Aitë

NICE · ACTIMIZE

DIGITAL ACCELERATION:

The Importance of Client Lifecycle Risk Management

Aité PARTNER. ADVISOR. CATALYST.

Digital Acceleration: The Importance of Client Lifecycle Risk Management

FEBRUARY 2021

Prepared for:

NICE · ACTIMIZE

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

Digital Acceleration: The Importance of Client Lifecycle Risk Management, commissioned by NICE Actimize and produced by Aite Group, examines the building blocks in orchestrating more fully integrated, data-driven, and analytical approaches to client lifecycle risk management (CLRM). Financial institutions (FIs) face an increasing dilemma as a result of digital acceleration—balancing the expectations of seamless customer experiences against the pressure to build better defenses against financial crime. The paper discusses the current obstacles faced by FIs and the importance of elevating CLRM capabilities through data enhancement, technology, and process and workflow orchestration.

Key takeaways from the white paper include the following:

- Over the last decade, the financial services industry has seen a huge pendulum swing from in-person customer experiences to online and mobile use. With digital acceleration, FIs must evolve the way that they do business and engage with customers. Digital-first strategies have now become instrumental to customer acquisition, onboarding, and maintenance.
- For FIs, digital acceleration expands their risks and challenges. Consumers are expecting more seamless experiences, and FIs are pressed to innovate and offer more digital products and services. With digital acceleration, the financial services ecosystem is becoming more vulnerable to malicious attacks. FIs are bombarded on all fronts.
- Current CLRM approaches may no longer be sufficient to elevate the customer experience, promote effective risk management, and sustain efficient operations and resource utilization. Many FIs struggle to bring the full client risk lifecycle together in a versatile and sustainable manner. Innovative data-driven CLRM strategies and solutions are needed.
- An integrated CLRM system can address today's pain points. It can increase operational efficiency, amplify data sharing, construct more holistic customer views and richer insights, and sharpen detection and prevention.
- The CLRM transformation journey is difficult, takes a long time, and requires significant planning and extensive resources. And balancing the demands for faster and frictionless customer experiences against the pressures for strong risk management and regulatory compliance can be tricky.
- In order to achieve success, FIs must improve their CLRM capabilities in three overlapping key areas: data enhancement, technology (through greater automation and analytics), and process and workflow orchestration. And orchestrating the CLRM framework under a single vendor ecosystem can bring considerable benefits.

INTRODUCTION

Serving customers and championing their best interests are the principal undertakings of all FIs. Significant resources are devoted to the customer experience, yet elevating it tests the financial services industry. The world is moving faster than ever, and every year brings new threats. Increasingly, consumers are demanding more seamless experiences, and FIs must innovate and offer more digital products and services. And facing growing competition from digital banks and other emerging fintech companies, FIs must furnish painless customer onboarding, deliver superior service, and uplift operational efficiency. Moreover, international crime rings are seeking new ways to exploit FIs for illicit gain. Application fraud, synthetic identities, and money mules are on the rise. As such, regulators are expanding their expectations of FIs. The COVID-19 pandemic has only accelerated and amplified these difficulties.

Optimizing CLRM is the key to overcoming these obstacles. CLRM spans the customer journey from initial onboarding to ongoing maintenance to eventual offboarding. Unfortunately, many FIs struggle to bring CLRM together in a versatile and sustainable manner. Loosely connecting disparate processes, systems, and data sources, current CLRM frameworks are often fragmented and inefficient. Instilling more automation, data-driven analytics, and orchestration can facilitate firms' know your customer (KYC) and customer due diligence (CDD) process, harness enterprise data more effectively, build more holistic customer profiles, and drive better insights and outcomes. FIs can deliver greater customer experiences and distance themselves from their peers while achieving regulatory adherence and dynamic financial crime risk management.

This white paper examines fully integrated, data-driven, and analytical approaches to CLRM. Today, FIs face an increasingly multifaceted dilemma as a result of digital acceleration—balancing the expectations for more seamless customer experiences against the pressure to build better defenses against financial crime. The paper discusses the current obstacles faced by FIs and the importance of elevating CLRM capabilities through data enhancement, technology, and process and workflow orchestration.

METHODOLOGY

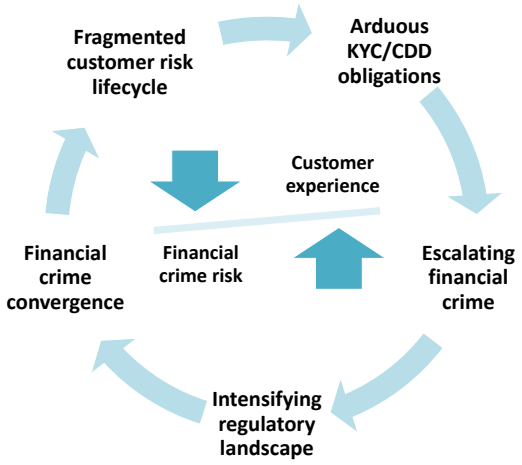
This research is based on ongoing Aite Group interviews with executives and financial crime risk practitioners at FIs. It is also informed by surveys of 30 financial services professionals at Aite Group's September 2019 Financial Crime Forum and 47 fraud executives from 30 financial services firms at its September 2020 Financial Crime Forum. Given the size and structure of the research sample, the data provide a directional indication of conditions in the market.

