encompass
the full picture, fast

Planning your journey to perpetual KYC

The pKYC maturity model

encompasscorporation.com

About the authors

Dr Henry **Balani** Chair of pKYC advisory board

Global Head of Industry & Regulatory Affairs

Dr Henry Balani is a noted industry thought leader and commentator on regulatory compliance issues and trends affecting the financial services industry. A published academic, Dr. Balani also lectures on international business, economics, and regulatory compliance courses globally.

Dr. Balani holds a Doctorate in Business Administration from the University of Wisconsin, an M.B.A. from Northern Illinois University, and a B.S. in Economics from the London School of Economics.

LinkedIn

Howard **Wimpory** Member of pKYC advisory board

KYC Transformation Director

Howard Wimpory works with Tier 1 banks to digitally transform their KYC onboarding and refresh processes. He has held a number of executive-level operational roles within a major global bank, including leading their wholesale KYC Onboarding and Refresh functions.

His most recent role prior to Encompass was Managing Director, Group Financial Crime Operations position at Barclays Bank, where amongst other functions, he was accountable for leading KYC remediation of corporate and investment bank client records to FCA committed timelines.

LinkedIn

Contents

01 Executive summary

Know Your Customer (KYC) regulatory obligations require financial institutions to periodically review and refresh relevant customer information to reduce the risk of illicit activity being funded by proceeds of crime.

This process includes reviewing customer documentation, screening against global and country-based watchlists, and a reassessment of risk ratings if there have been any material changes in circumstance. Such reviews are a critical tool used to protect financial markets and banks from criminal exploitation. Traditionally, organizations have assessed customer data across fixed time horizons dictated by the relative risk score of each account, with higher risk customers being reviewed annually, and lower risk customers assessed every three to five years. Approaches vary internationally, with the UK favoring one, three and five year reviews whereas, in the US, one, two and three year cycles are more common. Importantly, these conventions are not dictated by regulators themselves but by the risk appetite of institutions, as well as historical practice.

The existing paradigm of periodic KYC refresh is no longer effective when it comes to keeping pace with the evolving financial crime landscape and risk appetite. The Pandora Papers, Coronavirus pandemic and Russia's ongoing invasion of Ukraine provide real examples of just how quickly the social, environmental and economic climates can evolve. Institutions can no longer afford to rely on time-bound assessments to unearth material risk, instead they need to be adaptable, dynamic and proactive in the face of challenges.

Perpetual KYC (pKYC) represents a shift in the way institutions monitor customer information. It replaces manual, time-consuming and expensive periodic reviews with a technology-centered, data-enabled alternative. pKYC is a continuous process of safeguarding an organization against financial crime by monitoring customer information and responding to changes. Consequently, firms maintain up-to-date customer profiles and achieve a state of ongoing compliance. The ultimate aim of pKYC is to know the customer better by truly understanding the nature of the change in circumstance being flagged by a range of data points and, with that context, making an informed decision in real time.

Replacing traditional reactive KYC checks with proactive data-driven processes increases effectiveness and facilitates additional standardization across global financial institutions, as well as reducing regulatory and financial crime risk. Some firms have also already begun to realize the efficiency gains associated with pKYC, achieving effort savings of 60%-80%[1].

While pKYC represents a marked improvement, transitioning to a data-enabled perpetual process is not easy. A lack of understanding of the scale of the transition required and general process inertia still hold many firms back from achieving true automation. As a result, periodic customer refresh remains the industry standard.

[1] pwc.com/sg/en/consulting/assets/pkyc-a-new-approach-to-periodic-reviews.pdf

02

The formation of Encompass' pKYC advisory board

The formation of Encompass' pKYC advisory board

At Encompass, we are passionate about driving material KYC improvements through innovation, and taking the pKYC discussion from concept to practice. So, in November 2021, we set out to bring this aim to life by convening a group of senior KYC program owners from a range of financial institutions, as well as the technology and data providers whose solutions they use to achieve KYC compliance. By leveraging their first-hand experience of KYC transformation, we started working towards developing practical guidelines for institutions to map their individual journeys to pKYC.

Over the next year, the group participated in a series of roundtable discussions, ultimately agreeing that understanding the customer better, on a near real-time basis, through a continuous KYC approach can deliver tangible value back to a business, both from a risk mitigation and revenue generation perspective. Indeed, a flag on a customer record could, for example, highlight the need for an account review or a potential cross-sell opportunity that could help the firm in question better meet the needs of its customer.

It is important that firms consider the end customer as a driver of pKYC adoption, alongside regulators and the internal stakeholders seeking cost savings and efficiencies. If firms can reduce costs while delivering better interactions through pKYC, and in a way that isn't intrusive, they can also deliver significant improvements in client experience and KYC outcomes.

