Views on AML Transaction Monitoring Systems

*From System Selection to Effective Governance*
# Table of Contents

Introduction............................................................................................................................................................ii

Factors to Consider When Selecting an AML Transaction Monitoring System................................................. 1

Implementing AML Transaction Monitoring Systems: Critical Considerations................................................. 4

Enhancing AML Transaction Monitoring Scenarios by Leveraging Customer Segmentation................................. 8

Validating Suspicious Transaction Monitoring Systems – Combining Anti-Money Laundering Expertise and Data Analytics ................................................................. 11

Tuning Suspicious Transaction Monitoring Scenarios: Combining AML Expertise and Data Analytics................................. 14

The Importance of a Strong AML Transaction Monitoring Governance Framework in Today's Regulatory Environment................................................................. 17

Examples of Protiviti’s Work With AML Transaction Monitoring Systems.......................................................... 20
Introduction

Over the past year, Protiviti has published a series of point-of-view (POV) papers on anti-money laundering (AML) transaction monitoring systems. These papers address issues ranging from selecting and implementing the right system to employing a proper governance framework. Given the ever-increasing regulatory scrutiny related to AML issues and the ever-more-complex compliance challenges faced by financial services organizations in that regard, it is not surprising that the response from the market to our insights has been enthusiastic and overwhelmingly positive.

This publication is a compilation of these six POV papers that we have published. The compilation includes not only specific guidance regarding various aspects of deploying and leveraging AML transaction monitoring systems, but also highlights key institutional challenges and opportunities that come with an AML system deployment. We offer specific examples from our client portfolio, detailing the ways in which we have helped our clients achieve their AML transaction monitoring goals.

We hope this information will be of interest and help to you in your organization. We would welcome the opportunity to speak with you further about your organization’s specific needs and challenges regarding AML transaction monitoring systems, and about AML compliance in general. Our team includes highly skilled AML technology experts and Ph.D.-level professionals with deep quantitative skills, many years of experience and global exposure. Together, we can help your institution articulate and maintain a sound and robust AML program that meets its goals and fits the new regulatory climate.

In addition to our AML transaction monitoring system POVs, we have published numerous other white papers and guides on anti-money laundering. We invite you to visit us at www.protiviti.com/AML and download a complimentary copy of Protiviti’s Guide to U.S. Anti-Money Laundering Requirements: Frequently Asked Questions (Fifth Edition).

Protiviti
November 2013
Factors to Consider When Selecting an AML Transaction Monitoring System

**Issue**

A well-designed transaction monitoring (TM) system is an important component of an effective anti-money laundering (AML) compliance program. It supports efforts to combat money laundering and terrorist financing by helping financial institutions identify unusual or suspicious activity that must be reported to regulatory authorities, and aids law enforcement in tracking and prosecuting criminals involved in money laundering and terrorist financing.

Due to intensifying regulatory scrutiny, the increasing sophistication of criminals and the rapid pace of technological advances, financial institutions must update their AML TM efforts constantly; therefore, it's not surprising that these organizations are increasing their investment in TM systems.

Yet despite these budget increases that also include additional personnel dedicated to support TM functions, AML TM efforts remain suboptimal in many organizations. Often, TM initiatives and systems are deficient from the outset – among the many issues, institutions may fail to incorporate lessons learned from past errors into their new TM programs in an appropriate or timely manner.

**Challenges and Opportunities**

In our experience, financial institutions face multiple challenges throughout the lifecycle of selecting, implementing and maintaining their TM systems. In the analysis that follows, we focus on the challenges and opportunities that can emerge during the TM system selection process. These challenges include:

- **Unreasonable expectations** – Management often has unreasonable expectations about how a vendor’s TM system can improve the institution’s TM program, as well as the level of effort required to implement the system. It’s not unusual, for example, to hear one or more of the following claims:
  - “We can implement an ‘out of the box’ solution to improve our TM program – no need to customize.”
  - “A new TM system will actually save us money because we’ll need fewer people. Installation won’t be a problem; our IT department will work with the vendor to implement the system.”
  - “The system can do it all – KYC, risk scoring, monitoring, case management.”

- **Poor data integrity** – Even the best-designed TM system cannot mask a TM process that is ineffective due to data quality issues. During the selection process, financial institutions can underestimate, often significantly, the level of effort required to identify and integrate required data sets from across the institution (e.g., customers, accounts, transactions) that will enable the TM system to perform optimally.
• **Improperly identified requirements** – Without a strategic approach to deploying an enterprise-level TM solution, the financial institution may define inadequate business and compliance requirements across the institution (e.g., customer activity across products or lines of business, country-specific data privacy laws, availability of scenarios for various bank products, system security, system capacity, and infrastructure planning).

