Aite PARTNER. ADVISOR. CATALYST.

AML Model Risk Management: Too Critical to Ignore

JANUARY 2021

Charles Subrt

This report provided compliments of:

SymphonyAI NETREVEAL

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACT POINTS

- Compliance with anti-money laundering (AML) regulations has long been a never-ending battle. And the goal posts are constantly moving. As a key pillar of AML control frameworks, transaction monitoring is a significant instrument in fighting illicit actors and providing law enforcement with valuable intelligence.
- Establishing and sustaining robust AML model risk management practices holds the key in unlocking the true potential within AML transaction monitoring models. Effective AML model risk management enables financial organizations to continually challenge their AML models and establish the reliability and validity of their design, development, and ongoing administration and optimization as well as the quality and accuracy of the data feeding into them.
- This Impact Report explores the imperative of robust AML model risk management and the varying approaches being taken by financial organizations. Financial crime practitioners will discover how strong model risk management can help overcome existing challenges to effective AML detection, better leverage big data and technology, and drive better outcomes and more actionable intelligence.
- Ineffective transaction monitoring has led to regulatory enforcement and censure. Many common AML control deficiencies stem from ineffective designs and care of AML transaction monitoring systems. Regulators are pressing for increased use of innovation while expecting AML model transparency and explainability.
- Excessive false-positive alerts require significant analyst and investigator time that could otherwise be allocated to higher value-added activities. No matter the size of the organization, financial institutions (FIs) are converting a very low percentage of transaction monitoring alerts to suspicious activity reports (SARs). Even slight improvements in AML models can yield sizeable benefits in resource utilization and actionable intelligence, particularly given the heavy investment in investigation teams at FIs. The investigation function is often the largest team under the AML organizational umbrella, especially in the case of larger organizations with higher and more complex transactional activity.
- Typically at FIs, AML model optimization and AML model validation comprise two disparate exercises that are performed by separate functions. Generally, AML model optimization is carried out by the AML compliance organization. Conversely, model validation is viewed as an independent challenge to the AML model owners.
- AML model risk management requires time, effort, and resources. However, it cannot be an afterthought. The benefits of successfully doing it and doing it right are too great, and the risks of doing it wrong or not at all are potentially too severe and punitive. Without strong model risk management practices, AML models tend to be less effective, reliable, and aligned with the FI's risk exposure.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INTRODUCTION

"The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency." Bill Gates[1]

Today, AML compliance leaders are confronted with an abundance of challenges, hazards, and threats emanating from all directions. Money launderers, terrorists, and other criminals are constantly attacking their financial organizations looking to cash in. And with recent advancements in technology, they are only becoming smarter and more skilled in keeping ahead of AML defenses. Finding them is like finding the proverbial needle in a haystack. Attempting to stem the ever-rising tide of financial crime, regulators and lawmakers around the globe are continually elevating their expectations of and increasing their scrutiny of the financial services industry. And there does not appear to be any end in sight. As AML compliance leaders work tirelessly to combat financial crime and achieve regulatory compliance, these efforts are complicated by a rapidly evolving business landscape. To stay ahead of the competition and increase revenue, firms are launching new products and services, and are gravitating to more seamless and digital customer experiences. And to reduce operational overhead, executive management is pressing all leaders, including compliance and risk management executives, to rein in spending and to do more with less.

More and more, to overcome these challenges, AML compliance leaders are embracing the enormous upside in big data and technology. Innovation can drive more effective and efficient AML monitoring and detection. However, without transparency, explainability, and constant vigilance and fine-tuning, AML transaction monitoring models may fail to deliver on their promise and purpose, and can often lead to inadequate, and perhaps incorrect, intelligence, decision-making, and outcomes. Establishing and sustaining robust AML model risk management practices holds the key for AML compliance officers to unlock the true potential within AML innovation.

This Impact Report explores the evolving financial crime risk landscape, the imperative of robust AML model risk management, and the approaches being taken by financial organizations. Through these insights, financial crime practitioners will discover how strong model risk management can help overcome existing obstacles to effective AML detection, better leverage big data and technology, and drive better outcomes and more actional intelligence.

METHODOLOGY

Commissioned by SymphonyAI NetReveal, Aite Group conducted interviews with 14 executives from financial organizations across the U.S. and Canada, and supplemented these with additional research of publicly available material.

1. Nicholas Carlson, "20 Quotes Show Us How Bill Gates Became The World's Second Richest Man," Busines Insider, March 4, 2013, accessed January 20, 2021, https://www.businessinsider.com/quotes-from-the-worlds-second-richest-man-2013-3.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

THE MARKET

Compliance with AML regulations has long been a never-ending battle. And the goal posts are constantly moving. Since the advent of global AML regulatory regimes, regulated entities, no matter how large or small, are obligated to design, construct, and maintain risk-based programs that effectively deter, prevent, detect, and report on financial crime and minimize the threats to the soundness and safety of the global financial system. Yet the world is in constant flux, altering the risk and threat landscape that AML compliance leaders must overcome.

As a key pillar of AML control frameworks, transaction monitoring is a significant instrument within financial organizations in fighting illicit actors. Through their filing of SARs, FIs provide law enforcement with valuable intelligence that they use to uncover and thwart criminal networks. To facilitate that key AML program objective, financial organizations establish processes and systems to dynamically monitor the behavior of customers, identify unusual transactions and suspicious activity, and report them to law enforcement. Moreover, financial organizations are expected to pinpoint those customers presenting with higher risk for potential illicit activity and apply enhanced due diligence commensurate with their elevated risk profiles.

Historically, to detect anomalies and patterns that may give rise to potential money laundering or other criminal conduct, many financial organizations deployed software solutions with predefined rules. Although financial organizations devote much time and resources to the design, construction, testing, and documentation of these systems, many FIs still struggle with effecting risk-based financial crime monitoring. Table A illustrates the primary challenges impeding current AML transaction monitoring systems and their implications.

Table A: Today's AML Transaction Monitoring Challenge Trends and Implications

Trends	Implications
Increasing regulatory expectations and potential censure	For some FIs, ineffective transaction monitoring has led to regulatory enforcement. Many common AML control deficiencies stem from inadequate designs and care of AML transaction monitoring systems. Regulators are pressing for increased use of innovation in elevating financial crime detection while expecting transparency and explainability of AML models.
Rapidly evolving business landscape and rising illicit activity	Today's rapidly changing, fast-paced, and unpredictable financial and business world tests AML compliance leaders and current financial crime detection. The volume of fraud, money laundering, and other financial crime continues to rise. Increased innovation can link connected parties, build more holistic customer profiles, identify hidden threats, and expand risk coverage and financial crime detection.
Legacy-based AML transaction monitoring limitations	Often, rules-based AML transaction monitoring systems are ill-equipped to cope with and adapt to the rapidly changing business landscape and emerging financial crime threats and typologies.
Too many false-positive alerts	A high number of alerts require extensive resources to investigate and decision, often diverting resources from higher value-added activities. One larger U.S. bank interviewed is gradually testing behavioral suppression rules in hibernating certain generated alerts for further analyst work-up.

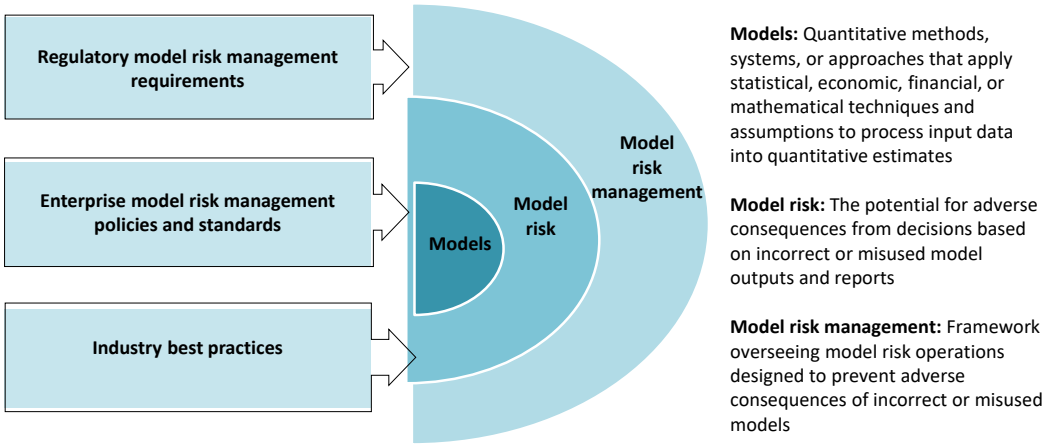
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Trends	Implications
Complexity and expected transparency of next-generation technology adoption	To address current operational pain points, many FIs are integrating next-generation technology into their transaction monitoring systems. Yet as a result, AML transaction monitoring models are getting more complex and more challenging to design, build, and maintain.