A transition to pKYC is more than a risk mitigation exercise. It can also lead to better customer outcomes, by:

- Reducing the gap between current technology capability towards addressing regulatory remediation requirements
- Prioritizing relevant customer profiles for review
- Substituting arbitrary periodic customer checks with enhanced data-driven decisioning

03

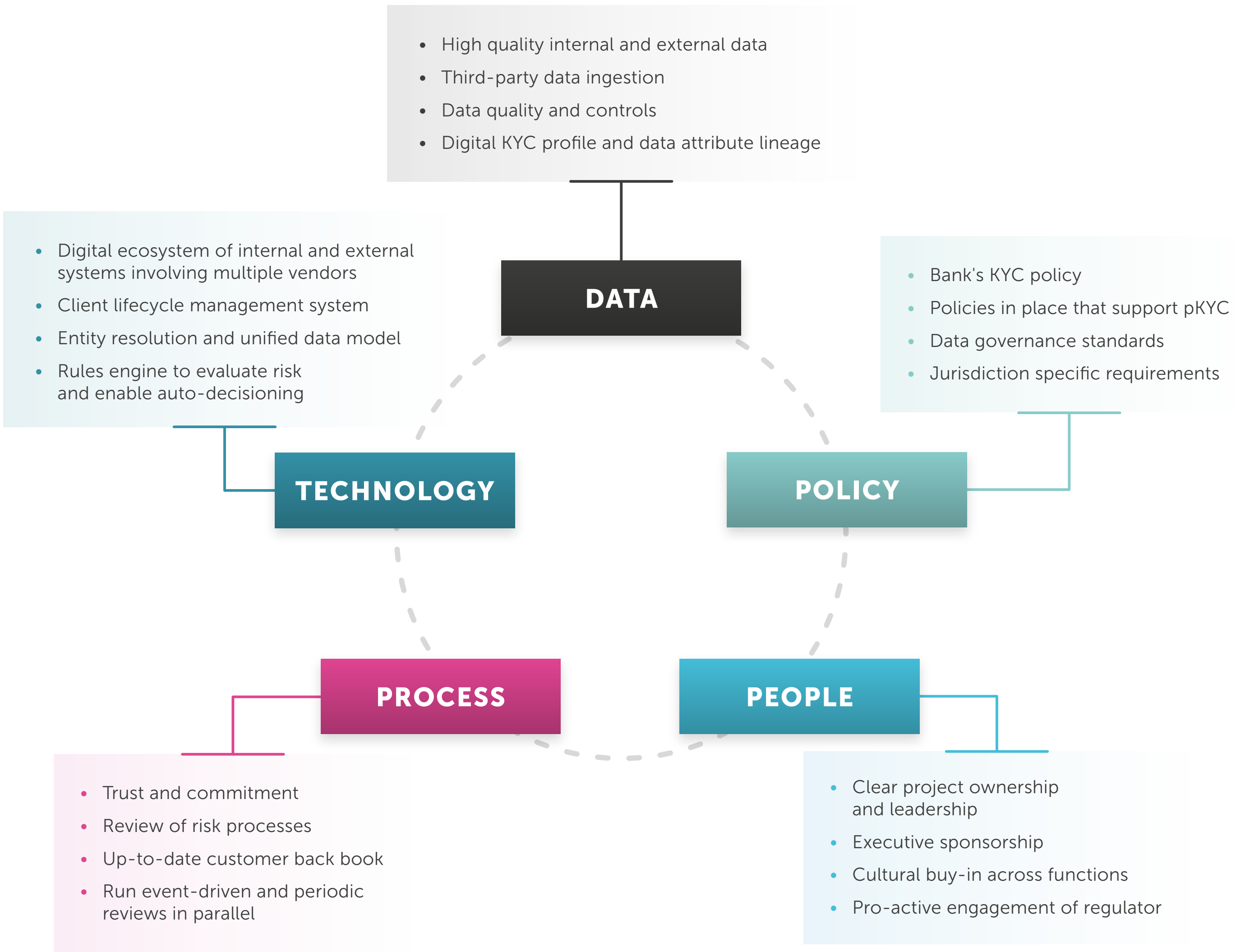
A framework for pKYC

A framework for pKYC

The journey to pKYC is not straightforward. Aside from a widespread lack of understanding of what it takes to get to a truly perpetual process, firms are likely to face a number of other challenges to be negotiated along the way. We have worked with our advisory board members to develop a standardized framework that illustrates the primary considerations involved in the journey.

This framework consists of five categories, each housing four sub-components that are considered to be enablers of pKYC adoption (see **Figure 1**).

Figure 1 A framework for adopting pKYC[2]



[2] Data, Policy, People, Process and Technology will hereon be referred to as categories, unless otherwise specified. Each of the components within the categories will be referred to as sub-components.

DATA

Regulatory pressure is growing around KYC effectiveness, with supervisors challenging firms to do more with data and improve their systems and controls. This pressure, together with a wider availability of data, will certainly help to make full pKYC a more achievable goal. After all, it is built on the premise that collecting and transferring the correct data in the right way, at the right time, enables firms to better assess customer risk and comply with regulatory requirements.

POLICY

pKYC transformation projects will come under close scrutiny by regulators. As a result, institutions must ensure data governance standards are upheld, and it may be necessary to introduce specific policy or operational guides to support pKYC.

PEOPLE

Engaging the right blend of stakeholders is critical for a transformation project of any kind. Clear project ownership, and sponsorship, are pivotal to driving change, with the transformation team forming the backbone of a pKYC change program. These internal champions will ensure that best practices are upheld throughout by delivering unbiased, collective action.

