Aite Novarica

IN PURSUIT OF KYC MODERNIZATION

TRANSLATING CUSTOMER DATA INTO INTELLIGENCE

PREPARED FOR

NICE Actimize

A word from NICE Actimize

Know your customer (KYC) is the backbone of customer risk management in any organization. If KYC controls are poor or they fail, it adversely impacts the entire ongoing risk management process. Failure to get KYC right from Day One can result in inaccurate customer risk profiling and scoring, ineffective monitoring, and the potential to miss suspicious activity.

These days, customers expect quicker decisions, faster transactions, and streamlined processes. Financial institutions must successfully balance risk management with a smooth customer process. Failure to create this balance results in poor risk controls that provide an ineffective risk rating or cause unnecessary friction, which inspires customer defection.

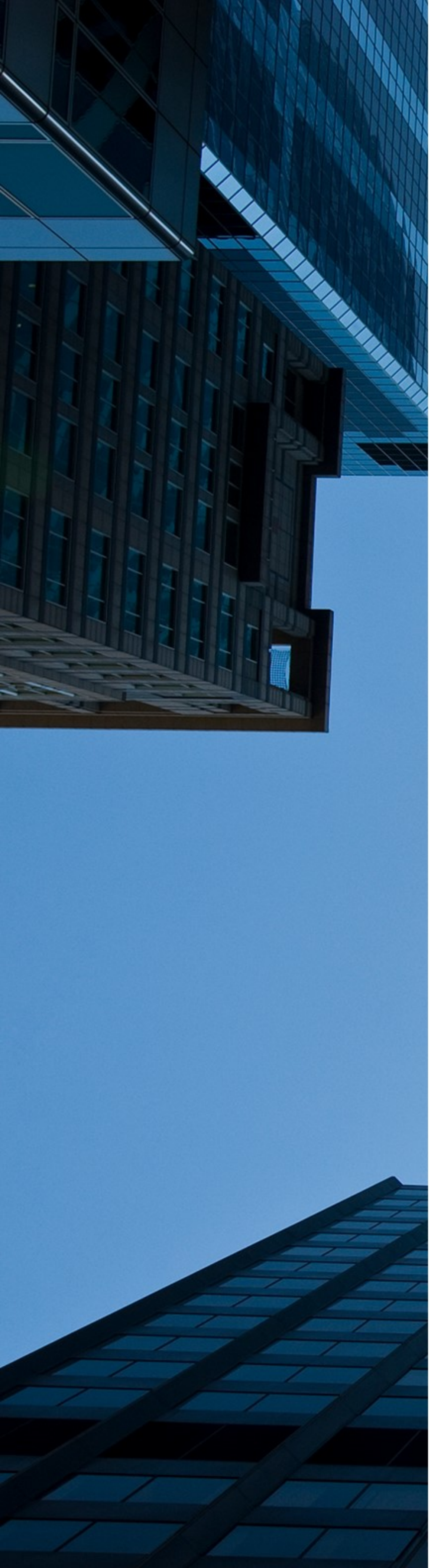
Understanding customers and their risk, especially for corporate entities, is critical. Where do you start? With data—it's the lifeblood of any KYC system. Ultimate Beneficial Owners (UBOs) and controllers often hide behind a complex web of ownership structures to obfuscate real ownership from financial institutions. Access to the right internal and external data enables financial institutions to better manage customer risk.

Financial institutions need to move from periodic to trigger-based reviews, so changes in risk are identified quickly and any updates are accurately reflected in the updated customer risk score. Real-time customer risk scores ensure that compliance systems are optimized to monitor and detect appropriate financial crime risk for each customer. This can be achieved using the latest advances in analytical technology.

Modernize your KYC program by improving access to the right data. You'll have a better understanding of your customers and their risk to make accurate, fast decisions. This is especially true when it comes to corporate customers where there's an increasing need to understand their structures, ultimate beneficial owners, and controllers.

In this whitepaper by Aite Novarica, they discuss modernizing your KYC program. By improving data access and using the latest technology, you'll move from a reactive to proactive approach when managing risk.

Adam McLaughlin
Global Head of AML Strategy and SME
NICE Actimize



Aite Novarica

SEPTEMBER 2022

IN PURSUIT OF KYC MODERNIZATION

TRANSLATING CUSTOMER DATA INTO INTELLIGENCE

PREPARED FOR:

NICE ACTIMIZE

SEPTEMBER 2022

IN PURSUIT OF KYC MODERNIZATION

Translating Customer Data Into Intelligence

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This report, commissioned by NICE Actimize and produced by Aite-Novarica Group, explores how adopting a modern entity-centric Know Your Customer (KYC) model underlain with innovative technologies and techniques can transform customer data into actionable risk intelligence. Enriched and integrated KYC intelligence can uplift anti-money laundering (AML) regulatory compliance and financial crime risk management while improving operational efficiency, minimizing customer friction, and supporting organizational growth.