DIGITAL ACCELERATION: CUSTOMER EXPERIENCE VS. RISK MANAGEMENT

Over the last decade, the financial services industry has seen a huge pendulum swing from in-person customer experiences to online and mobile use. With digital acceleration, FIs had to evolve the way they do business and engage with customers. Digital-first strategies have now become instrumental to customer acquisition, onboarding, and maintenance. Significant investments are continually being made to launch new products and services, speed up the customer lifecycle, and improve customer satisfaction and loyalty. However, the digital transformation spawns a hodgepodge of challenges. Current CLRM approaches may be insufficient to improve the customer experience, promote effective risk management, and sustain efficient operations and resource utilization. New strategies with innovative and data-driven capabilities are needed.

Figure 1 illustrates the key challenges impacting the delicate balance between delivering faster, frictionless customer experiences and appropriately managing intensifying financial crime risk.

Figure 1: Current CLRM Challenges



Source: Aite Group

ARDUOUS KYC AND CDD OBLIGATIONS

For many FIs, complying with KYC and CDD obligations conflicts with customer expectations for easy and convenient experiences. And the obligations, particularly around legal entity ultimate beneficial ownership (UBO) information, only intensify as global regulators continue to stress the importance of corporate transparency. As such, FIs must take great pains to know with whom they are doing business. At a minimum, FIs must collect all required customer information, ensure the gathered information is valid, and maintain sufficient record-keeping to evidence compliance. They should also assess their customers' risk profiles and apply appropriate risk

mitigation measures. Establishing and maintaining customer relationships can be challenging with numerous impediments and friction points:

- Disjointed systems, fragmented data sets, and heavy reliance on back-office staff and manual processes delay processing times, increase costs, and tarnish customer experiences. Complicated onboarding processes hinder new customer acquisition and erode customer satisfaction and engagement. Often, potential consumers abandon their applications during onboarding (Figure 2).
- Onboarding high-net-worth individuals and corporate entities can take between one and three months, costing FIs millions of dollars every year. While UBO information on public companies is generally available, it is not as readily accessible for private entities.
- Post-onboarding, sustaining the customer relationship has many headaches. FIs must keep customers' information and risk profiles up to date, which is no easy task. Further, FIs must continuously monitor customer behavior in order to spot changes in risk, such as negative news events, and respond appropriately.
- The absence of single customer profiles and inconsistent KYC and CDD standards across business lines increase operational inefficiency and frustrate best efforts to expedite customer experiences while managing financial crime risk.

Figure 2: Retail Banking Customer Onboarding Metrics

30% to 69%
of consumers start an application and complete the application

5%
of consumers save an application

31% to 70%
of consumers start an application but do not complete it

Source: Aite Group's interviews with 24 executives, January to May 2019

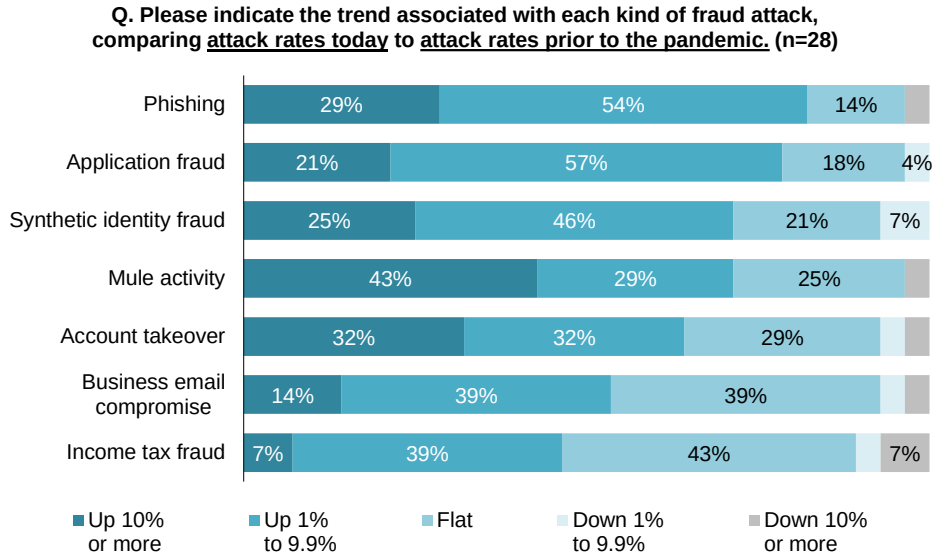
ESCALATING FINANCIAL CRIME

Financial crime continues to rise. With digital acceleration and the rapid shift to faster products and services as well as frictionless customer experiences, the financial ecosystem is becoming more vulnerable to malicious attacks. FIs are being bombarded on all fronts—branches, ATMs, online, mobile, and contact centers. With each passing year, organized crime is becoming more skillful at exploiting weaknesses and avoiding detection. Leveraging a litany of inexpensive tools and technologies, fraudsters are increasingly automating their barrage against FIs.