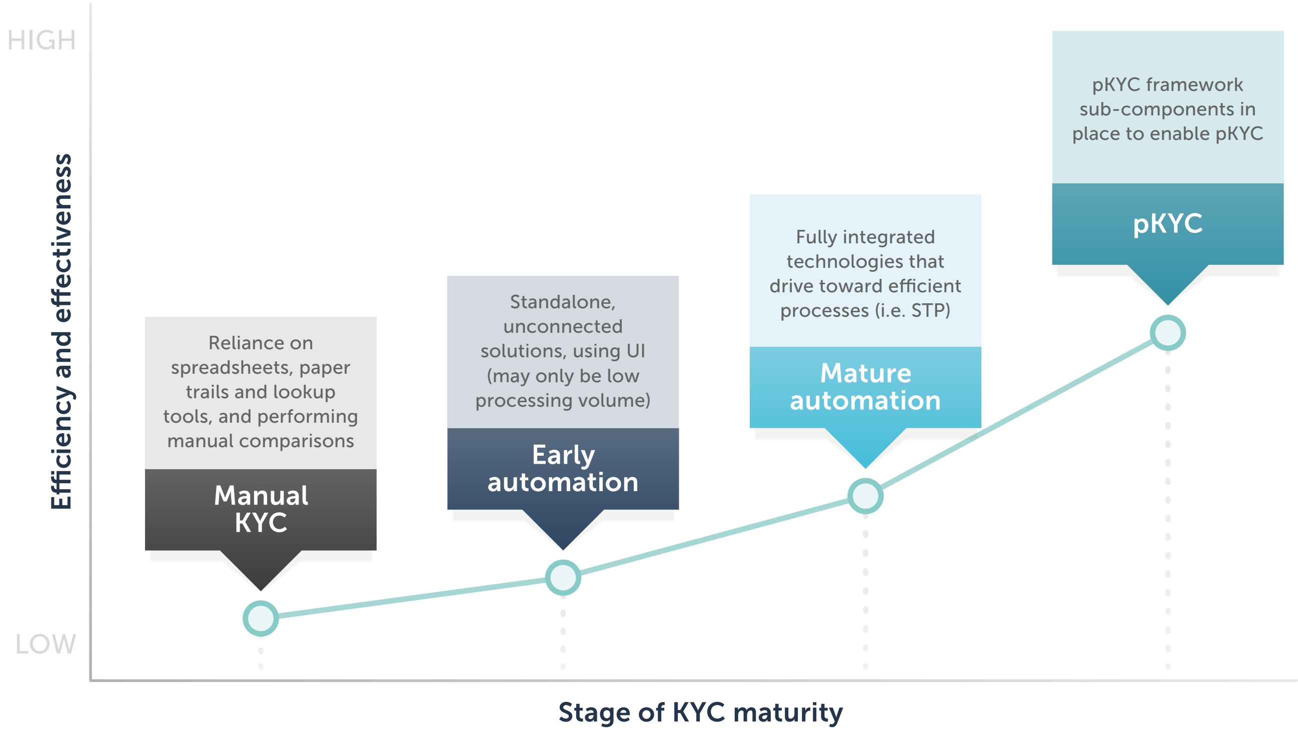
PROCESS

Successful pKYC implementation involves managing multiple stakeholders, data inputs and technology stacks. Defining clear process requirements, both at an organizational and individual level, will enable firms to build and maintain stakeholder trust while ensuring compliance and reducing risk exposure.

TECHNOLOGY

Technology becomes increasingly important as firms pursue more mature automation, and institutions must leverage emerging software to control how data is stored, structured and assessed. They shouldn't necessarily expect to solely develop these solutions in-house, rather, pKYC is made possible by a digital ecosystem of internal and external systems, often involving multiple vendors. Effective entity resolution and a unified data model are paramount if firms are to realize the utility of their technology stacks.

Figure 2 The KYC maturity curve



The pKYC maturity model

The journey to pKYC delivers iterative benefits throughout the transformation program. As part of developing a realistic roadmap, we have highlighted the relative stages of KYC maturity used to frame discussions with our advisory board and progress the framework into a pKYC maturity model. The aim is to highlight critical components at each level so firms can break down and prioritize the categories and sub-components to progress along the curve, irrespective of their starting point (see **Figure 2**).

Using the MoSCoW prioritization model, the importance of each sub-component across the maturity model was assessed. Developed by Dai Clegg of Oracle, this method aids task prioritization during development work on product releases, as part of the Dynamic System Development Method[3]. For us, it offered a standardized scoring system to suitably evaluate the criticality of each sub-component during pKYC transformation. The scoring system is briefly explained below:

Must-have
Non-negotiable initiatives for pKYC deployment

Should-have
Important initiatives that are not vital, but would be considered operationally required for pKYC automation

Could-have
Nice-to-have initiatives that will have little impact if left out

Won't-have
Initiatives that are not relevant or not a priority for pKYC deployment

[3] agilebusiness.org/dsdm-project-framework/moscow-prioririsation.html

04

Data

High quality internal and external data

pKYC, by definition, requires a degree of automation, with the trigger-based model being underpinned by access to accurate and timely data. For institutions looking to adopt an event-driven approach to KYC, outdated, incorrect or missing customer information significantly reduces the reliability of associated triggers. If these cannot be trusted, the process cannot function as intended and firms are forced to rely on periodic reviews out of fear of missing key risk indicators.