Key takeaways from the whitepaper include the following:

- **KYC is a foundational component of any successful AML program**. Financial organizations must conduct risk-based KYC and due diligence on all customers. This includes individuals, corporations, trusts, partnerships and other legal entities, banks, non-bank financial institutions, insurance carriers, asset and fund managers, hedge funds, governments, municipalities, charities, and non-profit organizations. Strong KYC practices facilitate an understanding of customers and their risk profiles and ensure appropriate scrutiny of customer activity in compliance with all relevant AML and sanctions obligations.
- **Conducting and maintaining appropriate risk-based KYC is a complex endeavor**. KYC has been an operationally challenging enigma that many financial organizations struggle to solve. These challenges can lead to compliance gaps and deficiencies, regulatory issues, and regulatory censure. AML compliance leaders must overcome many internal barriers, including conflicting data and documentation requirements, legacy systems, manual and redundant processes, customer demands for less friction, and competing organizational priorities. Leaders question if they can develop adequate customer risk profiles and if ongoing customer due diligence and monitoring measures are appropriately risk-based, reasonable, and sufficient.
- **Building one customer truth is the ultimate KYC goal**. Financial organizations must excel at three key activities across the KYC life cycle: data collection and verification, dynamic risk assessment, and ongoing monitoring.

- **Unlocking the actional risk intelligence within KYC data requires a modern entity-centric approach**. A modern KYC model is founded upon a diverse set of data attributes. It can construct holistic, dynamic, enriched risk insights that center the customer. Meaningful risk intelligence demands a multidimensional customer view built on a foundation of quality data linked together accurately and enriched from multiple internal and external sources. Intelligent automation, sophisticated data wrangling, and entity resolution are tools that can cope with poor data quality. Advanced analytics and machine learning-based techniques can help combine and harness KYC data more effectively.
- **Financial organizations cannot afford to delay on embarking on a KYC modernization journey indefinitely.** Enriched and integrated KYC risk intelligence can uplift regulatory compliance and risk management. It can also improve operational efficiency, reduce the total cost of ownership, minimize customer friction, and support organizational growth.

Introduction

AML compliance programs tackle many external and internal pressures: criminal attacks, increasing regulation, digital acceleration, growing demands for frictionless customer experiences, and a greater urgency to operate more efficiently and do more with fewer resources and smaller budgets. Unlocking the enormous potential within KYC data is often seen as the best weapon in the battle against financial crime. However, legacy KYC approaches frustrate financial organizations and their abilities to harness data effectively and efficiently. This inability can lead to insufficient customer risk appreciation, inadequate decision-making, and poor outcomes while creating operational lag and resource misallocation.

The volume of risk-relevant customer information continues to expand, often coming from diverse sources, forms, and formats. Traditional KYC checklists and customer risk profiling may no longer be adequate to fully comprehend and recognize the wide-ranging risks emanating from diverse individual and corporate customer bases and evolving transactional behavior.

AML and KYC leaders recognize that they must find and deploy innovative approaches to transform customer data into one customer truth and actionable risk intelligence. This white paper will explore how adopting new and emerging technologies can support this critical mission with innovative capabilities, empowering more effective digestion and orchestration of data points and enriching risk insights continuously across the customer life cycle. Harnessing, orchestrating, and monitoring KYC data more effectively can drive holistic views of customers and their activity and elevate the efficacy of financial crime control frameworks.

Methodology

The research for this white paper is based largely on ongoing Aite-Novarica Group interviews with leaders and financial crime risk practitioners at financial organizations. It is also informed by a survey of 26 financial crime professionals in September and October 2021. Given the size and structure of the research sample, the data provide a directional indication of conditions in the market.

KYC: ESTABLISHING AML PROGRAM EFFECTIVENESS

KYC is recognized as a foundational component of any successful AML program. It buttresses most core AML and counter-terrorist financing operations. Financial organizations must know to whom they are proving products and services, starting with customer onboarding and acceptance and extending throughout the ongoing servicing.

Financial organizations must conduct risk-based KYC and due diligence on all customers: individuals, corporations, trusts, partnerships and other legal entities, banks, non-bank financial institutions, insurance carriers, asset and fund managers, hedge funds, governments, municipalities, charities, and non-profit organizations. Strong KYC practices facilitate a dynamic understanding of customers and their ever-changing risk profiles, ensuring appropriate scrutiny of customer activity commensurate with their assessed risk.

However, conducting and maintaining appropriate risk-based KYC is a complex endeavor that financial organizations struggle to solve. It can often end up leading to compliance gaps and deficiencies, regulatory issues, and regulatory censure (Figure 1):

- Fraudsters, money launderers, sanctioned actors, and other corrupt parties work tirelessly to disguise their true identities, unlawful behaviors, and illicit wealth. They have gotten exceptionally good at it. Many have turned to various corporations, partnerships, trusts, and other business entities to operate with anonymity.
- Countless spending and hours go into effecting KYC. Still, AML compliance leaders question whether they can develop adequate customer risk profiles and whether ongoing customer due diligence and monitoring measures are risk-based, reasonable, and sufficient. Many AML compliance leaders point to onboarding and ongoing KYC as one of its primary AML pain points.
- Inadequate KYC often leads to improper customer risk classification and inexact and inconsistent AML transaction monitoring, which can miss potential indicators of unusual or suspicious events that require further due diligence and reporting to law enforcement. Inabilities to uncover these true positive alerts can keep AML compliance leaders up at night. Responsible executives recognize the need for superior risk intelligence. To that end, they seek more enriched data sets and better tools to harness KYC more effectively.

