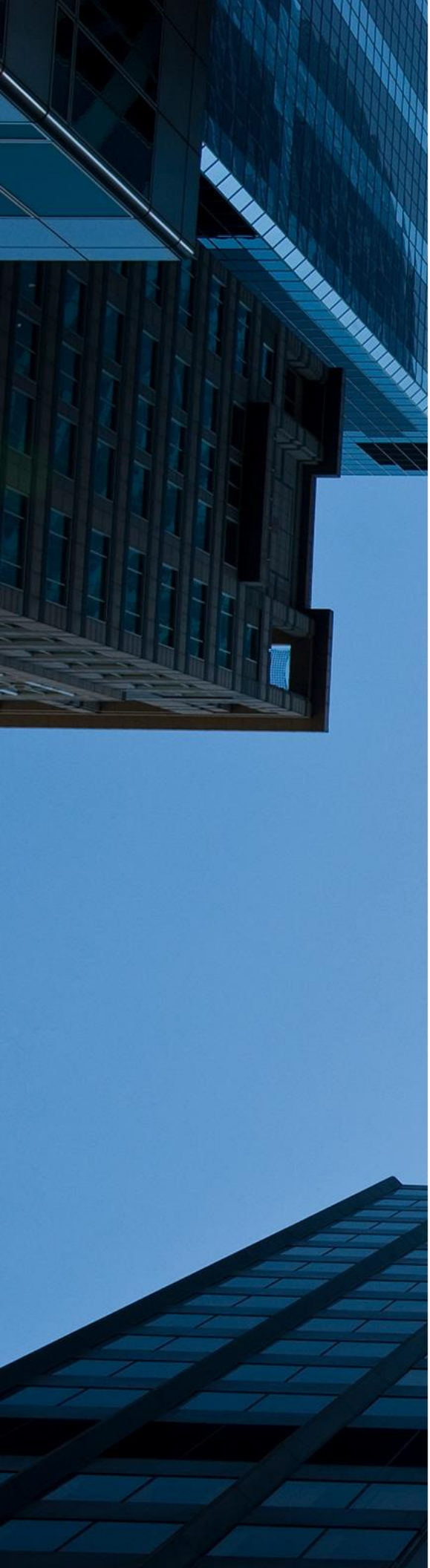


Aite Novarica

JUNE 2022

AML MODERNIZATION

EMBARKING ON THE JOURNEY

PREPARED FOR:

sas

JUNE 2022

AML MODERNIZATION

Embarking on the Journey

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

AML Modernization: Embarking on the Journey, commissioned by SAS and produced by Aite-Novarica Group, examines the benefits of financial organizations investing in digital-first strategies to empower financial crimes program (FCP) leaders who must consider new and existing customer expectations, address organizational needs, and meet regulatory requirements. This white paper explores current organizational challenges, outlines the benefits of new AML technology adoption, and identifies how to embark on a journey of discovery and modernization.

FCP leaders must balance the organizational need to minimize unnecessary friction in the customer experience against the imperative to cultivate a risk-based AML compliance management program satisfying anti-money laundering (AML) and Know Your Customer (KYC) regulatory mandates. Uplifting customer experiences and complying with AML regulations do not always line up neatly. But strategic adoption of today's AML technologies helps organizations strike the necessary balance and equip AML programs with the tools and capabilities to cultivate the necessary risk intelligence and deliver an effective, efficient, and customer-centric AML control framework.

Key takeaways from the white paper include the following:

- A thoughtful AML modernization journey can advance financial crime prevention, detection, and investigation, and make them smarter, faster, and more holistic. Surveillance can more nimbly adapt to ever-changing circumstances. AML modernization can reduce false positives and discover hidden/unknown risk events.
- Transforming AML processes, tools, and systems can corral, enrich, and aggregate fractured, incomplete, and disconnected data sets more effectively. Advanced analytics can produce more holistic risk profiles of customers, accounts, and transactional activity, and elevated intelligence can be attained automatically and refreshed with greater frequency based upon a defined triggering event.
- More well-informed alert and case investigations can yield better, accelerated, and more consistent decisions and outcomes as well as maximize the benefits of a skilled investigative staff.

INTRODUCTION

Today's FCP leaders confront countless challenges on many fronts. Their primary jobs are to safeguard the financial system against exploitation from money launderers, terrorists, and other bad actors as well as satisfy countless ongoing AML regulatory obligations. Their AML programs must accurately assess customer risk profiles, apply appropriate mitigation measures, conduct ongoing customer and event monitoring, identify potential money laundering activity, provide actionable intelligence to law enforcement, and anticipate new and emerging attacks and threats against their organizations. Moreover, as organizations invest in digital onboarding, peer-to-peer payments and digital-first strategies, FCP leaders must consider new and existing customer expectations as well as organizational needs. By virtue of the many hats they are asked to wear, they must balance the organizational need to minimize unnecessary friction in the customer experience against the imperative to cultivate a risk-based AML compliance management program satisfying AML and KYC regulatory mandates and expectations.

