Modernizing
Anti-Money Laundering Transaction Monitoring Program

Modernizing AML Transaction Monitoring

From Reactive Compliance to Proactive Intelligence

At a time when financial crime is growing in scale and sophistication, traditional rule-based Anti-Money Laundering (AML) Transaction Monitoring (TM) programs are no longer sufficient. Despite significant investments, financial institutions continue to face high false positives, operational inefficiencies, and regulatory risks. The need for transformation is urgent.

This research explores how financial institutions can modernize their AML TM systems to meet the demands of today's complex financial landscape. Drawing on insights from a 2025 survey of 50 Tier 1 banks across global markets, the report outlines a clear path forward—from legacy systems to AI/ML-powered, adaptive monitoring frameworks.

The report introduces a four-stage maturity model for AML TM modernization and highlights the role of advanced technologies such as AI, machine learning, robotic process automation, and graph analytics. It also addresses the operational, data, and regulatory challenges that institutions must overcome to scale these innovations effectively.

At Capgemini, we believe that the future of AML lies in intelligent, integrated, and explainable systems that not only detect financial crime but also adapt in real time to emerging threats. With the right strategy, technology, and partnerships, financial institutions can build resilient compliance frameworks that are both efficient and future-ready.

The Path Forward

Building Future-Ready AML Compliance Frameworks

The fight against financial crime is entering a new era—one that demands agility, intelligence, and collaboration. As this report outlines, legacy rule-based AML Transaction Monitoring programs are no longer sufficient to detect and deter increasingly complex laundering schemes. Financial institutions must embrace a phased, strategic transition toward AI/ML-powered systems that are adaptive, explainable, and scalable.

This research identifies the key challenges and opportunities shaping this transformation—from data fragmentation and operational inefficiencies to the promise of agentic AI, graph analytics, and real-time monitoring. The six-step roadmap presented in this report offers a practical guide for institutions to modernize their compliance operations while aligning with regulatory expectations.

At Capgemini, we believe that the future of AML lies in intelligent orchestration—where technology, data, and human expertise converge to create resilient, proactive compliance ecosystems. Institutions that act boldly today—investing in innovation, breaking down silos, and partnering with trusted advisors—will not only reduce risk but also gain a competitive edge in the evolving financial landscape.

Let's modernize AML together—intelligently, ethically, and effectively.

Everest Group®

December 2025

Modernizing Anti-money Laundering (AML) Transaction Monitoring (TM) Systems

Contents

03 Introduction

04 TM systems' origins and challenges

05 Hidden compliance costs: from fragmentation to frustration

10 Roadblocks to scalable AI/ML in AML TM and their solutions

15 Conclusion and the way forward

Introduction

The global financial services industry is facing increasing challenges in combating money laundering and financial crimes. Despite significant investments in compliance frameworks, financial crime continues to rise, threatening financial institutions' integrity, eroding customer trust, and destabilizing the global economy. According to the United Nations Office on Drugs and Crime, the scale of money laundering is alarming, accounting for 2-5% of global GDP, an estimated US$2.4-6 trillion by 2025. In response, financial institutions are projected to spend US$20-25 billion annually on Financial Crime Compliance (FCC) operations, particularly Anti-money Laundering (AML) Transaction Monitoring (TM). Investments in compliance technology systems are expected to rise to US$8-12 billion globally.

Recent high-profile penalties, such as the US$3 billion fine imposed on a North American bank for its AML failures, highlight the importance of effective TM. These instances reveal the vulnerabilities in current AML systems, which rely on outdated, rule-based approaches that cannot keep pace with increasingly sophisticated criminal tactics. Thus, financial institutions must move from reactive to proactive strategies and adopt more dynamic, adaptive solutions to safeguard operations and maintain compliance.

This Viewpoint examines the ongoing transformation of AML TM systems, focusing on the role of AI and ML in modernizing compliance processes. The research draws insights from a 2025 survey of 50 Tier-1 banks and financial institutions across North America, Europe, the UK, APAC, and Australia. The participating institutions represent a balanced mix of global investment, commercial, and retail banks. North American and European participants are largely characterized by their strong investment and commercial banking focus, while institutions in APAC and Australia tend to operate with a heavier retail and commercial banking portfolio. This diversity provides a holistic view of how institutions with differing business models and market priorities are advancing AML modernization. The survey explored financial institutions' priorities, challenges, and strategies for enhancing AML TM capabilities.

