ankura

Factors to Be Considered by Financial Organizations for an Effective Transactional Monitoring System

Ankura Consulting India Private Limited
Office No. 20-118, 20th Floor, Commerz II,
Off Western Express Highway,
Oberoi Garden City
Goregaon (E), Mumbai – 400 063

Content

Ankura Consulting India Private Limited
Office No. 20-118, 20th Floor, Commerz II,
Off Western Express Highway,
Oberoi Garden City
Goregaon (E), Mumbai – 400 063

Factors to Be Considered by Financial Organizations for an Effective Transactional Monitoring System

The rising incidence of financial crime continues to haunt financial institutions globally. As per a recent industry report, more SARs (suspicious activity reports) were filed by ~80% of the firms in 2021.[1] COVID-19 pandemic and its allied consequences like the supply chain shocks, remote working, internet shopping rise, etc. have only added to the woes of the financial services industry which was already battling a slew of factors including cybercrime, cryptocurrencies, insider trading, tax crime, customer fraud, misappropriation of assets, to name a few. Economic crime is reported to have peaked in 2020 at $42Bn[2]. Financial crimes can be covered under broadly three categories- Anti-Money Laundering (AML) violation, corruption/fraud and sanctions violation. Such crimes have far-reaching consequences not only financially but also from the company's reputation perspective. €6.4Bn worth of fines were given out by the US enforcement authorities, making them the highest globally, followed by the UK with €0.7Bn[3].

In their quest to fight and prevent fraud, financial institutions have embraced new technologies that can enable building strong and resilient organizations for the future. Adoption of the latest technologies aims at enabling organizations to offer excellent customer service, ensure compliance, and guarantee financial success. It is, hence, not surprising to see Anti-money laundering (AML) become one of the critical priorities for financial institutions.

AML is a set of regulations, laws, and procedures that are aimed to detect and prevent criminals from disguising illegal funds as legitimate income.

Every financial institution needs to adhere to local and international regulations in order to ensure compliance. Local banking regulators define norms and guidelines, conduct audits, and also look at international statutes and requirements. The purpose of these regulations is to protect the integrity and stability of the financial system and to detect and report suspicious activity, including underlying money laundering and terrorist financing activities. Thus, regulators have obligated financial service organizations to follow these regulations, making it critical for organizations to have an effective compliance program in place that includes advanced technology monitoring systems for continuous analysis of financial transactions and a dedicated

[1] https://complyadvantage.com/wp-content/uploads/2022/01/ComplyAdvantage-State-of-Financial-Crime-2022.pdf
[2] https://worldline.com/en/home/knowledgehub/blog/2021/march/mitigating-financial-crime-in-a-covid-19-world.html
[3] https://www.amlintelligence.com/2022/01/aml-intelligence-launches-2021-financial-crime-fines-review/

team responsible for internal controls, AML compliance testing, and compliance management. Most financial institutions' AML compliance program depends on the three pillars below.

1) Process

'Process' in the AML framework defines the steps or actions that bring together people and technology to prevent fraudulent activity and be compliant with the AML regulation. For setting up the AML compliance process, the financial institution should have a set of policies and procedures that must be followed to prevent money laundering activity.

Below are a few considerations financial institutions should bear in mind while defining the process in the AML compliance program:

- Having policies and procedures that aim to define money laundering within the financial institution.
- Adherence to and compliance with local and international regulations. Also, create awareness of these regulations within the organizations.
- Implementing AML checks in the customer onboarding process.
- Establishing procedures and scenarios for sanction screening, and AML scenarios.
- Creating investigation workflows and channels for suspicious activity reporting.
- Reporting and communication procedures for any AML activity.
- Defining Know Your Customer (KYC) and Know Your Business (KYB) processes and procedures that need to be carried out to identify and verify the identity of their customers in compliance with prevailing regulations.

2) People

'People' refers to the human resources accessible to the financial institution. People are the ones who carry out the tasks outlined in the AML framework, often with the assistance of technology. It is very important to onboard the right people when creating the AML team- with the necessary abilities, experience, and attitude to do the task. The AML team also needs to be clear on the AML role definitions, so that everyone understands their obligations. This will aid decision-making, communication, technology selection, process implementation, and personnel hiring.

