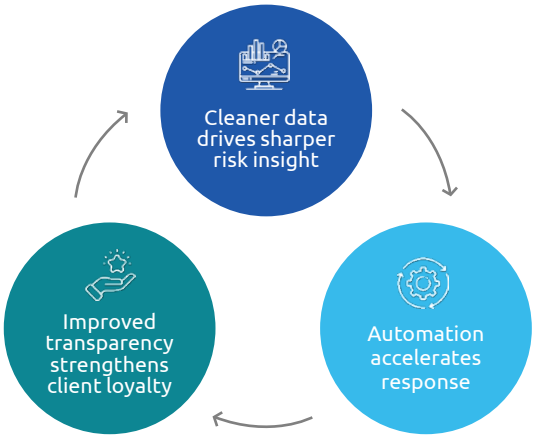
By moving away from periodic, manual refresh cycles and toward more adaptive, risk-based practices, institutions gain a view of risk – one marching ever-closer to true real time – that strengthens both regulatory control and commercial agility. The modernized operating model reduces dependency on costly remediation cycles, and lets compliance teams spend their time on higher value work.

As noted above, pKYC transformation delivers a tangible Return on Investment (ROI) that translates into meaningful financial impact through lower operational expenditure, faster customer activation, and reduced revenue leakage from abandoned onboarding journeys.

Beyond these measurable efficiencies, the broader ROI lies in resilience – fewer regulatory findings, reduced capital drag from compliance buffers, and enhanced customer trust.

Each improvement reinforces the next.

The pKYC improvement loop



Together, these benefits and outcomes reposition compliance from a reactive cost center into a strategic capability – one that protects, enables, and differentiates the institution in an environment of constant regulatory and competitive change. They show that pKYC is a major step-change in how risk, cost, and growth are simultaneously managed.

Data management improvements are critical

As many industry leaders have observed: you're only as good as your data. Without authoritative identity data, lineage, and interoperability, no future-state KYC model – however well it's designed – can operate effectively. This calls for modernizing data foundations.

Key takeaway

Transformation is underway. Firms already modernizing their KYC systems are cutting costs, catching risks sooner, and delivering smoother customer onboarding.

Chapter 2

pKYC as the transformational goal

Conceptually, pKYC can be understood as a closed loop: signals enter, logic evaluates, actions execute, and risk is recalibrated. But unlike periodic reviews, the loop never resets – it tightens as new data arrives. This is a structural redesign of how customer risk is understood, maintained, and acted on across the lifecycle. It's a shift towards a live, always-on understanding of risk.

One consolidated risk profile

This provides a consolidated view of customer-level FinCrime risk by integrating KYC, transaction-monitoring, sanctions, and adverse-media data into one, continuously refreshed risk profile. "This unified perspective helps institutions detect emerging threats in near real time and allocate investigative resources more efficiently," says Jason Shane, Head of Strategy & Innovation for Financial Services at SymphonyAI.

This isn't to say that financial institutions should abandon their classification of customers into high-, medium-, and low-risk buckets. Why? Because this categorization is still a useful way to understand and triage risk actions. Under pKYC, these risk tiers remain as prioritization lenses, but no longer dictate fixed review cycles.

pKYC uses internal and external information – combined with ongoing monitoring – to capture and address immediate risk signals. This includes changes in beneficial ownership, sanctions updates, adverse media hits, odd transactions, SAR filings, or other anomalies in customer behavior. For example, pKYC's non-stop data ingestion lets institutions capture sanctions list updates and other critical, restricted-party changes in near real time, making sure emerging risks are identified promptly and helping prevent inadvertent sanctions violations before they crystallize into serious compliance breaches. As one expert notes, "This brings a much more mature, holistic articulation of the risk presented by different cohorts of customers and the products, services, and geographies attendant to them."

A dynamic model doesn't just strengthen FinCrime prevention – it also aligns directly with global regulatory expectations emphasizing risk-based, ongoing due diligence. "Perpetually understanding your customer," observes Ben Hargreaves, "is now the lifeblood of a satisfactory AML program."

How pKYC impacts onboarding

A pKYC framework enhances the onboarding process itself, acting as a more effective gatekeeper to keep bad actors out. By fusing data from external intelligence sources, entity-resolution tools, and adverse-media analytics even before account opening, pKYC lets institutions identify hidden linkages or early-stage risk indicators that might otherwise only come up during periodic reviews.

Brian Ferro, Global Director of Product Management for Anti-Financial Crimes at SymphonyAI, says, "Beyond strengthening onboarding and refresh, a mature pKYC framework also helps institutions decide if and when to restrict or exit customer relationships." By integrating internal risk signals, adverse-media developments, sanctions hits, and behavioral anomalies, pKYC enables early, evidence-based determination of when a client's residual risk exceeds the institution's appetite – supporting defensible, data-driven debanking decisions that are transparent to both compliance teams and senior management.

From separate to orchestrated

At its core, pKYC is an orchestration system. Triggers enter, logic processes them, and specific actions follow: update attributes, escalate, request evidence, or re-score risk. This replaces the batch-driven, calendar-driven, and manual processes of traditional KYC.

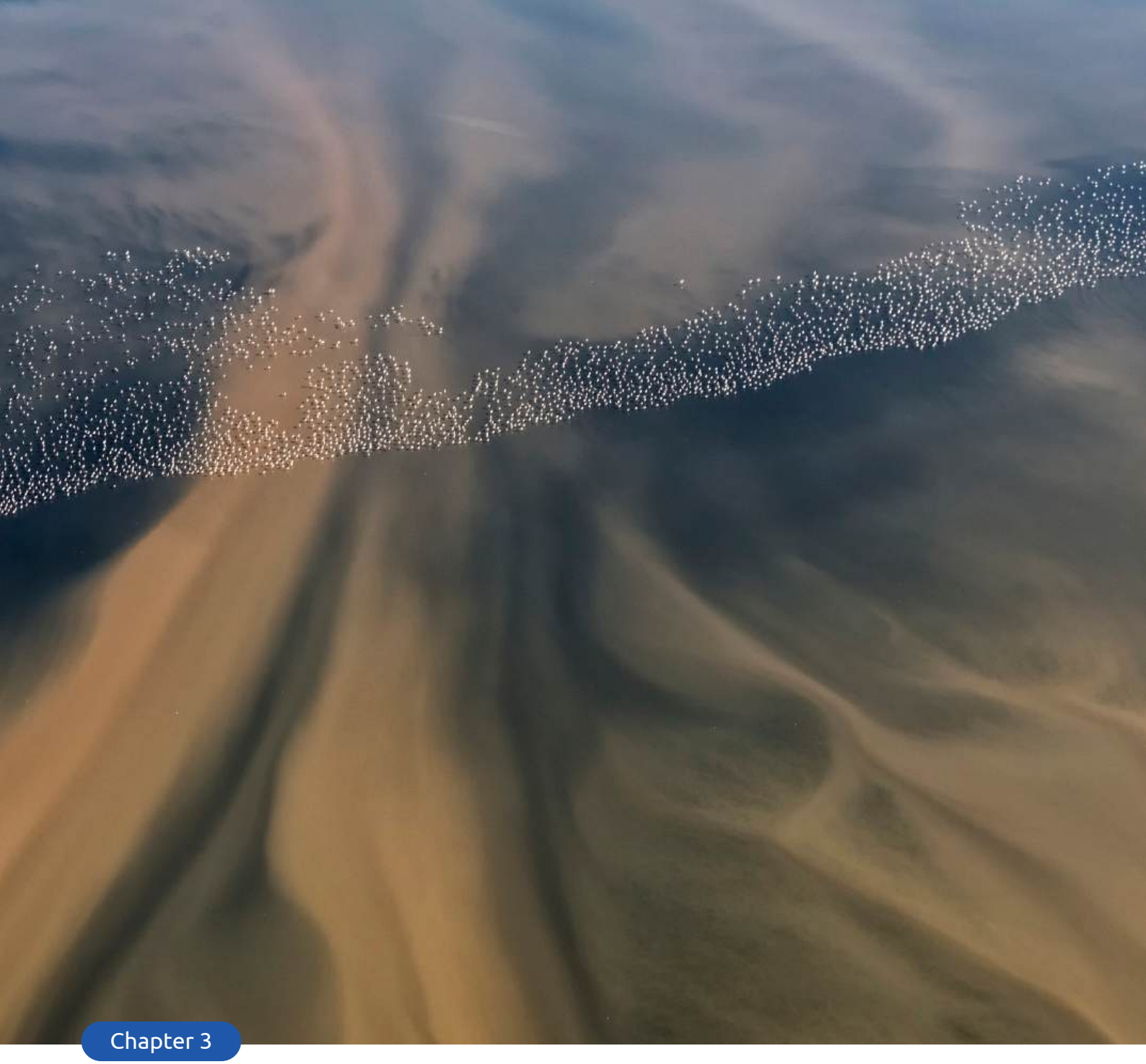
The richness of KYC data provides prompt points for new business opportunities. One industry leader offers an example: "If there's a change in a director or beneficial owner of a legal entity customer, this should prompt a discussion with the customer to understand what may change in terms of the offerings we can provide."