The report offers a comprehensive roadmap for financial institutions transitioning from traditional, rule-based systems to advanced AI-/ML-driven compliance models. Key questions explored in the report include:

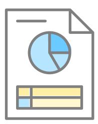
- Strategic priorities for AML TM in 2025
- Rising operational compliance costs
- Technologies that institutions are adopting to enhance their AML functions

This report will equip financial institutions, compliance teams, and technology providers with insights to navigate the evolving landscape of financial crime prevention.

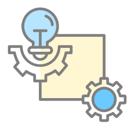
TM systems’ origins and challenges

TM originated in the early 2000s as a regulatory imperative to comprehensive AML laws, such as the USA PATRIOT Act. Financial institutions implemented rule-based systems as a direct response to meet regulatory requirements. These systems rely on predefined scenarios and thresholds to identify potentially suspicious activities. Their simplicity and regulatory alignment made them the default choice for financial institutions navigating stringent AML mandates. The adoption of these systems was driven by several factors that made them the preferred choice for financial institutions at the time.

Factors leading to rule-based scenarios’ rapid adoption:



Simplified oversight and audits



Ease of implementation

Transparent and standardized outputs

Cost-effective start

Despite their initial advantages, rule-based systems struggle to keep pace with modern financial crimes. They create operational inefficiencies, compliance gaps, and customer dissatisfaction, making them inadequate for today’s complex financial landscape. Other challenges related to rule-based systems are:

- **High false positives:** These systems overwhelm compliance teams with non-actionable alerts, diverting resources from addressing real risks
- **Lack of adaptability:** Crude detection methods fail to provide nuanced insights into evolving laundering techniques, such as cryptocurrency layering and trade-based money laundering
- **Fragmented customer profiles:** Disconnected data across retail, institutional banking, and Payment System Providers (PSPs) creates blind spots in monitoring
- **Complex rule management:** Several embedded rules make systems hard to maintain, fine-tune, and optimize, leading to operational inefficiencies
- **Bottlenecks investigation:** Backlogged workflows delay case resolutions, while legitimate transactions are frequently flagged, frustrating customers
- **Regulatory risks:** Reactive, threshold-based monitoring leaves banks vulnerable to emerging financial crime threats rather than proactively mitigating emerging risks

Banks must move beyond rule-based reactive compliance and adopt AI-/ML-driven transaction monitoring solutions to improve efficiency, accuracy, and regulatory resilience.

Hidden compliance costs: from fragmentation to frustration

TM is among the most vital components of a bank's compliance framework and the first line of defense against financial crime. Yet, several banks struggle to build effective, scalable, and adaptive TM systems. Significant gaps persist despite billions in annual investments in workforce, technology, and operational processes. High false positives, fragmented data, legacy technology, and inefficient workflows prevent TM systems from keeping pace with evolving financial crimes. Our analysis reveals that banks rate their rule-based TM systems' effectiveness at 3.5 out of 5, highlighting a clear gap between expectations and performance.

Workforce allocation in AML TM

Workforce allocation in AML TM varies significantly across countries and institutions. Banks prioritize compliance operations differently based on geography, risk appetite, and regulatory expectations.

Now, we discuss banks' AML TM workforce allocation across the US, the UK, and Europe.

Exhibit 1 shows banks' AML TM workforce allocation across the US, the UK, Europe, and APAC. It shows workforce allocation of top banks in AML TM, including FTE distribution across AML and sanctions.

