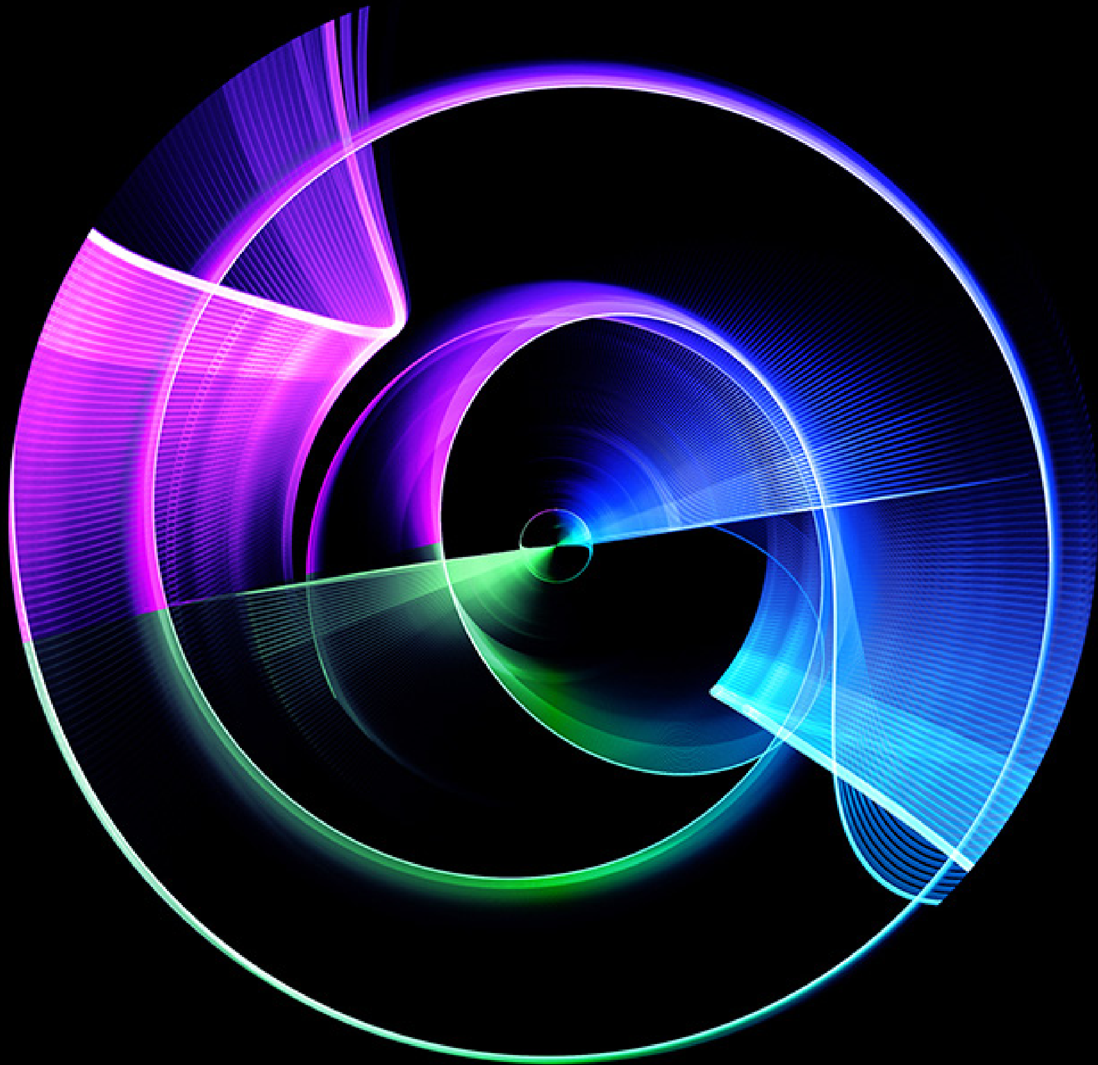
Deloitte.