Needless to say, uplifting customer experiences and complying with AML regulatory requirements do not line up neatly. Frequently, the lack of holistic, dynamic customer risk profiles impedes the organizational ability to achieve these goals. But strategic adoption of today's AML technologies can help organizations successfully strike the necessary balance and equip AML programs with the tools and capabilities to cultivate the necessary risk intelligence and deliver an effective, efficient, and customer-centric AML control framework. Yet embarking on a modernization journey is tricky and complicated, with numerous options, considerations, and decisions.

This white paper explores current organizational challenges, outlines the benefits of new AML technology adoption, and identifies how to embark on a journey of discovery and modernization.

METHODOLOGY

This research is based on ongoing Aite-Novarica Group interviews with leaders and financial crime risk practitioners at financial institutions. It is also informed by surveys of 26 financial crime professionals, including those who attended Aite-Novarica Group's fourth annual Financial Crime Forum 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.

AML OPERATIONAL CHALLENGES

In Lewis Carrol's "Through the Looking-Glass," the Red Queen explains to Alice that, in her world, one must run as fast as possible merely to remain in place. A humorous statement certainly, but FIs running as fast as they can to attract new customers, meet existing customer expectations, and manage daily operations with the intent to comply with AML regulatory obligations wouldn't laugh. AML compliance leaders find themselves perpetually working harder yet feeling stuck in essentially the same place. Their AML compliance programs must be grounded in accurate identification of risk so that the allocation of controls and resources is commensurate with the assessed risk. However, enterprise as well as customer risk is dynamic and never stands still.

This conundrum has never been more real than it has been since the outbreak of the COVID-19 pandemic. The pace of the global financial landscape has accelerated significantly. Various faster payment options as well as new digital, mobile, and online products and services have grown in adoption, and the pandemic has simply sped up the digital acceleration. An increasing number of consumers have now adopted online and mobile banking services, relying less upon in-person branch banking or even ATM visits. While digital-first strategies are instrumental in terms of customer acquisition and delivering positive customer experiences, digital acceleration increases an FI's risk exposure and amplifies the challenges in combating financial crime.

Table A delineates just some of the key challenges impeding effective AML risk control frameworks.

TABLE A: KEY AML CHALLENGES

AML CHALLENGE	IMPACT
Ineffective and inefficient AML systems	Many current platforms for watchlist screening and ongoing transaction monitoring generate a large number of false positives. Having too many false positives can degrade AML function effectiveness and increase operational risk (for example, by creating a backlog of unreviewed alerts). Staff become inundated with unnecessary noise that distracts them from their primary objective of detecting and reporting financial crime. Moreover, false positives can delay customer onboarding and customer transaction request processing.

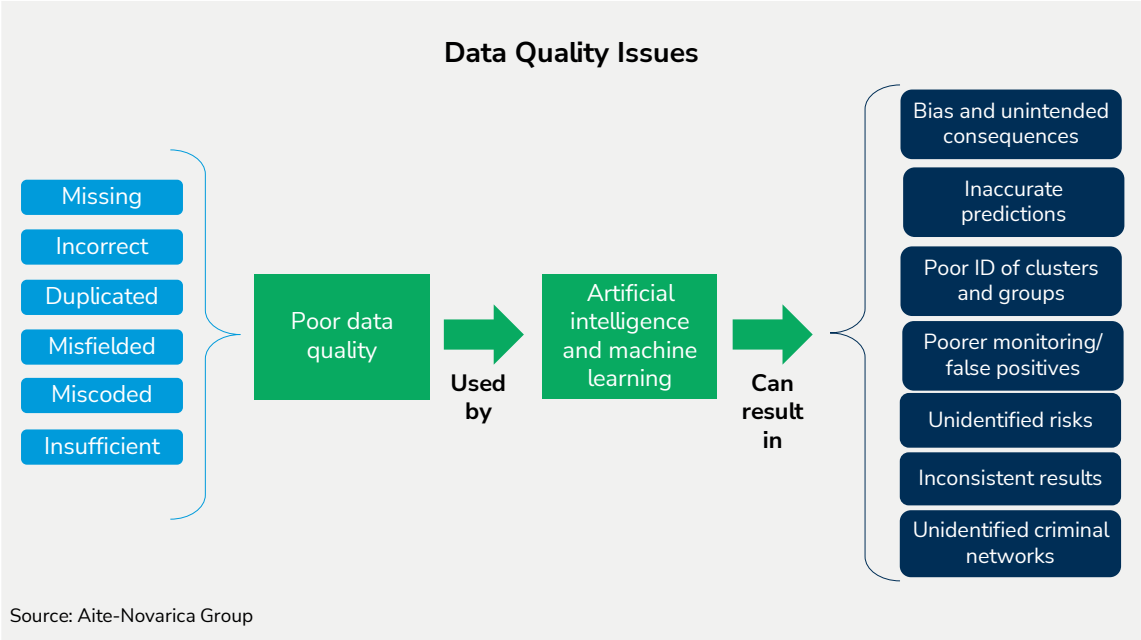
AML CHALLENGE	IMPACT
Escalating financial crime threats	Digital acceleration is expanding the opportunities for fraudsters, money launderers, and other bad actors. Social engineering, automated attacks, mule activity, and synthetic identity fraud are flourishing. Human trafficking, ransomware attacks, and cryptocurrency-related fraud are on the rise as well, Advancements in technology have provided fraudsters with new ways to conduct their criminal activity.
Evolving regulatory landscape	Regulators are pushing for more risk-based and outcome-based approaches to prevention, detection, and compliance. Scrutiny will only increase, leading to more enforcement actions and higher penalties. In 2021, eight large FIs were collectively fined a staggering US$2.44 billion for AML violations.[1] The current regulatory landscape mandates a more advanced, risk-forward, and proactive AML program.
Highly manual processes	AML operations rely heavily on people—the "human in the loop"—especially for data gathering, consolidation, and analysis as well as documentation and reporting. The manual, laborious, and time-consuming nature of many of these activities can ultimately lead to demoralized staff as well as poor decisions, exposing the firm to heightened AML risk.
Fragmented systems and data sources	Often residing in multiple systems, internal data tends to be fragmented, messy, and incomplete. And heaps of valuable information exist in unstructured, hard-to-access, and translated formats. Moreover, third-party firms are delivering diverse and expanding sources of valuable risk intelligence and data to the fight against financial crime. However, disparate and unconnected systems and data sources lead to high costs and consume significant resources. Most firms prefer fewer systems and a more cohesive and integrated ecosystem supporting financial crime controls, enabling data—both internal and external—to be brought together more easily for more accurate, holistic views of the customer and financial crime risk.