- Insufficient KYC can lead to inadequate monitoring and screening, creating unmanageable false positive alerts. These conditions exhaust financial crime analysts and investigators, resulting in delayed and poor decision-making and bad outcomes.
- Lack of holistic views of customers and their risk profiles extends customer onboarding, adds unnecessary friction, frustrates applicants and customers, and erodes customer satisfaction and loyalty.

FIGURE 1: TODAY'S KYC CONUNDRUM

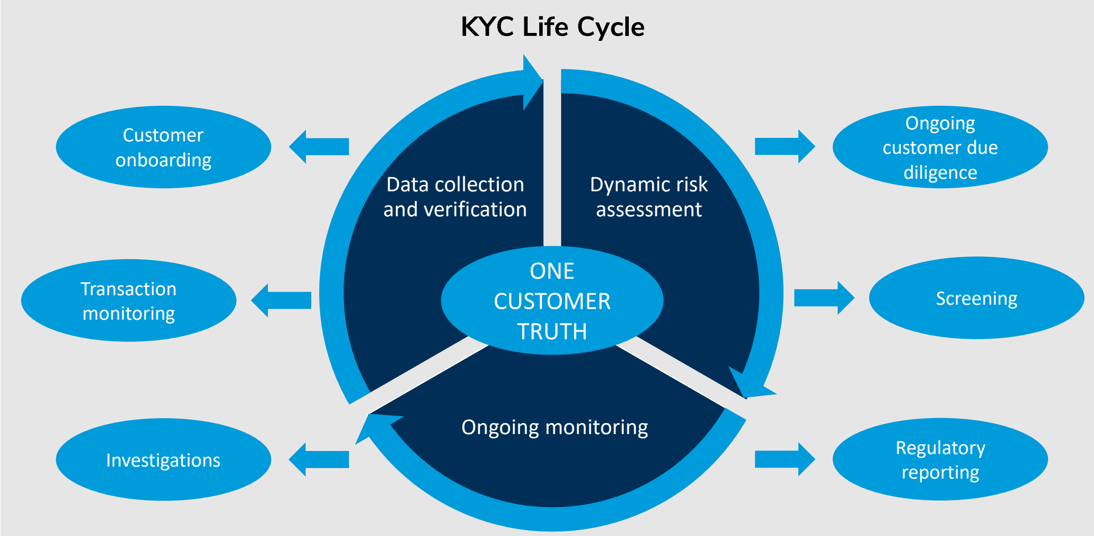
KYC challenges	Too many false positives	Need for holistic customer views	Data enrichment
Over 40% of surveyed AML executives identified onboarding and ongoing KYC processes as top AML pain points	**50%** of surveyed AML executives identified too many false positives as a top AML pain point	**58%** of surveyed AML execs identified the ability to build holistic entity views of customers and risk as a top AML technology priority	**58%** of surveyed AML executives agree their firms will increase the use of enriched data sets

Source: Aite-Novarica Group's survey of 26 AML executives at financial services companies, September to October 2021

KYC LIFE CYCLE: THE FUNDAMENTALS

KYC supports almost every other aspect of a financial organization's AML control framework. The proper identification and verification of legal entity parties support so many other critical functions across a financial organization, such as credit, legal, audit, management, finance, and regulatory reporting. As such, it is vital that a firm's KYC build an accurate truth of the customer starting at onboarding and extending throughout the customer's relationship with the firm. Financial organizations must excel at three key activities across the KYC life cycle to achieve one customer truth: data collection and verification, dynamic risk assessment, and ongoing monitoring (Figure 2).

FIGURE 2: KYC LIFE CYCLE



Source: Aite-Novarica Group

Data Collection and Verification

Financial organizations are obligated to collect, verify, and record customer identification information based on the specific nature and risk profile of the customer. Numerous steps are taken to collect sufficient customer information to ascertain identity and establish the general purpose and nature of the customer relationship with the financial organization.

- Identity and other documentation content must be verified at onboarding to establish a customer relationship. The information must be captured, stored, and cascaded across multiple systems in a way that supports applicable written enterprise policies and procedures.
- Processes supporting customer identity can include documentary methods, non-documentary methods, or a combination of both:
    - Financial organizations can rely on certain types of documents to reasonably evidence and verify customer identity. Such identity documents can include unexpired government-issued forms of identification such as a driver's license or passport. Other forms that can provide a reasonable assurance of true customer identity can also be used.