• **Inappropriate scenarios or thresholds** – A TM system will not support the institution’s AML objectives if scenarios and thresholds are determined by the vendor rather than in accordance with the institution’s risk profile (e.g., products, locations).

A comprehensive AML TM system selection process not only will help the institution overcome these challenges, but also will deliver a number of benefits, including:

• **Improved data quality and architecture** – Developing a comprehensive set of data requirements to support an effective TM system will help identify data quality and architecture issues. Addressing these issues at the source system by changing operational procedures, implementing application controls (e.g., edit checks, validations) and dealing with system gaps can enhance operational efficiencies, allow for better management reporting and improve the overall AML TM program.

• **Better use of time by compliance personnel** – Investing time during the TM system selection process to identify data, monitoring, geography and production requirements is critical to implementing an effective TM system, as well as ensuring its long-term effectiveness. Over time, a well-designed TM system will enable compliance resources to spend more of their time on investigations to identify suspicious activity, rather than running manual reports, linking customer activity using multiple reports, or sorting through false positive alerts caused by data or functional issues.

• **Knowledge sharing** – Forming a cross-functional team during the TM system selection process (with representation from compliance, IT, data architecture, bank operations and internal audit) brings together resources with differing responsibilities and perspectives, thus enhancing the knowledge base needed to make the best-informed decision.

## Our Point of View

Selecting the most appropriate TM system and executing an effective implementation is a multiphase process and a number of factors must be considered. Following are some of the critical areas to address during the TM system selection process:

• Inventory of standard scenarios in the system and the ability to modify the existing scenarios or add new ones

• Capability to employ the TM system for various product types and services – correspondent banking, international ACH, remote data capture, etc.

• Case management and workflow capabilities, as well as the ability to log actions taken by the users of the TM system

• Reporting capabilities beyond the standard suspicious activity report and currency transaction report

• Process used to validate the TM system

• Capability and process to map current transaction codes to the TM system’s transaction codes

• Customer segmentation capabilities

• Data analytics capabilities that would allow the financial institution’s data analyst to determine or tune threshold values

• Capability to integrate with other financial crimes solutions implemented by the financial institution

• Capability to customize the alert/case management user interface and workflow without vendor support
• Scalability and performance/responsiveness of the TM system
• Pricing model
• Ability to integrate into the current and, potentially, future technology environment

As with any software or vendor selection initiative, a financial institution should have a defined process to evaluate the solution that fits best with the organization’s requirements. Following are some actions the institution should consider undertaking as part of this initiative.

**Project Planning, Management and Communication**

• Establish a project management team, including an executive sponsor.
• Obtain bank strategy, operations and compliance perspectives from executive management.
• If opting for a phased implementation (adding scenarios or products incrementally over time), establish a risk-based implementation strategy.

**TM Program Needs Assessment**

• Assess gaps in current TM program.
• Understand the institution’s growth strategy (e.g., acquisitions, new products).
• Identify any manual reports used in the current TM program.
• Outline desired red flag scenarios to include in the new TM system.
• Assess the alert and case information along with workflow requirements that will improve the decision-making ability of the investigator.

**Data Assessment and Inventory**

• Inventory data elements used by existing AML monitoring processes and programs developed in-house.
• Assess completeness, quality and accessibility of existing data elements.
• Determine potential data elements to be captured and assess business changes required to capture this data.

**Requirements and Vendor Scorecards**

• Develop an RFP based on business and technology requirements as well as standard institution RFP requirements (e.g., company financials, experience, warranties, cost).
• Develop a customized vendor scorecard and metrics based on prioritized business and technology requirements.
Implementing AML Transaction Monitoring Systems: Critical Considerations

Issue

From a software implementation perspective, implementing an anti-money laundering (AML) transaction monitoring system may seem no different from implementing any other system; however, there are numerous AML risk factors that an institution should consider during such an implementation. For a successful implementation, institutions should address, among other standard considerations, issues such as identification of risk-based suspicious activity monitoring scenarios, determination of initial thresholds for the identified scenarios, and deployment of the system while integrating it with the institution’s technology infrastructure. Improper consideration of these factors could lead to a high number of false positives, increased operational costs, missed reporting deadlines, and, most importantly, undetected suspicious activity and regulatory criticism.