The continuous Know Your Customer (KYC) journey

Contents

Introduction to continuous KYC 1

The need for continuous KYC 2

The challenges of continuous KYC 3

Leading practices 4

What can be achieved in the short vs. long term 6

Endnotes 7

Contacts 8

Introduction to continuous KYC

Continuous KYC, otherwise known as perpetual KYC or event-driven KYC, is an alternative approach to conducting ongoing customer due diligence (CDD). The goal of continuous KYC is to automate portions of the due diligence process allowing a real-time view, which enables risk insights into the customer profile to inform better decisions."

Traditionally, financial institutions have been conducting time-bound "periodic" refreshes based upon an assigned refresh interval (e.g., one, three, or five years), typically driven by the customer risk rating designated at the time of onboarding. This has been the status quo for a number of years as it's been perceived as a generally accepted risk-based approach. It's important to note that there can be great variability in the refresh cycles outlined by different financial institutions ranging from every six months for factors such as very high-risk Project Estimator and Planning Suite (PEPS) to more than five years for a low-risk consumer. However, this timeline can be too long from an anti-money laundering (AML) risk perspective and has been noted as such by some regulators during public remarks.[1] In more recent years, this time-bound refresh approach has often been combined with certain trigger-based reviews that also have great variability in application, in an attempt to make the CDD process more dynamic.

Continuous KYC looks to shift further away from the time-bound approach to periodic review—transitioning, in part or in whole, toward an approach that leverages ongoing monitoring to identify events that affect the customer's risk profile (e.g., increase in risk rating, change in customer type or persistent anomalous transaction activity) and results in a more streamlined due diligence process focused on changes that affect risk decisioning, as opposed to a repapering exercise. This allows a bank to focus resources on clients and events that present the greatest risk.

The need for continuous KYC

In the United States, financial institutions are required to follow a risk-based approach to identify and assess information relevant to customer AML risk. Several global regulators and industry groups assert that financial institutions are required to identify and verify the identity of customers as well as the beneficial owners of companies opening accounts; understand the nature and purpose of the customer relationships to develop customer risk profiles; conduct ongoing monitoring to identify and report suspicious transactions; and on a risk basis, maintain and update customer information.[2] This essentially boils down to an expectation to perform ongoing and risk-based due diligence on customers. In addition, the Financial Crimes Enforcement Network (FinCEN) has issued guidance that "some banks are also experimenting with artificial intelligence and digital identity technologies applicable to their BSA/AML compliance programs. These innovations and technologies can strengthen BSA/AML compliance approaches."[3] In preparation for adhering to regulatory expectations, institutions should consider how they will implement innovation into their risk-based BSA/AML compliance programs (e.g., risk-based testing and oversight of relevant systems to facilitate calibration and evaluation of the effectiveness of implementation).

Traditional KYC is a predominantly manual process that can be riddled with issues such as poor data quality, privacy concerns, and the pace of changing regulation. Advancements in artificial intelligence (AI), machine learning (ML), robotic process automation (RPA), and application programming interface (API) have provided the ability to automate some of the process, but only in small or siloed areas and, in many cases, still require the need for manual review of screening alert hits.

The right foundation of data, controls, and workflow, combined with layered risk intelligence for optimization, provides the opportunity to transform KYC programs with intelligent automation, continuous risk monitoring, and event-driven KYC refresh. The Wolfsberg Group[4] (Wolfsberg) recently published guidance supporting the use of AI and ML in AML. In 2022, Wolfsberg stated in a standards publication that financial institutions can use AI and ML to holistically analyze data more effectively and efficiently to investigate, detect, and manage the risk of financial crime, as well as satisfy regulatory requirements.[5]

More banks are exploring continuous KYC as they seek to reduce the significant time, effort, and resources it takes to maintain the current structure, which has not resulted in a correlating increase in risk mitigation management.

The challenges of continuous KYC

There are four main challenges you can expect to face when transitioning to continuous KYC: 1) availability of data; 2) technology, tools, and skilled staff; 3) cost of implementation; and 4) evidence and documentation.

Availability of externally sourced data, whether from free public sources or paid subscription services, to allow for ongoing monitoring continues to be a challenge for particular customer types such as high-net-worth individuals, personal investment companies (PICs), and personal investment vehicles (PIVs). Therefore, the lack of publicly available data drives complexity for some ongoing monitoring requirements.

Moreover, implementing a continuous KYC process requires the technology, tools, and skilled staff to integrate data into legacy systems. Consolidation of data from various sources will be essential in providing the 360-degree customer view. Legacy systems will likely need to be enhanced to combine data from nonbank sources.