- The sizeable upsurge in synthetics, identity theft, and money mules elevate application fraud and account takeovers. The past decade's major data breaches have bestowed criminals with a significant amount of compromised personally identifiable information. The transition to chip cards and increasing consumer vulnerability to social engineering further expands FIs' susceptibility to these fraud types.
- Unless an FI knows what to look for, fraudulent synthetic identities are extremely difficult to detect. In most cases, fraudsters fabricate new fake identifies by using data attributes from one or more stolen genuine identities. Synthetic identity fraud is often written off as credit losses, and the extent of it is unknown. Moreover, FIs may unknowingly have an anti-money laundering (AML) issue on their hands.
- Needing to funnel illegally gotten gains without detection, organized fraud rings are enlisting money mules to move around the funds. At times, money mules are willing and eager participants, and other times, they have been unknowingly victimized by online romance or job scams.

As reflected in Figure 3, fraud accelerated in 2020 as organized crime rings manipulated the global pandemic, its underlying chaos, and the economic uncertainty. When financial conditions deteriorate, millions of people turn to crime or agree to serve as money mules.

Figure 3: Fraud Attack Trends in 2020 vs. Pre-Pandemic



Source: Aite Group's survey of 47 financial services fraud executives, September 2020

Unfortunately, current fraud and AML systems and practices may be unable to keep pace with escalating financial crime. However, the needs to combat financial crime and find the bad actors must be balanced against the demands to uplift the customer experience and avoid unnecessary disruption for good customers. When done correctly, new technology adoption can meet both objectives concurrently.

INCREASING REGULATORY PRESSURES

Compliance with AML regulations has long been a complicated endeavor. And with the ongoing growth of global crime, authorities around the world are intensifying their pressure on and scrutiny of the financial services industry. Pressing for more risk-based and results-oriented approaches to combating financial crime, they are toughening AML standards, expanding sanctions, and extending their reach beyond financial services:

- In late 2020, the U.S. Financial Crimes Enforcement Network (FinCEN) proposed an "effective and reasonably designed" standard intended to propel greater risk-based approaches to AML compliance and resource allocation.
- In the EU, the fifth and sixth AML Directives raised CDD and beneficial ownership requirements and enhanced the powers of EU financial intelligence units.[1]
- More than ever, governments use sanctions to exert pressure on dangerous persons, entities, and political regimes for perceived risks to national security and human rights abuses.
- Noncompliance with AML obligations can lead to regulatory enforcement as well as reputational damage.

For many FIs, achieving effective and compliant practices is hampered by current CLRM frameworks' inherent operational pain points—loosely integrated internal networks of diverse systems, poor data quality, a lack of a holistic customer profile, and a high volume of false-positive transaction monitoring and watchlist screening alerts, just to name a few. These challenges and headaches amplify the importance of more responsive, integrated, and data-driven approaches to CLRM.

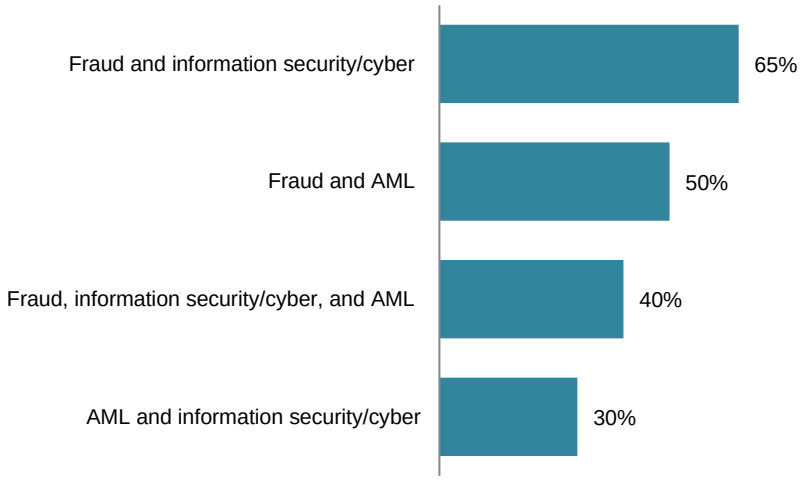
INCREASING FINANCIAL CRIME CONVERGENCE

With digital acceleration and the surge in illicit activity, FIs can no longer effectively fight crime in silos. Organized crime rings are too smart, too tech-savvy, and too good at evading detection. More dynamic and real-time financial crime defenses are demanded. As reflected in Figure 4, fraud prevention and AML compliance units are working more closely together, collaborating more regularly, and increasingly exchanging ideas and information. Increased dialogue can yield richer and more actionable intelligence, and can boost operational effectiveness and efficiency. Through greater alignment, data and innovation can be harnessed more effectively, and more holistic views of customers and enterprise risk can be built. Subsequently, threats can be identified and addressed more quickly. However, the growing convergence of AML, fraud prevention, and cybersecurity units only reinforces the need for increased capabilities and higher-functioning CLRM frameworks that facilitate and expedite the flow and exchange of information.

