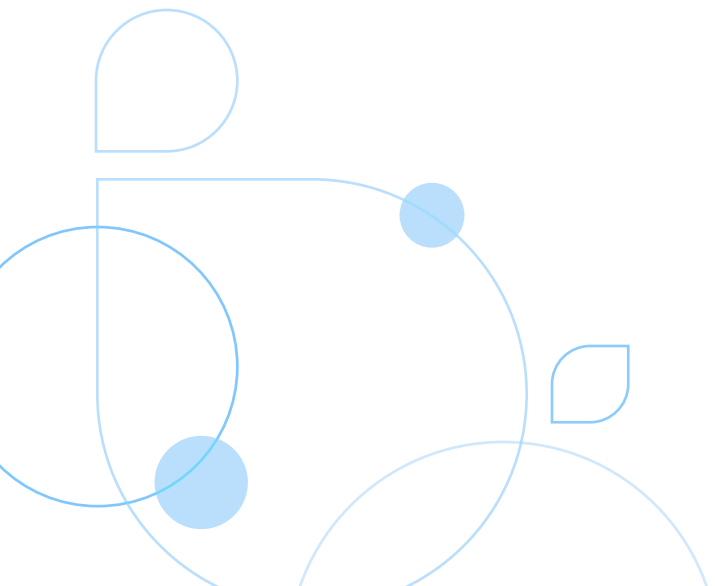
WHITE PAPER

Building a foundation for innovation: Five steps to keep your AML program efficient and effective

Why a return to fundamentals is essential to AML innovation

Contents



> Many financial institutions (FIs) are trying to solve issues with their money laundering detection and transaction monitoring rules by leveraging advanced technologies such as AI. However, despite the promise of these technologies, money laundering has proven to be a persistent problem. A more comprehensive and effective solution is for financial institutions to instead reevaluate their core AML strategy.

When it comes to detecting and preventing money laundering, FIs face a number of operational issues. First, significant volumes of non-productive alerts — which can be the result of poor tuning and calibration efforts, inadequate coverage models and/or lack of dynamic segmentation — can burden the transaction monitoring system. Next, weak integration of data sources, and the manual steps and processes typically associated with traditional AML systems, can hamper a program's effectiveness. A shortage of staff with relevant knowledge and expertise in AML compliance can also hamper efficiency.

With the intent to curb financial crimes and ensure transparency in all types of financial transactions, entities such as the European Union, the United Nations, and the Financial Action Task Force (FATF) have increased regulatory pressure and developed more stringent guidelines. As a result, financial institutions are spending **$100 billion annually** to maintain compliance, with smaller firms disproportionally impacted by the cost. However, many others are still falling short, even with the threat of serious consequences. In some cases, banks have been ordered to pay fines as high as $3 billion after failing to comply with regulations.

$100 billion spent annually on compliance by financial institutions, with smaller firms disproportionately impacted by the cost.

Largest AML bank fines in 2024

Source: *The Biggest AML Fines: Annual Report,* Skillcast

This has put FIs in a precarious situation. At best, they must spend more to remain compliant while still dealing with persistent rates of money laundering. At worst, they must not only contend with the increasing costs of preventing financial crimes, but also face the threat of severe penalties if they fall short. It should be little wonder, then, why the adoption of advanced techniques, such as AI and machine learning (ML), are now often considered the only way to improve the efficiency and effectiveness of transaction monitoring and AML programs. But amid the hype surrounding these technologies, have we overlooked the basics?

In preparing for the future, FIs need to first review the core components that make up a competent and comprehensive AML strategy. By returning to the fundamentals, FIs will not only bolster their efforts at countering money laundering today, but will also build a strong AML and compliance foundation that gives them the necessary footing for pursuing innovative technologies and methodologies tomorrow.

Step 1: Documentation of policies and procedures

> The most powerful and advanced technology in the world will hardly matter if it is not backed by effective policies and procedures. Banks that know how to establish good hygiene activities and rigorous change management processes will be better prepared to adopt more advanced solutions later on.

Remaining compliant with money laundering and terrorist financing regulations relies on effective processes. This includes anything from an institution's formal commitment to preventing money laundering to the specific policies and procedures behind its AML program. It also encompasses customer due diligence (CDD) and know-your-customer (KYC) procedures, reporting and record keeping (including the timely filing of SARs), internal controls and audits, data and asset management and employee training. In other words, these processes make up the backbone of an effective strategy to combat money laundering.

But, as is evident from the persistence of undetected financial crime, the policies and procedures in place at many banks are falling short. These weak processes can take many forms. In some cases, they may be the product of poor risk assessments. If an institution fails to account for the many ways money laundering can occur, its strategies for management and mitigation will prove equally inadequate. In other cases, they may be the result of a failure to update internal controls or risk profiles in response to regulatory changes. Inadequate risk rating, especially in the face of rapid growth, can also result in institutional vulnerability.