Myths vs realities of pKYC

Myth	Reality
1. pKYC is just "faster periodic reviews"	pKYC essentially replaces periodic reviews entirely. It isn't just speeding up an old model – it's a structural shift from calendar-based assessments.
2. pKYC eliminates the need for risk tiers	Risk segmentation is still essential. pKYC strengthens it by making sure a customer's risk tier reflects present conditions, not historical snapshots. pKYC also distinguishes between mandatory triggers that require action and contextual signals that inform risk scoring and analyst judgment. It replaces fragmented, calendar-driven KYC processes with a single operating model in which risk signals trigger defined actions in near real time.
3. Straight-Through Processing (STP) = pKYC	While STP is an essential enabler of modern KYC, the two aren't synonymous. STP focuses on operational efficiency – reducing manual touchpoints through deterministic automation, workflow orchestration, and clean data flows. By contrast, pKYC is a risk-management paradigm that requires dynamic triggers, continuous ingestion of internal and external signals, event-driven refreshes, explainable risk narratives, and near real-time escalation paths. An institution may achieve high levels of STP but still operate a fundamentally static, periodic review model. As Alex Ford says, "STP accelerates the process, but pKYC changes the process."
4. pKYC is an analytics project	pKYC is an operating model redesign that embeds automation, governance, explainability, and cross-functional alignment – not just new technology.
5. pKYC increases regulatory exposure	External regulators and supervisors increasingly expect ongoing monitoring. pKYC strengthens a firm's defenses by making decisions traceable, timely, and evidence based.

Key takeaway

In short, pKYC replaces static, calendar-based reviews with a continuously updated, unified view of customer risk, so institutions can detect changes and act in near real time. By orchestrating signals across KYC, transactions, sanctions, and media data, it strengthens onboarding, monitoring, and decision making through a dynamic, always-on risk model.



Chapter 3

The pKYC triad: The capability stack that makes pKYC real

pKYC is a finely tuned, tightly integrated stack where data, automation, and analytics components work in harmony. Institutions that try to modernize without this truly integrated foundation will inevitably discover that partial transformation can't overcome the frictions of legacy KYC.

The pKYC triad – data modernization, intelligent automation, and intelligent analytics – forms the operating core of the perpetual model. Each element is necessary, but insufficient on its own. Together, they create a durable, regulator-ready framework that detects risk faster, reduces operational burden, strengthens defensibility, and improves CX.

Data modernization: The foundation of trustworthy risk understanding

pKYC is a finely tuned, tightly integrated stack where data, automation and analytics components work in harmony. Institutions that try to modernize without this truly integrated foundation will inevitably discover that partial transformation can't overcome the frictions of legacy KYC.

The pKYC triad – data modernization, intelligent automation, and intelligent analytics – forms the operating core of the perpetual model. Each element is necessary, but insufficient on its own. Together, they create a durable, regulator-ready framework that detects risk faster, reduces operational burden, strengthens defensibility, and improves CX.

Every modern KYC system begins with data. Without authoritative, interoperable, and comprehensive data, no amount of automation or analytics can meaningfully improve risk detection or regulatory resiliency.

Traditional KYC data is fragmented: identity attributes differ across lines of business, ownership structures must be manually reconciled, and analysts spend inordinate time stitching together customer profiles from internal and external sources. The result? Inconsistent decisioning and significant exposure to supervisory criticism.

A modernized data layer needs:

- **Authoritative identity resolution:** a single, validated view of the customer that gets rid of redundant records and conflicting attributes.
- **Unified ingestion pipelines:** integration of Customer Due Diligence (CDD) attributes, transaction data, sanctions updates, adverse media, registry data, and behavioral events into a single risk-relevant profile.
- **Lineage, quality scoring, and explainability:** transparency into where attributes came from, when they were updated, and how they're used in risk decisions.
- **Interoperability across controls:** a data architecture where KYC, transaction monitoring, sanctions screening, and fraud systems reinforce – not contradict – one another.

This is the first step in designing a sustainable pKYC framework.

Intelligent automation: The operating spine of pKYC

Automation makes pKYC operationally viable. It lets an institution convert data flows into structured actions, removing manual noise while preserving human judgment for the points where it matters most.

Traditional workflows are inconsistent, email-driven, and dependent on analyst interpretation. Intelligent automation replaces this with orchestrated, API-driven processes that ensure signals move to the right decision points with speed, transparency, and repeatability.

Key capabilities of intelligent automation

- **Workflow orchestration and routing:** triaging events like ownership changes, sanctions hits, adverse media escalations, or anomalous transactions.
- **Deterministic logic to enforce policy consistency:** every material trigger generates a defined next step, whether it's to update an attribute, escalate, seek documentation, or re-score risk.
- **Digital intake and structured data capture:** minimizing repetitive outreach and making sure information is captured once, then reused.
- **STP where appropriate:** reducing delays, eliminating manual re-keying, and improving both CX and unit cost.

Crucially, automation in pKYC doesn't diffuse accountability. Ownership of outcomes remains explicit, with defined escalation paths, approval authorities, and audit trails ensuring that speed never comes at the expense of responsibility.

Intelligent analytics: The accelerator of insight, speed, and defensibility

Analytics – especially AI-enabled analytics – provide the interpretive capability that transforms data and automation into meaningful risk understanding.

With periodic reviews, analysts have to manually piece together documents, search results, transaction records, and narrative evidence. But with pKYC, analytics pre-assemble this context, surface anomalies, generate rationale, and propose risk-based actions. Human oversight remains essential, but the cognitive load is radically reduced.

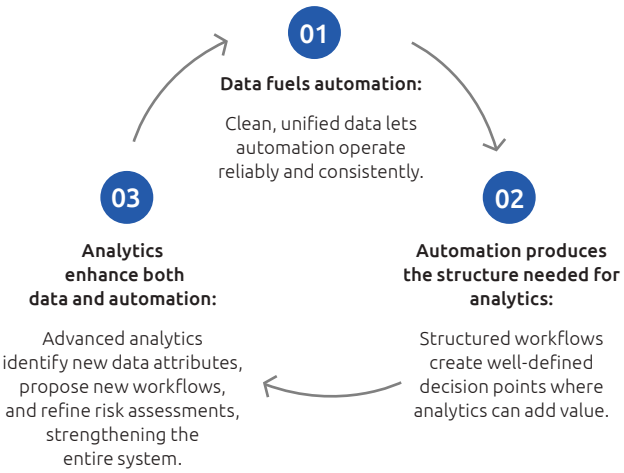
Core analytic capabilities in the triad include:

- **Trigger detection and material change identification:** recognizing new directors, beneficial owners, linked entities, sanctions changes, or emerging adverse media.
- **Risk scoring, classification, and prioritization:** producing understandable outputs rather than opaque model decisions. As one industry leader shared with us: "You need people to look at output and be inquisitive. You might get things that might look okay and pass the sniff test, but if you dig deeper – including back-testing, exception sampling, and manual challenge – you realize that it's just not right."
- **GenAI and agentic AI:** summarizing case history, creating draft rationale, drafting adverse-media assessments, or preparing external supervisory-ready documentation.
- **Bias controls, transparency, and auditability:** making sure analytics remain compliant with regulatory expectations for explainability.

Why the triad must function as a single system

Institutions often try to modernize by focusing on one pillar of the triad: automating onboarding, introducing a new analytics layer, or upgrading customer data architecture. While this improves things slightly, it doesn't ignite transformation – because pKYC requires a new form of operational unity.