1. See Aite Group's report *The EU's Sixth Anti-Money Laundering Directive: Another Iteration?*, February 2021.

Figure 4: Convergence of Financial Crime Functions

Q. Please indicate if the following functions in your FI are converging to work more closely. (Check all that apply; n=20)



Source: Aite Group survey of 30 financial crime professionals, September 2019

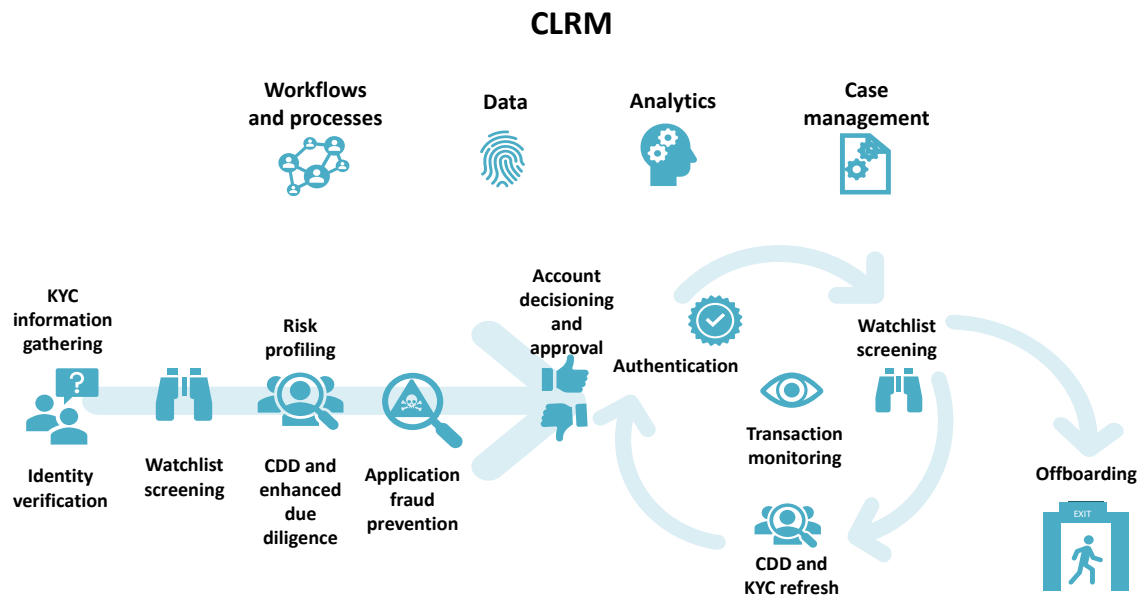
CLRM: THE ART OF THE POSSIBLE

CLRM frameworks tie together the systems and technologies underpinning the customer journey, as well as guide and document its underlying processes. Different organizations apply different strategies and approaches. Even with no universal or standardized structure, some basic and fundamental characteristics are expected:

- CLRM should support financial crime prevention, detection, and investigation; adherence to AML regulatory obligations; and strong risk management.
- CLRM should facilitate the onboarding process and expedite customer engagement, satisfaction, and loyalty throughout the customer journey.
- CLRM should enable and orchestrate the systems and processes supporting customer identity collection and verification, application fraud prevention, customer authentication, risk-based ongoing customer and transaction monitoring, and information record-keeping and retention.

Figure 5 depicts the customer journey and its mandated activities, from initial onboarding to ongoing maintenance to eventual offboarding.

Figure 5: A Simplified Overview of CLRM



Source: Aite Group

- **KYC:** FIs must verify and record customer identification information. Enough information should be collected to ascertain the customer's identity and establish the general purpose and nature of the customer's relationship with the FI. Third-party identification verification (IDV) services are used to confirm customer identity

against public and proprietary databases. Many IDV solutions bring risk-scoring capabilities, leveraging advanced analytics against a breadth of physical and digital identity data. To accelerate the onboarding process, IDV document authentication services can perform liveness and authenticity checks in real time while also using optical character recognition technology to pre-populate application data. Some organizations will invest in multilayered IDV schemes to expedite the application and onboarding process while extending the capacities to identify and stop application fraud, synthetic identities, and money mules.

- **Watchlist screening:** Applicants, customers, and counterparties, as well as incoming and ongoing payments, are screened against relevant international sanctions and prohibited lists. And screening against politically exposed person (PEP) registers, adverse media lists, and other risk-relevant databases helps to identify higher-risk parties and increased reputation risk. Although not prohibited from servicing PEPs and other higher-risk actors, FIs should scrutinize these parties more closely. To balance effectiveness with efficiency, leading third-party screening and data solutions integrate sophisticated technology and analytics to reduce false negatives in addition to false positives.