In addition, the cost of implementing the required changes can be daunting. However, by moving toward a more automated method that applies AI and ML to distill key customer information, a long-term cost reduction is likely to be recognized as a result of less manual intervention. Skilled and costly compliance resources can be better aligned to focus on other value-add risk areas. Luckily, these innovations can augment current systems without the need for replacement. In fact, some of these enablers can be layered on top of existing frameworks.

Finally, being able to evidence and document the ongoing monitoring of CDD information through audit logs and other means will be necessary as regulators will still want to see how customer risks are being managed without selecting the traditional refreshed KYC files for examination.

Leading practices

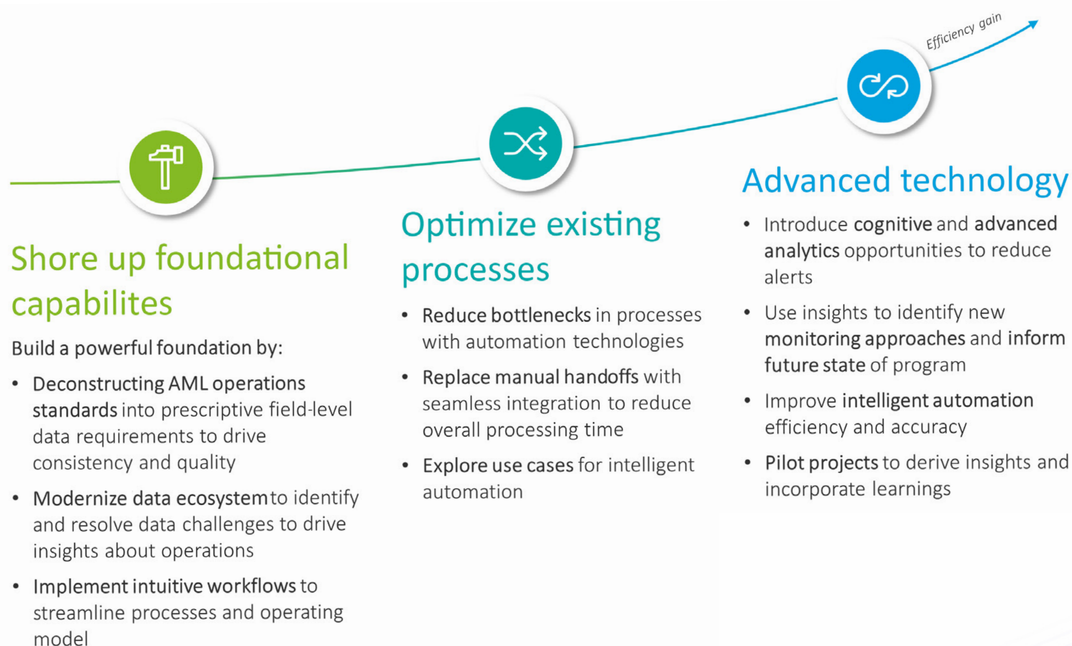
1. Use of technology to optimize workflows

Continuous KYC requires a foundational base of good data, integrated systems, consistent processes, controls, and workflow, combined with layered risk intelligence for optimization. This creates the opportunity to transform KYC programs with intelligent automation, continuous risk monitoring, and event-driven KYC refresh. Ongoing data capture (through external and customer-provided data) enables institutions to implement a more dynamic customer risk assessment.

The transition to continuous KYC should be approached in three phases: 1) shoring up foundational capabilities, 2) optimization of existing processes, and 3) transformation leveraging advanced technology.

Commissioners, such as Mississippi's Mike Chaney, showed interest in more use of reinsurance to help absorb risk instead of raising rates. Birnbaum offered a true public-private partnership for reinsurance as a solution, but he said he sees a federal role with federal resources as part of it. Birnbaum expressed concern for unstable property insurance markets that could risk financial stability. In one of his last appearances as an NAIC consumer advocate, he raised the specter of the failure of mortgage insurers in 2008. The more reinsurance bought by thinly capitalized insurers, the greater costs of reinsurance, which will then be passed on to consumers in the former of higher premiums, Birnbaum said. Coupled with a volatile reinsurance market, a sellers' market could lead to property insurance market instability, he warned.