Source: Aite-Novarica Group

[1] "AML Fines 2021," Kyckr, February 3,2022, accessed June 24, 2022, https://www.kyckr.com/resources/aml-fines-2021.

Data and the inability to harness expanding yet often fragmented and incomplete data sources for effective financial crime risk detection, prevention, and analysis are often at the heart of ongoing AML operational deficiencies and shortfalls. Data shortcomings lead to inadequate risk and threat identification, inadequate investigations, inconsistent decision-making, and poor outcomes (Figure 1). Discovering the capabilities to solve the data riddle will transform data into insights and intelligence, and elevate financial crime control effectiveness; however, the question for many institutions is how to embark on that exercise.

FIGURE 1: DATA QUALITY ISSUES



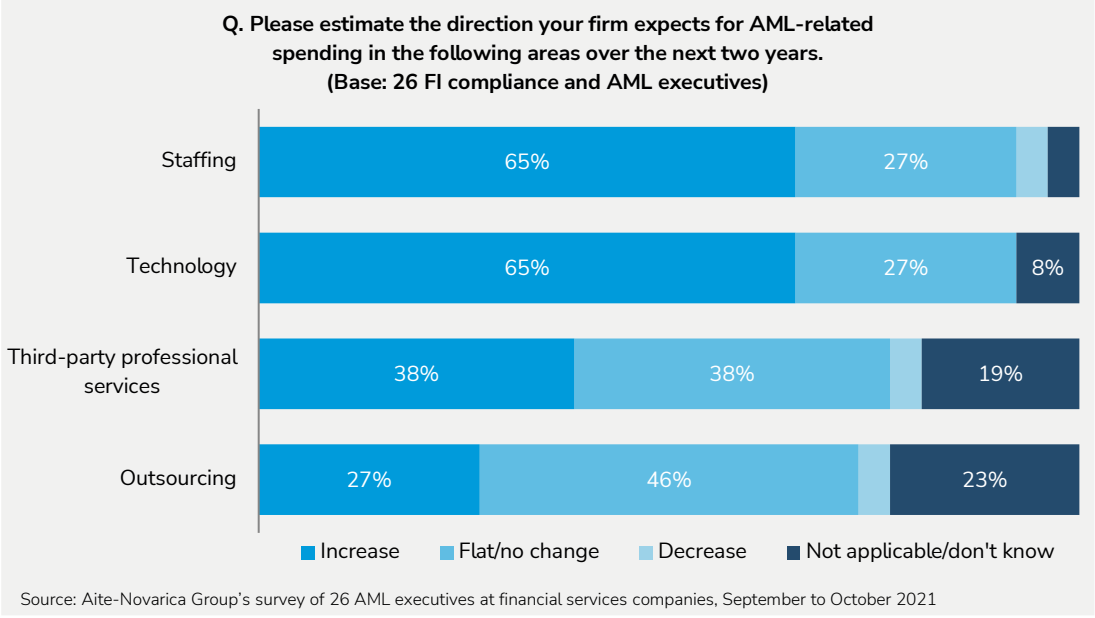
Source: Aite-Novarica Group

MODERNIZING AML THROUGH INNOVATION

To effectively transform risk-relevant data into actionable intelligence, smarter and more agile platforms are needed. Increasingly, legacy and rules-based AML systems are becoming less capable of keeping pace with and adapting to the escalating and more sophisticated threat landscape, leaving anomalous activities and questionable parties and networks undetected.