- **Onboarding CDD:** FIs must assess new customer risk profiles and apply CDD commensurate with the risk. Profiling considers different customer attributes across various data sources—for example, occupation or nature of business, PEP status, source of funds and wealth, geographic presence, and adverse media indicia. To mitigate heightened risk exposure, more customer information may be required, and additional research and investigation may be done. For parties for which risk is deemed too high, FIs may elect not to onboard.

- **Application fraud prevention:** Various defenses are in place to spot potential application fraud and stop the infiltration of bad actors. Historically to catch fraudsters, FIs have embedded multiple identity verification steps in the application process. With the push for better customer experiences, FIs are adopting more frictionless solutions that integrate behavioral biometrics, device fingerprinting, and mobile device authentication, or consortia-based suspicious identity, account abuse, and known fraudster information. Tools that can spot automated bot attacks, which are increasing in online customer interactions, are also embraced.

- **Ongoing CDD:** Periodic refreshes are conducted to ensure KYC and CDD information is up to date. Maintaining information allows an organization to better direct its monitoring and investigation efforts. But refreshes can be operationally taxing, especially without enabling automated solutions. Enhanced analytics and automation can streamline these processes and sharpen customer risk profiling.

- **AML and fraud transaction monitoring:** Solutions are in place to monitor and investigate customer transactions to detect activity indicating fraud, money laundering, terrorist financing, and other illicit conduct. FIs vary significantly in their design, approach, and execution of detection and investigation. For many, rule-based systems, a high volume of false-positive alerts, less than ideal data quality,

and a lack of holistic customer profiles make transaction monitoring less effective. Inadequate solutions can disrupt the customer experience.

- **Identity authentication:** As part of any interaction or request, authentication controls ascertain and validate user identity by cross-checking against previously designated and internally recorded identifiers. Good authentication protocols protect customers and organizations from fraud, as well as build customer trust and elevate the overall customer experience.

TODAY'S CLIENT RISK LIFECYCLE CHALLENGES

For many FIs, CLRM represents a major challenge. Numerous pain points impede its successful operation and cause friction and inefficiencies throughout the client risk lifecycle. The digital acceleration and shift to more seamless customer experiences only add to the hardships.

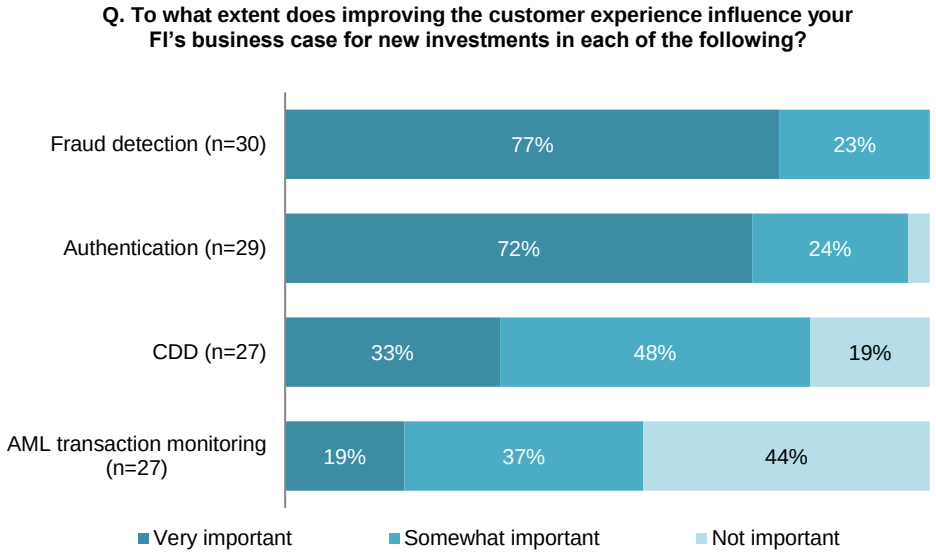
- Many firms loosely tie together in-house systems and vendor solutions underlying CLRM. Information, reviews, and decision-making can cascade across disjointed functions, platforms, and data sources. This operational structure and the required number of internal touch points can impede the overall process.
- Without fully integrated processes or centralized data sources, FIs lack single enterprise views of customers' transactions and risk profiles, which would further advance customer experiences, regulatory compliance, and risk management. Moreover, there can be a disconnect and a lack of visibility and transparency into the customer journey among different business lines as well as across business operations and the financial crime units.
- FIs struggle with highly manual and tedious processes, especially at onboarding. Customer information is manually gathered, vetted, and put into various systems via inefficient processes that can delay onboarding and other customer-initiated requests. This can disrupt a seamless customer experience and erode engagement, satisfaction, and confidence. Moreover, manual and repetitive processes lead to poor data quality, and less-than-ideal data often hinders effective risk management.
- Given the complexity of many legal entity structures, capturing and sustaining UBO information is demanding even with an optimal CLRM structure. Inadequate UBO information hamstrings effective risk management because organized crime rings frequently use complex structures to funnel dirty money and avoid detection. Many regulator enforcement actions trace back to insufficient KYC, CDD, and customer risk profiling, particularly for corporate entities.