The financial institution must take into account the following points while keeping 'People' in mind for the AML program to operate effectively.

- A dedicated team should be assigned which needs to undertake independent compliance supervision daily and should not be directly or indirectly involved in daily business operation activities.
- Conduct AML training and awareness programs for the team on a regular basis, making them aware of the latest AML rules and regulations, and educating them on best industry practices.
- Define roles and responsibilities to identify and review suspicious account holders with their transactions and report information that illustrates the organization's overall performance in terms of risk mitigation.

3) Technology

'Technology' provides the tools that the AML teams use to implement the process. By use of technology tools, the financial institution can improve its ability to mitigate financial crime risk and remain compliant. AML technology is used to analyze customer data, detect high-risk transactions/patterns, and simplify AML activities of the financial institution.

An effective AML compliance program should be multi-pronged and lean heavily on technology. It is very critical for the financial institution to choose the right "Transactions Monitoring solution" that will minimize false positives with near real-time checks on millions of transactions.

"Transactions Monitoring" involves a sophisticated advanced technology system to process terabytes of financial data in a few seconds to identify potential AML non-compliance gaps.

Why Transaction Monitoring Is Key to Effective AML

Transaction Monitoring (TM) is "the process of monitoring transactions after their execution in order to identify individual unusual transactions, including single transactions as well as transaction flows"[4].

It also involves banks and financial institutions constantly checking on their customers for potentially risky transactions. End-users' backgrounds and financial profiles are considered to accurately assess the risk level and predict future transactions. In addition, suspicious activity reports (SARs) based on the user's actions are generated and sent to regulatory authorities for additional investigation.

[4] [4] 1. Wolfsberg Statement: Monitoring Screening and Searching

For transaction monitoring, financial institutions use a blend of manual and automated systems, depending on the volume and complexity of the transactions they need to process. Organizations configure and deploy transaction monitoring systems to automatically spot suspicious transactions (*i.e - Unusual transactions or account activity, transactions over a certain value, domestic or international transfers over a certain value, etc.*), automate their data analysis in real-time, manage investigations, leverage external data source, and submit regulatory filings. This system has customized risk-based AML rules and other screening modules to process the transactions in real-time and generate an alert whenever a situation violates the rules or violates the customer profile during a transaction. Once the alert is generated, the suspicious transaction is automatically notified to the dedicated compliance team for closer scrutiny and for generating SAR reports for the regulators. The volume of transaction data that gets generated every second, along with the need to analyze it for various AML risks, makes this an unrealistic activity to process manually. However, with TMS, organizations can effectively implement a risk-based approach to the AML compliance program that balances their resources and compliance obligations. Overall, TMS helps in increasing accuracy and efficiency and enhancing compliance performance by collecting and analyzing a significant amount of data which can be resource-intensive and time-consuming if the task is performed manually.

For TMS to work efficiently, the application must be deployed, configured, and integrated into the existing infrastructure to provide positive alerts. Implementation of TMS may seem like implementing any other system from an implementation perspective; however various factors need to be considered by the organization including identifying risk-based monitoring scenarios, setting up scenarios thresholds, deploying compatible hardware, integrating the system with the current technology architecture, etc. The repercussions of any lapses in following the aforementioned considerations could include an increased number of false positives, increased operational costs, missed reporting deadlines, and most importantly, undetected suspicious activities that could later lead to regulatory action on the organization.

Technologies Important for Transactions Monitoring System

A typical manual approach would be a daunting task in the rapidly evolving AML regulatory space amidst changing customer behaviors leading to an exponential volume of transactions. Thus, financial institutions need to be nimble at embracing

these changes in order to stay relevant and compliant. To address rapid adaptability and the capacity to prioritize alerts, Artificial Intelligence (AI) and its subset - Machine Learning (ML) technologies need to be part of the Transactions Monitoring system, which can potentially help in improved identification of risks and response to, communication of, and monitoring of suspicious activity.

Using AI and ML technology, a TMS based on historical data can learn and identify complex patterns when provided with new data. While the rise in the number of alerts requires a consequent increase in the number of personnel to triage and process them, implementing AI and ML at the alert triage stage can suppress alerts, save them for further review, or even close automatically tickets at some point in the future. Also, the team can analyze a wide range of data to enable better decisions, provide more insights for the review team, prioritize high-risk transactions, identify patterns, enable more false positives and false negatives to be filtered out, and adapt quickly to customer behavior.