Source: Aite Group

Given the criticality of effective transaction monitoring systems and processes—and the considerable efforts to build and sustain them—it behooves financial organizations to establish robust AML model risk management and governance practices. Moreover, global regulators expect them. Regulators mandate that financial organizations be able explain and defend how AML models work to effectively spot financial crime. As such, financial organizations must continually challenge their AML models and establish the reliability and validity of their design, development, and ongoing administration and refinement as well as the quality and accuracy of the data feeding into them. Figure 1 illustrates the model risk management ecosystem and provides definitions for models, model risk, and model risk management.

Figure 1: The Model Risk Management Ecosystem



Source: Aite Group

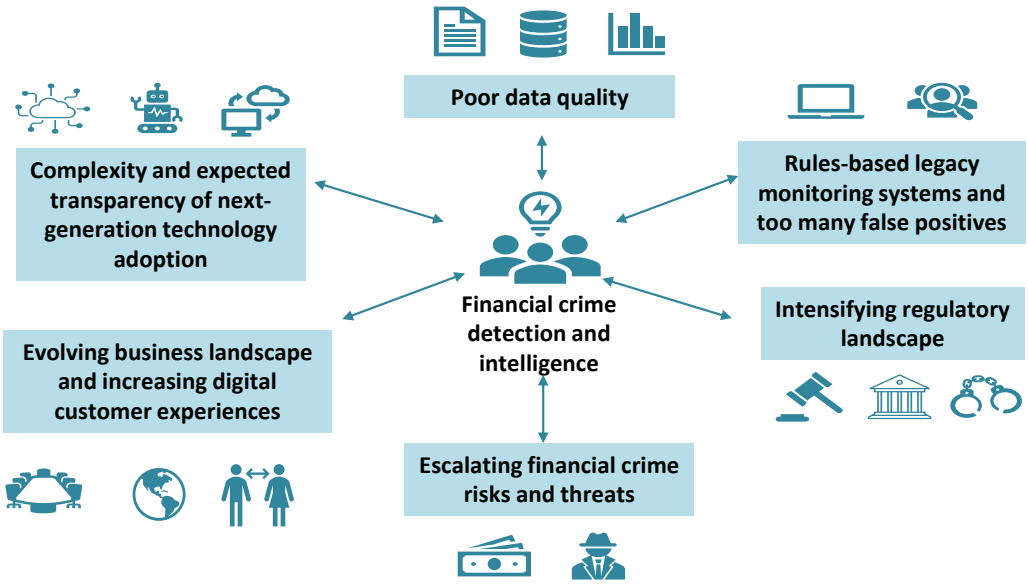
AML model risk management requires time, effort, and resources. However, it cannot be an afterthought. The benefits of successfully doing it and doing it right are too great, and the risks of doing it wrong or not at all are potentially too severe and punitive.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

HEADWINDS TO EFFECTIVE AML MONITORING

Figure 2 illustrates the primary challenges impacting AML transaction monitoring platforms.

Figure 2: Primary AML Monitoring Platform Challenges



Source: Aite Group

INTENSIFYING REGULATORY LANDSCAPE

With persistent angst of the corroding harm of financial crime and the inabilities to curb its growth, regulators around the globe as well as the Financial Action Task Force and similar AML industry groups increase expectations for the financial services industry. They are pressing for more risk-based, more results-oriented, and more innovative approaches to combating financial crime, greater corporate transparency, and expanded use of big data and technology:

- In September 2020, the Financial Crimes Enforcement Network (FinCEN) published an advance notice of proposed rule-making forecasting potential regulatory amendments "intended to modernize the [AML] regulatory regime." FinCEN's proposals attempt to articulate an "effective and reasonably designed" standard that would drive greater risk-based approaches to AML compliance and resource allocation.[2] In 2019, FinCEN and other U.S. regulatory bodies issued a joint

2. "Anti-Money Laundering Program Effectiveness: A Proposed Rule by the Financial Crimes Enforcement Network on 09/17/2020," Federal Register, September 17, 2020, accessed December 20, 2020, https://www.federalregister.gov/documents/2020/09/17/2020-20527/anti-money-laundering-program-effectiveness.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

statement underscoring the importance of appropriately calibrating AML programs with identified risks.[3]

- In early 2020, the U.S. Department of the Treasury published its 2020 Strategy for Modernizing the U.S. AML Regime mandating more dynamic, risk-based, and targeted approaches to AML compliance; innovative and intelligent financial crime detection; and actionable intelligence for law enforcement.
- In the EU, the Fifth AML Directive increased customer due diligence (CDD) and beneficial ownership requirements, enhanced the powers of EU financial intelligence units, and brought virtual currency platforms and wallet providers under its umbrella. Published in 2018 and effective in December 2020, the Sixth AML Directive addressed gaps in preceding directives, provided additional clarity, and promoted increased information sharing and collaboration among EU member states.[4]
- In Canada, the Financial Transactions and Reports Analysis Centre of Canada significantly amended the regulations to its Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Becoming effective in 2021, the amendments elevate client identification, CDD, and regulatory reporting obligations, and extend expectations upon virtual asset service providers and other industries.
- In 2019, the Wolfsberg Group issued its Statement on Effectiveness championing a supervisory approach that focuses more on effective outcomes and less on technical AML compliance. The Wolfsberg Group stressed that too much focus was concentrated on technical compliance, not always elevating the detection and deterrence of illicit activity.

REGULATORY PROMOTION OF INNOVATION

Recognizing the potential of innovation to accelerate elevated prevention and detection of financial crime, global regulators have been promoting financial technology and regulatory technology for a number of years. Innovation labs, regulatory sandboxes, and tech sprints are progressively becoming the standard around the world. For almost a decade, the U.K. Financial Conduct Authority has supported fintech investment and has launched numerous tech sprints. In the U.S., FinCEN and other federal banking regulators issued a 2018 joint statement that encouraged private innovation and experimentation.[5]

3. "Federal Bank Regulatory Agencies and FinCEN Improve Transparency of Risk-Focused BSA/AML Supervision," FinCEN, July 22, 2019, accessed December 20, 2020, https://www.fincen.gov/news/news-releases/federal-bank-regulatory-agencies-and-fincen-improve-transparency-risk-focused.
4. See Aite Group's report *Introducing the Fifth Anti-Money Laundering Directive: Are You Ready?*, February 2020.
5. See Aite Group's report *Regulatory Innovation, Sandboxes, and Tech Sprints: Trends and Global Initiatives*, March 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

REGULATORY CONCERN FOR EXPLAINABILITY AND TRANSPARENCY

Even as global regulators push for innovation, they concurrently press for the ongoing reliability, effectiveness, transparency, and explainability of AML transaction monitoring and detection models. For regulators, AML model risk is simply another risk that AML compliance functions must continually assess, monitor, and manage, and have processes in place to do so:

- The Office of the Comptroller of the Currency's (OCC) Supervisory Guidance on Model Risk Management (OCC 2011-12) sets forth the mandates of prudent model risk management frameworks, practices, and standards. The guidance elaborates the key attributes expected for model development, implementation, and use as well as the governance and controls. Effective challenge is recognized as a central principle of sound model risk management.[6]

- The New York Department of Financial Services (NYDFS) Superintendent's Regulations Part 504 (NYDFS Part 504) obligates regulated entities adopt and maintain risk-based transaction monitoring programs that are "reasonably designed" to adhere to AML obligations. NYDFS Part 504 outlines specific standards for data identification, validation, and extraction, transaction monitoring model validation, vendor management, and program governance and oversight. The rule also requires annual certifications from senior officers attesting to compliance with NYDFS Part 504. With New York State being an international financial hub, NYDFS Part 504 is far-reaching.[7]

- In the EU, the European Banking Authority's Supervisory Review and Evaluation Process mandates that model risk must be identified, mapped, tested, and reviewed.[8]

As such, financial organizations are being asked to construct AML model risk management practices to monitor and confirm the ongoing functionality and effectiveness of their end-to-end AML transaction monitoring frameworks. Good AML risk model management should identify the sources of model risk, assess its probability and severity, and establish a documented framework for appropriately managing it. On an ongoing basis, it should confirm data quality, detection rules and methodologies that are proportionate to firms' assessed risk exposure, adequate model development, deployment and testing, and ongoing maintenance, monitoring, validation, and fine-tuning. On top of identifying gaps or deficiencies, model risk management must also pinpoint opportunities for improvement and operational efficiency. As AML models integrate

6. "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management," OCC, April 4, 2011, accessed January 20, 2021, https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12.html.