PROGRESSING TO A SUPERIOR CLRM MODEL

Faced with many challenges and trying to keep up with the digital acceleration, FIs desire to strategically bring the systems and processes supporting CLRM closer together into a more cohesive and versatile framework. An integrated CLRM system can address today's pain points. It

can increase operational efficiency, amplify data sharing, construct more holistic customer views and richer insights, and sharpen detection and prevention. As illustrated in Figure 6, the customer experience significantly influences the nature and extent of technology investment in financial crime. The considerable pressure to support revenue growth by optimizing new customer acquisitions motivates the demands to strengthen the layers of identity verification controls.

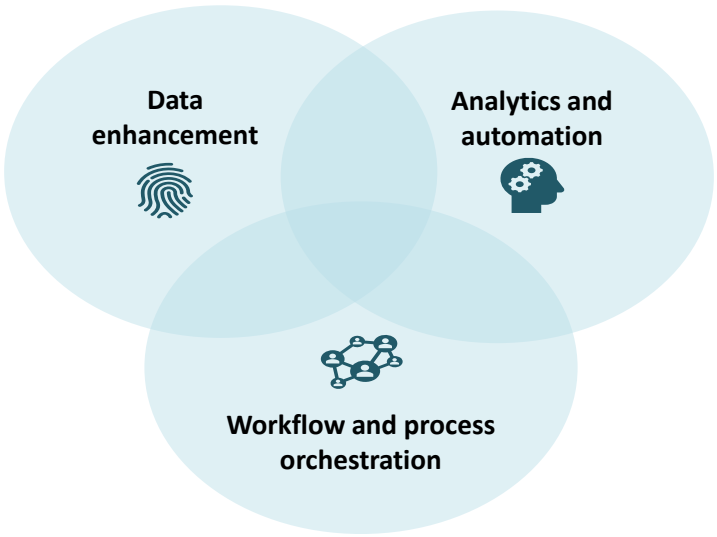
Figure 6: Influence of Customer Experience on Financial Crime Technology Adoption



Source: Aite Group survey of 30 financial crime professionals, September 2019

The CLRM transformation journey is difficult, however, and can span multiple years. It requires significant planning and extensive resources. And balancing the demands for faster and frictionless customer experiences against the expectations for strong risk management and regulatory compliance can be tricky. To achieve success, FIs must improve their CLRM capabilities in three key areas: data enhancement, technology (through greater analytics and automation), and workflow and process orchestration (Figure 7).

Figure 7: Progressing to a Superior CLRM Model



Source: Aite Group

DATA ENHANCEMENT

Elevating risk management and customer experiences starts with uplifting the data. Many FIs lack an omnichannel, holistic customer view. Internal data is often less than ideal, with much of it in formats and schemas that are difficult to access. Moreover, critical identification and other risk-relevant data—sanctions, PEPs, adverse media, and digital identifiers—have been aggregated and made available by many third-party providers. Addressing the internal data imperfections and pulling internal and external data together in an enriched state can elevate customer risk profiling and solidify financial crime defenses and controls, all while uplifting the customer experience. Increasing contextualization can expedite the onboarding processes as well as many facets of effective AML compliance and fraud prevention controls. By empowering quicker and more informed decision-making across the client lifecycle, enriched and holistic data can minimize the onboarding delays as well as the protracted KYC refresh and transactional inquiries frequently encountered by good customers.

Many emerging technologies and data solutions support the data enhancement pursuit:

- Entity resolution technologies can dedupe and elevate imperfect internal data sets and create aggregated customer profiles.
- Link/network analysis techniques can uncover relationships and connections (often unknown and hidden) among customers and accounts, and graphically display them.
- Natural language processing tools can ingest unstructured data and translate it into more structured formats that can be extracted and ingested more easily for additional purposes.
- Digital identity data, such as behavioral biometrics, device identity and reputation, mobile phone ownership, and email tenure and reputation, can drive enlightened

risk-based decisions and sharpened identity verification and authentication, elevating both the customer experience and fraud prevention and detection.

TECHNOLOGY: AUTOMATION AND ADVANCED ANALYTICS

At many financial organizations, much time is spent on highly repetitive and laborious tasks, leaving less time for thoughtful analysis and decision-making. Intelligent automation and robotic process automation (RPA) can streamline activities required for gathering and verifying customer identity information and watchlist screening of applicants, customers, and counterparties. As a result, data can be enriched. Lags and human errors within the onboarding process can be minimized. Extensive data gathering and aggregation tasks required for periodic KYC and CDD refreshes, alert reviews, and case investigations can be optimized. Internal and external communications can be improved, and redundancy and duplication across the customer risk lifecycle can be recognized and eliminated. However, adopting intelligent automation and RPA must be done thoughtfully. Otherwise, automation can create more problems than it will solve.