Key Considerations for Selecting & Implementing an Effective Transaction Monitoring Solution

- **Identifying the risk and choosing the right TMS for your organization. –** Selecting the right TMS for your organization is the first step. Several technical and business factors should be taken into account before finalizing a TMS. If not considered carefully, it can lead to financial implications and/or the need to explore alternatives or conduct repairs. The organization should be able to gather the user requirement, map the risk for each business process and finally identify the features that should be available in the TMS.

- **Selecting the vendor –** Based on the requirement gathered, selection of the right vendor is the next step, and the vendor should be assessed based on the following factors

    - Data volume - Ability to manage large data volume from the existing infrastructure.
    - Technology infrastructure – Given the substantial operational costs involved in implementing and maintaining the TMS, ensuring that the chosen solution can coexist seamlessly within the existing technology infrastructure.
    - Ability to cope with different scenarios - The vendor's solution should be able to provide the correct coverage of various red flag detection scenarios to cover the organization's risk and ensure all transactions and data points are adequately monitored. *"One size fits all doesn't apply"* as there are different

data points. The vendor system must provide the flexibility to customize the algorithms and threshold of the risk scenarios. As a general rule, the more complex the activities of an institution, the more likely customization will be required. Also, it is crucial to note that not every vendor-developed scenario will need to be implemented in TMS. This is because each institution has a distinct level of risk exposure, and each scenario needs to be chosen individually.

- Asses after-sales support - It is an integral part of the selection and key to determining the support that the service provider will be able to provide in cases of downtime, troubleshooting, or upgrades.

- **Identifying the Data Source and integrating it into TMS –** In order to provide quality output and minimized false outcomes, the data ingested in the TMS module must include in-scope transactions and all the attributes needed for monitoring. The implementer should have in-depth knowledge of the business' functional and technical aspects to identify and map the scenarios with the right data source and fields. It is often noticed that data architecture and data mapping problems of source systems to TMS are frequently discovered during the AML implementation phase. These challenges must be resolved as part of the project to guarantee appropriate and correct data flows into the TMS. Also, the following points need to be considered for source data.
  - Availability of the data that will be considered as part of the scope and how often data should be refreshed.
  - The quality of the data needs to be validated and verified before considering it for the TMS. Inaccurate information or data elements can lead to skewed analysis and inaccurate results**.**
  - The data volume should be supported either by existing hardware infrastructure or by additional hardware resources.

- **Identification of the scenario and development** – This process involves identifying, selecting, and mapping the scenarios against the risk identified. Further, translating the functional specification of each scenario into the technical code that will be deployed and configured in the TMS. It is the responsibility of the service provider to perform the design and test of the technical code and customize it as per the business requirement. Nevertheless, the organization should also conduct independent assessments of the output generated once the scenarios have been selected and configured. If a scenario is missed or wrongly configured in the process, it may result in undetected suspicious activity.

- **Threshold setting and ongoing tuning Process-** Setting threshold values for each of the selected scenarios should be set at optimum levels that alert the respective team about suspicious activity. However, the team must also be cautious about

setting the threshold values too low, which would result in an excessive number of false positive alerts and create operational barriers**.** In addition, the organization and project teams should develop a method for setting thresholds and tuning scenario thresholds that can be easily validated by the audit team.

- **Performing analytics** – To arrive at the threshold value with a rationale, various data analytics need to be performed on the sample period to determine the number and type of customer segments that need to be considered. Further, statistical analytics is to be performed to determine the threshold value for each customer segment and risk level.
- **Threshold tuning** – The Implementation team should perform a dry run of the alert generation cycle to produce alerts that can be validated in the test environment. Additionally, the organization's investigation team should provide insights on the quality of the alerts that are generated and recommendations for the expected output. This step, thus, allows fine-tuning thresholds before deploying them in the production environment.
- **On-going reduction of false positives** – For reducing the false positive rates, the implementation team needs to carefully evaluate the data collection process and properly harmonize the data received. Further, evaluate the performance of the scenarios on the historical data and fine-tune the threshold to get optimized alerts. In addition, an organization should retrieve relevant information about suspicious activity clusters by analyzing previously filed SAR. Using this information, threshold values can then be tuned based on the patterns of activity identified in SAR.