7. "New York Department of Financial Services, Part 504 Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications," Thomson Reuters Westlaw, accessed January 20, 2021, https://govt.westlaw.com/nycrr/Document/If190167558ac11e6806bc9321b10fb4e.

8. "ECB Guide to Internal Models," European Central Bank Banking Supervision, October 2019, accessed January 21, 2021, https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.guidetointernalmodels_consolidated_201910~97fd49fb08.en.pdf.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

machine learning, advanced analytics, and other next-generation technologies, the need for strong AML model risk management practices only becomes more acute.

EVOLVING BUSINESS AND RISK LANDSCAPE

Today's rapidly changing, fast-paced, and unpredictable financial and business world tests AML compliance leaders and current financial crime detection processes and systems. The COVID-19 pandemic further accentuates these difficulties:

- More than ever, consumers are seeking more digital and frictionless experiences, and are increasing their use of remote and mobile banking services. For financial organizations, keeping current customers happy and acquiring new ones mandate more innovative, digital, and consumer-friendly onboarding, products, and services.
- To boost profits and fuel growth, financial organizations are expanding into new markets and channels. Payments are getting faster and more complicated.
- The pandemic has left FIs with an unclear future. Even before the pandemic, FIs expected a down economy. Now, many may be pressed to curtail expenses and operational infrastructures, particularly in the short term.

As financial organizations navigate this increasingly capricious landscape, global networks of criminal organizations hunt for opportunities to exploit the underlying vulnerabilities for illicit gain. The volume of fraud, money laundering, and other financial crime continues to rise. As technology advances and becomes more easily accessible, bad actors are becoming more tech-savvy, innovative, and sophisticated. Their attacks are now more automated and complex. They are extremely adept at concealing their identities and evading detection. Moreover, with the pandemic and the unleashing of stimulus programs across the globe, many firms are witnessing an upsurge in mule activity, identity theft, and application fraud. For instance, organized crime rings are procuring the assistance of money mules to seize and divert massive sums of stimulus money into their coffers.

In order for AML compliance leaders to successfully confront this challenging landscape and beat back the onslaught of illicit attacks against their organizations, their AML transaction monitoring and detection systems must continually account for and adapt to the ever-evolving risks and financial crime threats. Increasingly, firms must connect the dots across disparate data systems and across multiple business lines and channels. As AML compliance leaders embrace big data and technology as the only path in keeping pace with financial crime, monitoring solutions are becoming smarter and more agile. Increased innovation can link connected parties, build more holistic customer profiles, identify hidden threats, and expand risk coverage and financial crime detection.[9] Yet without constant scrutiny, validation, and recalibration of AML detection models, rules, parameters, and thresholds, in addition to the underlying data, AML monitoring will fail to fully deliver on its true objectives.

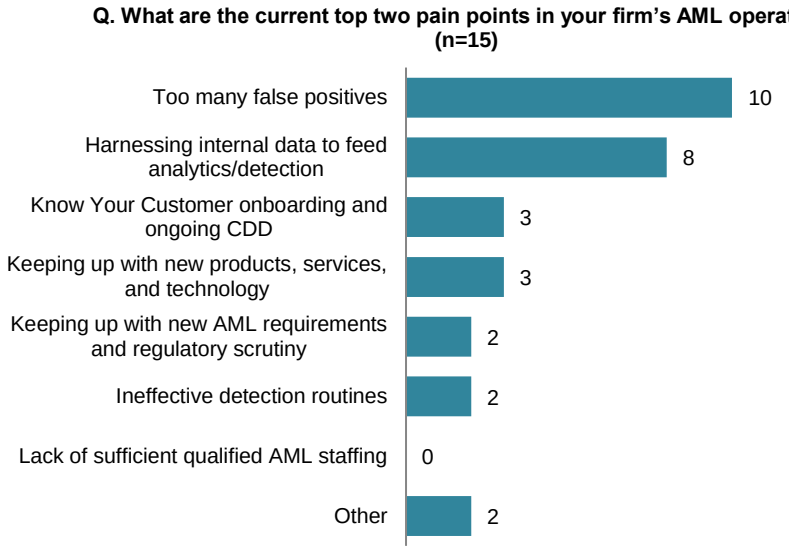
9. See Aite Group's report *AI-Enabled Anti-Money Laundering: From Theory to Reality*, July 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CURRENT AML OPERATIONAL CHALLENGES AND EMBRACING INNOVATION

AML compliance leaders often point to the inabilities in harnessing data for effective analysis and detection and a high volume of false-positive alerts as primary challenges to sustaining effective AML compliance practices (Figure 3). Many firms suffer from fragmented, messy, and often incomplete data sets, largely driven by a loosely connected amalgamation of diverse data sources, systems, and repositories. Much vital customer and transaction information resides in unstructured or hard-to-access formats. Inferior and incomplete data prevents holistic views of customers and enterprise risk, degrading risk-based financial crime detection. Bad data can cause duplicate alerts and too many false positives, leading to unnecessary investigations and due diligence, lower productivity, missed risks, and faulty decision-making. Heavy dependence on manual investigative processes leads to further control degradation. These pain points can quickly erode effectiveness, operational efficiency, and customer experiences.[10]

Figure 3: AML Operational Pain Points



Source: Aite Group survey of 22 financial crime professionals, September 2020

IMPACT OF AML INVESTIGATIONS

Often the result of rules-based AML monitoring systems, excessive false-positive alerts adversely impact AML investigation practices. They require significant analyst and investigator time that could otherwise be allocated to higher value-added activities. At many firms, investigators are a huge expense. An FI's specific AML investigation practices and the required number of investigators are influenced by many factors, largely the nature and complexity of the organization's business and operations, the applicable regulatory obligations, the volume of transactional activity and transaction monitoring alerts, and overall risk profile:

10. See Aite Group's report *Key Trends Driving AML Compliance Transformation in 2021 and Beyond*, November 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- The investigation function is often the largest team under the AML organizational umbrella, especially in the case of larger organizations with higher and more complex transactional activity. At some financial organizations, some staff who perform alert reviews and case investigations will also perform other AML-related tasks. Larger FIs often build more dedicated investigations functions, with multiple teams, including very specialized units of former law enforcement. At one top-20 U.S. FI interviewed for this report, the investigation team comprises more than 80% of the entire 250-member AML compliance function.

- Time spent on alerts, case investigations, and SAR review, preparation, and filing varies both within an FI as well as across the industry. In general, work on initial alert reviews (often referred to as level one or L1 reviews) ranges from 10 to 30 minutes, while escalated alerts and cases (referred to as level two or L2 reviews) take anywhere from a few hours to a full day, with some more complex matters taking much longer. One financial organization established a standard that any L1 alert review exceeding 15 minutes must be immediately escalated to an L2 investigation that will be handled by a more senior investigator.

