Integrating perpetual KYC (pKYC) into your regulatory compliance roadmap

Gain efficiencies, meet regulatory expectations, and better counter money laundering and terrorist financing

In partnership with

encompass
the full picture, fast

Capgemini

How well do you know your customers?

Regulators view the know-your-customer (KYC) process – performed by a financial institution at the time of onboarding and across the lifecycle of the relationship – as arguably the most important part of an anti-money-laundering (AML) program. KYC is the cornerstone of an AML program as it is integral to all other stages, including transaction monitoring, SAR filings, and sanctions screening.

KYC begins with verifying customer identity and, for certain legal entities, includes determining their ultimate beneficial owners (UBOs). Banks and other financial institutions are subject to the Bank Secrecy Act (BSA), which requires establishing customer identification programs. But far more than that is required for effective KYC.

The Financial Crimes Enforcement Network (FinCEN), the agency within the Treasury Department devoted to combatting money laundering, expects financial institutions to understand the nature and purpose of customer relationships and to conduct ongoing monitoring. Indeed, failure to adequately perform customer due diligence (CDD, which is largely equivalent to KYC) and identify, report, and freeze sanctioned entities, can result in enforcement actions by regulators, including large monetary penalties.

That's what makes the "know" part of KYC so critical. A financial institution must truly understand each customer – who the organization is controlled by; the level of AML risk presented, what types of activities or business are regularly conducted; their source of wealth and income; what deposits, withdrawals, and payments can be expected to be made– ultimately, how the organization can be expected to behave.

Only when a financial institution conducts strong KYC does the organization come to truly understand what the customer's "normal" activity is. When KYC is done well, it's easier to identify what's abnormal or suspicious and deserving of being reported to regulatory authorities. For these reasons, FinCEN has formally labelled CDD as the 5th pillar of AML compliance (along with internal controls, independent testing, training, and an adequate BSA/AML Officer).

Challenges to the traditional KYC process

The traditional KYC approach struggles to keep pace with modern money laundering activity, and can lead to a financial institution's resources, operating costs, and internal controls being overwhelmed. Previously, KYC has been conducted in a static, point in time, "nonintelligent" manner. Financial institutions have traditionally evaluated customers periodically, with frequency of review based on risk rating —low, medium, or high — and isolated major trigger events, such as a SAR being filed or Section 314 request being received. The typical schedule for these reviews is up to five years for low-risk customers and one year for high-risk organizations. These traditional KYC practices allow customers andone year for high-risk organizations.

These traditional KYC practices allow customers who move from low risk to high risk in a short period of time to remain unnoticed for months or even years, until the next review occurs. As a result, many financial institutions put themselves at risk while continuing to work with non-compliant organizations despite clear evidence of money laundering. Indeed, many of the enforcement actions and large fines that are made public are related to inadequate KYC.

Responsible innovation can be key to securing compliance

Industry standard, which financial institutions are expected to meet or exceed, has shifted greatly in the last few years. Accompanying this has been a sea change in the mindset of AML regulators, moving from mistrust to embrace toward use of new technologies including but not limited to artificial intelligence (AI), machine learning (ML), cloud computing, intelligent process automation and data analytics — all with the goal of enhancing AML processes.

Evidence of this shift is abundant. In January 2017, the Office of the Comptroller of the Currency, which supervises the largest banks in the U.S., established an Office of Innovation designed to ensure that national banks "have a regulatory framework that is receptive to responsible innovation and the supervision that supports it." Later that year, the Financial Action Task Force, the global agency that promulgates AML standards, formally endorsed responsible innovation for AML in a public statement. In 2019, a group of senior U.S. bank supervisors together with FinCEN released a joint statement encouraging financial institutions to adopt innovative approaches, including the use of AI, to meet their obligations under the Bank Secrecy Act.

This mindset was codified in the Anti-Money Laundering Act of 2020, with the goal of encouraging the adoption of new technology by financial institutions to more effectively counter money laundering and terrorist financing. Moreover, the New York Department of Financial Services has recently established its DFS Exchange Program to "foster the growth of responsible innovation in financial services in New York."

FinCEN itself has established an "Innovation Initiative" that seeks to promote "responsible financial services innovation that furthers the purposes of the BSA." Him Das, FinCEN Acting Director, told the American Bankers Association members earlier this year that regulators recognize that "relying on timeconsuming and onerous manual processes for research, analysis, and communicating and collecting data is a major problem".

We also see focus on innovation from regulators globally. In the U.K., the Financial Conduct Authority (FCA) has established an Innovation Hub that seeks to "support financial services firms to launch innovative products and services." Initiatives include regulatory sandboxes where financial services firms can test new propositions using synthetic data sets with real customers in a safe environment to develop innovative technology solutions. For years, the FCA has organized "Tech Sprints" that bring participants across the financial ecosystem to address industry challenges. Other global regulators like the Monetary Authority of Singapore, the Hong Kong's Monetary Authority, and Germany's BaFIN have also introduced similar programs.