The triad forms a closed-loop system:



Transformation only happens when all three elements mature in tandem under strong governance, regulatory alignment, and cross-functional ownership.

The triad as the blueprint for the industry's next decade

The pKYC triad goes beyond solving legacy inefficiencies. Instead, it positions firms to meet the next decade of FinCrime challenges: evolving typologies, geopolitical shocks, real-time sanctions regimes, AI-driven fraud, ESG-related risk, and global regulatory convergence around continuous monitoring.

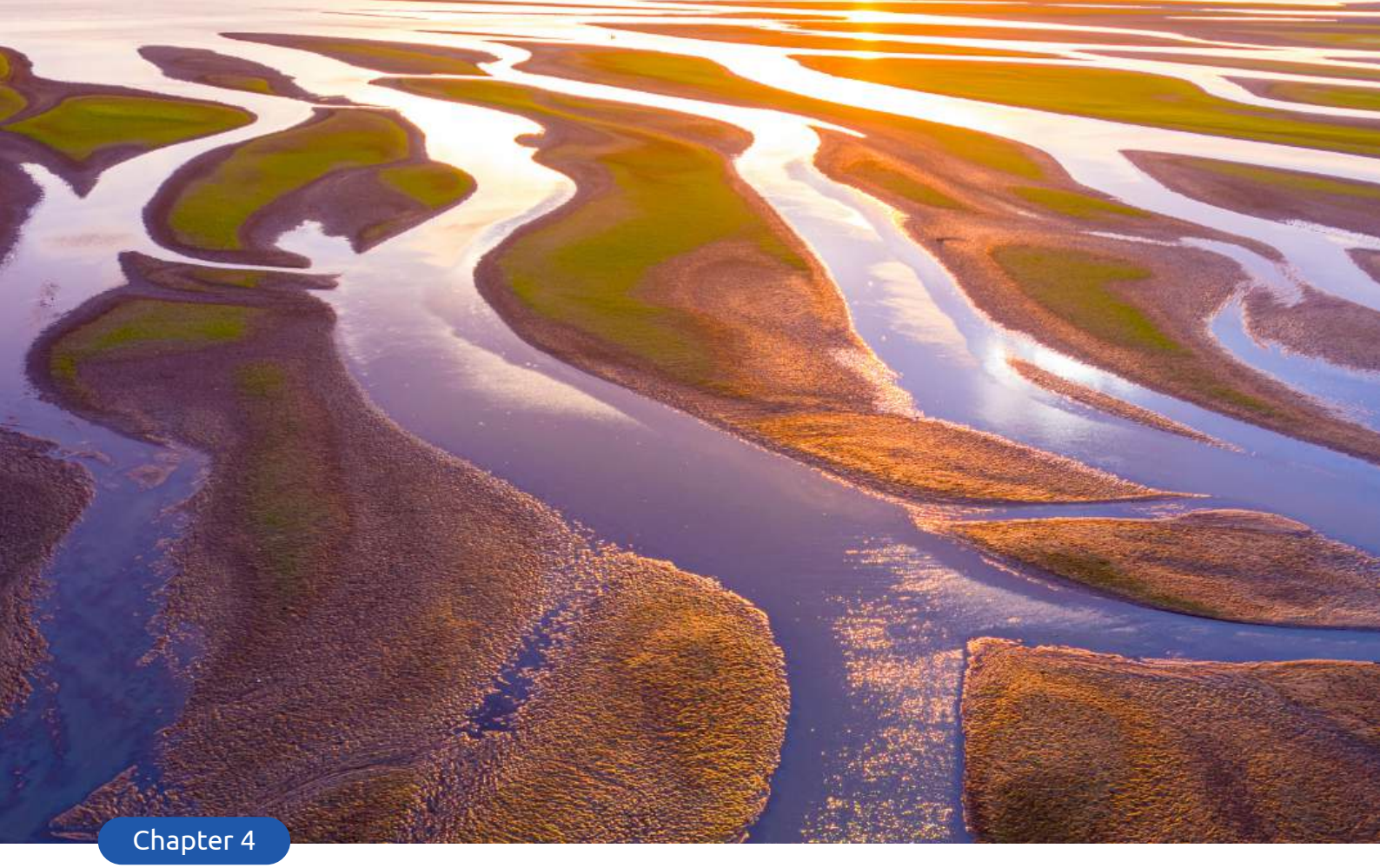
A mature triad delivers:

- Sharper risk insight.
- Fewer false positives and backlogs.
- Reduced unit cost and faster onboarding.
- Higher customer trust and lower friction.
- Improved audit readiness and supervisory confidence.
- A sustainable, adaptable foundation for future controls.

Section 4 examines the regulatory imperative for using the triad to move to pKYC. The capabilities that make pKYC operationally viable – namely clean data, disciplined automation, and explainable analytics – are the same ones regulators increasingly expect institutions to demonstrate.

Key takeaway

When institutions embed the triad as an operating mandate, they accelerate risk detection, strengthen resilience, and reduce the cycle of remediation and regulatory intervention. As for those who delay? They'll face widening operational gaps, cost pressures, and competitive disadvantages.



Chapter 4

The evolving regulatory landscape

The expanding mission of AML

The purpose and scope of AML have expanded dramatically in recent years. What started as a framework focused on money laundering and terrorist financing now includes sanction avoidance, fraud typologies, corruption, environmental crime, geopolitical threats, and the misuse of emerging technologies like AI and virtual assets. This expansion has made traditional KYC operating models difficult to sustain under a periodic, static approach. Static KYC is also increasingly incompatible with modern digital banking.

The growing scope of Enhanced Due Diligence (EDD) is in step with broadening AML policy objectives. It doesn't just cover traditional high-risk sectors and geographies – it also includes exposure to Politically Exposed Persons (PEPs), complex ownership structures, and ESG-related risks. This growing breadth – and reliance on external data sources – makes EDD one of the costliest components of the KYC process.

Traditional KYC operating models are increasingly unsustainable. Static systems can't keep up with the velocity and diversity of new risks. The need for transformation goes beyond efficiency: it's essential for institutions to stay relevant, resilient, and aligned with the expanding public policy objectives of AML.

In turn, the regulatory pressure on firms to maintain robust KYC systems is greater than ever, driven by frameworks like the Financial Action Task Force (FATF) recommendations,[5] the EU's Sixth AML Directive,[6] the US's Financial Crimes Enforcement Network (FinCEN) Beneficial Ownership Reporting Rule,[7] the UK's Economic Crime and Corporate Transparency Act and Economic Crime (Transparency and Enforcement) Act,[8] and the Monetary Authority of Singapore (MAS) Guidelines on Prevention of Money Laundering and Countering the Financing of Terrorism.[9]

The expanding breadth of what AML and FCC is asked to address, compounded by the misuse of AI tools by bad actors, leads to the constant generation of new typologies, red flags, and case studies that are near impossible to keep up with without a dynamic risk and compliance system that maximizes the use and predictive nature of its data.

The future requires pKYC that is robust and compliant, as well as real-time, interoperable, and digitally native. AML regulators must have confidence that the institution is continuously monitoring key data points across a customer's lifecycle that let it meaningfully understand and mitigate its AML risks.

Regulatory emphases

Senior government and regulatory officials have emphasized the need for financial institutions to transform and modernize their AML processes, particularly through digitization, risk-based approaches, and ongoing monitoring.

This growing focus comes in the context of several key legislative milestones:

- In 2024, the EU's new Anti-Money Laundering Regulation (AMLR) – the new 'single rulebook' directly applicable to banks and other obliged entities – came into force, with most substantive requirements scheduled to apply from July 2027, alongside related directive changes and the launch of the EU Anti-Money Laundering Authority[10].
- The UK Companies House launched voluntary ID verification in April 2025, and it became a legal requirement in November 2025 (with a transition period)[11].
- Despite the March 2025 pause on certain US domestic Beneficial Ownership Information (BOI) reporting obligations under the Corporate Transparency Act[12], financial institutions' CDD obligations are unchanged. With that in mind, most firms need to plan 12–24 months in advance, to stand up event-driven refreshes in at least one business line.

However, despite years of technological advancement, a lot of financial institutions still struggle with KYC compliance. Recent enforcement actions support the proposition that outdated KYC or transaction monitoring processes are significant regulatory liabilities[13].