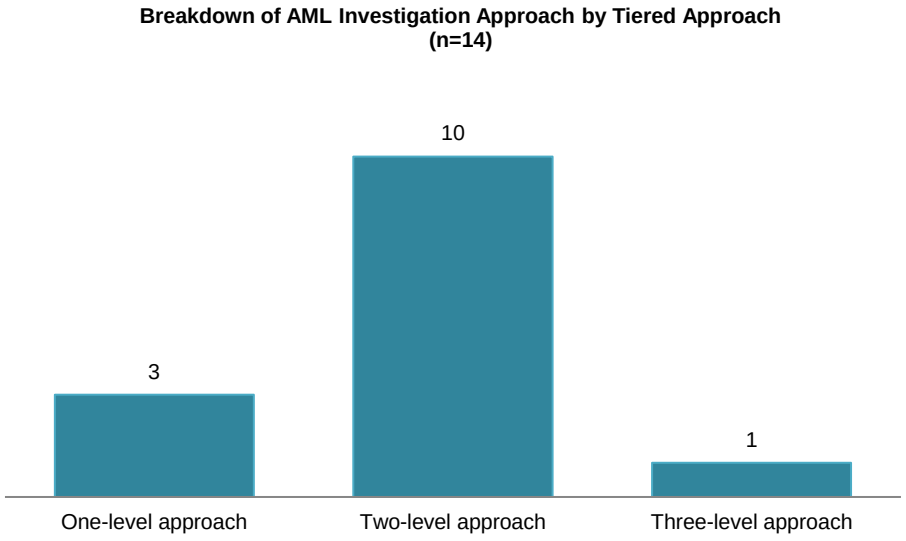
    - Most firms interviewed have moved away from using a three-tiered investigation approach (Figure 4). Many firms now incorporate an initial triage approach in order to immediately close clear false-positive alerts or assign alerts to the most relevant group of investigators, with more complex tasks going to more seasoned and experienced investigators:

    - One AML compliance officer interviewed recently transitioned to a triage approach to embed greater efficiency into the overall investigation process. Prior practice had work assigned to single analyst or investigator without consideration of the severity of the matter or the complexity of the investigation. Through experience, it became evident to that AML compliance officer that junior investigators tended to treat all alerts very much the same. Without years of experience, many generally lacked the necessary expertise, skills, and acumen to fully appreciate and deduce how much time, effort, and scrutiny should be expended on any given alert. The triage approach addressed this headache (Figure 4).

    - At one midsize regional bank interviewed for this report, there is no separation of duties across fraud and AML investigators, as they handle all phases of investigation from alert to investigation to SAR determination and filing. In the words of the AML compliance officer, suspicious activity is suspicious activity, and a red flag indicator can represent money laundering, fraud, or both.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 4: AML Investigation Approach Breakdown



Source: Aite Group interviews of 14 financial crime professionals, August and September 2020

LOW ALERT-TO-SAR CONVERSION

No matter the size of the organization, FIs are converting a very low percentage of transaction monitoring alerts to SARs. Conversion rates typically fall below 3%, many with significantly lower ratios. Very few organizations exceed a 6% alert-to-SAR conversion rate. AML compliance leaders continuously search for sharper detection and uplifts in their conversion metrics. Even slight improvements can yield sizeable benefits in resource utilization and actionable intelligence given the heavy investment in investigation teams at FIs.

Table B illustrates the number of investigator full-time equivalents (FTEs) and the annual alert-to-SAR conversion statistics across 12 FIs surveyed for this report.

Table B: Annual Transaction Monitoring Alert-to-SAR Conversion Metrics

FI location/asset size (In US$ billions)	Number of investigator FTEs	Annual number of alerts	Annual number of SARs	Alert-to-SAR conversion rate
Canada/under $10	4	6,000	2	0.03%
U.S./under $10	2	18,000	250	Less than 1%
U.S./between $10 and $25	12	22,000	1,000	4.50%
U.S./between $25 and $50	18	17,000	1,000	6.50%
U.S./between $25 and $50	3	18,000	800	2%
U.S./between $25 and $50	12	44,500	1,200	2.7%
U.S./between $25 and $50	50	140,000	2,800	2.50%

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

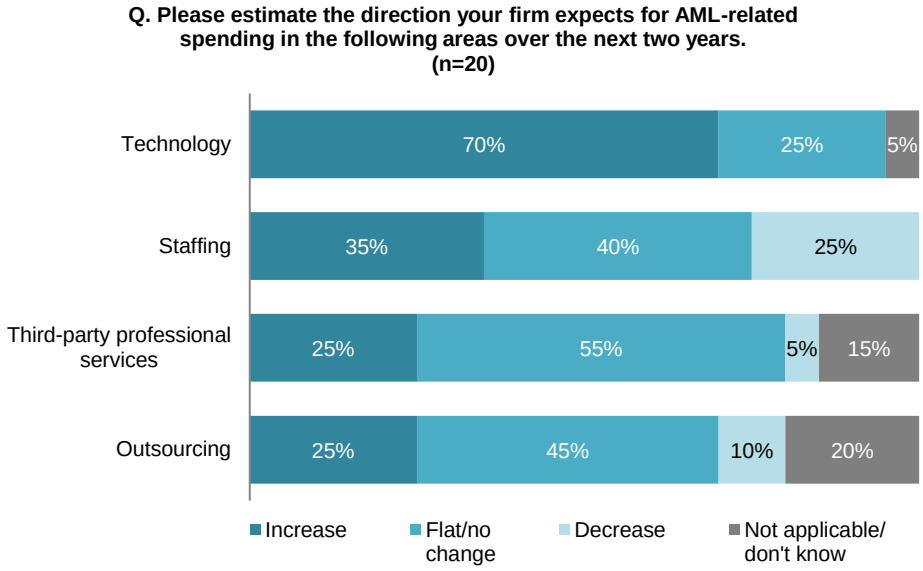
FI location/asset size (In US$ billions)	Number of investigator FTEs	Annual number of alerts	Annual number of SARs	Alert-to-SAR conversion rate
U.S./between $25 and $50	30	160,000	1,600	1%
U.S./greater than $150	24	25,000	300	1.50%
U.S./greater than $150	43	60,000	1,200	2.50%
U.S./greater than $150	125	144,000	4,200	3%
U.S./greater than $150	200	144,000	17,000	11%

Source: Aite Group interviews of 14 financial crime professionals, August and September 2020

INCREASING AML TECHNOLOGY ADOPTION

To conquer these challenges, AML compliance leaders are increasingly adopting next-generation technologies into their surveillance systems. When surveyed on the direction for AML-related spending over the next two years, 70% of FIs expect to increase spending on technology (Figure 5). Advancements in computing power and new techniques such as entity resolution, robotic process automation, network and link analytics, natural language techniques, and advanced analytics can ingest and process massive data sets and unlock the potential within, elevate current detection schemas, identify hidden risks, and harvest more actionable intelligence.[11]

Figure 5: AML-Related Spending Forecasts Over the Next Two Years



Source: Aite Group survey of 22 financial crime professionals, September 2020

11. See Aite Group's reports *AI-Enabled Anti-Money Laundering: From Theory to Reality*, July 2020, and *Key Trends Driving AML Compliance Transformation in 2021 and Beyond*, December 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

However, the task of adopting and integrating new technologies is complex—with many options and many pitfalls:

- Organizations may move to replace and upgrade existing monitoring systems and processes. Those can span from manual surveillance through Excel spreadsheets or exception reports to automated homegrown solutions, at times with limited functionality and case management features, to third-party vendor software.
- Others may supplement and augment existing detection platforms with specialized functionality through other homegrown or third-party vendor applications.
- Some organizations with multiple platforms may choose to consolidate, as many favor a "single throat to choke" philosophy to IT solution management.

Irrespective of the approach taken, any technology adoption involves multiple steps requiring significant time and effort from many functions across an enterprise. Achieving the benefits from new innovation mandates strong model risk management. Embedding governance guards against going off-track and introducing biases or other unintended consequences into production. Furthermore, regulators mandate transparency, understanding, and explainability. To facilitate AML model risk management, some FIs have formed innovation hubs with a mix of financial crime subject-matter experts, data scientists, and business leaders.