- Non-documentary methods can independently compare and verify provided identity information against information obtained from other reliable sources such as consumer reporting agencies or public databases.
- APIs can be a more reliable and efficient non-documentary verification method reducing the reliance and dependence on requesting required identity documentation from customers.

- Organizations must check the names of customers and counterparties against relevant sanctions lists. Any potential indicator or connection to a sanctioned party or jurisdiction should be investigated and resolved promptly and efficiently before further business action can be taken. Confirmed sanction hits restrict further business and require additional organization action, including reporting to applicable governmental authorities. These sanction checks must be performed at onboarding and continuously throughout the customer life cycle.

- Customer information captured during initial onboarding helps financial organizations to construct their understanding of customer risk and expected customer activity. This information becomes vital when building smarter AML transaction-monitoring rules and models and vetting future customer behavior.

- When conducting KYC on corporate customers, financial organizations must also identify and vet those entities' ultimate beneficial owners (UBOs), i.e., individuals with an ownership share or control, management, or direction of the entity. In many jurisdictions, including the U.S., AML regulations mandate UBO identification of those with at least a 25% ownership or control. Sadly, true individual ownership and control can often be hidden easily beneath complex corporate and organizational layers, spanning multiple jurisdictions. Corporate structures are often simple to form, maintain, and operate; many jurisdictions do not require substantial information or documentation, especially on UBOs, officers, directors, and other key stakeholders.

Dynamic Risk Assessment

Financial organizations must continuously evaluate each customer's risks and apply enhanced due diligence commensurate with the assessed risk profile.

- Starting at onboarding and continuing throughout the customer life cycle, customer information is analyzed to attribute a customer risk score which drives the decision to open, retain, or exit the account relationship.

- In addition to mandatory sanctions checks, strong KYC expects organizations to screen customers against politically exposed persons (PEPs) and adverse media lists. PEPs are individuals associated directly or indirectly with positions of prominence in foreign governments or foreign-owned corporations; they can represent a higher risk for political corruption and, as a result, money laundering and other illicit activity. Financial organizations are not prohibited from servicing and transacting with PEPs and other high-risk parties. Still, they should scrutinize these individuals and monitor their behavior more closely than lower-risk customers.
- The customer risk assessment should factor in diverse data points: occupation, entities with cash-intensive businesses, PEP status, source of funds, wealth, frequency and nature of cross-border activity, geography, and adverse media indicia.
- To mitigate the heightened AML exposure of customers assessed as elevated risk, firms may mandate increased information, conduct enhanced due diligence, and in some cases, require senior management approval before account onboarding.
- Customer risk profiling frequently informs suspicious activity detection rules and alert prioritization.

Ongoing Monitoring

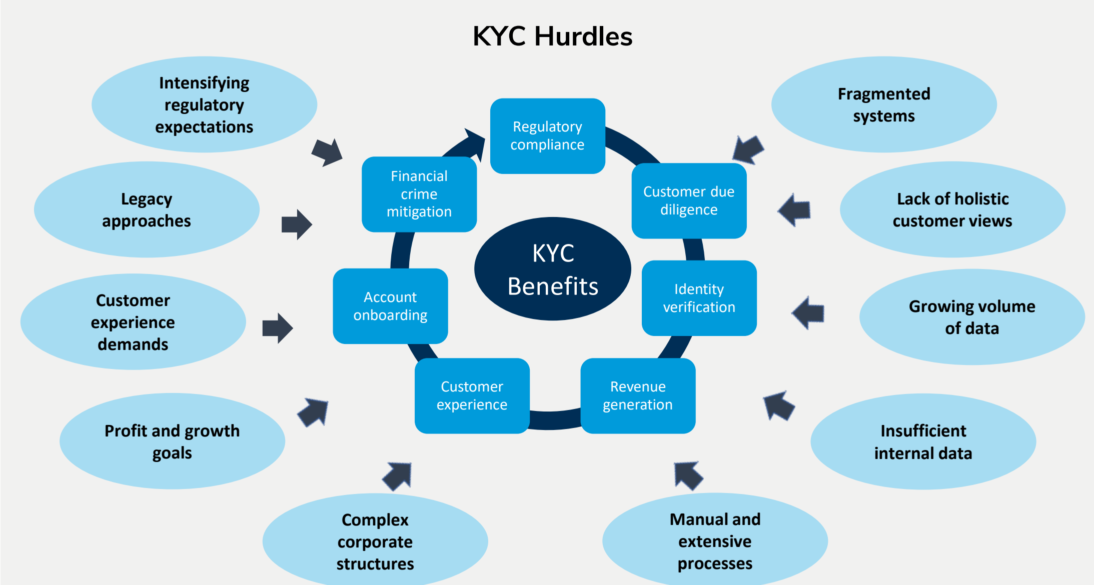
Financial organizations are expected to review customer accounts—the frequency is based upon the designated risk profile—and maintain current customer information.