Today's technology advancements are providing AML compliance leaders with the needed tools to modernize AML compliance frameworks. Recognizing the potential in innovation, AML compliance leaders are spending more on AML technology investment (Figure 2).

FIGURE 2: PLANNED AML TECHNOLOGY SPENDING



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

Table B identifies a number of key technologies that can elevate AML operational processes and controls.[2]

[2] See Aite-Novarica Group's reports Aite Matrix : Leading Fraud & AML Machine Learning Platforms, December 2021 and AI-Enabled Anti-Money Laundering: From Theory to Reality, July 2020.

TABLE B: ADVANCED AML TECHNOLOGIES

AML TECHNOLOGY	DESCRIPTION AND IMPACT
Robotic process automation (RPA)	RPA has been used in many AML use cases, primarily for automating internal and external information gathering and creating case files, leaving the analyst and investigator to make decisions as opposed to performing mundane, time-consuming manual operations.
Dynamic segmentation	Dynamic segmentation enables organizations to leverage unsupervised models to identify customer segments and adapt thresholds within transaction monitoring detection strategies. Leveraging customer behavior, advanced analytics, and data clustering can create risk-based customer segments that evolve as financial and transactional profiles change. As such, dynamic segmentation can optimize detection, extend coverage by identifying unknown threats—often hiding "below the line"—and elevate resource use by lowering false positives.
Link/network analysis	Link/network analysis methods can produce more holistic customer and alert profiles and deliver enriched intelligence and context. By continually discovering connections and relationships across parties, accounts, and transactions within disparate data sets, link/network analysis can elevate detection schemes and investigation practices. These tools can visually display linkages and relationships, particularly higher-risk clusters, enabling improved investigations.
Entity resolution	Entity resolution can triangulate data across disparate internal sources, enriching it with externally developed data. Entity resolution can connect data across internal and external data sources and generate holistic party and event profiles. Using entity resolution, data elements that seem identical, but may not be, are matched without the need of a unique identifier.
Machine learning	Supervised machine learning leverages a variety of algorithms and approaches based on data and statistical analysis, topological data analysis, probability, and predictions. Models use a training set of data and valid outputs to "learn" and "train," and produce predictions and recommendations. Alternatively, unsupervised machine learning explores data without knowing precisely what the designed output should be; models identify groups and clusters in the data, identifying data that are the same.

AML TECHNOLOGY	DESCRIPTION AND IMPACT
Natural language processing (NLP)	NLP technology converts unstructured data into structured data that can then be more easily used by downstream detection and investigation operations. NLP enables automated summarization, language translation, and adverse media analysis that can yield valuable context to improve detection and investigation. Further, NLP can be designed to identify specific activity from an alert—for example, structuring—and provide investigative teams with the opportunity to either review and affirm or override and move on to the next alert or case review.
Natural language generation (NLG)	NLG uses artificial intelligence to translate data into readable text or even spoken narratives. Such capabilities support financial crime investigations as well as narrative text building suspicious activity or transaction report filings as well as evidencing documented rationale for determinations to not file a regulatory report.