Our advisory board members cited the need for clean data when pursuing automation. In the context of pKYC, this refers to accurate and reliable customer data. As a result, data cleansing - while perhaps considered tedious and mundane - should be a primary focus for firms as they progress to mature automation and pKYC. Data cleansing refers to the process of detecting and correcting corrupt or inaccurate records in order to identify incomplete, incorrect or irrelevant attributes for remediation.

Data relevancy is another key consideration. With pKYC, it is not simply a case of more is better. Instead, in the interest of enhancing efficiency and effectiveness, institutions must identify the attributes necessary for pKYC, or KYC more generally, and focus on accessing, storing and analyzing those. Questioning data relevancy enables institutions to limit the data remediation workload and foster a more robust pKYC framework. Ultimately, organizations need to ensure that they have the data needed to comply with the latest regulations and their own financial crime risk management policies, while having the required attributes to effectively assign customer risk scores to ensure that this continues to reflect the appropriate risk rating.

Our previous advisory board whitepaper, Identifying your logical start point[4], discussed the role that data can play in driving change. Specifically, it outlined the utility of organizational data and how this can be used to prove and disprove internal hypotheses. As a result, it can be an important tool, used to overcome internal resistance and guide policy and process decisions, as well as improve client relationships, to drive better KYC outcomes.

Third-party data ingestion

Third-party data ingestion is a critical element of obtaining a single view of a client an institution can trust. While clients provide certain data points, true behavior is revealed in external data. Tracking sources and history of third-party data ingested is also key. Triangulation is needed to understand where internal and external data is misaligned, reveal areas of risk and generate review triggers.

If monitored appropriately, third-party data sources can highlight a plethora of information relevant to a risk assessment or the emergence of new information; for example, a new customer relationship with a Politically Exposed Person (PEP), the implementation of new sanctions, new pieces of adverse media, or fresh law enforcement investigations or operations regarding an individual or a company.

[4] insights.encompasscorporation.com/pkyc-advisory-board-identifying-logical-start

Digital KYC profile containing source documents and data attribute lineage

Gone are the days when institutions could rely on maintaining physical KYC profiles for their entire customer base. Most firms will have digitized this information to some extent, however, the sophistication of these profiles varies greatly. At its most basic, a digital KYC profile may refer to storing client information in a manual spreadsheet, however, as firms chase mature automation and pKYC, it is important to evolve and move towards fully integrated digital KYC profiles[5].

Each digital KYC profile should include:

- **Complete customer information** relevant to identifying KYC risks
- **A visualization of corporate ownership structure**, with beneficial owners, PEPs and sanctions clearly identified
- **Packaged documentary evidence** and relevant metadata
- **Any adverse media identified**, and actions taken, recorded in a dynamic audit trail

Firms can increase efficiency by sourcing data directly from third parties via API feeds. As a result, data attribute lineage and an accurate audit trail become increasingly important as they introduce more mature automation. Data lineage is the process of understanding, recording, and visualizing data as it flows from data sources to consumption. This includes all transformations of data, how it was transformed, what changed and why.

[5] encompasscorporation.com/kyc-aml-platform/ekyc-digital-kyc-profile/

05

Policy

The bank's KYC policy and operational standards

All financial institutions will have some form of KYC policy documentation, irrespective of the sophistication of surrounding processes. The KYC policy will contain guidelines produced to limit the firm's exposure to money laundering, based on regulatory requirements for each jurisdiction it operates in, while enabling better customer service and risk management. KYC policies typically include four key elements:

- **Customer acceptance policy**
  Defining the basis upon which the institution enters into relationships (for example, no accounts shall be opened in the name of shell companies).
- **Customer identification procedures**
  Detailing the type of documentation required for customer verification.
- **Risk management**
  Classifying customers by risk level, based on the organization's broader risk appetite. This may vary based on company culture, competitors, broader industry trends or the nature of operations.
- **Ongoing due diligence**
  Routinely monitor customer transactions to ensure they remain in line with expectations.

> "Large institutions often have an overarching KYC policy which rarely changes, instead, you would make the change in the associated operating standards. Policy sets risk appetite, then how you operationalize those steps is held in supporting documents.
>
> pKYC advisory board member

KYC policy is a must-have at any stage of the pKYC journey. As firms progress toward more mature automation, it is important to realize that this overarching KYC policy won't necessarily need to change. Instead, the operationalization of the principles should evolve. Broad risk thresholds, data source requirements and customer acceptance criteria remain largely static, with alterations being driven by external factors or changes to service offerings.