Six components of a strong pKYC program

Regulators now look for – due to available technology – improvements in process akin to what has come to be known as perpetual KYC ("pKYC"), or the continuous monitoring of customers, providing organizations the ability to respond to customer behavior changes in real time. When done correctly, pKYC proactively alerts financial institutions to significant milestones in a customer's lifecycle that affect its risk level and the organization's overall risk exposure. PKYC helps firms maintain up-todate customer profiles and achieve a state of continuous compliance.

Implementing pKYC is, of course, not without challenge. Roadblocks include the consolidation of data across internal systems and external sources, choosing the right pKYC technology, and ensuring that the new process will meet supervisory expectations, all of which involve a number of considerations.

The following are six industry best practices to building and optimizing a pKYC program across your operation:

1. **Explainability/transparency:** "Explainability" is the extent to which new technologies, particularly AI decisioning processes and their underlying algorithms incorporated into a pKYC solution, can be reasonably understood. Regulators don't want black box solutions that are opaque and non-intuitive. Where cloud computing is leveraged, the ability to trace customer data across jurisdiction also should be clearly documented and understood. Audit trails are especially important here. Sufficient explainability should be present for both the overall functioning of the pKYC process and for each individual outcome. Moreover, compliance, audit, and risk personnel also need to sufficiently understand AI models to ensure that they conform to regulatory and legal requirements, as well as the firms' policies, procedures, and risk appetites.

2. **Human judgment:**
   Though new AML technologies play an increasingly important role, by reducing manual effort (and subsequently human error), they should not be expected to fully replace human input and judgment. A proper balance must be struck between integrating pKYC's new technologies and retaining human oversight – by leveraging AI, machine learning and data analytics with the use of skilled investigators.

3. **Residual risks:**
   Financial institutions should assess whether there are residual risks that may arise with the use of new technologies, such as bad data being inputted, difficulty in integrating into legacy systems, 'cleansing' customer data, or biased conclusions being drawn. Where such risks are identified, financial institutions should demonstrate awareness of these risks and the ability to mitigate them. Note also that parallel approaches to introducing new pKYC models alongside traditional KYC operations provide the opportunity to help compare outputs and further reduce residual risk.

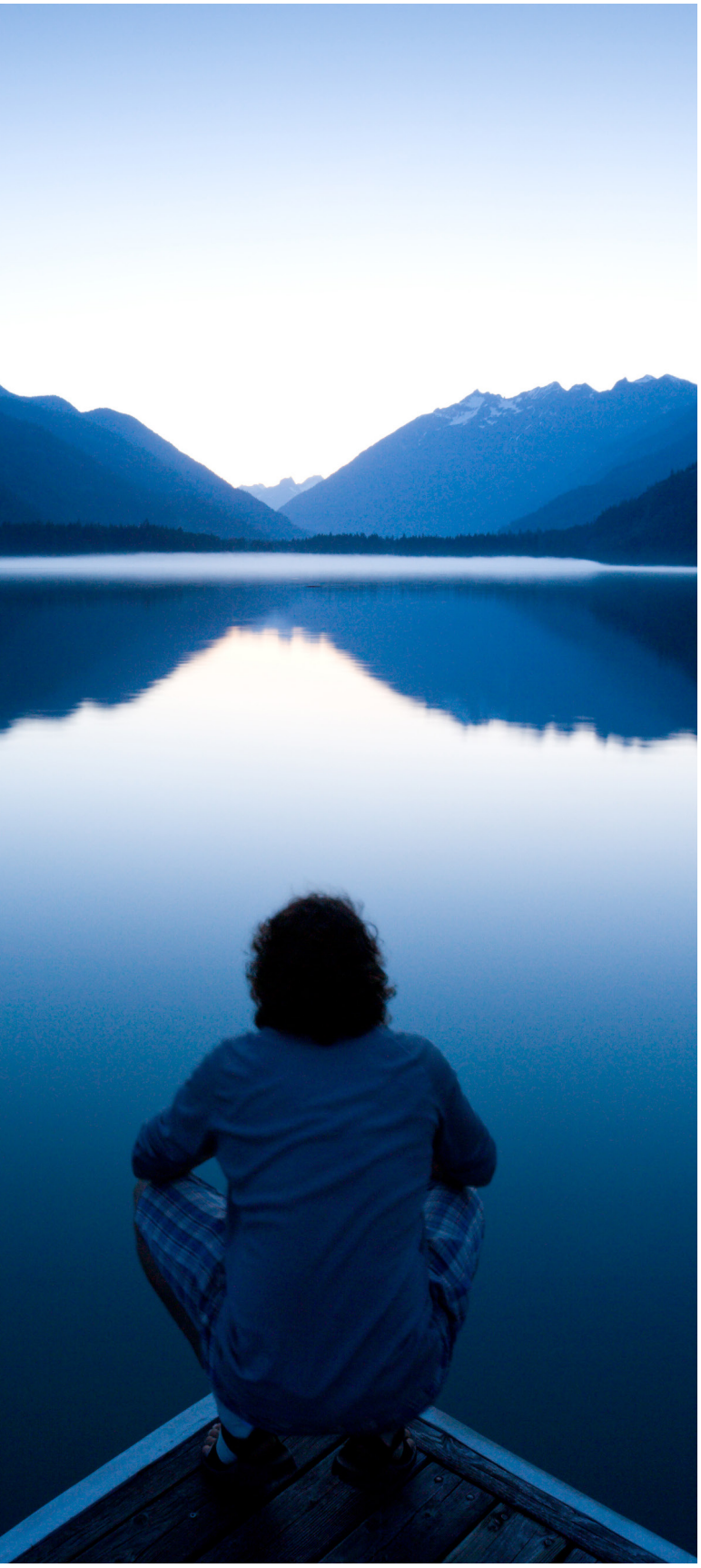
4. **Data management, provenance, and governance:**
   Data governance, provenance, and management are fundamental to maintaining the confidentiality, integrity, and availability of information needed to assess AML risk. The FFIEC Manual requires examiners to review for considerations such as data identification and classification processes, data management controls for safeguarding data in physical and digital form, and the effectiveness of processes for securing databases, analytics tools, and reports. When a pKYC solution is deployed that leverages AI, external data sources and process automation; understanding data origins, use, and legitimacy is crucial – even more so when it involves dynamic updating or algorithms that identify patterns and correlations without human context or intervention.