- Keeping KYC information updated enables sharper financial crime monitoring and investigation efforts. During periodic reviews, actual customer activity should be compared against the expected behavior captured as part of onboarding.
- A risk-based approach is required to respond to triggers (e.g., changes to authorized signatories on an account, a new subaccount opened for a business, a change in ownership structure for the business), which can be a significant operational hurdle.
- As a principal element of KYC and an AML program, ongoing risk-based monitoring of customers must be conducted. This requirement is primarily to detect and report suspicious or unusual activity, indicating potential money laundering, terrorist financing, or other illicit activity. Legacy approaches to ongoing monitoring require constant refinement, and transaction monitoring platforms can frequently generate a high volume of false-positive alerts.

TODAY'S KYC HURDLES

AML leadership is ultimately responsible for regulatory compliance, but many functions across the organization must work together and ensure cohesive and effective execution of interconnected KYC procedures and practices. Numerous internal and external systems and data sources are involved, all of which must be put into place, integrated, and maintained to gather, assemble, validate, and analyze KYC information. Financial organizations must overcome many obstacles to turn KYC data accurately into one customer truth and actionable risk intelligence (Figure 3).

FIGURE 3: KYC HURDLES



Source: Aite-Novarica Group

Intensifying Regulatory Landscape

As regulators worldwide worry about the impact of rising financial crime, they are enacting new AML laws and regulations in search of increased corporate transparency and more risk-based and outcome-based approaches to financial crime prevention and detection. KYC obligations are increasing, particularly around identifying the UBOs of corporate customers and managing high-risk parties such as PEPs. However, different jurisdictions will have different legislative standards and regulatory expectations, further complicating the inherent challenges confronting AML organizations when dealing with corporate structures. Enforcement actions with higher penalties are likely as regulatory scrutiny increases.

Internal KYC Obstacles

Table A identifies the internal obstacles that inhibit KYC for financial organizations.

TABLE A: INTERNAL KYC OBSTACLES

OBSTACLE	IMPLICATION
Financial organizations often lack a holistic customer profile	Many financial organizations lack unified or holistic customer records. Data and documentation are generally siloed across different business groups, functions, and unconnected systems. Siloed approaches often fail to expose hidden records and links within organizational data, build complete customer profiles, and accurately identify, assess, and monitor high-risk parties, accounts, and events.
Some financial organizations suffer from poor KYC data	Insufficient and fragmented data tests an organization's capability to understand customer risk fully. Moreover, valuable customer and transaction data can reside in unstructured or hard-to-access formats. Incomplete or inadequate KYC data can degrade screening against sanction watch lists, leaving organizations vulnerable to transacting with individuals and entities subject to international sanction prohibitions and regulatory censure for sanction failures.
Processes can be laborious and highly exhaustive	Onboarding processes have tended to be manual, slow, tedious, and challenging to execute, especially with business-related accounts. These factors can often impair customer risk profiling and ongoing monitoring. Conducting periodic refreshes of accounts and maintaining records with complete, accurate, and current information are operationally taxing, particularly as behavior can change through the customer life cycle. Relying largely on periodic assessments can leave inaccurate or underestimated customer risk scores unchallenged, potentially for years, exposing organizations to known yet preventable threats.
Risk-relevant data continues to grow	An increasing volume of available risk-relevant customer data can often drown KYC and customer risk profiling activities. Unreliable risk assessments trigger ineffective ongoing monitoring and high false positives. Higher risks can go hidden and reportable suspicious activity undetected.

OBSTACLE	IMPLICATION
KYC on UBOs is a complicated endeavor	Identifying UBOs of corporate entities requires a good deal of resource investment to be performed satisfactorily. UBO information is available on public companies, but it is not as readily accessible for private firms, partnerships, trusts, and firms registered in tax havens or offshore locations.

Source: Aite-Novarica Group

INADEQUATE KYC: THE INEVITABLE COSTS

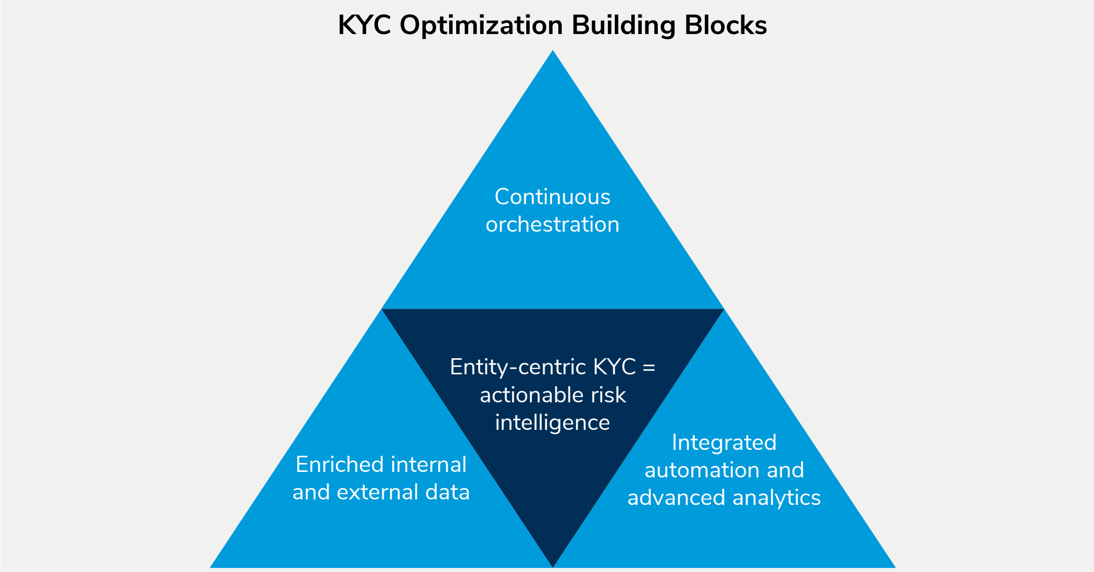
Maintaining poor KYC practices can lead to severe consequences for financial organizations.