Continuous KYC is only as good as the current data and technology to support it; therefore, as technology is enhanced, the continuous KYC process is expected to evolve. Institutions should reassess the continuous monitoring they've implemented over time to understand its effectiveness in meeting end objectives. For example, piloting with a controlled population and implementing monitoring processes to track the effectiveness of the trigger events put in place. Institutions should also consider piloting continuous KYC with smaller controlled populations (e.g., lower risk customers) and progressively increasing its use based on effectiveness and efficiency results of the pilot.



2. Training and awareness

Implementing continuous KYC will require properly trained first-line personnel who will interact with clients to reconfirm or obtain updated information for ongoing data capture. These roles should understand continuous KYC and how it differs from periodic refresh, and fully grasp their part in the continuous KYC process. This includes understanding the natural touchpoints required to reconfirm and verify the client's information, such as 1) the client wants to add a new product; 2) the client wants to add a new signer to their accounts; or 3) the client wants to add a new account. Maximizing natural touchpoints instead of creating unnecessary required touchpoints will improve customer experience and reduce repetitive refreshes.

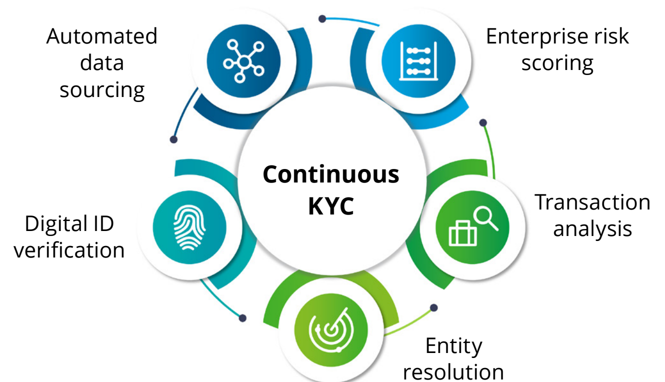
3. Novel new sources of data

Continuous KYC requires institutions to vet large amounts of data from external and internal sources in order to perform real-time risk monitoring. Vendors that provide financial-crime-specific external data include LexisNexis, Dun & Bradstreet, Thomson Reuters, and Moody's. It is important for institutions to vet and perform due diligence on all sources of data, especially new data sources, to verify the best sources of data for the given purpose. Institutions should consider whether the data is from a trusted source that can be relied upon for accurate, real-time information. Data sources include public/external sources (e.g., incorporation databases, watchlist databases, newspaper, blogs, social media), credit, internal client, judicial, transactional, and KYC and policy management data. Consolidation of data across all these various sources will provide a holistic view of the customer and enable better real-time risk monitoring.

4. Use of analytics in terms of dynamic customer risk ratings

The exchange of risk insights between transaction monitoring (TM) and KYC processes is limited because these are kept separate at most institutions, and the design of TM detection models typically does not include refreshed customer behavioral insights gained from KYC processes (e.g., updated expected activity, new products). This leads to a low understanding of customer profiles, which can cause a high misclassification in alerts and customer risk rating models.