Challenges and Opportunities

In our experience, organizations face multiple challenges with AML transaction monitoring system implementations, including:

• **System Planning** – The planning phase is very important and if not carefully deliberated will result in costly errors, and/or the need for future workarounds or remediation. A critical issue to be considered during this phase is scenario selection based on the institution’s AML risk assessment, customers and products. In addition, data source systems will need to be identified and data extraction processes developed.

• **Implementation** – The implementation phase poses numerous challenges and requires the financial institution to have a disciplined approach to various aspects of project planning, effective coordination among various stakeholders of the project, and an overall oversight of the system implementation from a project management office (PMO) level.

• **Initial Threshold-Setting and Tuning** – The threshold values driving each of the selected scenarios should be set at a risk-responsive level to ensure the institution is alerting on potential suspicious activity. At the same time, the institution should be mindful of not setting the threshold values too low, which can result in a high volume of false positive alerts that create operational bottlenecks.
Despite these challenges, a disciplined system implementation approach yields opportunities and favorable outcomes, including:

- **Implementing Risk-Focused Scenarios** – By executing a systematic scenario selection process, the financial institution is able to select targeted scenarios tailored to the institution’s AML risk profile. Implementing appropriate risk-based scenarios can improve the efficiency of the financial institution’s compliance personnel.

- **Deeper Understanding of Source Data and Coverage** – AML implementation projects often uncover data architecture issues with source systems or transaction codes that need to be addressed as part of the project to ensure adequate and accurate data is flowing into the AML transaction monitoring system. As a by-product of this exercise, the implementers will gain in-depth knowledge of data coverage (e.g., products, transactions, accounts) associated with the chosen scenarios which in turn will enable the institution to answer system “metadata”-related questions posed by the regulators in a more confident and precise manner.

- **Ongoing Scenario and Threshold Maintenance Process** – Challenges during the implementation process that are due to lack of a systematic threshold-setting and tuning process could be used as lessons learned, and allow the institution to develop an ongoing methodology for scenario threshold-setting (limits) and tuning, which can also lend itself to easy validation by the internal audit team.

- **Efficient Deployment Process** – The existence of a PMO promotes clear coordination among various teams responsible for a flawless deployment of the monitoring system. This coordination will enable the project’s key stakeholders to gain a clear understanding of the project state and react in a timely manner to make the required changes.

**Our Point of View**

Significant effort is needed to achieve an effective AML transaction monitoring system implementation. Based on our past experiences, we have identified some of the most important considerations that should be addressed to successfully implement a technology-driven transaction monitoring system.

**System Planning**

**Understanding Risks and Potential Red Flags:** This task involves effectively mapping the risks identified in the institution’s AML risk assessment and common money laundering red flags (i.e., “Money Laundering and Terrorist Financing Red Flags” included in the FFIEC BSA/AML Examination Manual) for the respective lines of business with current transaction monitoring controls. Mapping these risks will be the first step in identifying potential gaps in the current monitoring controls and the scenarios that are necessary to ensure adequate coverage of products/services, and mitigation of money laundering risks.

**Vendor Selection:** To perform effective vendor selection, the following points should be considered:

- **Data Volume** – Will the chosen product be able to manage the data volume imposed on it? Failure to perform this analysis can result in significant performance bottlenecks.

- **Technology Infrastructure** – Given the significant operational costs associated with the deployment and maintenance of a monitoring solution, will the selected solution be able to coexist seamlessly in the existing technology infrastructure?

- **Scenario Selection** – Does the vendor’s solution offer the correct coverage of red flag detection scenarios to meet the institution’s risk tolerance and ensure all products and services are adequately monitored? Similarly, does the vendor’s system allow for easy customization if it does not offer all scenarios desired by the institution? As a general rule, the more complex the activities of an institution, the more likely customization will be required. Failure to pose such questions up front could drive the need for costly
workarounds later or additional development time to program such scenarios. It is also imperative to note that not all vendor-developed rules or scenarios may be required to be deployed by the institution, as the risk exposure for each institution is different and the scenario selection should be performed on a case-by-case basis.

**Data Source Identification** – From a technology perspective, this task involves identification of various source systems which house the required data. It also involves determining processes that will be responsible for extraction and loading of the data into the chosen monitoring system. The implementers can then create a “dictionary” (metadata) of data sources, and determine which products/transactions should be in scope for monitoring.

The following items are key points to note for data sourcing:

- **Data Availability** – Is the in-scope data readily available?
- **Data Quality** – Has the validity of the data quality been verified? This is a critical step, as inaccurate information (e.g., miscoded transactions) can lead to skewed data analysis and undesired/inaccurate results. For example, when designing scenarios to capture wires flowing to high-risk jurisdictions, it is imperative that the data elements containing all the countries through which the wire was routed are present, and that country codes/values are accurate.
- **Data Refresh Rate** – How often is the data refreshed?
- **Data Volume** – Has data analysis been performed to determine data volume? The data volume should be supportable by existing hardware infrastructure either “as-is,” or additional hardware resources should be procured.