When designed, constructed, and deployed properly, innovation can reap responsive, agile, and elevated financial crime detection while driving down false positives and driving up operational efficiency, enabling reallocation of resources, both in people and in funding, to higher value-added activities. However, when done without vigor, vigilance, and validation, FIs will be challenged to attain the full breadth of these benefits, and they may degrade control performance.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

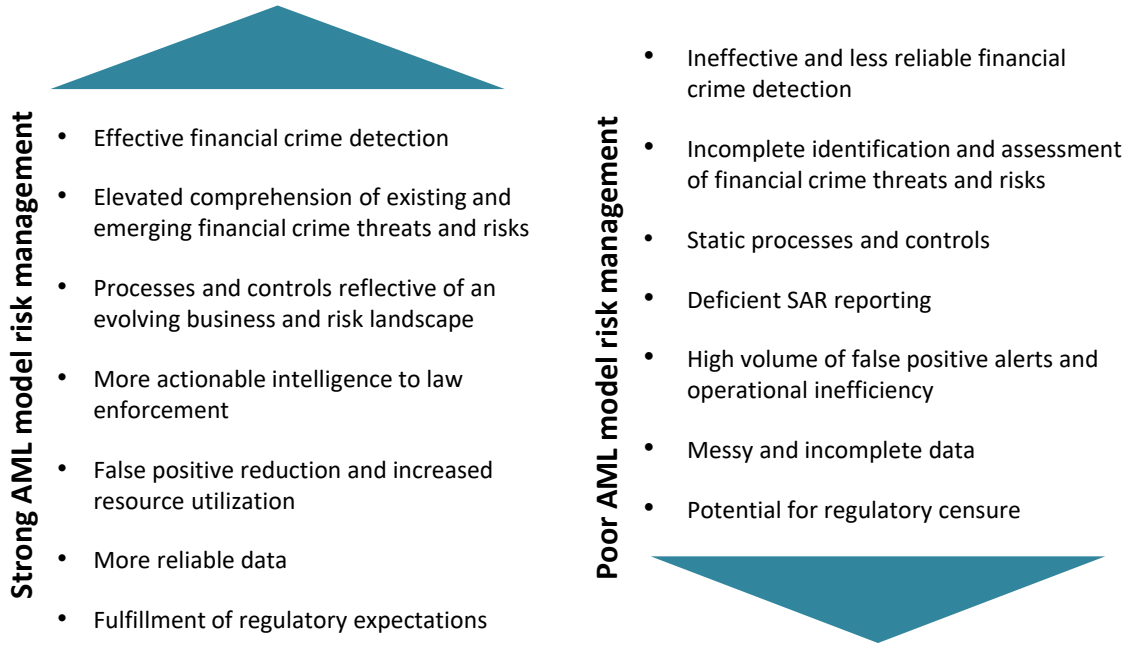
THE INCREASING IMPERATIVE OF AML MODEL RISK MANAGEMENT

Historically, FIs have deployed automated monitoring platforms with defined rules, scenarios, parameters, and thresholds to identify typologies and patterns of known suspicious conduct. These platforms are generally based upon and tailored to the FI's specific risks associated with its assessment of customers, products, distribution channels, geographical footprint, and cross-border activity. Higher-risk customers and activities are scrutinized more closely than those assessed with lower risk. Political figures, connections to sanctioned or higher-risk jurisdictions, or complex corporate structures are a few examples of potential higher-risk factors.

FIs devote much time and resources to the design, construction, testing, and documentation as well as the ongoing refinement of these platforms. However, organizations are frequently tripped up by a lack of alignment to assessed risk exposure—failure to adapt models to changes in the regulatory expectations or the business and risk landscapes, inefficient models, data integrity deficiencies, and inaccurate or incomplete documentation or evidence to support model design, development, and ongoing sustainability. Moreover, as FIs adopt new techniques to elevate surveillance and adapt to evolving financial crime risks, AML monitoring systems are becoming more complex to manage. Without strong model risk management practices, AML models tend to be less effective, reliable, and aligned with the FI's risk exposure.

Figure 6 highlights the likely upsides of instilling effective AML model risk management as well as the potential downsides when doing it poorly.

Figure 6: Impact of Strong and Weak AML Model Risk Management



Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

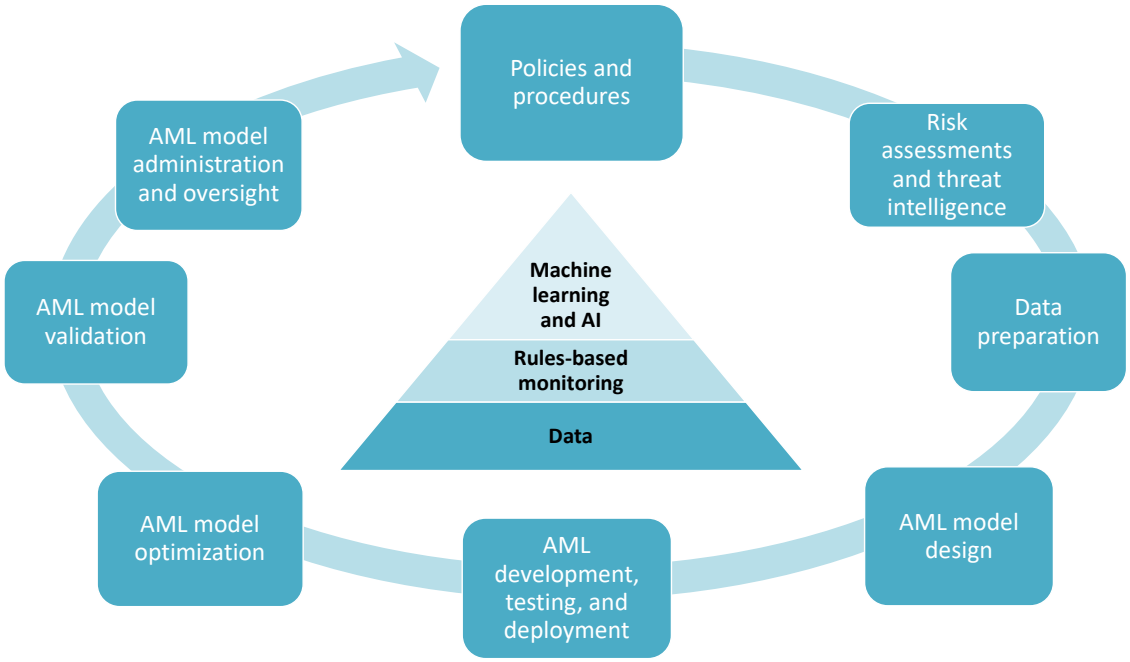
Strong model risk management practices can guard against stumbles and deliver dynamic transaction monitoring:

- They can ensure financial crime detection and reporting is effective and relevant as well as meet regulatory expectations for model transparency and explainability.
- They can minimize false-positive alerts, increase resource productivity and utilization, elevate operational efficiency, and help with cost management.
- They can ensure that the design of rules and models continue to be fit for purpose and the ever-changing risk landscape and the configurations continue to work as designed.
- They can ensure ongoing completeness, accuracy, and integrity of customer and transaction data being extracted from internal and external sources and ingested into AML monitoring platforms.

CORE PRINCIPLES OF AML MODEL RISK MANAGEMENT

The following sections outline the different components of AML model risk management, each of which is essential to sustaining reliable, dynamic, and efficient designs, construction, and maintenance (Figure 7).

Figure 7: AML Model Risk Management Framework



Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

AML MODEL RISK GOVERNANCE

Built on well-defined policies and standards and vigorous risk assessment practices, AML model risk governance helps to ensure that the primary objectives of the transaction monitoring processes are achieved, the models meet the evolving demands and threats, and the AML program produces the appropriate documentation and evidence:

- **Policy and standards:** Financial organizations should have a well-documented policy and set of standards that are based upon applicable regulations, enterprise model risk management policies, and general good practice. Together, they should establish the core foundation for and enable strong AML model governance practices. At a minimum, they should set the following:
    - A clear AML model definition with clearly stated inclusion and exclusion criteria and standards
    - The primary objectives and rationale of the AML models themselves
    - The specific attributes of AML model life cycle management: data preparation, model development, deployment, testing, monitoring and optimization, issue and change management, ongoing administration, documentation, and audit trail
    - The roles and responsibilities of accountable stakeholders, including the AML compliance officer, IT, enterprise model risk management, internal audit, executive management, and the board of directors
- **Risk assessments and threat intelligence:** Prior to AML model creation, financial organizations should identify, assess, and understand their primary risks and threats with an acute focus on those emanating from their products, services, delivery channels, customers, operations, and geographical footprints. These assessments should consider the impact of the regulatory landscape in addition to the current and emerging threats and typologies. Moreover, as circumstances always change, financial crime risks will evolve, so the AML risk assessment should be an ongoing, continual, and dynamic endeavor.