- **Financial crime risk becomes harder to detect**. Criminal behaviors are becoming more sophisticated, leveraging evolving technology to avoid detection and legal and regulatory loopholes that allow corporate formations without capturing UBOs. Without effective KYC delivering enriched risk intelligence, financial organizations may fail to spot high-risk events and emerging criminal threats. Dependence on manual processes degrades control effectiveness.
- **AML operations become less effective and efficient.** Inferior KYC intelligence can cause inadequate financial crime detection, with transaction monitoring systems generating too many false positives. As a result, AML operational and back-office functions become less effective and efficient as considerable time is allocated to unnecessary alert reviews and customer due diligence activities.
- **Digital acceleration and customer experience demands become encumbered.** Extensive KYC protocols and highly manual processes often delay customer onboarding and transaction processing, causing frustration and negative customer experiences. Extended onboarding leads to high application abandonment rates.
- **Regulatory compliance becomes more difficult.** Insufficient or inadequate KYC is often the genesis of AML gaps and deficiencies. Noncompliance with AML obligations can trigger severe regulatory censure, high fines, reputational harm, loss of investor and consumer confidence, and diminished market value. Failures can also lead to potential criminal prosecutions for the financial organization, senior executives, and other responsible individuals. Reprimanded firms will devote substantial time, money, and resources to remediating KYC deficiencies.

THE IMPERATIVE FOR A MODERN KYC APPROACH

Unlocking the actionable risk intelligence within KYC data requires a modern entity-centric approach—one that is founded upon a diverse set of data attributes and constructs holistic, dynamic, and enriched risk insights centered around the customer at its core (Figure 4).

FIGURE 4: KYC OPTIMIZATION: BUILDING A MODERN, ENTITY-CENTRIC APPROACH



Source: Aite-Novarica Group

Integrating today's technologies can facilitate this pursuit by delivering groundbreaking ways to embed and orchestrate intelligence, efficiency, and effectiveness into AML and KYC compliance programs. These technologies can help organizations achieve regulatory compliance and build vibrant risk management practices across the customer life cycle. Financial organizations can make more informed decisions and achieve better risk-based outcomes while optimizing operational efficiency and elevating customer experiences.

KYC DATA: BUILDING ENRICHED RISK INTELLIGENCE

Modernizing KYC must start with optimizing the use of relevant customer data, which is expanding rapidly. Meaningful risk intelligence demands a multidimensional view built on a foundation of quality data linked together accurately and enriched from multiple internal and external sources.

Uplifting Internal Intelligence

Financial organizations must identify and take advantage of all of the risk-relevant internal sources of customer data attributes:

- Valuable customer risk intelligence can be derived from front-line employee escalations of unusual or suspicious customer behavior, automated transaction monitoring alerts, referrals from fraud and information security departments, completed and ongoing investigations, and recent suspicious activity/transaction report filings.
- Financial organizations are building massive data lakes fed by cross-product and cross-channel data. Traditional paper-based information is becoming digitized.
- Beneficial customer insights can be derived from digital identity data attributes used internally across the organization to support identity verification and authentication. Digital identity data can include behavioral biometrics, geographical location, device identity and reputation, mobile phone ownership, and email tenure and reputation.

Enriching With Third-Party Sourced AML Information

Significant third-party sourced information is available to enrich an organization's risk intelligence. AML data solution providers offer repositories of thousands, and frequently millions, of individual profiles associated with risk-relevant individuals and entities from around the world.

- These databases encompass profiles linked to hundreds of sanctions programs and enforcement lists. Comprehensive sets of secondary identifiable data attributes further support a financial organization's KYC processes. Information may include dates of birth, places of birth, citizenship, residency, addresses, genders, entity types, national identification and passport numbers, and nationality and other country affiliations.
- Beyond sanctions-related profiles, extensive libraries are carved into other risk categories ranging from PEPs and their related close associates to adverse media and various criminal activities, such as bribery, corruption, and drug trafficking.