**Scenario Development** – This task involves translating each monitoring scenario’s functional specifications into a deployable module based on the chosen transaction monitoring system. Typically, this task is executed by the vendor of the monitoring system, but the institution may choose to design, code and test the scenarios itself. In addition, the institution may desire customized scenarios to adequately cover money laundering risks specific to the institution itself.

**Implementation (PMO)**

**Project Planning** – This task requires the creation of project plans by taking into consideration the people, resource constraints and effort required to implement the chosen scenarios. This may encompass the creation of a multiphase deployment plan, which will require placing multiple deployments into production in a phased manner.

**Resource/Financial Management** – This task requires understanding and effectively managing the constraints arising due to people and process resources. Additionally, the time and money spent due to the current project is closely tracked such that any issues arising are communicated to key stakeholders in a timely manner.

**Change Management** – During the course of the implementation cycle, there are multiple instances where there may be a need to modify the functional, technical or business requirements. To manage this change effectively and ensure that the appropriate functionality is deployed in production, there is need for a disciplined change management process that focuses on managing the change requests, procuring required approval from key stakeholders, and maintaining an open communication channel among all responsible parties. Additionally, this task involves working with the technology deployment team to transition the system into the production environment effectively.
Threshold-Setting/Tuning

**Customer Segmentation** – This task involves applying various data analysis techniques to the in-scope data to determine the number and type of the customer segments that can be deployed in the system. Successful execution of this step enables the implementation team to determine appropriate thresholds based on the behavior exhibited by the respective customer segment, as opposed to a threshold gauged on the entire customer base.

**Initial Threshold-Setting** – In this step, advanced statistical analysis is used to determine effective threshold values which should be applied to a given scenario for successful execution. The threshold-setting exercise should be performed for each customer segment and risk level. Therefore, it is possible to have multiple threshold values for a given scenario, as each value will be applicable at a given customer segment and risk level.

**Threshold-Tuning** – Prior to going live with the chosen thresholds from the initial threshold-setting exercise, a dry run of the alert-generation cycle should be performed to produce alerts that can be investigated in the test environment. A successful investigation of these alerts can provide insight into the alert quality to be expected in the production environment. Therefore, this step gives an opportunity to perform further threshold-tuning before deploying the selected thresholds in production.

**Ongoing Tuning and Threshold Enhancements** – Additionally, it is imperative to execute a threshold-tuning exercise on a periodic basis that consists of generating and investigating alerts just below the threshold values. This exercise gives insight into the existence (or lack) of suspicious activity just below the set thresholds. Existence of such activity will require the thresholds to be lowered. If there is no suspicious activity just below the threshold values, then a separate exercise consisting of lifting the threshold values above the current values can be performed. If this exercise yields the same alerts, then there may be a case for lifting the threshold values in production.
Enhancing AML Transaction Monitoring Scenarios by Leveraging Customer Segmentation

Issue

Many financial institutions expend considerable time and money reviewing customer and transaction alerts that ultimately are deemed to be of little real value. One of the key contributors to false positive alerts is ineffective threshold setting and tuning based on flawed customer segmentation methodologies.

Threshold setting and tuning is one of the phases in the overall transaction monitoring system development lifecycle. Typically in this phase, the focus is on identifying relevant threshold values (limits) for the scenarios used to capture activity conducted by customers that is outside of the normal or expected activity (outliers). Identifying the normal activity is a challenge many institutions face during this phase. Poor customer segmentation leads institutions to use an approach that derives a threshold value of a given attribute (i.e., transaction channel) based on the activity exhibited by the entire customer population. This approach may not be efficient and can lead to high volumes of false positive alerts, which result in higher operational costs, can cause potential suspicious activity to go undetected and may provoke regulatory criticism.

Challenges and Opportunities

Organizations face multiple challenges with respect to the initial and ongoing threshold setting of scenarios for AML transaction monitoring systems because of poor customer segmentation. Some of these challenges include:

- **Activity-focused thresholds** – Lack of data analyses on the customer base and product usage leads to thresholds being based on the transaction activity exhibited by the institution’s entire (in scope) customer base. For example, when identifying the thresholds for a given scenario customers might be segregated irrespective of their type (e.g., large corporations, middle market companies, sole proprietors) or transaction activity might be aggregated without regard to the transaction channel (e.g., ACH, wire, check), when a better approach would be to analyze the transaction activity at the customer type and channel level to determine the thresholds.