Financial institutions should take a more prescriptive approach by implementing workflow management practices that ensure effective risk analysis, consistent compliance procedures and comprehensive documentation.

While it may be tempting to try to address the shortcomings of individual procedures and identify their root causes, this can be a laborious process — especially at large institutions. Instead, FIs should take a more prescriptive approach by implementing workflow management practices that ensure effective risk analysis, consistent compliance procedures and comprehensive documentation. For example, by creating predefined workflows to guide documentation of procedures during an annual review cycle, financial institutions can codify step-by-step processes. This can help ensure that all required steps are both completed and documented, such as regulatory gap analysis, AML policy updates, internal review and subsequent employee training.

Ideally, these workflows can be automated. The workflow management capabilities of **SAS Anti-Money Laundering**, for instance, make it possible to seamlessly integrate best practices from a bank's AML procedures. The CDD workflows will automatically prompt analysts with dynamic checklists to ensure consistent KYC information, while its drag-and-drop interface makes it easy to build out and configure custom workflows to address specific needs. The result not only helps train and upskill employees on efficient practices and regulatory requirements but also provides a firm record of documentation banks can use when integrating advanced technologies like AI and large language models.

Step 2: Data governance

> Financial institutions can no longer let traditional silos persist between fraud and anti-money laundering. The interconnected nature of financial crime demands centralized and converged data models that give every group access to high-quality information.

Without access to quality data, FIs will not be able to adequately assess and respond to illicit activity. This is particularly true as financial crimes continue to become more complex. While criminals have long concealed fraudulently obtained funds through money laundering, actors involved in money laundering schemes may also rely on fraudulent methods, such as cybercrime and identity theft, to gain access to financial systems or cover their tracks. Yet despite the sophistication of these methods, many banks have not yet integrated their data across fraud and compliance, leading to consequences down the line.

Many banks have not yet integrated their data across fraud and compliance, preventing FIs from achieving a holistic view of their customer.

For example, traditional CDD methods often use narrow streams of data to build risk profiles, a strategy that will not be able to accommodate sudden changes or unexpected scenarios. What happens if a long-time, low-risk customer begins transacting outside of their typical geography? What if their spouse or partner was a victim of fraud or identity theft, possibly also exposing the customer's information? Without a holistic view of a customer's risk factors, it will be challenging to conduct thorough and effective due diligence.

All this makes it necessary to rely on data models that are not limited by traditional silos. Instead, financial institutions should fundamentally reassess how they access and share data. They need to ensure they have strong data governance capabilities that allow them to access the information they need to conduct monitoring, analysis, reporting and investigations with precision. Furthermore, they should make it possible to trace the lineage of their data so that they can ensure the information they are using is accurate, relevant and up to date.

Built on top of the unified **SAS® Viya®** platform, solutions like SAS Anti-Money Laundering make all this possible by providing a centralized repository of data, giving users a converged, end-to-end view of customers, possible threats and more. This makes it possible to build more powerful, fit-for-purpose data models that can capture the complexities of today's financial crimes. It also makes it easy to continuously pull data from multiple sources, allowing institutions to create more accurate and comprehensive risk profiles of customers. Ultimately, this helps ensure they are taking in consistently high-quality data that yields high-quality results.

Step 3: Coverage analysis

> Traditional rules-based AML frameworks can mire financial institutions in nonproductive alerts, making it difficult to investigate truly suspicious activity. To catch up with the complexities of the modern threat landscape, banks need to reevaluate how they review both known and unknown risks.

Financial institutions have long relied on an approach to evaluating and identifying risks that is rules-based and deterministic. If a transaction exceeds a certain amount, for example, then it will trigger a review. But the reactive nature of this framework often makes the work of weeding out actual crime from normal behavior both costly and inefficient. Although advanced technology, such as neural networks and machine learning algorithms, offers a possible solution, it can also obscure how risks were evaluated and identified. While promising, this black box approach poses significant regulatory challenges.

Instead, financial institutions should rethink how they conduct coverage analysis altogether. One way to do this is by adopting a more proactive framework that defines rules based on risk categories. While the specifics will depend on the needs of each institution and their customers, this approach should generally use predefined criteria based on known patterns of risk and money laundering typologies. Drawing from multiple sources of data, financial organizations can use this method to move away from broad-based alerts triggered by thresholds and shift toward rules based on both historical patterns and established guidelines.

Once enough data has been gathered and risk-based triggers identified, FIs can begin building model-based scenarios using statistical methods and machine learning algorithms while still meeting the validation requirements of their local regulations. Doing so will make it easier for financial institutions to leverage their historical data to identify subtle patterns and anomalies in transactions, as well as make adjustments to risk thresholds based on emerging trends.