Exhibit 1: Top banks' workforce allocation in AML TM

Source: Everest Group (2025)

	Headquarters	FTEs	AML FTE	Percentage	Sanctions	Percentage	TM	Percentage
Tier-1 bank	US	193,021	9,408	4.76	1590	0.82	1,002	0.51
Tier-1 bank	US	220,960	3,945	1.78	631	0.28	305	0.25
Tier-1 bank	UK	172,475	6,815	3.95	1,453	0.84	1,196	0.69
Tier-1 bank	UK	72,874	2,207	3.03	450	0.62	482	0.66
Tier-1 bank	APAC	44,000	2,900	6.59	704	1.60	920	2.09
Tier-1 bank	APAC	52,000	931	1.79	416	0.80	258	0.5
Tier-1 bank	Europe	74,877	3,428	4.58	887	1.18	662	0.88
Tier-1 bank	Europe	164,921	3,656	2.22	1,122	0.68	649	0.39

Banks' AML TM spending allocation

AML TM spending ranges emphasize the increasing shift toward data and technology for modernization while highlighting persistent labor and infrastructure costs. Strategic spending alignment will be essential for banks to enhance compliance efficiency, lower costs, and improve detection accuracy. Large financial institutions in North America lead with an average annual AML TM spend of US$1-1.2 billion, followed by the **UK at US$850-1,000 million, Europe at US$700-800 million, and APAC at US$550-650 million.**

The spending breakdown in AML TM is listed below.

- **Labor** represents **25-30%** of total AML TM spending driven by manual alert handling, investigations, and compliance reviews
- **Data and technology** is the largest category, accounting for **30-35%,** and reflects investments in AI/ML platforms, data integration tools, and TM systems to drive automation and innovation
- **Infrastructure** accounts for **20-25%,** covering system upgrades, real-time processing capabilities, and cloud-based platforms for transaction growth
- **Managed services** represent **15-20%,** strategically leveraging specialized third-party expertise to improve efficiency and reduce costs

Further analysis shows event detection is the most cost-intensive process in AML TM, followed by review/triage and investigation. These early-stage processes exert the most cost pressures.

Challenges with rule-based monitoring systems

Despite growing financial crime challenges, the top four reasons banks rely on rule-based AML TM systems are data privacy and security concerns, internal policy and regulatory guidance, risk appetite, and technology costs.

Everest Group's survey reveals that nearly 50% of financial institutions still rely on rule-based scenarios, with static rules driving around half of their AML TM processes. These systems received an average effectiveness rating of 3.7 out of 5.

Exhibit 2 illustrates key benchmarking data points in TM.

Exhibit 2: TM benchmarking data points

Source: Everest Group (2025)

Factors	Insights
High alert volume	**False positives account for 85-90% of total** alerts, overwhelming compliance teams and driving significant operational inefficiencies
Manual alert handling burden	The **average handling time is 30-45 minutes at L1** to over 200 minutes at L3, placing a heavy manual burden on investigative resources and delaying resolutions
Cost escalation	Inefficient workflows result in **10-15% of alerts requiring escalation from L1 to L2**, with an additional 8-12% escalating to L3, significantly increasing workload and operational costs
Limited technology integration	On-time **L1 alert closure has a 95% median**, but this rate declines during high alert volumes, delaying resolutions and compounding inefficiencies
Failure to detect behavior-based anomalies	With **only 2-4% of alerts flagged as actionable** for further escalation and SAR filing, rule-based systems fail to capture relevant patterns, reducing overall effectiveness

However, this heavy reliance comes at a high cost, with institutions facing persistent challenges related to rule-based systems. The top pain points include high alert volumes, overburdening compliance teams, and straining investigative resources. The high L1/L2 review costs compound this burden, while false positives drive inefficiencies. Additionally, these systems struggle with limited technology integration and are ill-equipped to generate behavior-based alerts essential for detecting sophisticated laundering techniques.

This data highlights that rule-based systems remain a foundational AML TM component, but their static and siloed nature fails to meet modern financial crime detection demands. To bridge this gap, institutions must embrace dynamic, scalable, and intelligence-driven solutions that can adapt to evolving threats. Financial institutions identified key areas where AI/ML adoption could significantly improve AML TM effectiveness. **Top areas include transactional behavior analysis, enhanced transaction screening, and anomaly detection in expected account activity.** These findings highlight the need for intelligent systems beyond static thresholds, enabling financial institutions to detect financial crime patterns.