- **Case Management –** Considering the volume of alerts that are generated, the case management module should have a technology-driven compliance workflow incorporated in order to monitor, detect, investigate, and report alerts identified for suspicious activity. Case management should have:
  - Review features – it should include features to track and manage alerts and notifications, customize alert levels, drill down and smart workflow to configure responses, and a 360-degree view of the customer, related events, or parties for flagged transactions.
  - Workflows – It should contain various workflows such as Know Your Customer (KYC) rules for verifying customers and monitoring suspicious transactions, and compliance reporting through the filing of suspicious activity reports (SARs) to regulators.
  - Alerts notifications – Create custom alerts to notify key stakeholders when a KPI moves above or below a specified threshold, when a goal is reached, or when a new issue arises.

- **Dashboard and Reporting –** For Financial institutions to make informed decisions, data need to be presented in an easy-to-read, standardized format, summarized using a dashboard and other reporting formats which can enable the executives and compliance team to better visualize the organization's current risk position and access the information easily to saves time and effort.
    - Dashboard features – Should have a platform having all information in a summarized format to provide a bird's eye view, collectively displaying different attributes that may be of concern. Data is represented using various types of drill-down charts and graphs which can make it easier to find insights at various levels of detail in the data. Also, it enables one to focus on crucial tasks and improve productivity.
    - Custom Reports – It allows the organization to have report templates based on any combination of criteria, with many formatting options that present data in an easy-to-interpret, usually visual, summarized tables. Having reporting module allows the user to quickly generate and distribute reports within the organization. Generating a report using a custom reporting module requires less time and effort in comparison to generating the same report manually.

- **Project Management Office (PMO) & Implementation Project Planning:** For all the above-mentioned activities to execute in a timely fashion, it is very important to have a project plan in place considering multiple factors such as people, resource constraints, infrastructure, and efforts required to implement the TMS with the scenarios. Also depending upon the requirement, there may be a need for creating a multiphase deployment plan, which requires putting multiple deployments into production phase by phase. A dedicated PMO resource should be assigned who will act as a bridge between the organization's business team and the service provider. Further, the PMO resource will keep track of the multiple activities to ensure the completion of the project within the agreed timelines.

Role of PMO in Implementation

The maturity of PMO is measured by its ability to develop efficiency and become proactive rather than reactive. For the implementation of AML applications, a PMO is involved in various stages to ensure smooth and effective implementation.

- **Gathering organization requirements:** - PMO works with the organization team to analyze the current situation by checking the processes and tools that are being used and talking to the respective business teams. Based on the information gathered, PMO is able to identify the AML solution requirement as per the business need, define the project on a broad level, and identify and take approval from the respective stakeholders.
- **Request for proposal (RFP**) – Once a requirement is approved, the process of bids from the implementation partners is done through an RFP document. PMO supports the organization in preparing the RFP and ensures the requirement of the AML solutions is mentioned in the document. Also, PMO works with the organization to plan the project budget, milestones, project deadlines, and technical and functional requirements that need to be mentioned in the RFP documents.
- **Demo and selecting the implementation partner** – Post submission of the RFP document, PMO evaluates the details submitted by the implementation partner against the organization's requirement and shortlists the implementation partners for the solution demo. PMO schedules a solution demo from the shortlisted partners and performs an in-depth review of the features and functionality and ensures that it conforms to the requirements finalized with the organization's stakeholders. PMO further provides a detailed analysis report highlighting the rationale for shortlisting the AML solution and provides recommendations to the organization to finalize the AML partner. Finally, PMO supports the organization team in negotiation with the implementation partner.
- **Project Planning and monitoring**: PMO works with implementation partners and creates a project plan taking into consideration the people, resource constraints, and level of effort required for solution implementation. The PMO creates procedures and employs best practices to ensure smooth implementation, timely completion, and quality delivery. Further, PMO monitors the effectiveness of the procedure they have outlined and constantly looks for ways to enhance the project execution and increase efficiency.
- **Validating the Business Requirement Document (BRD) –** The BRD document captures the detail of the implementation details such as project summary and background, project scope, operating model, project governance, use cases, assumptions and constraints, and prioritized requirements. These are prepared by the implementation partner before starting the solution implementation. Any change or incorrect details in the document can affect the budget and timeline. PMO validates the details mentioned in the BRD and aligns them as per the project requirement. Further, PMO will refer to this document to cross-check the activities of the implementation partner for each phase.
- **Resource/Financial Management:** An important responsibility of the PMO is to understand and effectively manage the constraints of the people and process resources,

develop a project budget, and track it closely, as well as escalate any issues to the key stakeholders in a timely manner.