Regulatory guardrails

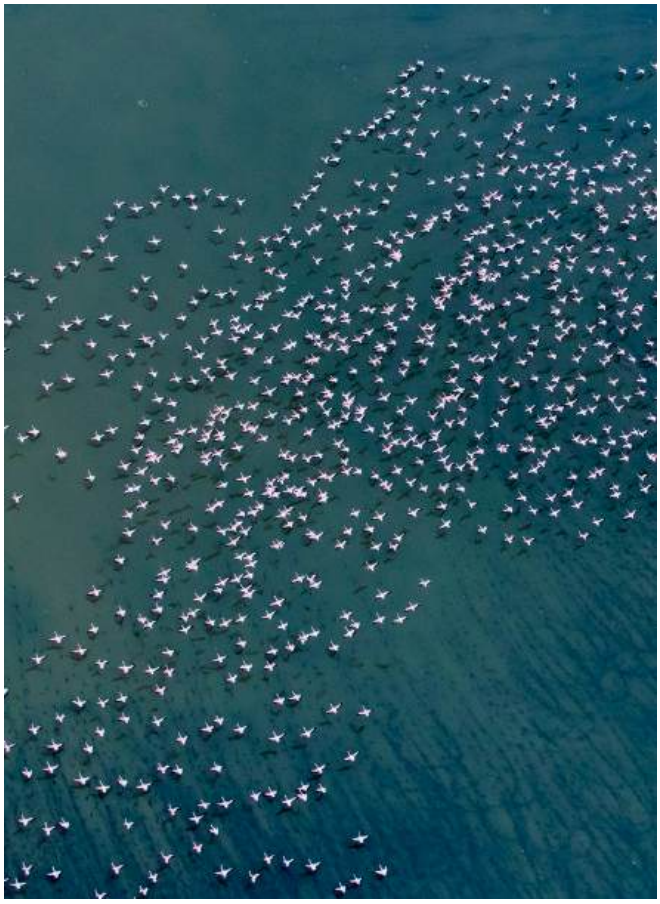
Regulators aren't neutral observers of AML innovation. They expect firms to show that new technologies strengthen their controls, governance, and accountability. So, strong regulatory alignment is essential.

> **"You need to provide assurance to your regulators about your transformation process and goals, giving comfort that what you're doing will enhance compliance and risk management."**
>
> - John Wiethorn, Head of Financial Crime Compliance & AML/BSA Officer, Gusto

Staying aligned requires financial institutions to have regular touchpoints with their regulators and supervisors. Collaboration underscores success. Financial institutions should participate in sandbox environments and proactively share transformation roadmaps, including ongoing information about progress on milestones, how performance is being enhanced, issues experienced and, critically, how FinCrime risk is being monitored, controlled, and mitigated.

When a financial institution engages with a regulator about incorporating innovation into its compliance and risk management processes, there are several guardrails that aren't just aspirational, but expected. These represent baseline supervisory expectations that institutions must evidence throughout design, deployment, and operation.

However, despite years of technological advancement, a lot of financial institutions still struggle with KYC compliance. Recent enforcement actions support the proposition that outdated KYC or transaction monitoring processes are significant regulatory liabilities[13].



10 guardrails regulators expect for AML innovation

1. Compliance as a non-negotiable

Innovation must always strengthen, not weaken, AML and sanctions compliance. Regulators expect that any new technology clearly reduces compliance risk, even at the expense of lessening business benefits.

2. Risk-based design

Tools should be designed and deployed in alignment with the firm's specific risk profile. This means tailoring controls to its products, services, geographies, customer base, and delivery channels, rather than applying one-size-fits-all solutions.

3. Operational resilience

Innovations mustn't compromise business continuity or the resilience of AML operations. Institutions should be able to withstand and recover from system outages, cyberattacks, or technology failures, consistent with the EU's Digital Operational Resilience Act (DORA)-style disciplines.

4. Explainability and transparency

Models and algorithms shouldn't operate as "black boxes." Regulators expect firms to document logic, data sources, and assumptions in a way that management, auditors, and examiners can understand and challenge.

5. Human oversight

Automation can augment accountability – but doesn't replace it. Escalation paths and human-in-the-loop reviews are needed for high-stakes decisions, like suspicious activity reporting, to make sure judgment sits with qualified colleagues.

6. Governance and accountability

Strong governance structures must oversee innovation projects from inception through to operation. Clear roles, escalation lines, and board-level accountability provide assurance that innovation is managed with the same rigor as traditional compliance processes.

7. Model validation and monitoring

Regulators expect robust Model Risk Management (MRM), including independent validation before rollout and ongoing performance monitoring. Testing must confirm effectiveness, detect drift, and capture unintended outcomes. Supervisory letter (SR) 11-7 (Model Risk Management Guidance, 2011) is still the US gold standard for validation, monitoring, and independent review – even with tools-assisted explainers, including from Large Language Models (LLMs).

8. Third-Party Risk Management (TPRM)

Where vendors are involved, regulators expect rigorous oversight consistent with supervisory TPRM guidance (such as OCC Bulletin 2013-29). Contracts, monitoring, and exit strategies should ensure accountability for outsourced services and prevent gaps in compliance coverage.

9. Supporting metrics

Success must be measured with transparent, defensible metrics – such as a higher ratio of true positives to alerts, reduction in SARs rejected by law enforcement or regulators, reduced false positives, and shorter average case handling time – to show balanced outcomes.

10. Data integrity and responsible use

Innovation depends on reliable, unbiased, and properly sourced data. Guardrails must ensure data accuracy, prevent the use of impermissible or poor-quality data, monitor for bias, and safeguard customer privacy throughout the lifecycle of the tool.

Institutions typically demonstrate proper risk mitigation outcomes to a regulator by quality control (QC) sampling, maintaining audit-ready lineage for every automated decision, publishing model cards that document logic and data sources, and tracking performance metrics like false-positive ratios, time-to-truth after an event trigger, and SAR-to-alert conversion rates.

Key takeaway

Regulators expect outcomes that are measurable, consistent across customer segments, reproducible in a sandbox environment, and supported by human-in-the-loop oversight for material decisions. Together, these artifacts show that the transformed KYC process isn't only faster and more efficient – but also more controlled, more explainable, and more defensible than the legacy model.

Chapter 5

Institutional momentum: Early movers in KYC transformation

Across global financial institutions, KYC transformation has shifted from aspiration to execution. A growing cohort of early movers across banking, payments, and securities are reshaping their KYC programs around cleaner data, continuous monitoring, and intelligence-driven operations.

These industry leaders recognize that transformation requires capabilities that match the speed and complexity of today's FinCrime landscape.

> **"We need to speed up the technological change and evolution when it comes to AML/CFT. The sector needs to progress its capabilities and adjust to the rapid pace of technological change."**
>
> Helène Erftemeijer, Sector Coordinator AML/ Countering the finance of terrorism (CFT) and Sanctions of the Dutch Banking Association

Helene's observation reflects the widening gap between institutions clinging to static review cycles and those adopting continuous, intelligence-driven monitoring.

A consistent learning from the current application of modern KYC is that success starts with high-quality, authoritative data and that the ability to leverage trusted external sources meaningfully reduces friction and operational burden. As Greg Zielinksi, Chief Operating Officer Americas and Global Head of Client Technology and Operations at Societe Generale, emphasizes: "A central goal of pKYC is to maximize the use of authoritative external data sources – such as corporate registries, sanctions and PEP databases, and adverse media – to minimize repetitive outreach to customers for information that's already available elsewhere."

Future-forward KYC architecture demands data collection and analytics that directly enable action. "Simply gathering more information without clear escalation or decision pathways creates the worst of both worlds," Peter Cousins, CTO of WorkFusion, observes. "Regulators will hold the institution accountable for having identified risk indicators but failing to respond to them. That's why a future-ready KYC architecture must integrate governance and workflow mechanisms that translate insight into action, ensuring that every signal triggers a defined next step."