The transition from rule-based to AI-/ML-driven AML TM

As financial crimes grow more sophisticated, financial institutions must implement a robust and adaptable TM framework. This section introduces a **4-stage AML TM framework** to help banks transition from traditional rule-based systems to dynamic, intelligence-driven solutions. By following this structured approach, institutions can improve operational inefficiencies, leverage advanced technologies, and meet evolving regulatory requirements.

The framework offers a clear roadmap for modernizing TM, enabling institutions to integrate advanced analytics, AI/ML capabilities, and real-time detection mechanisms. This approach enhances detection accuracy, optimizes resource allocation, and strengthens the compliance ecosystem.

Exhibit 3 details the four stages of the AML TM framework, empowering financial institutions to modernize their AML TM processes.

Exhibit 3: The 4-stage AML TM framework

Source: Everest Group (2025)

Operational impact/effectiveness

Optimized rule-based monitoring

- Combines traditional rule-based systems with basic optimization techniques
- Leverages predefined thresholds with periodic rule adjustments, with anomaly detection
- Includes risk profile segmentation
- Automates rule calibration and maintenance

Advanced rule-based monitoring with statistical enhancements

- Enhances rule-based systems with data-driven tuning
- Incorporates statistical anomaly detection
- Refines rules calibration using historical patterns
- Includes segmented risk scoring for prioritized alerts
- **Integrates external data for risk detection**

Hybrid monitoring (rules and ML)

- Combines optimized rules with ML to improve detection capabilities
- Uses ML for risk scoring and rule optimization
- **Agentic AI systems for investigations**

Fully AI-/ML-driven monitoring

- **Enables real-time adaptive monitoring with AI/ML**
- **Uses graph analytics to uncover hidden entity links**
- Uses generative AI for SAR narratives and investigations
- Integrates structured and unstructured data for risk detection

Sophistication/Capability

To effectively implement the 4-stage AML TM framework, institutions must adopt key innovations that address evolving challenges in detecting and mitigating financial crimes. These innovations enhance each framework stage, ensuring compliance and operational efficiency.

The future of AML TM systems will shift toward predictive, autonomous platforms that adapt to emerging sophisticated financial crimes. These systems integrate self-learning models, leverage global collaborative data networks, and offer real-time insights to outpace evolving typologies. Regulatory frameworks will also evolve, requiring institutions to prioritize greater transparency, explainability, and ethical AI deployment to maintain compliance.

There are four pivotal innovation areas integral to the framework.

1 AI/ML in detection engines

AI and ML transform detecting by enabling dynamic, data-driven monitoring. Key benefits include **real-time detection, fewer false positives, and adaptability to emerging threats.**

For example, supervised ML models classify transaction types based on historical data, while unsupervised models uncover previously undetected patterns by clustering similar behaviors.

2 Graph-based entity resolution and network analysis

Criminals exploit complex networks to hide illicit activities. Graph analytics uncovers hidden connections and suspicious patterns across entities. Key capabilities include **entity resolution, network analysis, detection of sophisticated schemes.**

3 External data integration

Integrating external data sources strengthens TM systems by providing a comprehensive view of customer behavior and risk. Innovations in this area include leveraging data from public registries, sanction lists, and risk databases. Additionally, using information from beneficial ownership registries, adverse media sources, and KYC utilities to fill gaps in customer profiles, creating dynamic customer profiles.

4 Agentic AI systems for investigations

Agentic AI systems streamline AML TM by automating manual tasks and enhancing decision-making. Key applications include alert triage and investigation, leading to improved operation efficiency. These tools improve investigation quality, increase efficiency, and lower operational costs.

Roadblocks to scalable AI/ML in AML TM and their solutions

AI-/ML-based AML TM systems are considered the future of financial crime prevention, offering capabilities beyond traditional rule-based systems. These advanced models reduce false positives, identify hidden patterns, and adapt to evolving laundering typologies in real time. However, many financial institutions face significant challenges in scaling AI/ML systems beyond pilot projects. Implementation remains complex, with obstacles in data, technology, and operations. While Proofs of Concept (POCs) succeed under controlled environments, they fail when faced with fragmented data, regulatory complexities, and operational bottlenecks. Addressing these barriers will be essential for financial institutions to build future-ready compliance frameworks that enhance detection, reduce inefficiencies, and meet regulatory expectations.