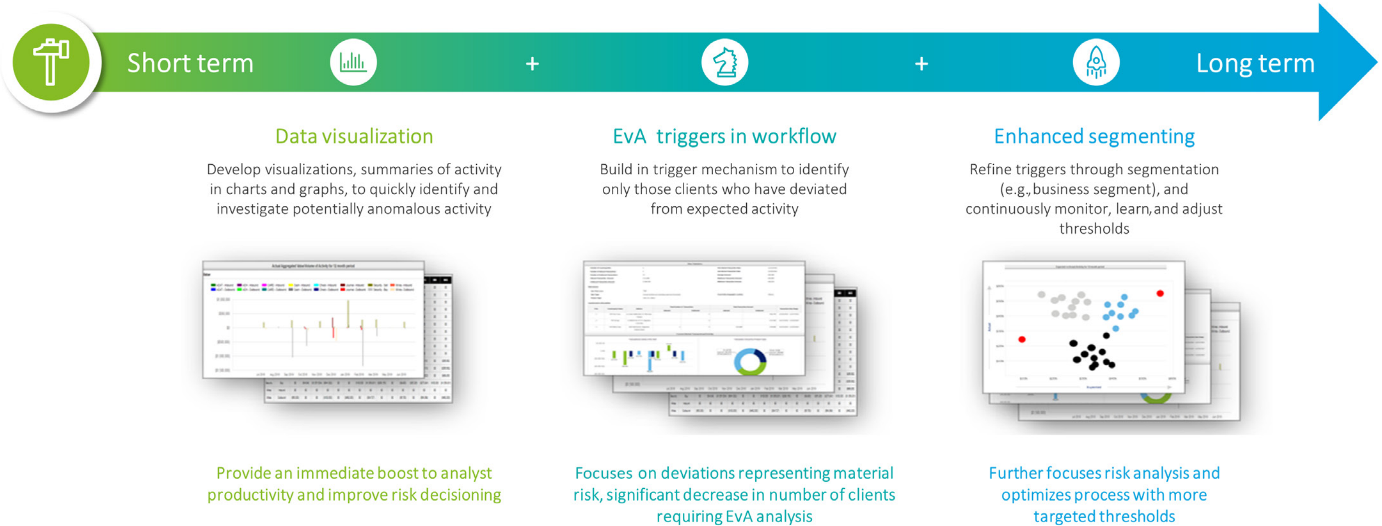
The customer risk rating is constantly monitored by the use of analytics in a dynamic risk assessment methodology. An integrated risk model that combines the risk assessment derived from continual observation and analysis from KYC with information from traditional TM monitoring processes provides a more holistic understanding of profiles and has the ability to maximize efficiency and operational capabilities.



What can be achieved in the short vs. long term

Institutions can start preparing for the transition to continuous KYC by developing and deploying more automation of processes throughout their business, building a foundational base of good data and integrating their systems across the AML technology ecosystem. Institutions should also develop a clear vision of what constitutes a meaningful or material change that would serve as a trigger. In the short term, examples of initiatives institutions could deploy include developing data visualizations for an immediate boost to productivity and risk decisioning; in the medium term, institutions could build expected versus actual (EvA) activity triggers in the workflow to focus on deviations representing material risk; and in the long term, institutions could consider enhancing segmentation and refining triggers to further focus on risk analysis and optimizing their process with more targeted thresholds. These illustrations are a subset of the broader range of actions institutions could undertake.

It will likely be several more years before we see wide-scale adoption and cultural buy-in for continuous KYC, but the positive impacts that can be gained from incremental steps toward the ultimate goal will prove out the long-term benefits.[6]



Endnotes

1. Financial Crimes Enforcement Network (FinCEN), "Prepared remarks for FinCEN Acting Director Him Das delivered virtually at the American Bankers Association/American Bar Association Financial Crimes Enforcement Conference," January 13, 2022; Board of Governors of the Federal Reserve System (FRB) et al., "Joint statement on innovative efforts to combat money laundering and terrorist financing," FinCEN, December 3, 2018

2. FinCEN; Monetary Authority of Singapore (MAS); Financial Conduct Authority (FCA); Financial Action Task Force (FATF).

3. FRB et al., "Joint statement on innovative efforts to combat money laundering and terrorist financing".

4. The Wolfsberg Group is an association of 13 global banks whose mission is to develop frameworks and guidance for the management of financial crime risks particularly related to KYC and AML.

5. The Wolfsberg Group, "Wolfsberg principles for using artificial intelligence and machine learning in financial crime compliance," 2022.

6. This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

   Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

Contacts

Theresa Donnelly-Staerk
Principal
Deloitte Transactions and Business Analytics LLP
tdonnelly@deloitte.com

Paul Burgoyne
Principal
Deloitte Transactions and Business Analytics LLP
pburgoyne@deloitte.com

Nikhil Aggarwal
Managing Director
Deloitte Transactions and Business Analytics LLP
nikhaggarwal@deloitte.com

Debopama De
Senior Manager
Deloitte Transactions and Business Analytics LLP
dede@deloitte.com

Roy Kantrowitz
Manager
Deloitte Transactions and Business Analytics LLP
rokantrowitz@deloitte.com

Important notice

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Copyright © 2024 Deloitte Development LLC. All rights reserved.