   Data lineage provides clarity as to sources of data for auditability purposes. Because AI and ML algorithms are dependent upon the quality of the data used, pKYC platforms could perpetuate or even amplify bias or inaccuracies inherent in the data or make incorrect predictions if a data set is incomplete, nonrepresentative, or otherwise flawed. For example, how multiple customer data is merged and reduplicated is important to identify and test before deployment.

   Regulators expect financial institutions to have in place effective governance that ensures data is consistent and trustworthy and doesn't get misused. Two best practices are key to doing this well:

   - Establish a customer 'digital profile.' This will develop a consistent picture of each customer, incorporating relevant, up-to-date information used for pKYC processes.

   - Have proper data governance. As digital profiles often incorporate data from internal and external sources, proper data governance requires reaching into all the places where relevant information resides, such as servers, desktops, tablets, smartphones, and cloud applications.



5.Model risk management:

Model risk is a fundamental concern for regulators. Potential adverse outcomes from use of new technologies can arise from poorly designed underlying mathematical models, faulty data, changes in model assumptions over time, inadequate model validation or testing, or limited human oversight, as well as inadequate planning and due diligence of all models. Financial institutions should periodically assess each AML risk model using a transparent validation process, including evaluation of conceptual soundness, and outcomes analysis. A central principle for managing model risk is the need for "effective challenge" of models: critical analysis by objective, independent parties who can identify model limitations and assumptions and recommend appropriate change as part of a pKYC utilization.

6.Metrics to demonstrate effectiveness:

Financial institutions need to be able to demonstrate the effectiveness of their pKYC process in improving ongoing due diligence, transaction monitoring, and SAR filings. This is done via metrics including, for example, showing achievement of a speedier reevaluation of the risk profiles of high-risk customers; a reduction in false positives and negatives; a higher alerts-to-SARs ratio; a decreased amount of time between alert generation and SAR filings; and a lowered backlog of due diligence reviews and alerts, which also includes reduced backlogs of customer refreshes. Having clear measurements will aid both supervisors in their assessment of a new pKYC implementation and financial institutions in their awareness of whether the new technologies are fit for purpose and perform adequately.

In conclusion

From theory to practice with pKYC

Shifting to pKYC and use of modern technologies is a must for financial institutions in 2023 and beyond, as it raises the level of AML compliance, better protects from reputational harm, reduces operational costs, increases efficiencies, improves the quality of human effort, and ensures that a financial institution maintains industry standards expected by regulators and examiners. Key to achieving this goal for financial institutions and their technology partners is to ensure regulators are well informed every step of the way-and that buy-in is obtained prior to pKYC deployment.

Meet our experts

Manish Chopra
Executive Vice President
Risk, Regulatory and Financial Crime
Capgemini

Jeffrey Ingber
Senior Advisory Consultant
Regulatory and Compliance
Capgemini

Dr. Henry Balani
Global Head of Industry & Regulatory Affairs
Encompass Corporation

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 a seamless integration of Encompass into existing workflows and systems.

www.encompasscorporation.com

encompass
the full picture, fast

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the future you want | www.capgemini.com

Capgemini