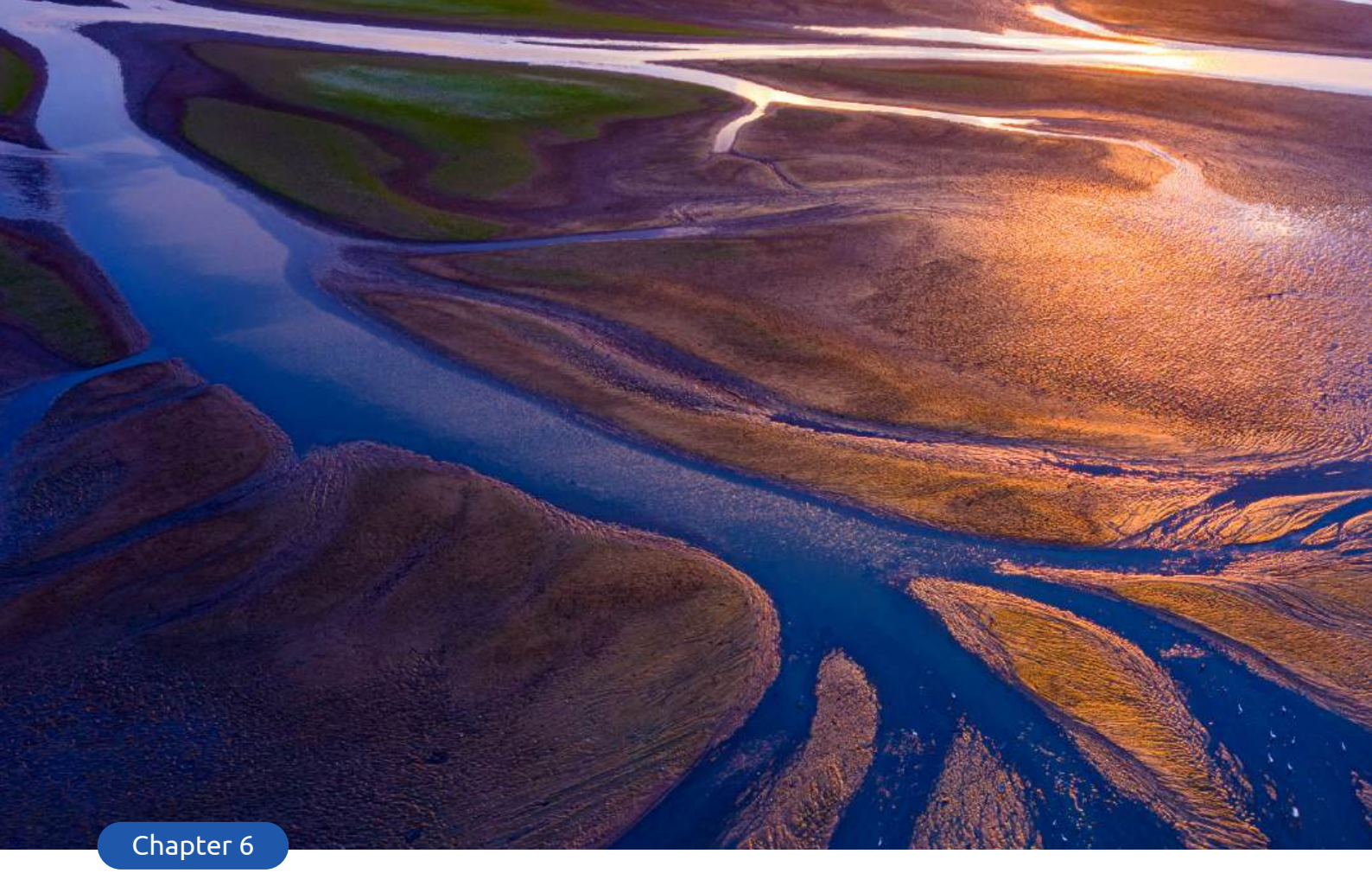
Across many early adopters, the shift toward pKYC is also reshaping the role of analysts and investigators. Institutions leaning into this model report that analysts are increasingly deployed toward judgment, escalation, and complex risk interpretation – exactly the areas where human oversight adds the most value.

Momentum is also visible on the CX front, where early movers are tying digital onboarding, transparency, and reduced outreach to higher satisfaction and better conversion. These firms recognize that customers now expect seamless, digitally enabled interactions. KYC must be designed to meet those expectations without compromising control.

Finally, early adopters are living proof that pKYC strengthens regulatory alignment rather than challenging it. Regulators across jurisdictions continue to stress the importance of dynamic monitoring and real time understanding of customer risk.

Key takeaway

These changes make one thing clear: the shift to pKYC isn't a distant, theoretical concept. It's happening now, driven by the need for speed, intelligence, and regulatory alignment. Institutions that invest in high-quality data, integrated workflows, and adaptive technology will reduce risk, lower costs, and improve CX. As for those who don't? They face rising remediation burdens, widening operational gaps, and increasing regulatory pressure.



Chapter 6

The path to KYC transformation

Institutions that have started shifting toward perpetual, intelligence-driven KYC share a common understanding: transformation can't be achieved through isolated tools or incremental process refinements. It requires an integrated, strategic foundation built on three enablers – modern automation, intelligent analytics, and structured experimentation – all governed with clarity, transparency, and regulatory alignment. These elements form the operating spine that lets KYC programs move from periodic, reactive reviews to continuous insight and proactive risk management.

If institutions follow a three phase approach to KYC transformation – process optimization, AI enablement, and real-time monitoring – with strong governance and regulatory alignment, they can unlock the full business case. In other words, they'll ensure that efficiency gains are sustainable, AI tools remain regulator ready, and risk is managed throughout the journey. With these elements in place, the business case becomes tangible: faster onboarding, reduced compliance costs, improved risk visibility, and enhanced customer trust.

Automation as the foundation of scale

Modern KYC operations depend on the ability to reduce manual burden, unify workflows, and ensure consistency across jurisdictions and business lines. Automation – whether through workflow orchestration, digital intake, or structured data capture – creates the stability and repeatability that a perpetual model requires. Institutions that are leading in this space aren't automating for efficiency alone: they're building the operational discipline that makes continuous monitoring sustainable.

Automation also helps shift work away from repetitive data collection and toward analysis and judgment. "Historically, KYC staff have spent about 80% of their time researching and gathering information from disparate data sources," observes Brian Ferro. "A good goal is to flip that on its head, using tools like agentic and GenAI."

Early movers are proving this rebalancing isn't just achievable, but that it strengthens both productivity and control integrity. As noted by one industry expert, "Agentic AI is becoming increasingly important, as it represents the next evolution of automation in KYC – systems capable not just of performing predefined tasks, but of reasoning through multi-step objectives, dynamically invoking other tools, and adapting workflows in real time. In contrast to static RPA or even prompt-driven GenAI, agentic AI can autonomously coordinate tasks such as gathering entity data, verifying documents, cross-checking sanctions lists, and drafting rationale for human review. This orchestration capability makes agentic AI especially powerful for event-driven refresh and perpetual KYC environments."

Why AI changes the economics of KYC transformation

Automation creates scale, but AI changes the economics of KYC transformation altogether. Traditional KYC programs are constrained by linear cost structures: as customer volumes, jurisdictions, and data sources expand, headcount and operational spend rise too. AI breaks this dependency by letting institutions process more information, identify risk changes faster, and generate defensible outcomes without proportionally increasing manual effort.

In practical terms, AI lets institutions shift KYC work away from labor-intensive research and reconciliation toward higher-value interpretation and escalation. ML and entity-resolution tools reduce time spent resolving identities and ownership structures. Natural language processing and GenAI summarize adverse media, corporate filings, and historical case data into consistent, review-ready narratives. Event-driven analytics surface only material risk changes, dramatically reducing unnecessary reviews.

The result isn't just faster onboarding or lower unit cost, but a structurally more sustainable KYC operating model – one that can absorb regulatory change, new data sources, and emerging typologies without recurring remediation cycles or repeated technology resets.

Intelligent analytics and AI as force multipliers

AI is the critical force multiplier that lets KYC transformation move beyond process improvement and into continuous risk management. While automation standardizes workflows, AI enables institutions to understand context, detect material change, and prioritize action across massive volumes of structured and unstructured data – something static rules and manual review can't achieve.

In modern KYC environments, AI is increasingly used to resolve complex ownership structures, identify subtle linkages across customers and counterparties, assess the relevance of adverse media, and generate explainable risk rationales at speed. Rather than replacing analysts, these capabilities compress time-to-insight and reduce cognitive load, so human judgment can be applied where it matters most.