Data challenges: a fractured landscape

- **Siloed data and fragmented workflows:** Banks operate with fragmented data across KYC, onboarding, fraud detection, and AML TM. This disjointed structure prevents the creation of unified customer profiles, which is essential for detecting suspicious patterns across touchpoints. For example, consumer and corporate banking data often remain separate, leading to incomplete investigations. Privacy regulations and internal barriers further complicate holistic customer behavior analysis
- **No single source of truth:** Without centralized data systems, banks rely on geo-specific data providers. Cross-border transactions, for instance, often have incomplete or delayed data, creating blind spots in risk assessments. This lack of a unified data repository increases false positives and operational inefficiencies
- **Data quality, completeness, and acquisition costs:** Poor data quality and inconsistent data format reduces AI/ML models' performance. High false positives overwhelm compliance teams, delaying legitimate transactions and causing customer dissatisfaction. Additionally, acquiring external data for completeness, whether from primary or secondary sources, adds significant costs for banks striving to enhance their AML systems. These costs can escalate further when integrating data from multiple external providers

Banks need a unified data strategy to address fragmentation across KYC, fraud, and AML TM. Standardized data dictionaries and secure integrations enable seamless data sharing and agentic AI can analyze this data to detect risks more effectively. Integrated systems help build consolidated customer profiles, reducing RFIs and improving accuracy.

Exhibit 4 provides a detailed overview of the technology provider landscape for AML TM processes, including core categories, key steps, activities, and technology providers.

Exhibit 4: Technology provider landscape for AML TM processes

Source: Everest Group (2025) [NOT EXHAUSTIVE]

Core process category	Data preparation and engineering	Screening and detection	Alert processing and prioritization	Investigation and compliance reporting	Continuous monitoring and improvement	Fraud and Anti-money Laundering (FRAML)
Key steps	Data engineering and preparation	Sanctions, PEP, and adverse media screening	Risk scoring and alert prioritization, digital worker automation	Case management and SAR filing	Continuous improvement	Integrated fraud and AML detection
	Entity resolution	Rule optimization				Behavioral analytics for fraud and AML
		Anomaly detection and typology identification				Cross-channel monitoring
		Network/ Contextual analytics				

Key technology providers

ACUMINOR, alertspeed, Bureau, COMPLY ADVANTAGE, cleareye.ai, FACCTUM, Flagright

fenergo, Google Cloud, Hummingbird, KHARON, LexisNexis RISK SOLUTIONS, LUCINITY, NAPIER AI

NICE Actimize, quantexa, RIPJAR, salv, sas, Senzing, SIGNZY, Solutions io

Palantir, SymphonyAI, THETARAY, TOOKITAKI, WorkFusion

Technology challenges: bridging legacy and innovation

- **Incompatibility with legacy systems:** Most banks rely on legacy systems designed for static, rule-based models. These infrastructures lack the flexibility to integrate AI/ML algorithms or support real-time monitoring. Batch processing delays important alerts, undermining timely intervention
- **Scalability issues:** AI/ML solutions require significant computational resources to process high transaction volumes. Banks struggle to scale these technologies globally, particularly with billions of daily transactions
- **Provider fragmentation:** Around 50% of respondents work with two to four providers, while 25% rely on four to six providers, complicating provider management in AML TM. Multi-provider reliance leads to integration challenges, compatibility issues, and higher maintenance costs. It also complicates technology selection and integration, with many platforms failing to detect complex laundering typologies, such as cryptocurrency mixing
- **Explainability and model drift:** Regulators demand transparency in AI/ML models, but complex algorithms often operate as black boxes. Without explainability, regulatory approval becomes difficult. Despite AI/ML's potential, their adoption faces multiple barriers. Two-thirds of respondents cite high technology costs and integration complexities as primary concerns. Regulatory uncertainty and data quality issues further impede progress. Skill and talent availability remains another challenge, noted by 50% of respondents

  The **Enterprise AML TM Maturity Assessment Framework** provides a step-by-step roadmap for banks to evaluate and upgrade their systems.