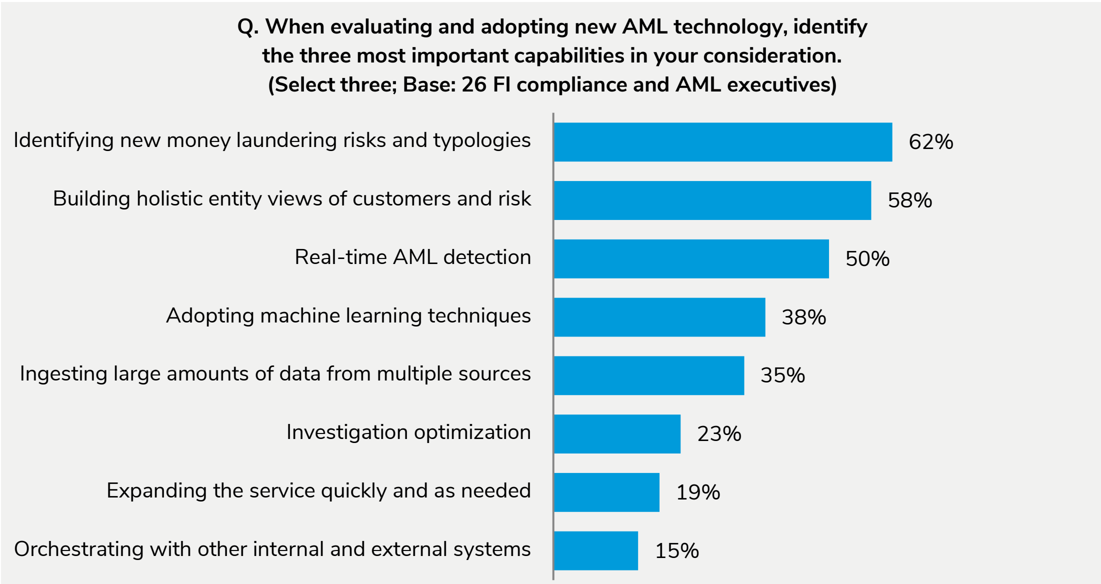
Adverse media is used during customer onboarding for reviews and can be used for ongoing monitoring.

- Many AML data solution providers produce valuable insights on high-risk businesses and activities, such as cannabis or marijuana-related businesses, money service businesses, virtual asset service providers, and other crypto-related firms.
- On corporate-related profiles, risk-relevant data from public and private sources may be found, attained, and aggregated on the entity and UBOs, including ownership interest percentages, officers, board members, and key associations and connections.

AUTOMATION AND ADVANCED ANALYTICS: SHARPENING RISK INTELLIGENCE

Harnessing KYC data into intelligence for effective financial crime analytics, monitoring, and detection is a top AML challenge for financial organizations. They persistently search for innovative tools and techniques that can transform KYC data into holistic customer profiles and rich customer insights that support the fast and accurate identification of new financial crime risks, threats, and typologies (Figure 5).

FIGURE 5: AML TECHNOLOGY PRIORITIES



Source: Aite-Novarica Group's survey of 26 AML executives at financial services companies, September to October 2021

Intelligent automation as well as sophisticated data wrangling and entity resolution tools can cope with poor data quality. Advanced analytics and machine learning-based techniques can help combine and harness KYC data more effectively. As more data is processed, more intelligence can be fed into the models, and customer risk profiling can become smarter.

Intelligent Automation

Embedding intelligent automation such as robotic process automation can streamline and optimize manual (and at times inefficient) KYC processes and make risk-based recommendations based on predetermined logic:

- Extensive data gathering and aggregation tasks required for periodic KYC refreshes, alert reviews, and case investigations can be optimized. Discrepancies in customer information can be identified and resolved quickly.
- Internal and external communications can be improved, and redundancy and duplication across the customer risk life cycle can be eliminated.
- Dynamic customer information forms and checklists can simplify, optimize, and accelerate customer onboarding and data collection, minimizing unnecessary delays and human errors.

However, automation can create more problems than it solves if firms do not adopt it methodically and scrutinize it periodically.

Entity Resolution

Entity resolution tools are designed to deduplicate entity records and build holistic views of entities and relationships. It is particularly advantageous as many financial organizations suffer from disparate data schemas and fragmented systems. Entity resolution deciphers and triangulates imperfect and incomplete data sets. Entity resolution with data intelligence gathers third-party data and associates it with the right entity to enrich the aggregated, centralized entity records. By harvesting additional contextual intelligence advantageous for smarter and faster risk profiling and segmentation, entity resolution can elevate KYC and customer due diligence activities and other AML processes such as transaction monitoring, alert investigation and case management, and regulatory reporting.