Source: Aite-Novarica Group

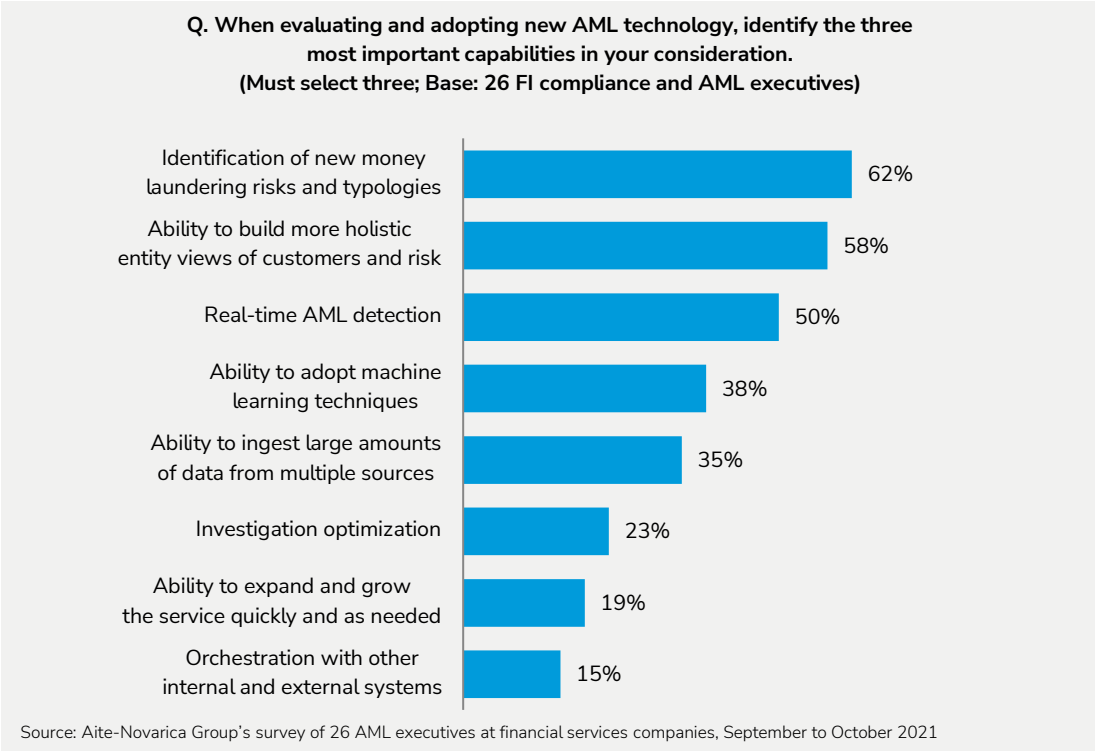
Advancements in computing capabilities, automation, advanced analytics, and cloud-based technology can uplift regulatory compliance and risk-based-approach management with the potential to improve operational efficiency, reduce the total cost of ownership, minimize customer friction, and support and drive organizational growth:

- Sixty-two percent of AML compliance leaders point to the identification of new money laundering risks and typologies as priorities when looking at adopting new technology (Figure 3). New AML technology adoption can make financial crime prevention, detection, and investigation smarter and faster. Surveillance can more nimbly adapt to ever-changing circumstances. Leveraging advanced analytics can also reduce or hide false positives or discover unknown risk events.

- When surveyed, AML compliance leaders identify the ability to build holistic entity views of the customer and risk as a priority. Entity resolution and link/network analysis can corral, enrich, and aggregate fractured, incomplete, and disconnected data sets more effectively. Advanced analytics can produce more holistic risk profiles of customers, accounts, and transactional activity, and attain elevated intelligence more dynamically.

- More well-informed alert and case investigations can yield better, faster, and more consistent decisions and outcomes as well as maximize the benefits of a skilled investigative staff.
- More intelligent and friction-appropriate controls can be embedded at account onboarding and throughout the customer risk life cycle while still protecting customers, securing their accounts, and meeting regulatory and internal policy obligations. Additionally, new market participants may find entry into banking opportunities that were not available before. Additionally, individuals previously excluded from certain banking and other financial services options may now access and benefit from those market opportunities.
- Building and executing a long-term modernization exercise can enable an organization to integrate disparate data sources, systems, and applications into more cohesive ecosystems. A tighter technology footprint can facilitate information and intelligence sharing across the organization and establish a more collaborative financial crime risk management program.

FIGURE 3: AML TECHNOLOGY CAPABILITY PRIORITIES



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

THE AML MODERNIZATION JOURNEY: THE BUILDING BLOCKS

Executing a technology upgrade is not easy, and it requires much time, resources, and funding. Starting down the path of increased financial crime technology adoption, an organization must first understand and define its specific objectives and prioritize them by their importance to the effectiveness and efficiency of the financial crime risk management ecosystem.

Table C outlines the critical steps to build the foundation of a successful AML modernization journey.

TABLE C: THE BUILDING BLOCKS

KEY STEP	DESCRIPTION
Assess enterprise risk exposures and tolerances	As an initial step, an organization must consider its overall risk appetite and tolerances; the nature and complexity of its products and services, channels, and customers; its geographic footprint; and its operational structures. Larger and more global organizations have diverse products and services, expansive footprints, huge financial crime functions, and deep pockets. In contrast, smaller financial firms have more concentrated customer bases, products, and services as well as limited resources and funding. They rely less on technology and more on manual processes.
Inventory all AML systems	Another critical step involves completing a full assessment of existing AML programs and applications, and mapping and calibrating it to the organization's assessments of risk exposure and tolerances. By establishing an inventory matrix calibrating all the underlying features and functionality to risk coverage, the modernization roadmap becomes clearer.
Ask the hard questions	Throughout this process, an organization must ask itself many, often challenging, questions: • Are current risks and emerging threats being adequately managed? • Are there any systemic gaps and weaknesses that must be remediated? • Is the current monitoring system generating too many false alerts, or are analysts and investigators spending too much time on alerts and cases? • Are existing systems being used to their fullest capability? In some FIs, unfamiliarity with an application can be misunderstood as a need for upgraded technology. Sometimes all it takes to start adding new functionality is turning on a switch on an

KEY STEP	DESCRIPTION
	existing platform. (In other words, an organization should be certain of what capabilities it already has in house.)
Build near- and long-term strategies	A firm must pinpoint the most essential tools, features, and functionality, and formulate a near-term as well as long-term technology adoption strategy. Organizational priorities, feasibility of deployment, expected or required timelines, availability of internal resources, and allocated budget must be carefully weighed. As organizations grow into new digital channels, products, and services, their financial crime risks will evolve and expand. Moreover, with the proper financial crimes control framework, financial services organizations can expand to new digital channels, products, and services.
Engage key stakeholders and experts	A critical step in the process is to ensure all the key stakeholders and subject-matter experts are at the table. Excluding an important voice from any assessments or decision-making opportunity may negatively impact the overall success of the journey.