- The framework assesses institutional readiness across seven dimensions. Institutions fall into four maturity stages: **Optimized rule-based monitoring, Advanced rule-based monitoring with statistical enhancements, Hybrid monitoring (rules and ML), and Fully AI-/ML-driven monitoring.** This framework empowers organizations to:
  - Assess their current status
  - Identify specific gaps and improvement areas
  - Implement scalable solutions for emerging financial crime threats

Exhibit 5 demonstrates the Enterprise AML TM Maturity Assessment Framework across dimensions.

Exhibit 5: The Enterprise AML TM Maturity Assessment Framework

Source: Everest Group (2025)

Dimension	Optimized rule-based monitoring	Advanced rule-based monitoring with statistical enhancements	Hybrid monitoring (rules and ML)	Fully AI-/ML-driven monitoring
Data infrastructure	Basic transaction data Limited historical data Siloed systems	Centralized data repositories Historical data for statistical tuning Clean and integrated data pipelines	Real-time data ingestion Extensive labeled datasets for training ML models Data governance policies	Comprehensive data lake infrastructure Access to structured and unstructured data Continuous data validation
Technology readiness	Simple rule engines Basic IT infrastructure Low processing power	Advanced statistical tools Enhanced processing capabilities Integration with analytics platforms	ML platforms Compatibility with legacy systems Modular IT architecture	Advanced AI/ML infrastructure Autonomous decision-making tools High-performance computing
Operational approach	High manual workload Focus on meeting basic compliance Low automation	Partially automated repetitive tasks Moderate workload reduction Improved alert prioritization	Significant reduction in false positives Hybrid workflows leveraging ML for prioritization Scalable operations	Fully automated workflows Proactive risk identification Continuous learning and self-optimization
Regulatory alignment	Basic compliance with regulatory requirements Reactive to regulatory updates	Enhanced audit readiness Stronger scenario-based detection	Explainable ML models for compliance Detailed audit trails Enhanced transparency in detection decisions	Proactive engagement with regulators for autonomous AI adoption Supports dynamic, global regulatory requirements
Integration capability	Minimal integration with other systems Standalone rule engines Limited connectivity to KYC or sanctions screening tools	Moderately integrated with transaction systems Analytics partially linked with monitoring systems Cross-system data flows enabled for analysis	Seamless ML models' integration with legacy systems Connected to upstream systems Supports external data ingestion	Fully integrated systems with real-time data sharing Seamless connectivity with KYC, sanctions, and fraud monitoring Supports external ecosystem collaborations
Risk typology coverage	Basic typologies only Focused on predefined scenarios Limited ability to detect emerging patterns	Expanded to cover more nuanced risk patterns Partially automated typology detection Moderate adaptability	Covers complex typologies through ML models Enhanced anomaly detection for unknown typologies Context-specific detection	Real-time detection of new typologies Continuously evolving models for unknown risks Fully adaptive typology library
Collaboration and ecosystem readiness	Siloed operations with no external collaborations Limited use of third-party tools Standalone internal systems	Collaboration with analytics providers Initial use of third-party risk tools Limited integration with the broader ecosystem	Collaboration with FinTechs for ML models Ecosystem engagement for data and tools Integration with RegTech for compliance support	Full ecosystem integration for data sharing and innovation Co-creating AI/ML solutions with partners Seamless external tool adoption

Cloud-native platforms support the modernization of legacy systems, enable real-time anomaly detection, and allow AI/ML to operate at scale. The use of explainable AI improves transparency, adoption, and regulatory compliance. However, stringent privacy requirements and regulatory constraints may require additional security measures, potentially limiting cost-saving opportunities.

Operational challenges: inefficiency costs

- **Resource strain across LoBs:** Separate compliance teams for KYC, fraud, and transaction monitoring create redundancies and inefficiencies. High workloads in L1 and L2 investigations divert resources from strategic initiatives, delaying resolutions
- **Evolving threat landscape:** Criminals continuously innovate with cryptocurrency laundering and DeFi schemes. Many banks lack the agility to update detection models quickly to counter these threats
- **Customer-experience impact:** The reliance on RFIs and outdated workflows delays legitimate transactions and increases customer frustrations. For example, repeated information requests due to incomplete data can erode trust and lead to customer attrition

Optimizing AML TM operations using agentic AI and generative AI

Agentic AI and generative AI are reshaping AML TM by improving operational inefficiencies and adaptability to emerging threats. Agentic AI optimizes core detection and investigative workflows by reducing false positives, consolidating siloed data into real-time customer profiles for faster investigations, and dynamically adapting to evolving crypto-enabled laundering without frequent reprogramming.