- **Change Management:** The functional, technical, or business requirements may need to be modified multiple times during the implementation cycle. It is necessary to have a disciplined change management process in place to manage this change effectively and ensure that the appropriate functionality is deployed. In addition to managing change requests, procuring necessary approvals from key stakeholders, maintaining open communication between all parties involved, and working with the IP team, the solution must be effectively deployed. Having the PMO ensures the smooth execution of these activities in change management. Any gap or miscommunication can lead to errors or technical issues which directly affect the project budget and timeline.
- **Solution Implementation and Monitoring –** PMO plays a proactive role in the implementation by establishing efficient workflows and carefully monitoring the progress of the team. Additionally, PMO is responsible for ensuring effective collaboration between project stakeholders and providing regular updates. As a result, everyone is on the same page and the project runs smoothly without any hiccups.
  Also, PMO ensures that the IP team does not deviate from the original plan by establishing critical success factors (CSF) and key performance Indicators (KPI).
- **User Acceptance Testing (UAT) –** UAT is key in ensuring that the end users are able to use the solution effectively**.** Once the solution is developed as per the BRD, the PMO manages/guides the organization team to perform UAT to ensure the solution handles real-world tasks and performs up to the development specifications. The PMO coordinates with the respective team and provides access to interact with the software before its official release (Go-Live), to determine if there are any errors or features that have been overlooked. Additionally, PMO works with the team to perform positive and negative testing of the solution to identify instances where it can fail. For all the changes identified, PMO ensures those changes have been clearly documented and communicated to the IP team and again performs UAT once the changes are incorporated into the solution.
- **Go Live** – Post approval of the UAT, the PMO coordinates between the implementation partner and organization team to finalize a go-live date of the solution where it is ready to be used for business operations. At this stage, PMO ensures the timeline for deployment to the production environment, pre-checks before “Go-Live”, coordinates for the required approvals from the stakeholder, create a backup strategy in case the implementation does not go as planned, and takes steps to prevent this from happening.
- **Project Closure –** This is the final stage of the PMO activity. The project closure stage indicates the end of the project after the “Go-Live” of the TMS. The PMO reviews all project milestones and provides a detailed report covering all aspects. In addition, all the necessary data is stored in a secure location that can be accessed by the respective team of the organization.

Conclusion

It is recognized in the financial industry that investments in transaction monitoring systems with limited returns or output cannot be sustained in the long run. Rather than simply seeking to meet the current regulatory compliance standards, the industry is witnessing a paradigm shift wherein the mindset is moving towards realizing the benefits of proactively working with AML and technology consultants and identifying the right technology provider to suit their business needs. Also, taking into consideration various implementation factors, working with professionals focused on AML technology can support the organization in implementing and maintaining a sound, robust TMS and facilitate an effortless eventual transition to the organization's technical support team.

Ankura Consulting India Private Limited
Office No. 20-118, 20th Floor, Commerz II,
Off Western Express Highway,
Oberoi Garden City
Goregaon (E), Mumbai – 400 063

For more information, please contact

Amit Jaju
Senior Managing Director

+91 9820073695 Mobile

amit.jaju@ankura.com

Amit Jaju is a Senior Managing Director with Ankura Consulting based in Mumbai, India. Amit leads the Data & Technology Segment in India and has over 17 years of experience in forensic technology consulting covering data analytics, cyber, e-discovery, software licensing and information governance.

He has created market leading solutions to solve data related challenges for clients around a wide spectrum of areas such as financial crime, bribery and corruption (FCPA / UKBA), sanctions and AML, transaction monitoring, cyber incident response, piracy and threat monitoring, analytics and software licensing. He has delivered engagements for global and Indian clients in over 20 countries and his experience spans across multiple sectors including financial services, information technology, pharmaceuticals and media and entertainment.