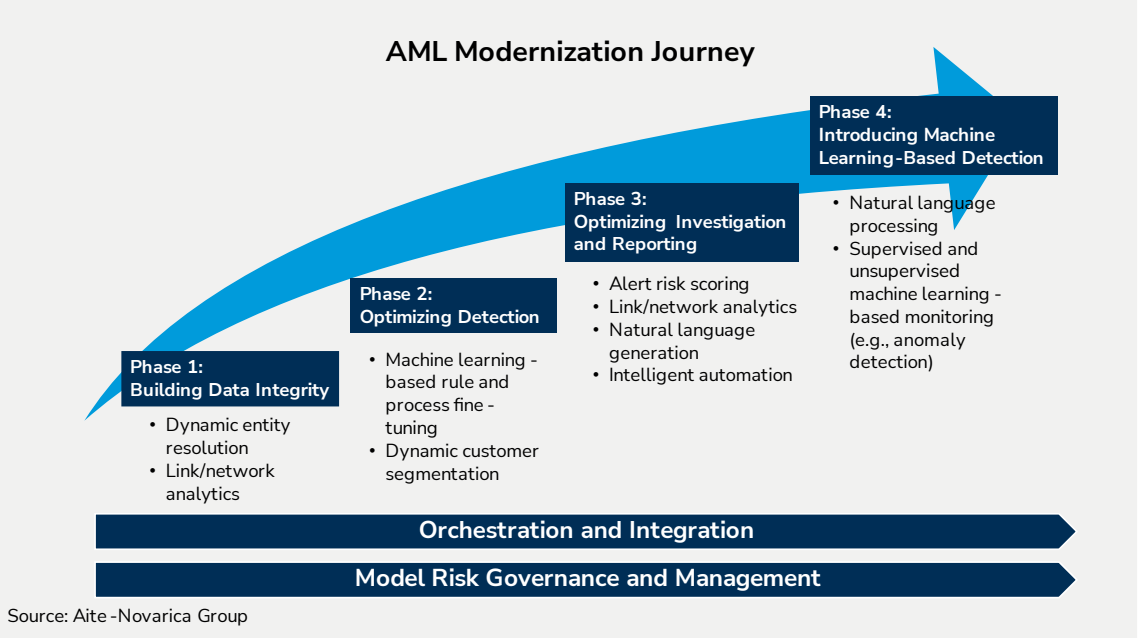
Source: Aite-Novarica Group

Most of the above steps may be familiar to many institutions. Surprisingly, though, many firms begin by searching for potential new solutions based upon the assumption that it is time to pursue new arrangements rather than leading with required capabilities and functionality.

AML MODERNIZATION JOURNEY: THE ROADMAP

As FIs embark on this modernization journey, there is no one-size-fits-all approach. However, Figure 4 illustrates elements that an organization should integrate at each phase in the modernization journey.

FIGURE 4: AML MODERNIZATION JOURNEY



Source: Aite-Novarica Group

Phase 1: Building Data Integrity

Improving data quality is a foundational element in building AML program effectiveness. Yet data still presents a major stumbling block for many financial organizations. Internal data tends to be fragmented, messy, and incomplete, and often resides in multiple, loosely connected systems. Valuable information often exists in unstructured, hard-to-access formats that require translation. Thankfully, significant third-party-sourced information is available to enrich an organization's risk intelligence. These include digital identity verification; public records; and device, behavioral biometrics, and consortium data.

Addressing internal data imperfections and pulling internal and external data together in an enriched state can elevate customer identification and risk profiling, solidify financial crimes defenses and controls, and uplift the customer experience. Firms must integrate robust capabilities for ingesting, wrangling, aggregating, and enriching data from a wide range of internal and external sources:

- Dynamic entity resolution can support high-quality data, removal of duplicates, and the creation of aggregated and unique customer profiles, which is particularly beneficial for holistic transaction monitoring and investigation of potentially suspicious behavior.

- Link/network analysis can uncover relationships and connections (often unknown and hidden) among customers, parties, and accounts.