Complementing these capabilities, generative AI automates the creation of Suspicious Activity Reports (SARs) narratives, extracts actionable insights from unstructured data in non-standard documents, and guides analysts through complex workflows. Additionally, it enables advanced scenario simulation, **what-if** analysis, and synthetic dataset generation to improve model training and adaptability.

Together, these AI technologies create a synergistic framework. This combined approach optimizes resource allocation, streamlines compliance processes, and helps institutions proactively combat financial crimes. However, rigorous validation, phased implementation, and regulatory alignment remain vital to their successful deployment.

AI and automation reduce false positives and minimize manual effort. Agentic AI helps prioritize high-risk alerts, supports triage and RFIs. Integrating data across KYC, fraud, and onboarding processes enhances detection accuracy, improves the identification of cryptocurrency-related threats, and strengthens both compliance and operational efficiency.

Conclusion and the way forward

As financial crimes grow more sophisticated and regulatory scrutiny increases, financial institutions must modernize their AML TM systems. This Viewpoint highlights key challenges, such as fragmented data, legacy technologies, operational inefficiencies, and evolving threats, that demand a transformative approach. Traditional rule-based systems can no longer keep pace with today's financial crime landscape.

Looking ahead, 58.33% of respondents foresee a hybrid model combining rule-based and AI/ML techniques, while 16.67% expect a complete shift to fully AI-/ML-driven systems. This gradual transition reflects both opportunities and challenges in modernizing AML TM processes.

To remain resilient, compliant, and efficient, institutions must adopt a structured, forward-looking strategy. Financial institutions must implement AI-/ML-based TM systems through phased, use case-specific rollouts rather than full-scale replacements. This gradual approach ensures that AI/ML models are tested thoroughly for consistency, reliability, and compliance while retaining traditional rule-based systems as complementary control mechanisms. These measures mitigate transition risks and align with regulatory expectations.

The following roadmap outlines **six key steps** to guide banks in transitioning from static, reactive models to dynamic, AI-/ML-powered AML TM systems. The way forward demands bold action, innovation, and collaboration. Institutions that adopt this roadmap – leveraging advanced technologies, breaking data silos, and partnering with trusted providers – will strengthen compliance frameworks and position themselves as leaders in combating financial crimes.

Based on our survey, banks evaluating AI-/ML-based AML TM solutions prioritize reducing false positives (75.00%), enhancing operational efficiencies (75.00%), and achieving measurable cost savings (70.83%). Improved risk detection (54.17%) is another key success indicator to ensure systems effectively target emerging financial crime patterns.

Now, we discuss the six key steps in detail.

Step 1
Strategic assessment and alignment

- Identify data, technology, and operations gaps
- Align AML strategies with enterprise-wide risk management and regulatory requirements
- Ensure stakeholder engagement across compliance, IT, and leadership

Step 2
Data integration and management

- Consolidate data sources into a single source of truth and ensure continuous data quality
- Employ federated learning and encryption for compliant data sharing

Step 3
Technology enhancement

- Transition to cloud-native, modular platforms for real-time monitoring and scalable AI/ML adoption
- Prioritize modular, incremental deployments aligned with their budgets and operational priorities
- Partner with technology providers
- Leverage cloud-based pay-as-you-go solutions to reduce upfront costs and cost-effective modernization
- Employ Explainable AI (XAI) for transparency and regulatory confidence

Step 4
Operational optimization

- Automate through agentic AI and digital workforce solutions to reduce operational inefficiencies
- Use customized workflows for retail, corporate banking, and PSPs for efficiency and accuracy

Step 5
Governance, monitoring, and defense mechanisms

- Define clear roles and responsibilities across compliance, IT, and operations
- Establish centralized processes to comprehensively document and organize decisions, workflows, and audit trails
- Leverage centralized case management systems for detailed and accessible SARs, model validations, and decision-making processes
- Ensure alignment with regulatory expectations by proactively identifying compliance gaps and mitigating operational risks