Policies in place that support pKYC

pKYC represents an entirely new operating model so, as institutions progress along the KYC maturity curve, operational policies and standards become increasingly important. Specifically, as an organization transitions to a data-enabled and event-driven approach to customer refresh, the associated thresholds for investigation must be carefully reviewed and agreed, based on existing objectives and capabilities. Supporting policies should clearly articulate the data inputs and associated risk metrics that constitute material change and subsequently trigger cross-checks, manual intervention or full client refresh. Similarly, non-material changes may be addressed by straight through processing to the customer record. Failure to clearly define such thresholds puts compliance officers at risk of becoming inundated with false positives[6], also increasing analysts' workload.

As systems evolve, supporting policies may need to be digitized or encoded to feed rules engines, with our advisory board members suggesting that firms may wish to engage regulators when making these changes.

Data governance standards

Data governance standards are designed to protect the availability, utility, integrity and security of data (typically customer information and transaction records) within the enterprise and its systems. These frameworks are often set at the organizational level, as prescribed and enforced by business executives or data management professionals. These stakeholders are also responsible for data quality controls and related accountability mechanisms, which are particularly important when related to personal data used in anti-money laundering (AML) KYC checks.

> "It is rare that a firm will bring in pKYC operational guidelines without engaging a supervisor.
>
> pKYC advisory board member

KYC and broader compliance functions must adhere to the organization's data governance standards but are unlikely to dictate the structure of the framework itself. As a result, a pKYC transformation project is considered a consumer of data governance policies rather than a driver. KYC professionals must support the execution of the data governance framework by defining the essential data processing components of a pKYC program, including implementing protocols to improve and manage data quality, identify data issues and assign data owners – and all while ensuring security and privacy.

While data governance considerations are crucial at all levels of KYC, they become far more complex to integrate and manage as firms introduce more automation, and platform technology enablers such as data profiling and lineage become critical to the ability to automate and scale KYC processes that accelerate time to value.

[6] Customer records that trigger a positive match based on the system algorithm, but on further research turn out to be an incorrect positive match. Contrast to false negatives where the system algorithm fails to detect a true match.

Jurisdiction-specific requirements

Regulatory approaches to innovation, and pKYC specifically, differ significantly across jurisdictions, with supervisors existing along a continuum of openness to automation.

Some Asian regulators are extremely vocal in their desire for institutions to automate, with principles being released about the fair use of automated solutions in the financial sector in order to encourage adoption. However, while some are open to innovation, guidance is rarely tailored to solutions or specific use cases, such as pKYC.

In the EU, 6AMLD does not call for pKYC specifically but it does highlight the need for up-to-date technology to manage lower risk KYC profiles[7]. European regulators have embraced automation but lack prescriptive regulations providing relevant guidance, which may have held back uniform adoption. Part of the challenge here is the regulator's lack of understanding of how pKYC works in practice, so there is the need to be more familiar with the approach prior to issuing any guidelines.

Elsewhere, there are more stringent regulatory requirements to navigate, particularly in terms of what institutions can and cannot outsource. For some supervisors, utilizing data collection processes via external services that are not reviewed step-by-step by a human is considered outsourcing and therefore not permitted.

Adhering to regulations is one of the most important considerations for firms at any stage of KYC automation. However, as they progress to a more automated KYC approach, it will remain important to have some level of standard widespread automation across all subsidiaries and jurisdictions to reduce the resource burden. Our advisory board recommended that institutions begin by automating at a global level before tailoring the approach to different geographies. By dealing with each region separately from the outset, firms would forgo uniformity in operational standards.

[7] eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L1673

06

People

Executive sponsorship

The power of executive sponsorship cannot be overestimated in a pKYC transformation project, particularly when trying to convince the respective budget holders. Achieving mature automation, and pKYC, requires substantial and targeted investment as it represents a huge change to the organization's operating footprint.

Truly influential executive sponsors do more than just solicit financial support. They are instrumental in aligning internal stakeholders to the broad transformation goals by identifying and aggregating the resources necessary for the project to succeed, and they also provide the support needed to navigate the various challenges and stages of transformation. Additionally, executive sponsorship is vital when drumming up regulatory support, as it is these individuals who will be leading conversations with supervisors.

> You are not going to be able to get supervisors on board if the execs aren't convinced.
>
> pKYC advisory board member

So, which primary executives are most important from a KYC perspective? While the answer to this question may be influenced by a number of factors, such as the size or situation of the firm in question, our advisory board members highlighted a number of key personas:

- **Operations executives**
  An operations executive typically leads and direct aspects of banking operations, such as determining the operational plans and projects that best support the organization's objectives and business plan.

- **Business service owner**
  A business service owner plans, directs and coordinates the administrative processes that underpin various business functions.

- **Compliance executives**
  The role of compliance executive is to ensure that institutions operate with integrity and adhere to applicable laws, regulations and internal policies.

- **Board and C-suite**
  These individuals are often the most influential members of an organization, dictating the company's strategy and ensuring operations align with the strategic direction.

Clear project ownership and leadership

Having the right leadership throughout a transformation project is paramount. The concept of automation can be daunting for many, particularly when this automation is closely tied to compliance outcomes as is the case with pKYC. As a result, pKYC projects will benefit from tech-minded leadership figures who will be able to understand and articulate the operational processes involved. Having the right guidance can help teams to garner the necessary support to truly drive change.