Phase 2: Optimizing Detection

Historically, FIs have deployed automated monitoring platforms with defined rules, scenarios, parameters, and thresholds to identify typologies and patterns of known suspicious conduct. These systems are expected to manage the specific risks associated with the FI's assessment of customers, products, distribution channels, geographical footprint, and cross-border activity. Higher-risk customers and activities should be scrutinized more closely than those assessed as lower risk. As AML compliance leaders continue to depend heavily on rules-based surveillance, they must also leverage new techniques and approaches to elevate these legacy systems:

- Machine learning can automatically ingest and learn from historical analysis of alerts, and case investigations could make recommendations for continual finetuning and improvement of existing transaction monitoring detection scenarios, rules, and modules as well as spot manual investigation and due diligence processes that could potentially be automated and simplified. Successful execution can yield sharper alert quality, reduce false positives, and uplift analyst and investigator productivity over a reasonable period of time.
- Dynamic segmentation enables organizations to leverage unsupervised machine learning models to identify customer segments and adopt thresholds within transaction monitoring detection strategies:
    - Dynamic segmentation can assign customers into groups, often referred to as peer groups, in which all the customers are similar and have the same or similar characteristics as their "peers."
    - Dynamic segmentation considers ongoing behavior using additional data to identify any customer behavior or other factor that may have changed or deviates from the peer group.
    - Enabling the comparison of specific customers' transactional behaviors against those of peers, dynamic segmentation supports better transaction monitoring through anomaly detection with lower false positives.

Phase 3: Optimizing Investigation and Reporting

At most FIs, the time AML analysts and investigators allocate to alert reviews, case investigations, and suspicious activity or transactions, report review, preparation, and filing can be significant. High numbers of alerts impede effective AML investigation practices. Heavy dependence on manual investigative processes frequently leads to operational inefficiency, control degradation, and poor outcomes. Leveraging innovative techniques can drive more informed and faster decision-making:

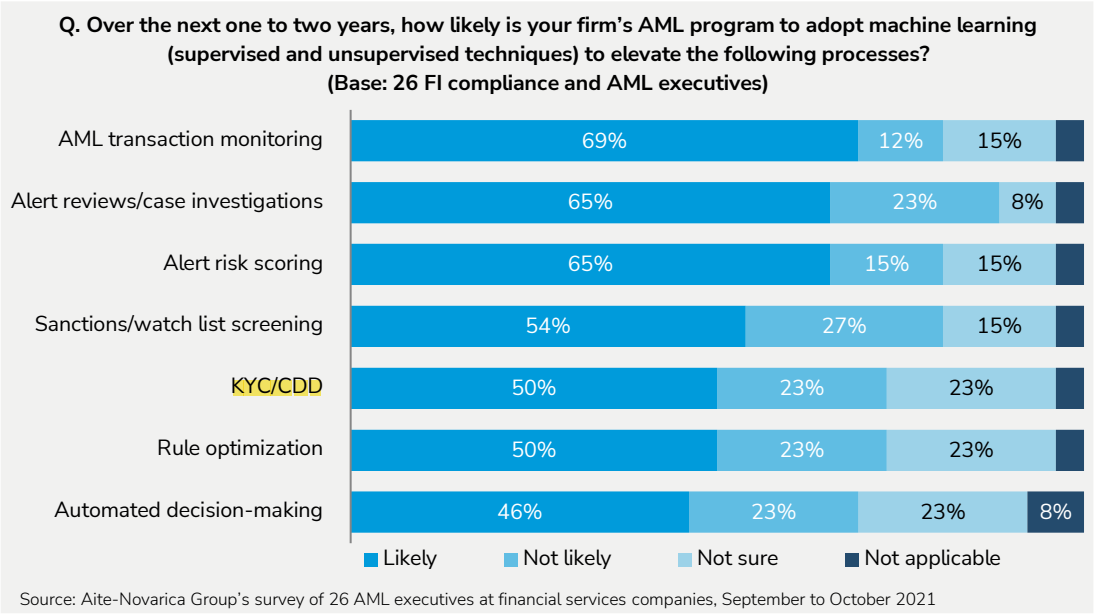
- Alert risk scoring can continuously connect and aggregate related alerts, and risk-rank them based on the probability or likelihood of illicit or potentially suspicious activity. Leveraging advanced analytics and machine learning, alert risk scoring integrates historical alert and case decisioning as well as investigator feedback:
    - As higher-risk events can be prioritized, alert risk scoring can promote a risk-based approach and quickly allocate resources to higher-risk alerts, parties, and events.
    - It can also qualify an alert for hibernation (or pending) until it can be combined with another alert with the same or similar risk score, so that both alerts are investigated at the same time.
- Link/network analytics can build network views of entities and the connections among them to enable analysts and investigators to uncover hidden relationships.
- NLG can optimize the production of case files and notes from the information gathering part of an AML alert review or case investigation. Instead of building a file from scratch, NLG enables analysts and investigators to add their personal comments to an existing case/profile, thus creating efficiency as well as consistency.
- Automation has clearly demonstrated value over the years, and it is often a preferred method for achieving elevated production goals. When working with large, fragmented data or multiple data locations, automation can often run with minimal supervision and eliminate the practice of assigning mundane operations to staff, which in and of itself presents risk (i.e., human error).