Step 6
Partnership ecosystem

- Access to domain expertise in AI/ML integration, cloud transformation, and managed services through providers
- Regulatory engagement to align with compliance expectations

Everest Group®
With you on the journey

Everest Group is a leading research firm helping business leaders make confident decisions. We guide clients through today's market challenges and strengthen their strategies by applying contextualized problem-solving to their unique situations. This drives maximized operational and financial performance and transformative experiences. Our deep expertise and tenacious research focused on technology, business processes, and engineering through the lenses of talent, sustainability, and sourcing delivers precise and action-oriented guidance. Find further details and in-depth content at www.everestgrp.com.

This study was funded, in part, by
Capgemini

For more information about
Everest Group, please contact:

+1-214-451-3000

info@everestgrp.com

For more information about
this topic please contact the author(s):

Dheeraj Maken, Practice Director
dheeraj.maken@everestgrp.com

Rahul Mittal, Senior Analyst
rahul.mittal@everestgrp.com

Notice and Disclaimers

Case study

A leading global multinational bank faced growing challenges in managing its Transaction Monitoring (TxM) systems. The existing setup generated a high volume of false positives, requiring extensive manual intervention and driving up compliance costs. The bank aimed to modernize its approach by leveraging advanced technologies while preserving a seamless customer experience. Additionally, it sought to align with a **Monitoring-as-a-Service (MaaS)** model to streamline inefficiencies in alert handling and high operational costs due to manual processes.

The solution

To address these challenges, Capgemini partnered with the bank to deliver a **comprehensive and tailored AI-driven TxM enhancement** solution that combined deep domain expertise with cutting-edge technology. The solution was designed not just to improve detection accuracy, but to embed intelligence and automation into the bank's compliance infrastructure. By combining domain expertise, proprietary accelerators, and a collaborative approach, Capgemini ensured the solution was both effective and sustainable. A comprehensive assessment of the bank's current systems informed the design, while all developed assets were transferred to the client to ensure long-term value. This partnership model enabled rapid innovation while maintaining full transparency and control for the bank.

Key aspects of the Implementation

- **POC-led design and leadership**
  Industry SMEs led a proof-of-concept phase to validate the approach and align the solution with the bank's risk and compliance objectives.
- **Data-driven model development**
  Historical transaction and suspicion log data were used to pre-train machine learning models, improving detection accuracy and contextual relevance.
- **Automation and real-time detection**
  Prediction APIs were developed to automate anomaly detection and escalation, reducing manual intervention and enabling faster response times.
- **Collaborative integration**
  Capgemini worked closely with the bank's Risk and Fraud teams to ensure the solution aligned with internal workflows and regulatory standards.
- **Scalable architecture**
  The solution was designed with modularity in mind, allowing for future enhancements and seamless integration with evolving compliance requirements.

The benefits

Through the implementation of Capgemini's enhanced Transaction Monitoring (TxM) framework, the bank is steadily transforming its compliance operations from a fragmented, manual-heavy process into a proactive, intelligent, and business-aligned function with the following benefits:

Modernized financial crime detection

The enhanced TxM solution improved anomaly detection, risk modeling, and fraud management by leveraging machine learning tailored to the bank's specific needs.

Data-driven model training

Historical transaction and suspicion log data were used to pre-train models, ensuring contextual accuracy and relevance, with close collaboration from the bank's Risk & Fraud SMEs.

Reduced false positives and negatives

The solution significantly improved detection precision, reducing the volume of irrelevant alerts and enabling faster, more focused investigations.

Scalable and automated analysis

The system demonstrated strong expandability by automating key parts of the FinCrime division's analysis process, reducing manual workload and increasing throughput.

Real-time anomaly detection

Four prediction APIs were developed to identify and escalate anomalies in real time, enabling timely and targeted responses to potential threats.

Data-powered financial services

Contact us to learn how we can help your organization harness the power of data using AI, machine learning, process automation, and more.

fsid@capgemini.com

About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2024 global revenues of €22.1 billion.

Make it real.
www.capgemini.com