Network Analytics

Network analytic tools identify relationships and connections among parties, accounts, and transactions by ingesting and analyzing vast amounts of data. These connections and activity patterns are often otherwise hidden and unknown to AML functions. Network analytics can enrich KYC practices by identifying and tracking UBOs and their associations and facilitating customer risk evaluations and due diligence reviews. Large corporate entities and high-net-worth individuals have complex, interconnected ownership structures; conducting KYC frequently requires extensive research and can take months to complete.

Dynamic Segmentation

Dynamic segmentation enables more proactive, risk-based, and entity-centric approaches to KYC, ongoing monitoring, and financial crime detection. It applies advanced analytics and data clustering techniques to build multifaceted risk segments based on diverse customer data attributes and behavioral activity.

Defined customer risk segments will evolve when customer behavior changes. Dynamic segmentation can be particularly vital in uplifting KYC on corporate entities as it factors in company size, structure, associations, transaction networks, and the details associated with related parties and transactions.

CONTINUOUS ORCHESTRATION: SUSTAINING RISK INTELLIGENCE

An optimized, entity-centric KYC model demands a carefully orchestrated and integrated ecosystem. It must connect distinct functions, processes, systems, and data sources across an organization for seamless communication. It creates a constant feedback loop as KYC data is updated and customer activity and behaviors change. Organizations can build accurate customer profiles and intelligence that support faster onboarding decisions, enrich customer risk profiles, and build trust and operational efficiency throughout the customer life cycle.

- Customer behavior changes may be identified outside of any activity they pass through the financial organization, such as the locations from where they call the institution or log into an account or behavioral information obtained through a third-party source such as an employment change.

- Data and system integration tools can consume and analyze a large volume of structured and unstructured data and perform straightforward onboarding and ongoing monitoring. Tighter integration enables data to be brought together more easily for more accurate, holistic views of the customer and financial crime risk.
- A tighter technology footprint can facilitate information and intelligence sharing across the organization and a collaborative financial crime risk management approach.
- The right orchestration tools can facilitate access to the different systems; ingest, bring together, and analyze all internal and external risk-relevant data; and deliver faster, richer risk intelligence. As certain data sources and systems become less relevant, outdated, or obsolete, those changes can be more easily and quickly recognized so that organizations can ensure appropriate assessment and make any required substitution. Moreover, new data sources can be identified and ingested into the end-to-end ecosystem.
- Modern APIs, built-in connectors, and other tools simplify the ingestion and aggregation of diverse tools, technologies, applications, and cutting-edge data sources and intelligence, often in different data stores and formats.

KYC MODERNIZATION: REAPING THE BENEFITS

Financial organizations face many financial crime threats and challenges. AML compliance leaders must overcome countless internal barriers, including insufficient data, legacy systems and processes, customer demands for less friction, and competing organizational priorities. Embedding innovative technologies and techniques can optimize and automate KYC data collection, customer risk profiling and segmentation, due diligence and investigation, documentation refreshes, and more:

- Advanced analytics can produce holistic risk profiles of customers, accounts, and transactions and attain more accurate and dynamic intelligence.
- Disparate data sources, systems, and applications can be integrated into more cohesive ecosystems.
- More intelligent automation can be embedded at account onboarding and throughout the customer risk cycle, reducing friction while protecting customers and securing their accounts. Fewer unwanted and often unnecessary requests will elevate the customer experience, increasing satisfaction, trust, and loyalty.
- Well-informed AML operational and back-office staff can deliver higher quality and more consistent decisions producing better outcomes.
- Financial crime prevention, detection, and investigation can become smarter and faster. Surveillance can more nimbly adapt to ever-changing circumstances. False positives can be reduced, and hidden and unknown risk events can be uncovered.

Financial organizations cannot afford to delay on embarking on a KYC modernization journey indefinitely. The benefits of an optimized, entity-centric KYC model are too significant to disregard. Enriched and integrated KYC risk intelligence can uplift regulatory compliance and risk management. It can also improve operational efficiency, reduce the total cost of ownership, minimize customer friction, and support organizational growth.

ABOUT NICE ACTIMIZE

NICE Actimize is a provider of financial crime, risk, and compliance solutions for regional and global financial institutions, as well as government regulators. NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers' and investors' assets by identifying financial crime, preventing fraud, and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, AML detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence, and insider trading. NICE Actimize also offers cloud-based machine learning analytics optimization and development solutions, which leverage collective intelligence to proactively optimize analytics for members.

CONTACT

For more information, please go to www.niceactimize.com, @NICE_Actimize, or Nasdaq: NICE.

ABOUT AITE-NOVARICA GROUP

Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

CONTACT

Research and consulting services:
Aite-Novarica Group Sales
+1.617.338.6050
sales@aite-novarica.com

Press and conference inquiries:
Aite-Novarica Group PR
+1.617.398.5048
pr@aite-novarica.com

For all other inquiries, contact:
info@aite-novarica.com

Global headquarters:
280 Summer Street, 6th Floor
Boston, MA 02210
www.aite-novarica.com

AUTHOR INFORMATION

Charles Subrt
+1.617.338.6037
csubrt@aite-novarica.com