Banks and other FIs should not stop at assessing known risks – it's also important they evaluate areas that fall outside of their normal monitoring and review processes.

But banks and other FIs should not stop at assessing known risks – it's also important they evaluate areas that fall outside of their normal monitoring and review processes. These unknown risks can include specific gaps as well as general areas of inadequate coverage. This can be done through strategies such as white-space analysis, which will map out all potential risk areas so that FIs can easily see what their current analysis covers. Other strategies, such as targeted ad-hoc reviews and anomaly detection, are useful for diving deeper into revealed gaps and uncovering risks that may otherwise go undetected.

In addition to providing holistic, centralized data governance capabilities that help enable risk-based assessments, SAS also offers capabilities that make it easier to evaluate areas that may fall outside of automated monitoring. For instance, **SAS Visual Analytics** can be used to build coverage dashboards and conduct white-space analysis, ad-hoc reviews and anomaly detections to further identify gaps and reveal under-monitored areas. The end result of this approach will be a fully circular view that makes it more likely to identify patterns, transform unknown risks into known entities, and integrate more effective scenarios into the core coverage model.

Step 4: Iterative approach to compliance

> Just because an AML system is comprehensive and compliant today does not mean it will be tomorrow. The rapid pace of change across the regulatory landscape requires financial institutions to continuously reassess the reliability and robustness of their approach.

As quickly as new technology emerges, money launderers and other bad actors will create novel techniques to circumvent existing defense systems and evade detection. Although the rush of new regulations that follow these novel techniques is meant to help counteract this trend, the constant evolution of regulations poses yet another challenge for FIs to overcome. In response, the only effective way to adapt to this is to adopt an iterative approach to compliance with regular assessment of your AML program.

The only effective way to adapt to the constant evolution of regulations is to adopt an iterative approach to compliance with regular assessment of your AML program.

Specifically, this process should involve repeated and consistent optimization and tuning of all methods used to detect and assess risk. One of the most effective ways of doing this is through a Model Risk Management (MRM) framework. Serving as a way to gain comprehensive oversight over the model-based components of an AML framework, effective MRM should include capabilities such as governance tools, model validation and detailed documentation of data sources, model assumptions and methodologies. This will help ensure high data integrity and quality, as well as allow for continuous improvement. With a centralized model inventory, financial institutions can gain complete control over the workflow management of their models, regardless of type or technology.

An effective, iterative approach to compliance should involve more than just tools. FIs should also conduct realistic assessments of their systems. This should include a close look at data quality and an honest assessment of its limitations, scenario verification and validation, and an evaluation of employee knowledge, experience and bandwidth. As gaps are identified, FIs should remediate their AML program and repeat the steps of the AML program evaluation process until the theoretical “ideal AML program” closely matches the reality of the actual implementation. It is only when this is the case that innovative and advanced technology can be successful in enhancing AML/CFT programs.

Step 5: Advance and modernize

> The potential benefits of advanced technology like AI and machine learning are exciting. But while there is little doubt their capabilities will help redefine AML/CFT, the only way for organizations to take full advantage of these benefits is by building them on a strong AML foundation.

The past decade has seen incredible developments across a broad swath of advanced technology. Automation and machine learning capabilities have already become integrated into many industries, while AI (in particular, generative AI and large language models) has caught the attention of the wider public. It should come as no surprise then that many financial institutions are equally excited to begin applying these advancements to their own programs, especially considering that doing so often seems like one of the most effective ways to keep pace with evolving AML/CFT methods and regulations.

Indeed, the opportunities provided by the continued growth of technology like cloud-native infrastructures, unified analytics environments, automated alert management, machine learning and AI are enormous. Solutions like SAS Anti-Money Laundering are integrated with machine learning and AI capabilities out of the box, making it possible to run advanced analytical tasks and automations. Other solutions, like **SAS Financial Crimes Analytics**, build on this by giving organizations access to a low-code/no-code sandbox for experimenting with different advanced capabilities. This includes predictive models based on advanced machine learning techniques, dynamic customer segmentation and more.

Solutions like SAS Anti-Money Laundering are integrated with machine learning and AI capabilities out of the box, making it possible to run advanced analytical tasks and automations.

In many ways, the financial industry stands on the cusp of a new generation of innovation. Without a doubt, this new technology will make AML processes more effective and more efficient and result in more responsive models. It's critical for financial institutions of all types to take a closer look at their existing AML/CFT programs. That's because, as promising as much of this new technology is, the only way to truly benefit from it is to apply these methodologies on the back of an already strong AML foundation. First, you crawl, then, you walk; only then can you run.

Ready to learn more?
Find out how to transform your AML/CFT processes with SAS Anti-Money Laundering.