AI, GenAI, and other advanced analytic capabilities, play an important role in accelerating the KYC transformation. Helène Erftemeijer notes that, "AI is applied more frequently and in multiple AML/CFT processes to augment and replace traditional rule-based systems." Institutions can use AI to enhance decision making by summarizing information, identifying patterns, and contextualizing risk signals.

These tools support the deeper shift from point-in-time assessment to dynamic risk understanding, helping firms surface changes more quickly and respond more confidently. When paired with responsible governance and human oversight, AI becomes a strategic accelerator of both efficiency and defensibility.

Crucially, AI also reduces transformation risk. By embedding explainability, traceability, and performance monitoring into KYC processes, AI-enabled systems make it easier for institutions to evidence control effectiveness, reproduce decisions, and demonstrate supervisory alignment. This shifts KYC modernization away from opaque, one-off technology deployments toward measurable, auditable capability uplift – giving regulators greater confidence that faster processes are also more controlled.

The sandbox as a catalyst for safe innovation

To modernize at the required pace, institutions need controlled environments where they can test new detection logic, evaluate risk triggers, and validate AI-assisted workflows without jeopardizing production systems.

> **"The move to pKYC is an area where AI and digitization can substantively improve and transform various operational processes while reducing cost and enhancing the customer experience."**
>
> Greg Zielinksi, Chief Operating Officer Americas and Global Head of Client Technology and Operations, Societe Generale

Sandbox experimentation enables exactly that: rapid iteration, evidence-based refinement, and transparent engagement with regulators. Firms that use sandbox testing reduce implementation risk but build confidence – both internally and externally – that new approaches actually strengthen their compliance.

Reinforcing strength through synergy

The highest benefit of these enablers emerges when they operate together. Automation creates consistency and frees capacity, AI amplifies insight and speeds up interpretation, and structured experimentation ensures innovations mature safely before scaling. These efficiencies also support stronger governance and control integrity. As John Wiethorn puts it, "There's hardly a process where we don't find a use case for introducing AI to make it better. Often, it's a game changer. So I would argue that an AML program that doesn't actively use AI now is no longer sustainable." His perspective reflects a growing industry consensus: meaningful KYC modernization depends on intelligent tools embedded within a disciplined operating model.

Building trust through transparency and explainability

Regulators are increasingly clear that institutions must stay transparent about how they make risk decisions. Adam Famularo, CEO of WorkFusion, says, "This means that every model decision must be explainable, traceable, and open to scrutiny by compliance, risk, and audit teams." In the context of pKYC, this isn't simply a governance requirement: it's an enabler of trust, ensuring that monitoring is both reliable and defensible.

Institutions adopting these principles position themselves to move faster. By embedding governance into design, they avoid the pitfalls of retroactive validation and build a model that is adaptive, resilient, and regulator-ready.

A pKYC transformation roadmap: issues, interventions, and impact

Legacy pain point	What good looks like	pKYC interventions	90-day actions	KPIs and expected delta
Duplicative data entry across siloed systems	• Single client profile • Golden records mastered and reused across journeys	• Robotic Process Automation (RPA) or Intelligent Process Automation (IPA) to harvest and reconcile data • GenAI entity resolution • Sandbox to test sources and merge rules	• Inventory data fields • Build 3–5 RPA bots • Pilot match or merge policy in sandbox	• Re-keying reduced by 30–50% (or higher for EDD)[14] • Data defect rate down by 40–60%[15]
Slow onboarding and periodic reviews	• Risk-based, straight-through onboarding with dynamic (event-driven) reviews	• Workflow orchestration • GenAI doc parsing and gap detection • Sandbox to simulate risk triggers	• Stand up orchestration MVP • Deploy GenAI doc extractor on top 5 doc types • Define event triggers in sandbox	• Onboarding turnaround time down by 40–60%[16] • Case backlogs down by 50–70%[17]

Legacy pain point	What good looks like	pKYC interventions	90-day actions	KPIs and expected delta
High false positives in screening or alerts	• Tuned models with explainable decisions and lower noise	• Intelligence augmentation (IA) for list hygiene • GenAI for name matching context • Sandbox A/B for thresholds	• Cleanse watchlists • Run threshold A/B in sandbox • Calibrate phonetic/fuzzy match	• False positives down by 20–40%[18] • Analyst productivity up by 30–50%[19]
Manual document review and outreach	• Auto-classification • Extraction • Client-friendly digital requests	• GenAI for classification/ extraction • IA to pre-populate KYC packs • Sandbox to compare extractors	• Train extractor on 500–1,000 samples • Launch digital request templates	• Doc touch time down by 50–70%[20] • Client NPS up by10–20 points[21]
Fragmented risk view and static periodicity	• pKYC with continuous risk signals and explainable triage	• Event ingestion (payments, onboarding, external data) • GenAI risk narratives • Sandbox to validate triggers	• Define top 10 risk signals • Connect 2–3 event feeds • Author explainable AI narrative templates	• Unnecessary periodic reviews down by 40–60%[22] • SAR hit rate up by 15–30%[23]
Audit friction and weak defensibility	• Click-through lineage model cards, and replayable evidence	• IA for lineage capture • Sandbox for versioned test packs and approvals	• Enable auto-logging • Publish model cards • Run compliance “table-top” in sandbox	• Audit prep time down by 30–50%[24] • Policy exceptions down by 25–40%[25]
Rising run-costs and full-time-equivalent strain	• Lower unit cost with higher throughput and quality	• IA to remove low-value tasks • GenAI to augment analysts • Sandbox to prove ROI	• Build business case from sandbox metrics • Phased roll-out	• Cost per KYC file down by 25–40%[26] • Throughput up by 30–50% [27]

Key takeaway

KYC transformation isn't about isolated fixes. It's about building a connected, future-ready operating model. Firms that combine automation, AI-driven analytics, and structured experimentation under clear governance will move beyond compliance to achieve scale, resilience, and lasting trust.

Chapter 7

Leading the organization through KYC transformation

Delivering pKYC takes more than new tools or smarter analytics. It demands organizational alignment, cultural readiness, and disciplined governance. Firms that move successfully toward pKYC do so by addressing internal resistance, establishing clear direction, and anchoring innovation in accountability and trust. These are the strategic operating model principles that early movers employ, drawing on lessons surfaced repeatedly across the industry.

Meet resistance with clarity and empathy

Even when the regulatory and business case is clear, transformation is disruptive. Business leaders may worry about customers' reactions, operations teams may fear job losses, and oversight functions may be concerned about the risks of new technology.

Acknowledging these anxieties and addressing them through transparent communication, thoughtful design, and strong stakeholder engagement helps shift the narrative from disruption to progress.

Establish tone from the top

Transformation succeeds when leadership is explicit about priorities. A clear, sustained message from the board, CEO, and executive committee shapes the cultural and operational compass for the entire institution. When leaders articulate that pKYC is both a compliance necessity and a business enabler, the organization is more willing to re-examine entrenched processes and adopt new ways of working.

Strong leadership also accelerates cross-functional alignment, for faster decision making and less friction between operating units.

Coordinate the three lines of defense around a shared "North Star"

KYC transformation touches every part of the organization, which is why alignment across the institution is essential. As one industry leader puts it: "It's very useful to have functions across the three lines of defense come together to agree on a 'North Star' for achieving perpetual, risk-based, and customer-centric KYC by a certain date."

This shared destination gives teams a common language, clarifies priorities, and reduces the friction that arises when groups pursue parallel – but not coordinated – objectives.

Celebrate early wins to build confidence

Momentum is built through evidence. Firms that deliver early improvements – like reduced onboarding times or smaller review backlogs – show skeptics that transformation reduces risk rather than increasing it. Quick wins reinforce leadership messages, strengthen stakeholder buy-in, and prove that new approaches can be more consistent, transparent, and defensible than legacy processes.

Embedding compliance early in design and pilot work further ensures that innovations are aligned with policy expectations and avoid unnecessary rework.

Talent, ownership, and collaboration

Sustainable KYC transformation relies on cross-functional collaboration between compliance, operations, technology, data, and the business. Programs progress fastest when teams who design the solution are also accountable for implementing and operating it.