Advanced analytics and machine learning techniques can help FIs bring together and harness their data more effectively for richer customer insights, elevated KYC and CDD, sharper financial crime detection and investigation, and generally better, faster, and more consistent decisions and outcomes. A few illustrations follow:

- Applying advanced analytics to customer behavior, dynamic segmentation can drive sharper customer risk profiling and more proactive, risk-based, and customer-centric approaches to KYC and CDD, ongoing monitoring, and financial crime detection.
- Advanced analytics can drive more intelligent transaction monitoring across several use cases. Through iterative optimization, existing detection rules and scoring algorithms can be optimized. Subsequently, unknown threats can be identified, false-positive alerts can be reduced, and alerts can be appropriately prioritized, triaged, and, in some cases, auto-decisioned.

Like most other technology adoptions, appropriate governance can prevent unintended consequences and establish expected transparency and explainability.

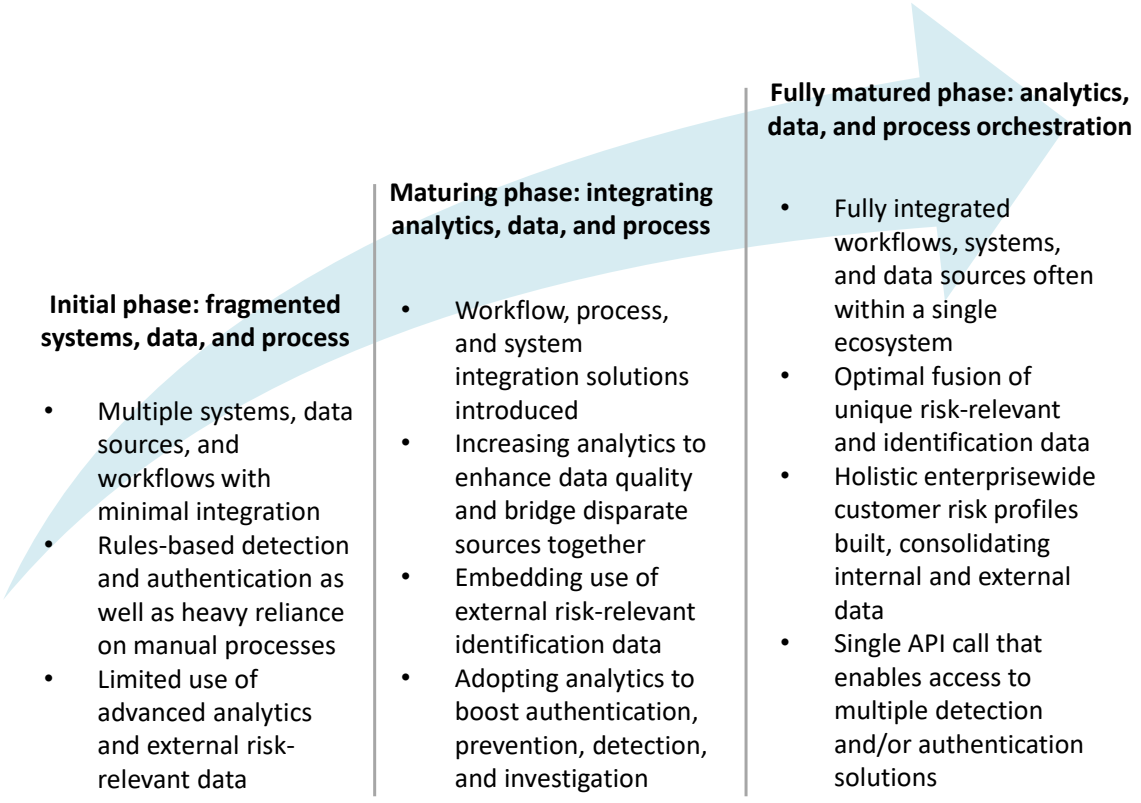
PROCESS AND WORKFLOW ORCHESTRATION

With so many disjointed systems, data sources, and processes, an effective CLRM framework demands a platform that cohesively and seamlessly connects all those moving parts together in a versatile and efficient way. The right orchestration tools can facilitate access to the different systems, ingest and analyze all internal contextual customer transaction data in addition to external risk-relevant data, integrate all output, and deliver faster, richer risk intelligence. Orchestration can help navigate customers as well as internal staff through the mandated protocols in a less obtrusive and more consistent manner. Leading orchestration tools support various data and system integration options, can consume a large volume of structured and unstructured data, and perform straightforward onboarding of third-party AML, fraud, and authentication systems in a cohesive ecosystem.

THE CLRM MATURITY CURVE

The following sections detail the roadmap to building and orchestrating more fully integrated, data-driven, and analytical models for CLRM. As FIs embark on this maturation journey, there is no one-size-fits-all approach. FIs must determine how much of the existing structure to replace and how much to supplement and augment. Much depends on the driving needs of the organization as well as the ability of its existing structures and systems to coexist and integrate with new technologies and data sources (Figure 8).