AML MODEL LIFE CYCLE MANAGEMENT

Robust and standardized AML model life cycle management practices introduce rigor across each phase of the 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 transaction monitoring models themselves:

- **Initial model design:** Only after the financial crime risk universe is fully defined and appreciated can an AML compliance officer begin to pinpoint and prioritize the key risks and the relevant AML transaction monitoring models for design and development. Historically, to monitor transactions, FIs have relied heavily on rules-based solutions deploying multiple risk-based scenarios with defined rules, parameters, and thresholds. Given the inherent limitations and challenges of those systems, financial organizations are increasingly integrating more advanced analytic techniques. Innovation can sharpen detection and harvest elevated intelligence.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- **Data analysis, preparation, and gathering:** To be effective, AML models need quality data. As the saying goes, "Garbage in, garbage out." Hence, as the models are being designed and developed, the potential data sources should be identified, mapped, and assessed. Often, needed data can be messy, incomplete, or hard to access. In some cases, the required data may not exist. For the models to work as designed, decisions have to be made regarding how the data will be brought together and ingested by the models. The availability, integrity, reliability, and completeness of data will influence the design, creation, and the ongoing viability of AML models throughout the end-to-end model life cycle.

- **Initial AML model development, testing, and deployment:** As models are being built, they should be continually scrutinized to confirm that they are working as designed and they are achieving the expected result. Typically working in close collaboration, IT, business, and compliance resources deploy mocked-up sample data along with historical production data to fully evaluate how the models are operating. Often, models will be recalibrated based upon the feedback and learnings of these exercises. Only until the models have been fully tested, tuned, and signed off by the responsible stakeholders (according to the documented policy) will the models move to production.

- **Ongoing AML model validation and optimization:** Once in production, the viability and reliability of the AML models should be assessed on an ongoing basis:

    - The cadence and frequency of these reviews and challenges are primarily informed and dictated by a risk-based approach, with higher-risk models being prioritized and evaluated more often. Yet off-cycle evaluations may be triggered by various events such as changes in financial crime risk exposure, amended regulatory requirements, new busines products and services, identified gaps or deficiencies in the models or the relevant data, or modifications in the models themselves. Reviews and challenges will be carried out by both model users and independent parties.

    - As the subject-matter experts, the AML model users should ensure that the underlying assumptions behind the model design remain relevant and the models are performing as expected. As circumstances change, the models may also need to adapt to the evolving environment. Often, performance-based metrics and industry benchmarking are used to gauge ongoing viability. Moreover, as model users learn more about the models with experience, they should look for opportunities in optimizing the models for elevated operational effectiveness and efficiency.

    - Periodically, the ongoing validity of the models should be challenged by parties not involved with the design, development, deployment, or use of the models. This independent validation should confirm the conceptual design (i.e., the model is continuing to achieve the desired objectives), system performance (i.e., the model is technically functioning as designed), data quality (i.e., the data feeds are properly mapped, accurate, and complete), and process management (i.e., model administration is effective and well-documented).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

AML MODEL ADMINISTRATION AND OVERSIGHT

Effective model management must deliver illustrative and instructive documentation. Moreover, model management must go beyond a "set it and forget it" approach, as change is a constant and too many things can go wrong during the life cycle of a model:

- **Process management administration:** Change management processes should be in place to ensure the ongoing operation and sustainability of the models and the data supporting them. Moreover, there should be sufficient oversight by the board of directors and executive management. This is often achieved through periodic reporting and briefings by senior AML compliance staff.
- **Documentation and audit trails:** FIs should construct adequate documentation of all activities, the assumptions supporting all of the models, and decision-making and approvals. For instance, documentation should inventory all of the relevant models, specify how each model is intended to work, and illustrate how each model was validated. This is vital to support ongoing administration, sustainability, optimization of the models, and evidence adherence with all internal and external obligations.

RISK AND THREAT INTELLIGENCE—HOW ARE FIS KEEPING UP WITH EMERGING RISKS?

To accumulate and maintain pertinent financial crime risk and threat intelligence, most FIs have implemented two distinct processes: a formal risk assessment process and ongoing emerging threat monitoring and detection (Figure 8).

Figure 8: Annual AML Risk Assessment vs. Threat Intelligence and Detection

Annual AML risk assessment	Threat intelligence and detection
• **Annual cycle:** FIs generally complete formal risk assessments on an annual schedule. • **Primary objective:** FIs examine inherent and resident enterprise risk exposure relating to products, services, delivery channels, customers, and geographic presence. • **Well-established methodologies:** FIs establish well-defined models with delineated risk and control elements, assessment criteria, and formulas; quantitative and qualitative data attributes are attained and assessed. • **Inform AML model design:** FIs use findings to design AML transaction monitoring models and inform ongoing optimization and tuning.	• **Ongoing and dynamic cadence:** FIs conduct threat intelligence throughout the year; these are less formality established. • **Primary objective:** FIs seek to identify real-time insights on current and emerging financial crime threats and typologies. • **Multiple intelligence sources:** Specific threat insights emanate directly from employees, internal detection systems, investigations, industry events, and information sharing with law enforcement. • **Inform AML model design:** FIs use insights to design AML transaction monitoring models and inform ongoing optimization and tuning.

Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ANNUAL AML RISK ASSESSMENT

At most financial organizations, formal risk assessments are completed on an annual basis to identify and examine all internal and external risks and threats, ascertain the highest ones, confirm the necessary controls, and inform future program enhancement opportunities. Using well-established methodologies with predefined sets of risk and control categories, assessment criteria, formulas, and assumptions, organizations examine their inherent and residual financial crime risks, taking into consideration the effectiveness of their AML programs and underlying mitigating controls. Among many other things, the annual risk assessment should inform and drive the initial model design and the full model life cycle management:

- After inventorying all of the potential financial crime risks, firms assess the potential severity and likelihood of each identified risk with the intent of pinpointing the higher risks mandating elevated controls. Through this process, the AML compliance organization will identify any new or emerging threats and typologies and will ensure that the current AML systems are designed to appropriately manage them. If not, plans are devised to enhance controls as deemed required.

- For most financial organizations, the annual risk assessment has become largely a reexamination of the prior year's exercise to account for, consider, and reflect changes in risk exposure within the last 12 months.

- The annual risk assessment process generally takes three to four months. At larger organizations, it often takes longer, and, in some cases, it may be a year-round process handled by a dedicated team. At some smaller institutions, it is handled primarily by AML compliance officers, largely because, in the words of one AML compliance officer, "He knows the bank the best."

- To assess the current risk exposure, various key data attributes (including metrics from the transaction monitoring systems) are extracted and considered. The AML compliance officer collaborates and takes input from leaders across the organization.

EMERGING FINANCIAL CRIME THREAT MONITORING AND DETECTION

At many FIs, emerging threat monitoring and detection is carried out by multiple teams or resources across the AML compliance organization throughout the year. At larger FIs, more formality is built, whereas smaller firms take more informal or ad hoc approaches. Yet they are increasingly looking to introduce more sophistication and formality to the process. More and more, AML compliance functions are assimilating resources with data analytics expertise to support these key tasks and glean better insights from the available data. Intelligence is gathered from multiple internal and external data sources:

- Internally, intelligence can be derived from front-line employee escalations of unusual or suspicious customer behavior, automated transaction monitoring alerts, referrals from fraud and information security departments, completed and ongoing investigations, and recent SAR filings. In addition, AML compliance staff are frequently plugged into all aspects of the business, such as new product and services development, to identify and assess emerging risks and their impact on current controls, systems, and processes.