A KYC transformation project will seldom be owned or championed by a single individual. Instead, institutions often find the most value in establishing a group of experts that can be given the space to understand the problem by evaluating existing processes in order to plot the right path forward.

This transformation team - as it was referred to by our advisory board members - may take several forms. Some institutions will establish an entirely separate team to better mediate stakeholders and manage budgets without inherent bias. Alternatively, others may find value in closely involving KYC and compliance teams to ensure satisfactory outcomes. Depending on the size of the firm, this team may be formed of an even larger group, with research and development functions collaborating with peers in risk, transformation and operations - all of whom would need to work closely to ensure the outputs are most valuable.

With that said, the availability of resources will depend on the size of the organization and budget, as well as the complexity of the project at hand. Regardless of the approach though, a clear leadership team remains a key piece of the proverbial puzzle, growing in importance as firms progress to more sophisticated automation.

Cultural buy-in across functions

Resistance to change is a potential barrier in a transformation project of any kind, with fear, uncertainty and corporate inertia often playing a prominent role in stifling innovation. Such challenges are exacerbated within firms as the number of stakeholders increases, meaning larger institutions can often be outdone by their smaller, more agile counterparts.

> “People do not necessarily resist the change itself, rather they resist the perceived outcomes.
>
> pKYC advisory board member

Over the course of the advisory board sessions, a number of members offered examples of instances when they presented stakeholders with ways to automate certain processes but adoption did not follow as it should. Resistance is an inevitable response to any change, as an individual’s initial reaction is to defend the status quo if they do not understand the benefits and/or feel their sense of security is threatened. People do not necessarily resist the change itself, rather they resist the perceived outcomes.

It is a must that cultural buy-in happens early in a KYC transformation project. One of the most challenging steps in a journey to automation is helping employees to trust technology, however, when achieved, adoption rises dramatically. From a pKYC perspective, this kind of buy-in involves articulating to employees that this is a process of upskilling rather than displacement. Indeed, while the desired outcome is operational efficiency, employees will be involved in reviewing relevant customer matches by leveraging more effective solutions. Individuals commonly fear losing their jobs to technology, so leaders must convey that their role will adapt, not disappear, and, in fact, leveraging technology can free up more time to focus on more valuable investigative tasks.

Proactive engagement of the regulator

AML regulations require firms to apply risk-based customer due diligence in order to limit exposure to undue financial crime threats. Supervisors largely leave it to firms to determine risk thresholds and, as a result, the frequency with which they reassess customer information. In theory, transitioning to pKYC does not require a firm to engage a regulator directly as many supervisors are technology agnostic and less concerned with how firms comply, than the effectiveness of controls.

What might this engagement look like?

Proactive regulatory engagement can be achieved through regular information-sharing exercises. These may include contributing to consultations and proactively seeking their input on matters within their jurisdiction by scheduling meetings and video conferences to build relationships.

Some regulators have also implemented innovation teams and created sandboxes to test new approaches in a safe environment. For example, in the UK, the Financial Conduct Autority (FCA) Regulatory Sandbox allows firms to test innovative propositions, while US regulators have introduced innovation hours where technology providers demonstrate latest solutions with Q&A feedback.

Overall, it is important to maintain open lines of communication as best you can to ensure regulators are not surprised by decisions that you make.

That said, the advisory board recommended engaging regulators early and often. Educating and obtaining feedback from supervisors as soon as possible enables leaders to make better and more timely decisions, while minimizing the risk of costly project disruptions at a later development stage. Such engagement will vary greatly depending on the regulator in question, while closer engagement may be required for those reluctant to automate.

Regulator discussions regarding pKYC can be difficult. Moving toward a more risk-oriented approach is precisely what regulators want, yet a public reluctance to automate can present challenges. Part of the issue lies in the fact regulators lack an internal mandate to understand new technology approaches - their focus is on the outcome rather than the process.

Our advisory board members offered some advice as to how firms can best approach supervisory conversations, concluding that language is key. Transitioning toward pKYC is about augmentation and firms should avoid drawing attention to deficiencies in existing processes. This is not necessarily a case of out with the old, in with the new; instead, firms should appreciate that regulators want to maintain a safety blanket of human involvement or periodic reviews where possible. It is important to frame the transformation as an exercise in adding controls rather than changing them. Maintaining a periodic review regime in pKYC, while improving all of the steps before and around it, will likely lead to a far easier regulatory conversation.

07

Process

Trust

Trust and cultural buy-in are two related, yet distinct, concepts. While buy-in represents an active acceptance of the project vision, trust develops more slowly and its effects are longer lasting. We have already outlined the importance of achieving stakeholder buy-in as early as possible, but, when it comes to trust, the advice is not quite as straightforward.

Focusing on earning employee trust too soon may generate unnecessary friction and it can also be costly for the organization if the project in question doesn't make it off the ground. Obtaining trust should be a natural evolution. There is often little to gain from pursuing this prior to process implementation, as it may differ in theory versus practice. Advisory board members recommended that institutions leverage data to gain this trust as objective organizational data, presented by internal stakeholders, is far more influential than subjective reasoning. Stakeholders must be able to effectively communicate the benefits to the bottom line while illustrating the urgency of adapting to the rapidly evolving threat and regulatory landscape.