Figure 8: The CLRM Maturity Curve



Source: Aite Group

INITIAL PHASE: FRAGMENTED SYSTEMS, DATA, AND PROCESS

At the early phase, multiple systems, data sources, and work streams are in place with generally minimal integration and cohesion. Business process management or orchestration tools are rarely used. Customer information can be fragmented across many systems. KYC and CDD standards can vary across business lines, and execution is likely to be inconsistent. Holistic customer views are limited and seldom bridge business lines. Financial crime prevention and detection depend largely on rules-based platforms. Workflow streams and processes tend to be manual, and duplication of activities is likely. Interaction and information sharing across financial crime units is minimal and complicated. Tackling the work streams in isolation is inefficient and cost-prohibitive, alienates customers, and exposes the organization to increased financial crime

risk and regulatory issues. As such, many firms are embracing and initiating projects toward more cohesive CLRM ecosystems.

MATURING PHASE: INTEGRATING ANALYTICS, DATA, AND PROCESS

At the next maturity phase, FIs integrate modular approaches to uplifting CLRM, concentrating first on remediating deficient elements as well as enhancing the most critical areas, often those exposed to the highest risks. Workflow and process orchestration are introduced. In many cases, FIs will invest in business process management tools that bridge applications, systems, and work streams, usually within an individual business line to start. Onboarding and application processing times see slight improvements. In parallel with process improvement and orchestration, initiatives are launched to elevate data quality and link disparate data sources in hopes of building a master file. Different technologies are adopted to consolidate, enrich, and connect the data. However, requiring a multiyear effort, work is often split into smaller projects with different timelines. Gradually, FIs will adopt advanced analytics and intelligent automation. Increasing cohesion and orchestration facilitates greater collaboration and information sharing among financial crime units.

FULLY MATURED PHASE: ANALYTICS, DATA, AND PROCESS ORCHESTRATION

At the final maturity phase, the end-to-end CLRM ecosystem is fully integrated. Internal data is enriched and brought together, and third-party-produced risk-relevant information, such as adverse media, device identity, and biometrics information, is incorporated seamlessly to build holistic views of customers and enterprise risk. Automation and analytics are adopted by business, operational, and financial crime units. KYC and CDD processes are expedited, operational efficiency is raised, and the end-to-end customer experience is elevated. Smarter and more responsive anti-financial crime controls are achieved. Multilayered and connected systems, data sources, and workflows advance the organization’s goals and pursuits.

Moreover, orchestrating CLRM under a single vendor ecosystem can bring considerable benefits:

- The vendor acts as the sole contact point and maintains the contractual relationships with the other third-party providers within the ecosystem. This structure reduces the usual burdens and costs associated with multivendor arrangements.
- Access to and integration with various third-party systems and data sources are simplified. The orchestration vendor has already constructed the necessary API connections and the communications layers to those point solutions. Deployments of new functionality and features are easier and quicker. This affords FIs with flexibility and scalability, especially when needs and circumstances change.

CONCLUSION

It started years ago, but the digital revolution is now at hyperspeed. More than ever, FIs are confronted with balancing the demands for faster and more seamless customer experiences against the pressure to build better defenses against financial crime. To stay ahead of the competition and keep pace with the bad guys, FIs must elevate their CLRM approach. To successfully do that, FIs must increase the capabilities in three key areas: data enhancement, technology (through greater automation and analytics), and process and workflow orchestration. The benefits are too high, and the risks are perhaps too severe to discount. Here are a few recommendations:

- **As the initial step, FIs must measure the efficacy of their existing CLRM capabilities carefully.** The end-to-end CLRM ecosystem—solutions, data sources, processes, and work streams—should be scrutinized. Vulnerable, deficient, and inefficient cogs should be pinpointed and prioritized for remediation and upgrading. Questions, such as whether to replace existing functionality or just supplement it and whether to build new in-house solutions or acquire third-party platforms, should be answered. This is an ongoing dynamic activity and not a one-time task.

- **A long-term roadmap should be developed.** There is no one-size-fits-all approach, as all firms are different. FIs have contrasting needs, demands, and risks as well as budgets and resources. They should start small but think big. Proof-of-concept deployments are useful in illuminating the potential fit, the benefits, and the downsides. To lead the effort, a global center of excellence with stakeholders and subject-matter experts from across the enterprise can accelerate the CLRM transformation as well as keep initiatives from going sideways.

- **A data-driven model should be entrenched.** The sophistication of financial crime mandates holistic customer views informed by risk-relevant information from many internal and external sources. Valuable data on UBO, adverse media, behavioral biometrics, device fingerprinting, and mobile device authentication offered by third-party providers should be strategically brought together. Techniques that can address internal data imperfections, enrich the data, and link previously unknown relationships, networks, and connections should be integrated.

- **Automation and advanced analytics are essential.** Automated intelligence can minimize repetitive and labor-intensive tasks. Advanced analytics can drive better customer experiences; faster, more informed, and more consistent financial crime prevention, detection, and investigation; and higher-quality intelligence. But integrating innovation is complex and requires strong governance and oversight.

- **At the end of the day, orchestration may ultimately define CLRM success.** A thoughtful, layered, and carefully integrated CLRM ecosystem will address the increasing yet evolving demands of digital acceleration. More cohesive tech-enabled financial crime strategies and information sharing will be promoted, and elevated customer experiences will be delivered.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Charles Subrt
+1.617.338.6037
csubrt@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

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.