> **"When those who develop the technology also own its outcomes, alignment between innovation intent, compliance defensibility, and day-to-day performance is far stronger because they have skin in the game."**
>
> Gareth Murray, Financial Crime Senior Director – Head of Financial Crime, Monzo Bank

Gareth Murray captures the importance of aligning innovation with ownership, for a model that promotes shared responsibility, accelerates feedback loops, and embeds ongoing improvement into the firm's operating rhythm.

Embed governance to protect pace and integrity

Strong governance isn't a brake on transformation – it's the scaffolding that lets transformation scale safely. Institutions that succeed establish governance frameworks that are firm enough to ensure transparency, accountability, and regulatory alignment, yet flexible enough to support iterative experimentation. These frameworks clarify decision rights, support explainability, and create durable audit trails that reinforce trust across all lines of defense.

Key takeaway

The operating model for pKYC is built on clear leadership, cross-functional alignment, accountability, and governance that enables rather than inhibits progress. Institutions that embrace these principles can navigate internal resistance, build momentum, and keep the right capabilities in place.

Chapter 8

The path forward: Delivering perpetual, intelligence-driven KYC

pKYC is an operating reality already taking shape across the industry. Institutions that succeed with this shift recognize that transformation is less about deploying new tools and more about building the conditions for continuous, intelligence-led risk management: strong data foundations, thoughtful automation, understandable analytics, disciplined governance, and cross-functional execution. The path forward isn't a single leap: it's a series of strategic steps that build confidence, capability, and momentum.

Establish foundational readiness

The transition to pKYC begins with clarity – about customer data, risk definitions, policy standards, and decision rights. Institutions that move fastest have:

- A trusted core of customer data that reduces noise and enables event-driven triggers.
- Clear policy alignment on what constitutes material change.
- Defined ownership across compliance, operations, technology, and the business.

This foundational work ensures that subsequent investments in AI, automation, or monitoring have a stable platform to operate on.

Demonstrate value early

Successful institutions avoid over-engineering or pursuing an end-state all at once. Some start with lower-risk jurisdictions and customer populations. Others target high-risk segments or high-pain journeys early, ensuring that the operational and risk benefits are most visible to senior stakeholders.

Early wins create organizational momentum, reinforce stakeholder trust, and make the broader case for sustained investment.

Scale through cross-functional delivery

As programs mature, institutions scale by bringing together the disciplines that collectively shape KYC outcomes: data engineering, risk management, policy, operations, technology, and product. The strongest performers embed ongoing improvement into these teams, so policies, controls, and systems can evolve in tandem.

Cross-functional alignment makes sure pKYC is entrenched as a strategic capability that touches every part of the customer lifecycle.

Embed governance and explainability

Regulators across jurisdictions expect institutions to embed governance into design (rather than bolting it on afterward) and move faster, with fewer reversals and greater confidence in their programs.

Clear documentation, transparent risk decisions, and reproducible workflows become essential enablers of both regulatory trust and operational scale.

Build toward a dynamic, future-ready model

Leading institutions see pKYC as a platform for long-term capability expansion. Continuous monitoring, richer identity data, and AI-driven classification power more adaptive customer journeys, earlier risk detection, and more efficient use of investigative resources. Over time, the organization transitions from reactive, periodic compliance activity to a living, intelligence-led risk program.

This maturity is characterized by:

- Consistent CX across products and channels.
- Faster, more accurate detection of risk-relevant events.
- A workforce focused on analysis and interpretation, not data gathering.
- Stronger regulatory posture and reduced reliance on remediation cycles.

pKYC becomes entrenched as a compliance standard and a critical differentiator that improves trust, reduces costs, and strengthens competitive positioning. Institutions with complex ownership structures, high customer volumes, multiple jurisdictions, or recurring KYC remediation findings have the most to gain by shifting to pKYC – and the most to lose if they delay.

Key takeaway

The shift to pKYC is neither binary nor instantaneous. It's an incremental, strategic journey driven by better data, smarter automation, and disciplined collaboration. Firms that take these steps today will operate with sharper risk insight, reduced friction, and far more resilient compliance programs. The rest will face rising costs, widening control gaps, and operational models that can't keep up with regulatory and customer expectations.

Conclusion: A KYC model for the future

To stay competitive and compliant, financial institutions must evolve from rigid, reactive KYC frameworks to adaptive, intelligence-driven compliance operations. Automation, GenAI, and the pKYC sandbox offer a path forward that is more efficient, customer-centric, and risk-aligned.

As financial institutions evaluate their readiness for pKYC, three questions can help translate aspiration into action:

1. **Data and connectivity:** do we have the data quality, lineage, and interoperability needed to detect meaningful customer risk changes in real time?

2. **Model and governance alignment:** are our risk scoring models, triggers, and ownership structures ready for ongoing calibration and regulatory transparency?

3. **Operating model and CX:** can we redesign processes so pKYC enhances trust and efficiency, rather than adding friction?

pKYC is rapidly becoming the baseline against which supervisory adequacy will be judged. Institutions that move now will define standards, shape regulatory dialogue, and compound advantage. Those that delay will inherit higher costs, weaker controls, and a narrowing set of strategic options. The question is no longer whether KYC must change: it's whether your firm is ready to lead the charge.

Ask the experts

Manish Chopra

Global Leader – Risk and Compliance
manish.chopra@capgemini.com

Manish is Executive Vice President and head of Capgemini's Risk and Compliance business for Financial Services. For over 3 decades, Manish has partnered with CXOs in financial services and payments organizations to develop end-to-end risk and compliance solutions powered by data, domain, process, and digital capabilities.

Jeff Ingber

Senior Advisory Consultant – Risk & Compliance
jeffrey.ingber@capgemini.com

Jeff is a Senior AML & Regulatory Compliance Advisor at Capgemini. An ex-regulator, he previously oversaw the Legal and Compliance Risk function of the Federal Reserve Bank of New York and was also a member of the Federal Reserve System's Risk Secretariat.

Samar Pratt

Global Leader – Financial Crime Compliance (FCC) Advisory Solutions
samar.pratt@capgemini.com

Samar leads the FCC Advisory business for Capgemini supporting clients in optimizing target operating models, regulatory readiness reviews, quality assurance, benchmarking, on-site audits, and training initiatives. Samar has led high-profile regulatory reviews, including Section 166 reviews for FCA and examinations for US authorities, offering deep insights into global compliance expectations.

Supriyo Guha

Global Leader – FCC Transformation
supriyo.guha@capgemini.com

Supriyo leads the FCC Transformation practice at Capgemini. With over 2 decades of experience in reimagining and architecting digital transformation, Supriyo partners with clients to transform their Financial Crime Risk Management functions through industry first, AI-led solutions.

Tom van Els

Head of KYC and CLM – Benelux
tom.van-els@capgemini.com

Tom leads the KYC and CLM business for Capgemini in Benelux. He has over 10 years of experience in leading Global KYC (Remediation) Programs, implementing core savings platforms and building high performance teams that deliver KYC & AML solutions and innovative services.

Florent Palayret

Global Compliance Leader – Capgemini Invent FS
florent.palayret@capgemini.com

Florent leads the compliance business for financial services at Capgemini Invent. Florent is a senior management consulting professional with nearly 12 years of experience in corporate investment banking in both front- and back-office operations, banking regulation (US and Europe), financial crime, risk, and digital transformation.

Luca Russignan

Head of Capgemini Research Institute for Financial Services
luca.russignan@capgemini.com

Luca provides strategic insights for financial services to shape industry dialogue on transformation. Each year, he partners with 80+ C-suite leaders at global financial institutions, drawing on research across multiple markets to identify emerging patterns and translate them into strategic guidance.

Key contacts

Global

Manish Chopra
manish.chopra@capgemini.com

Australia

Samar Pratt
samar.pratt@capgemini.com

France

Charles Dally
charles.dally@capgemini.com

Germany

Tobias Mohr
tobias.mohr@capgemini.com

India

Arvind Pal Singh
arvind.singh@wns.com

Ramya Ramakrishnan
ramya.b.ramakrishnan@capgemini.com

Nordics

Harinder Sudan
harinder.sudan@capgemini.com

Singapore

Xiao Wu
xiao.wu@capgemini.com

The Netherlands

Tom Kastelein
tom.kastelein@capgemini.com

United Kingdom

Oliver Hanmer
oliver.hanmer@capgemini.com

United States and Canada

Mike Roe
michael.a.roe@capgemini.com

Supriyo Guha
supriyo.guha@capgemini.com

Acknowledgements

We offer special thanks to the financial institutions, ecosystem partners, and industry experts who contributed their valuable time during the Financial Crime Compliance Report Executive Interviews.