The customer back book

A back book of customer data must reach a certain level of freshness before transitioning to pKYC.

Ideally, all periodic reviews should provide a robust foundation of KYC data that is both up-to-date and reliable. This baseline becomes increasingly important as firms progress along the maturity curve, as trigger-based reviews are made possible by comparing existing data with continuous inputs and flagging inconsistencies. If the underlying customer data is out-of-date, institutions are likely to expose themselves to greater volumes of false positives. Unsurprisingly, if the customer back book is not fresh, the first run through of a pKYC process will result in a large volume of matches, which can overwhelm existing staff.

> Ultimately, firms need to reach a base level that they are satisfied with. This involves reviewing all client data, then you have the basis from which you can evolve and begin looking at things from an event driven perspective.
>
> pKYC advisory board member

Performing parallel running of event-driven and periodic reviews

Sustaining parallel running of periodic reviews alongside event-driven investigations is a sure-fire way of maintaining security but this approach is not sustainable, nor is it necessary once pKYC is fully introduced. In the majority of cases, parallel running should only be performed during the transition phase - the length of which will be determined by a number of factors, such as the regulator's openness to innovation, the size of the firm, and its relative technological maturity.

The changeover period presents regulators and internal stakeholders with a degree of anxiety, so parallel running is necessary to perform quality assurance in order to sign off from one process to another. For example, comparing the output of the pKYC process to that of a manual process can provide evidence of whether or not the automated reviews are as effective as human reviews, or perhaps even more so. Stakeholders must demonstrate to regulators and board members that the manual review and risk engine are delivering the same results.

Can we get rid of periodic reviews entirely?

Importantly, our advisory board concluded that firms should always have the option to trigger manual reviews – no matter the stage - if a particular (higher risk) record has been neglected for a certain period. These reviews can continue to occur for specific business lines or jurisdictions where the operational risks have been found to be too high to move to a new pKYC process.

Data accessibility may also dictate a bank's choice when it comes to whether they solely rely on automated reviews. Some client types may remain on a manual, periodic review schedule indefinitely due to limitations in data coverage, whereas UK-based enterprises might not require periodic reviews as the volume of transactional, KYC and third-party data is sufficient to create an accurate real-time picture of client circumstance. Conversely, joint ventures can be more opaque in their organizational structure, making it more difficult to access information automatically, so it is important to have periodic dialog with the client.

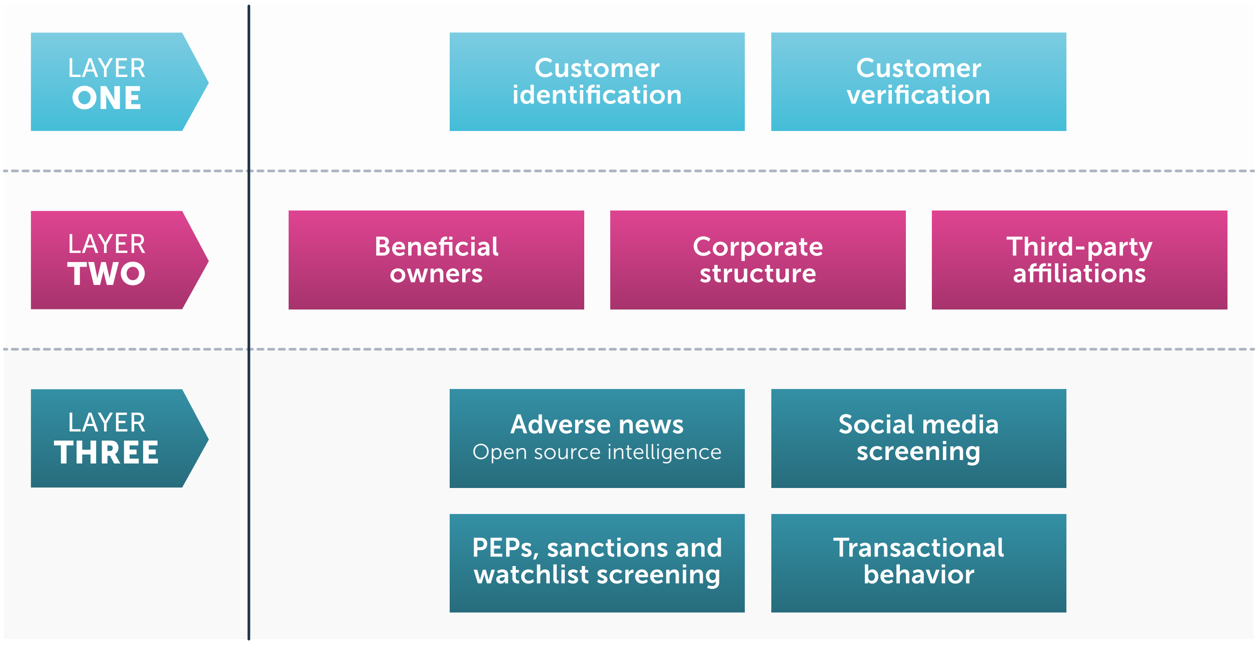
08

Technology

Digital ecosystem of multiple vendors

Conducting robust KYC checks, both during onboarding and in perpetuity, means analyzing vast amounts of data. **Figure 3** provides a simplified view of the layers involved in risk scoring a potential or existing customer[8].