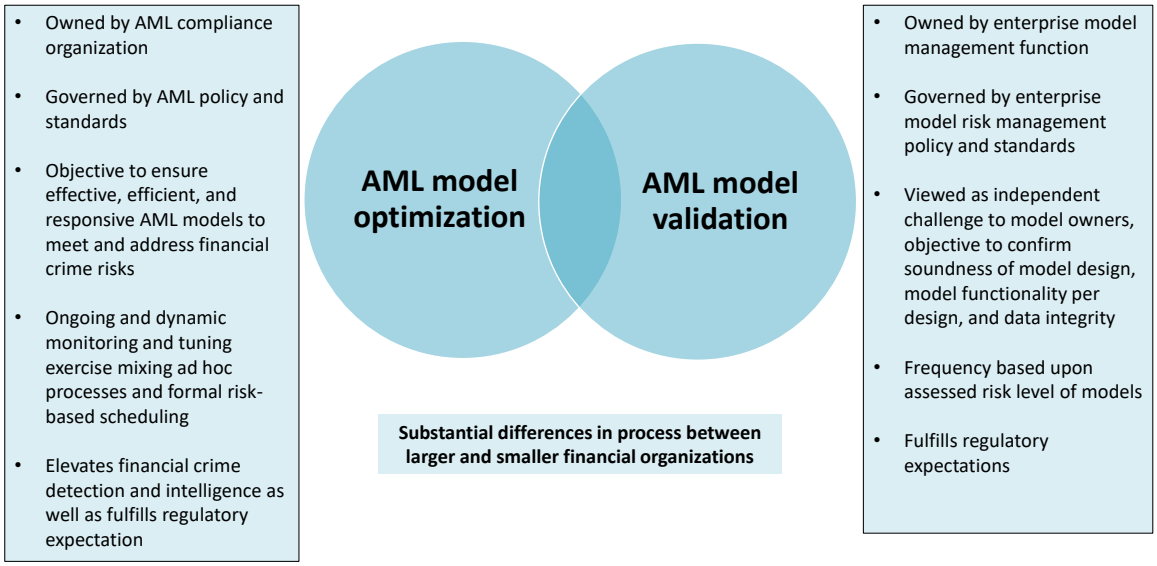
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- External sources of threat intelligence can come from law enforcement inquiries, AML regulatory guidance and advisories, industry events, publications, webinars and conferences, third-party databases of bad actors, and industry peer groups:
    - As a member of the Mid-Size Bank Coalition of America, an AML compliance officer interviewed from a regional community bank shares information on best practices and emerging threats at regularly monthly meetings with 80 other AML compliance officer officers from similar firms. He notes this group is the forum in which he gets his most valuable insights.
    - At one U.S. regional bank, the AML compliance officer interviewed talks regularly with the Federal Bureau of Investigation, the Internal Revenue Service, the Department Homeland Security, and other law enforcement agencies. This helps her stay on top of current and emerging threats impacting her organization, her customers, and the financial services industry.

AML MODEL OPTIMIZATION AND VALIDATION—STAYING AHEAD OF THE BAD GUYS AND THE REGULATORS

Typically at FIs, AML model optimization and validation comprise two disparate exercises that are performed by two separate functions (Figure 9). Generally, AML model optimization is carried out by the AML compliance organization. Conversely, AML model validation is executed by a separate independent group outside the AML compliance function, which frequently is the enterprise model risk or validation function, as it is viewed as an independent challenge to the AML model owners that are responsible for the model's design, development, and sustainability. Smaller FIs, with more limited staff, expertise, and budget, may be more likely to blend AML model validation and optimization activities together.

Figure 9: AML Model Optimization vs. AML Model Validation



Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

At one larger FI interviewed for this report, AML model optimization, validation, and general oversight are shared among four separate functions across the enterprise: AML compliance operations (a first line of defense function) as the business owners of the AML models; the enterprise risk modeling and analytics team, which is responsible for creating new models and performing ongoing tuning and testing; the AML compliance governance team (a second line of defense role); and the enterprise model risk management governance department, which performs model validations per the enterprise model risk management policy. The AML compliance officer notes that teams work closely with one another throughout the year.

AML MODEL OPTIMIZATION

Even though many AML compliance officers are generally content with their current transaction monitoring systems, they should, and many in fact do, continually assess and tune their AML transaction monitoring models. Overlooking unknown or hidden risks is a commonly voiced primary concern. AML compliance leaders recognize the increasing imperative to introduce more data-oriented and risk-based approaches in their detection tactics and become more responsive and proactive to evolving changes and trends. They often cite online payments and increasing digital customer experiences as primary illustrations. Moreover, they are on a continuous quest to reduce false-positive alert rates while uplifting risk identification, coverage, and analytics.

As such, optimization tends to be targeted data analytic exercises that scrutinize the efficiency, effectiveness, and relevance of AML transaction monitoring rules as well as the continuing quality, integrity, and reliability of the data feeding the models. The specific processes will vary across the industry:

- Relying on historical data, optimization involves a mix of art and science, and it often integrates above/below line testing, internal data quality validation and reconciliation, and performance statistical analytics:
    - One AML compliance officer interviewed notes reviewing those rules with the highest rate of false positives most often.
    - At another organization interviewed, each AML rule is reviewed periodically across various predefined metrics: alert-to-SAR conversion rate, flat SAR rate, SAR performance measure (i.e., percentage of SARs per alert scenario to percentage across total of all rules), and above-the-line/below-the-line testing.
    - Another AML compliance officer interviewed leverages law enforcement referrals and other external risk intelligence in combination with internal alert hit rates and performance statistics to refine his AML models, detect possible gaps in coverage, and identify opportunities for sharper detection.
- Larger organizations are more likely to formalize a multiyear risk-based schedule whereby rules are reviewed individually using very comprehensive data-driven methodologies. In many cases, these organization will have dedicated functions to perform these reviews.
- At one FI interviewed, all proposed modifications are vetted and overseen by a model governance committee to ensure emerging risks are managed appropriately.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- On the other hand, smaller firms tend to be less formulaic and prescribed in their approach. Some high-risk AML rules may be reviewed annually, with others reviewed on a less frequent basis.

Table C describes the contrasting AML model optimization structures in place at 14 FIs interviewed for this report.

Table C: AML Model Optimization Programs

FI location/asset size (In US$ billions)	AML model optimization program
Canada/under $10	AML transaction monitoring review and model validation are conducted annually.
Canada/under $10	AML model optimization and validation are conducted as part of an annual AML testing program.
U.S./under $10	Informal AML optimization process is led by the AML compliance officer and supported by an entire five-member AML team. Data is reviewed monthly.
U.S./under $10	Model validation and optimization are performed as a single process within the testing program of the governance and risk analytics function.
U.S./between $10 and $25	A three-member analytics team under the AML compliance officer is responsible for AML model optimization and tuning. Reviews are conducted on a two- to three-year schedule. The team is highly compensated.
U.S./between $25 and $50	Monthly alert reviews are conducted by the AML compliance function to identify opportunities to add, adjust, and remove rules. (Note: New AML transaction monitoring system was implemented in 2019, and the current model optimization program is under review.)
U.S./between $25 and $50	AML model optimization is largely an informal process led by the AML compliance officer and supplemented by a data analyst. The FI is looking to bring increased vigor into the process.
U.S./between $25 and $50	A four-member analytics team under the AML compliance officer is responsible for model validation, optimization, and data testing. Reviews are conducted periodically throughout the year.
U.S./between $25 and $50	AML model optimization is managed by a seven-member financial crimes compliance analytics and modeling team under the AML compliance officer. Periodic risk-based scheduled targeted reviews as well as ad hoc exercises are conducted. Tuning exercises frequently use historical production data.
U.S./between $25 and $50	A three-member analytics team under the AML compliance officer is responsible for model optimization and tuning and data reconciliation. Reviews are conducted on a three-year risk-based schedule.
U.S./greater than $150	A dedicated nine-member analytics team under the AML compliance officer is responsible for AML model optimization. Models and data are under constant review on a dynamic risk-based schedule. All models are reviewed at least once every two years.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

FI location/asset size (In US$ billions)	AML model optimization program
U.S./greater than $150	Dynamic optimization process is led by a dedicated data analytics lead under the AML compliance officer. Work and analysis are informed and supplemented by an enterprise AML model analytics team. A third-party service provider is brought in every three to four years to augment internal processes.
U.S./greater than $150	An ongoing, dynamic process is overseen by AML operations as model owners, an enterprise risk modeling and analytics team, and a financial crimes governance team.
U.S./greater than $150	AML model management and optimization are overseen by an eight-member model management and business intelligence team under the AML compliance officer. Ongoing and dynamic reviews are conducted. The team is paid at 30% premium to similar roles in other departments.