We appreciate the expertise of participating firms: Bank of Queensland, Encompass Corporation, Everest Group, Gusto, Monzo Bank, Nederlandse Vereniging van Banken, Societe Generale, SymphonyAI, and WorkFusion.

We recognize the following teams and individuals for analysis, composition, and production:

Capgemini Research Institute for Financial Services: Luca Russignan.

Executive Leadership Council: Cyril Francois, Gareth Wilson, Kartik Ramakrishnan, and Nilesh Vaidya.

Capgemini's global FCC network: Alister Coates, Amit Bhaskar, Arvind Pal Singh, Charles Dally, Florent Palayret, Harinder Sudan, Jack Williams, Jeff Ingber, Julie Curto, Maikel Miggelbrink, Manish Chopra, Mike Roe, Narinder Aggarwal, Neha Punater, Neha Saxena, Oliver Hanmer, Rahul Menon, Ramya Ramakrishnan, Preeti Malik, Samar Pratt, Sandeep Chakravadhanula, Shanmugaraj Rajamani, Supriyo Guha, Tom Kastelein, Tom van Els, Vivek Desai, and Xiao Wu.

Marketing: Amy Heydenrych, Anna Velasco Madeira, Anthony Tourville, Fahd Pasha, Hugh Collins, Jyoti Goyal, Meghala Nair, Manasi Sakpal, Manisha Singh, Neha George, Sophie Thrower, Sonali Saxena, and Sreemoyee Dutta for their marketing support for the report.

Appendix

1. Industry reports from technology vendors and global consulting firms show that financial institutions implementing event-driven KYC workflows, automated screening optimization, and high-quality external data sources have achieved 20–40% reductions in false positives. These findings are consistent across retail, SME, and corporate segments and reflect improvements in watchlist data quality, matching algorithms, and intelligent case routing.

2. Multiple public case studies – from Fenergo, BCG, McKinsey, and major banking groups – show that digital KYC workflow automation, straight-through processing, and authoritative data reuse commonly reduce onboarding turnaround time by 40–60%, particularly in complex corporate onboarding environments. Typical drivers include reduced document re-collection, automated validation, and elimination of sequential manual steps.

3. Banks adopting perpetual or event-triggered KYC models have reported 50–70% reductions in case backlogs thanks to fewer unnecessary case openings, automated attribute maintenance, and improved prioritization using analytics and risk signals. These results appear in industry analyses by Capgemini, Deloitte, and NICE Actimize and in early-adopter regulatory submissions describing workload reduction and productivity gains.

4. Industry estimates from global banks and consulting analyses show that replacing calendar-based refresh cycles with event-driven maintenance eliminates ~70–90% of the manual effort associated with periodic KYC reviews. This range reflects reductions in document re-collection, duplicate investigation work, case creation, and manual outreach observed in early-stage pKYC pilots across retail, SME, and corporate segments.

5. FATF, "The FATF Recommendations;" October 2025.

6. European Union, "Document 32024L1640;" June 2024.

7. Financial Crimes Enforcement Network, "Beneficial Ownership Information Reporting;" accessed December 2025.

8. Legislation.gov.uk, "Economic Crime (Transparency and Enforcement) Act 2022;" accessed December 2025.

9. Monetary Authority Singapore, "Prevention of money laundering and countering the financing of terrorism – banks;" March 2024.

10. European Central Bank. See Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Anti-Money Laundering Regulation), OJ L, 19.6.2024, p. 1–186. The Regulation enters into application on 10 July 2027.

11. See "Companies House confirms identity verification rollout from 18 November 2025," UK Government press release (5 August 2025) – noting that phased implementation will begin that date, subject to secondary legislation and company roll-out.

12. See "FinCEN Removes Beneficial Ownership Reporting Requirements for U.S. Companies and U.S. Persons," interim final rule effective March 21, 2025, in which FinCEN exempts domestic reporting companies and US persons from BOI reporting under the Corporate Transparency Act.

13. See Office of the Comptroller of the Currency, FinCEN, Monetary Authority of Singapore, U.S. Department of Justice, U.S. Securities and Exchange Commission, and Danske Bank.

14. WorkFusion case data.

15. IBM, "Transform banking operations with master data management," IBM Industry Solutions, 2020. The paper reports that banking institutions deploying IBM MDM achieved measurable improvements in data quality and operational efficiency, including up to ~30–50% reduction in data errors.

16. "Client onboarding turnaround time can fall by 40–60% when banks adopt streamlined digital onboarding and automation practices", see Coforge, "Elevating institutional client onboarding experience in a digital age" (McKinsey findings), and Newgen, "Digital Customer Onboarding Solution" case study.

17. "A banking institution saw a 50-70 % reduction in case backlog (or manual effort backlog) after mass-automation implementation", see "Wonderbotz Case Studies: Banking Institution reduces backlog with mass automation implementation."

18. External evidence confirms that optimized screening / AI-augmented models typically reduce false positives by ~20–40%. See Valley Bank's partnership with DataRobot (false positives fall by 30%) and McKinsey, "The New Frontier in Anti-Money Laundering" (false reports fall by 20–30%) for similar metrics.

19. External case studies indicate material gains in analyst throughput: Quantifind cites up to ~40% productivity improvement, and Tookitaki reports ~53% at a global bank.

20. In implementations using Intelligent Document Processing, document 'touch' or handling times (for review, approval, or processing) have been observed to fall by about 50–70%. For example, SMBs using IDP in logistics report 50–70% faster document processing, and a Deloitte-sponsored study via AppEnhancer found review and approval cycles decreased by 50–70%.

21. External evidence indicates that clients' NPS typically improve by about 10–20 points following implementation of CX improvements: e.g., in the Firstsource mortgage provider case, NPS rose ~20 points after enhancing agent consistency, monitoring, and service workflows; similarly, banks using concierge or lifestyle benefit programs reported ~15-point NPS gains among premium customers.

22. Banks adopting pKYC report large reductions in periodic-review workload: PwC describes pKYC models in which only a small subset of files require human intervention and cites up to 60–80% savings in total KYC effort; McKinsey observes 20–30% streamlining from automated/event-driven reviews; and Accenture notes 15–35% fewer KYC reviews with automation – together supporting a ~40–60% cut in calendar-driven, low-value reviews when firms move to event-driven refresh for low-risk segments.

23. External case evidence shows SAR conversion/hit-rates commonly rise by ~15–30% with ML-enabled tuning and alert prioritization. For example, SAS reports a 25% SAR-yield increase at a US regional bank; NICE Actimize's predictive-scoring case study (L2 queue hit-rate 27%) and McKinsey's report of larger (up to 3×) improvements with behavior-based segmentation.

24. External case evidence shows audit-preparation time commonly falls by ~30–50% with automation and centralized evidence: e.g., Google Cloud reports 40% lower audit prep time for plutos ONE; Drata's Softcat case notes a ~40% reduction in staff time required for audits; and Nanitor's Valitor case shows a 50% reduction in audit preparation time.

25. External case evidence shows audit-preparation time commonly falls by ~30–50% with automation and centralized evidence: e.g., Google Cloud reports 40% lower audit prep time for plutos ONE; Drata's Softcat case notes a ~40% reduction in staff time required for audits; and Nanitor's Valitor case shows a 50% reduction in audit preparation time.

26. External evidence indicates that KYC unit costs typically fall by ~25–40% when workflows are centralized or managed and automation is applied. For example, PwC's KYC Centre of Excellence reports 20–40% lower costs, while an Idenfo deployment shows ~30% compliance-cost reduction. Broader pKYC programs have documented even larger savings (PwC 60–80%), making 25–40% a conservative range for cost-per-file.

27. External case evidence shows materially higher KYC/alert-handling throughput once automation/ML is applied – for example, Idenfo reports a 45% processing-speed increase in AML/KYC operations (insurance case), AML RightSource documents a ~50% reduction in KYC process time at a global bank (effectively boosting file throughput), and McKinsey notes leading firms cutting review case-handling time to 20–30% of peers via STP (consistent with ≥30–50% throughput gains).

About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of over 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2025 global revenues of €22.5 billion.

Make it *real*.
www.capgemini.com

Capgemini