Phase 4: Introducing Machine Learning-Based Detection

With the limitations of rules-based detection in today's financial crime threat landscape, AML compliance leaders recognize the imperative for smarter and more nimble surveillance. Embedding machine learning can more effectively transform risk-relevant data into actionable intelligence:

- NLP can analyze text and search documents and adverse media, using sentiment or association analysis to identify patterns, code, and meaning that could indicate criminal behavior. This can be instrumental in minimizing the highly manual and labor-intensive nature usually associated with document reviews.
- AML compliance leaders can and have been leveraging machine learning to elevate many different use cases (Figure 5).
    - Supervised machine learning is often valuable for well-defined, targeted use cases (or known red flags, known risk factors, and existing typologies).
    - Unsupervised machine learning is often used in anomaly or outlier detection to identify normal and abnormal behaviors as well as unusual patterns of activity. Unsupervised machine learning looks for the "unknown unknowns"—those events that would otherwise be undetected because usually nothing is looking for them or they are new occurrences of risk that have not previously been considered.
    - Through adaptive or continual learning functionality, machine learning models in production can learn from future events and adapt to evolving circumstances. This reduces the periodic need to retune and rebuild models due to model degradation and deterioration.
    - Machine learning models can automate the decisioning of alerts identified as lower quality or minimal risk.

FIGURE 5: AML PROGRAM MACHINE LEARNING ADOPTION



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

AML MODERNIZATION JOURNEY: THE GUARDRAILS

FIs can devote much time and resources to the design, construction, testing, and documentation of new AML technology adoption as well as its ongoing refinement. But organizations can be easily tripped up by a lack of a cohesive ecosystem or misalignment to assessed risk exposure. Irrespective of the specific modernization phase or approach, technology adoption must fit and work seamlessly with the organization's control framework and system architecture, and strong governance must underpin each step:

- **Orchestration and integration:** With so many disjointed systems, data sources, and processes, an effective AML control framework mandates that all the systems and data sources are integrated and work together effectively and efficiently. Many third-party platforms facilitate quick and seamless integration by embedding numerous input and output adapters as well as prebuilt connections to core banking systems, payment processers, and third-party data sources.
- **Governance and model risk management:** Achieving the benefits from new innovation mandates strong model risk management. Without appropriate governance, the intended AML design may become inefficient or ineffective, as it may not adapt to changes in regulatory expectations or business and risk landscapes. Data integrity may be degraded. Needed documentation may be inaccurate or incomplete.

- Regulators mandate transparency, understanding, and explainability.
- Embedding governance guards against going off track and introducing biases or other unintended consequences into production.
- Robust governance practices should introduce rigor across each phase of the implementation and maintenance life cycle, engage the appropriate key stakeholders at each step, foster confidence throughout, and help to ensure the ongoing data quality and continuous effectiveness of the AML design.
- Model risk management is beneficial for mitigating potential financial crime risk exposure as a result of gradual model degradation over time.
- To facilitate AML innovation, some FIs have formed innovation hubs with a mix of financial crime subject-matter experts, data scientists, and business leaders.

CONCLUSION

When it comes to an AML modernization journey, financial organizations should experiment and be comfortable with failing fast and celebrating small wins. Quick failures frequently offer meaningful lessons, and small victories are necessary for building larger wins. Familiarity with and the ability to establish the fundamental building blocks, along with knowing how to guard against potential pitfalls along the technical journey, increase the likelihood of attaining a state-of-the-art (or best-in-class) FCP.

By establishing an ongoing, modern-day, intelligent, anticipatory, predictive, responsive, and risk-based compliance program, FIs can avoid the historic frustration of feeling they are running as fast as they can but not getting much, if any traction. By implementing technology designed to augment human decision-making, FIs can significantly minimize the risk of noncompliance, increase investigation product quality and overall production, generally meet customer expectations, improve employee morale, and accomplish most anti-financial crime objectives at a fraction of the cost of current regulatory fines.

ABOUT SAS

SAS is a leading provider of artificial intelligence and advanced analytics solutions, and one of the largest privately held software companies in the world. Used by 91 of the top 100 companies in the global Fortune 500, SAS provides software and services that help customers around the globe transform data into intelligence. SAS integrated solutions include a risk-based approach to monitoring for laundering and terrorist financing activities; the ability to rate new and existing customer scores based on key events and new information; identify and prevent first-party application and payments fraud; detect, prevent and manage fraud enterprisewide in real-time; and address a wide variety of intelligence analysis and investigation management needs with speed and precision.

CONTACT

For more information, please visit www.sas.com

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 leaders as well as experienced researchers and consultants, our experts provide actionable advice to our customer base, leveraging deep insights developed via our extensive network of customers 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

Wren York
+1.469.421.7145
wyork@aite-novarica.com

113102_G237303.0822