Figure 3 The layers of KYC



The complexity of KYC checks requires some form of digital software ecosystem at any level of automation. It remains at the discretion of the firm as to whether these solutions are developed in-house, or if they utilize one or multiple vendors. The RegTech landscape mirrors the needs of the institutions it services, with almost 500 different solutions, across nine subcategories of financial crime[9].

Typically, firms favor constructing an ecosystem of specialized third-party vendors that integrate to manage the entire KYC process end-to-end. This multi-vendor approach involves leveraging a separate product for each function, such as identity verification and watchlist screening. This reduces implementation risk while also offering greater flexibility and scalability as the firm grows. Developing solutions in-house can be resource intensive and the fast-evolving financial crime landscape requires constant revisions to, and investment in, software capabilities. Firms may therefore find it beneficial to enlist third-party vendors, focusing internal resources on investigations.

[8] While this process is largely linear during onboarding, a pKYC trigger can come from any layer, acting as a catalyst to review information across all of the other inputs.

[9] radar.rtassociates.co/

Entity resolution and unified data model

Accurate and reliable internal and external data is redundant if institutions are unable to use it effectively in a pKYC setting. There may be different interpretations of what type of data is needed to facilitate pKYC, which itself could be spread across multiple systems. Firms should consider aggregating this information into a single workflow system (for example, a Client Lifecycle Management (CLM) platform) to combine the necessary inputs.

The advisory board sessions saw members debate the data actualization vs data virtualization approach. Firms may aim to create a centralized repository to store all structured and unstructured customer data at any scale. This allows the organization to store data as-is and overlay dashboards and visualizations, real-time analytics, and machine learning to guide better decisions. However, some members were critical of this single system approach, saying that the limitations of legacy technology and information silos have forced many to think more creatively about their data infrastructure. As a result, it may be more effective to explore how existing systems can better integrate, so users can retrieve and manipulate data without concerns about where it is stored or how it is formatted.

Regardless, organizations should use technology to control how data is stored, structured and accessed. Effective entity resolution and a unified data model are paramount, with both of the aforementioned methods aiming to solve a common problem by bringing sources together and enabling firms to apply their rules effectively to better identify KYC triggers. Entity resolution serves as the bandage that firms can stick across data silos to grant stakeholders access to the information they require, enabling firms to bring external data into different internal systems to create an ecosystem that enhances collaboration and auto-decisioning.

CLM (or a business process workflow management) system

CLM workflow approaches represent an integral component to KYC processes today by automating end-to-end risk decisioning. While workflow solutions are used across multiple business processes, pKYC is particularly relevant given the ongoing and real-time nature of the review process. CLM systems automate and streamline the required decisioning rules inherent in the KYC policy and allow firms to automate every stage of the client's lifecycle, from the time they are onboarded as part of the KYC process, through the ongoing relationship until they are offboarded.

The CLM, whether home-built or a vendor solution, must connect to all the components within the ecosystem, serving as the central record for all of a bank's client KYC records. As with all sub-components of the pKYC framework, the level of sophistication within the CLM will evolve as the level of automation increases. As firms strive for pKYC, the CLM must automate the decisioning process and manage the review process without the need for manual intervention.

09

Setting your pKYC vision

Setting your pKYC vision

Even the terminology associated with pKYC can be daunting, causing it to be misunderstood as an unrealistic and revolutionary step for institutions. However, adopting a structured approach to process change, which focuses on individual tasks and outcomes that make KYC work better for the organization, will make the journey easier to plan, execute and sell - both internally and externally.

It is important to recognize pKYC approaches continue to evolve based on technology solutions available, and there is no one size fits all solution.

Whichever technology firms choose to deploy, they will need to have API integrations in and out of internal systems to be able to manage data seamlessly, as well as process expected alerts from both internal and external data sources to enable pKYC.

Institutions will approach this transformation from varying starting points and, wherever that may be, this research should support stakeholders in evaluating their current maturity, identifying gaps and planning a path forward that realizes the many benefits of pKYC.

About Encompass

Encompass enables firms to deliver revenue faster, drive operational efficiency and demonstrate consistent compliance with dynamic KYC process automation. Our award-winning platform, unrivaled data connections and industry expertise help clients to create and maintain real-time digital risk profiles of everyone they do business with.

Our customers include leading global banks and financial institutions, including Wolfsberg Group members. We have strategic alliances with a range of trusted data, technology and consulting partners, enabling the seamless integration of Encompass into existing workflows and systems.

Find out more at encompasscorporation.com.

encompass

the full picture, fast

t +1 332-245-4398 | +44 333-772-0002 | +61 300-362-667

e info@encompasscorporation.com

w encompasscorporation.com

New York • London • Singapore • Amsterdam • Sydney • Glasgow • Belgrade