Source: Aite Group interviews of 14 financial crime professionals, August and September 2020

Moreover, AML compliance leaders recognize the need to integrate greater analytics into detection as rules-based monitoring platforms are limited in how much data can be effectively ingested and synthesized. Working to construct more cohesive customer digital identity footprints, one AML compliance officer interviewed for this report is struggling with the limitations of his current transaction monitoring system. As these solutions integrate next-generation technology, optimization protocols become even more critical. For AML compliance teams, successful optimization faces numerous obstacles:

- Often, FIs struggle with constructing sufficient internal data samples and allocating sufficient resource time. Many organizations are exploring greater automation and greater analytics to support optimization and tuning. Automation can streamline tedious and labor-intensive activities such as data quality checks and documentation preparation, reduce human errors, increase productivity, and drive greater consistency. Advanced analytic tools can streamline tasks, accelerate analysis, and sharpen decision-making. However, it is a common belief that technology will never be able to fully replace human judgment.
- In this highly competitive environment, finding and keeping sufficiently skilled data analytical resources with the relevant and necessary knowledge of AML regulations, financial crime risks, and the business and operational composition of the financial organization are other common challenges. Such resources are not in abundant supply. And given their expertise and blend of critical skills, data analytic resources are very well compensated. One FI interviewed compensates these resources at a 30% premium to similar roles in other departments.
- Using a hosted transaction monitoring platform, one AML compliance officer interviewed notes that his platform failed to have a sufficient sandbox environment. As a result, his team lacked full control over optimization and tuning activities. The AML compliance officer desired a more readily accessible and dynamic testing environment with more real-time capabilities and outputs.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- Maintaining ethics and avoiding any unintended consequences are constant concerns. Doing the right thing is an essential consideration in everything that AML compliance officers do. This sense of purpose bleeds into how they design and build their transaction monitoring systems. They want their AML models to detect the illicit conduct that lies beneath the red flags without introducing any unwanted biases. For some FIs, AML innovation hubs are intended to guard against potential and unintended unfairness creeping into these models.

AML MODEL VALIDATION

Many FIs have independent model validation functions that are responsible for overseeing all enterprise models. AML model validation is largely conducted on a dynamic schedule, with the cadence and frequency dictated by the assessed risk level of the model. At many FIs, AML models are seen as higher risk that mandates more frequent reviews than other enterprise models. Some FIs complete these validation exercises annually, whereas others do them only every two to three years. On a yearly basis, one smaller bank alternates between deep-dive assessments and lighter-touch reviews. Many interviewees point to that fact that these independent validation protocols are in place, in large part, to defend transaction monitoring systems to regulators, examiners, and internal auditors. Table D lists the frequencies by which the FIs interviewed for this report conduct their independent AML model validation exercises.

Table D: AML Model Validation Cycles

FI location/asset size (In US$ billions)	Frequency of AML model validation
Canada/under $10	Part of AML internal audit exercise
Canada/under $10	Part of AML internal audit exercise
U.S./under $10	Biannually
U.S./under $10	Periodically (performed by third-party service provider)
U.S./between $10 and $25	Biannually
U.S./between $25 and $50	Biannually
U.S./between $25 and $50	Every 12 to 18 months (conducted by external service provider)
U.S./between $25 and $50	Biannually
U.S./between $25 and $50	Multiyear risk-based cadence (overall, three years with high-risk models reviewed annually)
U.S./between $25 and $50	Multiyear risk-based cadence (overall, three years with high-risk models reviewed annually)
U.S./greater than $150	Annually
U.S./greater than $150	Multiyear risk-based cadence (overall, five years with high-risk models reviewed annually)

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

FI location/asset size (In US$ billions)	Frequency of AML model validation
U.S./greater than $150	Ongoing
U.S./greater than $150	Multiyear risk-based cadence (overall, four years with high-risk models reviewed annually)

Source: Aite Group interviews of 14 financial crime professionals, August and September 2020

THIRD PARTIES—CAN THEY HELP?

Third-party consultants bring a deep understanding of model risk management principles and extensive expertise in qualitative and quantitative approaches to model validation and optimization. However, many FIs do not use them or have had many less-than-positive experiences with them. Consultants can be expensive. Moreover, they often lack sufficient knowledge of the FI, its business and operations, and its financial crime risks; hence, it is difficult for them to make critical observations and insightful recommendations. Often, a lot of time is spent just on educating the third party:

- At one top 20 U.S. FI interviewed for this report, the AML compliance officer brings in an external party every three to four years to supplement internal model validation and optimization.
- One small regional bank interviewed has minimal in-house model validation expertise, and a third-party consultant is engaged to conduct all model validation activities. This is done every two years, as the bank does not have sufficient budget for an annual exercise.
- For one AML compliance officer interviewed who used consultants in the past, those third-party service providers failed to add much value. Often, recommendations were conservative in nature, and thresholds did not change substantially.
- Conversely, another midsize FI interviewed that outsources most AML validation activities to a third-party service provider had very positive experiences. The provider had extensive AML knowledge and significant experience with the organization's specific vendor-built transaction monitoring system.

Wanting to do everything possible to protect their organizations and their customers, AML compliance officers crave as much intelligence as possible to support AML model creation, validation, and optimization. The risk landscape is evolving all the time. To that end, third-party constructed financial crime typology libraries and simulated data sets are options that appeal to many AML compliance officers. Though none of the AML compliance officers interviewed are using these types of aids currently, they would investigate their viability in sharpening risk and threat identification, building better models, introducing greater model effectiveness, and elevating operational efficiency. Moreover, AML compliance officers envision typology libraries and simulated data sets as vehicles to confirm the assumptions underlying their current models and providing additional evidence and support for internal audit and external examinations. However, the benefits are offset by concerns over ongoing data integrity, reliability, and relevance as well as the ease of use and integration with existing systems.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CONCLUSION

Building and sustaining effective transaction monitoring programs challenges even the most skilled and seasoned AML compliance practitioners. AML model risk management supports continual operational effectiveness and integrity, calibration with a changing risk and business landscape, and increased operational efficiency. Moreover, financial organizations can construct and maintain transaction monitoring programs that meet regulatory expectations, detect financial crime, and deliver high-quality and actionable intelligence to law enforcement.

Financial organizations:

- **Start with a strong AML model governance structure**. Clearly define mandates, roles, and responsibilities. Don't forget the true purpose behind the AML models; model risk management must go beyond merely checking the regulatory box.
- **Leverage your AML risk assessment.** Pinpoint your key threats. Engage industry peers and all sources of intelligence. Bring business leaders as well as regulators into the process. Update and adapt your AML models as the landscape evolves.
- **Manage model risk resources appropriately.** Train them on new data analytic skills and competencies. Collaborate with your vendor partners; they have substantial knowledge of AML models and industry best practices. Bring in consultants when needed; they can bring expertise, objectivity, and independence. Embed technology and automation for effectiveness and operational efficiency.
- **Document, document, and document again.** Inventory all AML models, record underlying logic, assumptions, and decisions, and evidence testing and monitoring. Not only will these activities evidence transparency and explainability to auditors and examiners, but they will also facilitate future model optimization and validation.
- **Don't forget about the data.** Identify all sources of valuable data. Rigorously assess quality and relevance.

Third-party vendors, service providers, and consultants:

- **Build user-friendly AML detection rules and models.** AML compliance practitioners want AML transaction monitoring systems that are easy to use, configure, and explain. Platforms should facilitate data ingestion as well as data extraction. Sandbox environments, dynamic dashboards, and reporting are musts.
- **Engage AML compliance leaders and global regulators**. Learn from them. Understand their challenges, needs, and priorities. Educate them on next-generation technology. Build close-knit customer advisory groups and collaborate frequently.
- **Build enhanced intelligence and data sets.** You have a view across the industry on current and emerging financial crime threats, and your insights can be priceless.
- **Expedite AML model risk management through innovation and automation.** Increased technology can process more data, empower accelerated data-driven insights, and optimize labor-intensive activities.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RELATED AITE GROUP RESEARCH

Key Trends Driving AML Compliance Transformation in 2021 and Beyond, December 2020.

Aite Group's Third Annual Financial Crime Forum: Collaboration Amid Crisis, October 2020.

AI-Enabled Anti-Money Laundering: From Theory to Reality, July 2020.

Global AML Vendors: Embracing Innovation, February 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

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

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com