- **Inaccurate Know Your Customer (KYC) data** – Lack of accurate KYC data inhibits leveraging KYC information such as the customer’s occupation, demographics, expected level of transaction activity, etc. When these attributes are not readily available, segmenting customers into meaningful buckets that group together customers with similar traits becomes challenging, if not impossible.

- **Increase in customer volume** – As the customer base of the financial institution grows, the thresholds identified based on the transaction data of the older customer base may not be relevant. If the financial institution does not re-segment its customer bases, there may be orphan customers, or customers may be grouped into incorrect segments, resulting in inadequate monitoring compared to peers.
• **Addition/modification of scenario logic** – As time progresses, deployed scenarios may undergo a logic change whereby a particular channel may be added for monitoring or migrated from the current scenario to a new one. In any such situation, the existing thresholds will need to be modified to reflect the change so that the new thresholds are relevant to the deployed scenario logic.

Despite these challenges, a customer segmentation-focused threshold-setting approach, when properly conducted, yields opportunities and favorable outcomes, including:

• **Targeted thresholds** – By implementing a systematic customer segmentation methodology that is based on transaction channel activity and customer type rather than a customer’s aggregate transactions, the institution is able to identify unique groups of customer behavior and, therefore, establish thresholds that are more targeted. For example, identifying segments for a customer who is exhibiting distinct wire, ACH and check activity will promote a more targeted threshold for wire scenarios versus setting a threshold based on the activities of all customers.

• **Deeper understanding of the customer and the corresponding product usage** – Apart from threshold setting, the customer segmentation effort yields meaningful insight into customer behavior and the frequency of the customer’s product usage. This information can be leveraged not only from an AML standpoint by using it to drive future scenario development, but also from a marketing standpoint to determine new product selling opportunities to existing customers or identify a customer base that the financial institution is lacking and may want to target. Furthermore, in instances where certain KYC information is missing, the institution may see opportunities to enhance the customer onboarding process to collect additional KYC information upfront that would allow for better segmentation and even enhance the factors used to determine the customer’s risk rating.

• **Decoupling of customer risk and transaction activity** – As the customer segmentation is based purely on a customer’s observed transaction activity, it is agnostic of the customer’s risk rating. This decoupling of the customer’s activity and risk promotes independent and, therefore, parallel model development of both aspects, but still allows coupling by merging the identified customer segments with all customer risk levels. For example, if it is determined that there will be five customer segments that capture all activity types and that there are three risk levels, then there will be a total of 15 customer segments where each customer segment is split into three risk levels.

**Our Point of View**

Significant effort is needed to determine unique customer segments that will prove to be effective. There are a number of important considerations that should be addressed to implement a data-driven customer segmentation methodology successfully.

**Attribute identification**: This task includes identifying various customer types served by the line of business based on the provided KYC information and the type of transaction channels that can be used by customers. KYC information such as customer type, occupation, salary and net worth may be used to segment the customer base initially. Transaction channel usage can then be utilized to segment the customer base further. For example, in the case of an individual customer (type), if the customer has a checking account and uses direct deposit for his/her paycheck, writes checks for bill payment and withdraws monies via ATM, then the activity types will be ACH (paycheck deposit), check and ATM activity.

Once the customer and the activity type attributes are identified, transaction data can be extracted from the warehouse in the data structure that has been determined by the chosen attributes. In the event of high transaction volumes, a statistically valid sample may be extracted for further downstream data analyses.

**Segment identification**: Effective segment identification is multiphased:

• **Algorithm identification** – In this step, the clustering algorithm that will be used to perform customer segmentation is identified. The key consideration points in selecting the algorithm are the data analyses
results from the attribute identification step, data volume and the level of data transformation required before data can be supplied to the chosen algorithm.

- **Membership analyses** – After the execution of the selected segmentation algorithm, the created segments are analyzed for their constituents. This is necessary because the existence of highly polarized segments (one segment having 80 percent of the customer population, for example) will not allow for targeted threshold setting. Additionally, this step enables the institution to classify the collection of customers based on their exhibited transactional activity.

- **Multiple iterations** – If, after the execution of membership analyses, the segments are highly polarized, then there may be a need of re-executing the segmentation cycle on the polarized segment. This will further break a “lumpy” segment into more granular segments.

**Implementation approach identification**: As the customer segmentation exercise leverages advanced statistical algorithms, a detailed process describing how customers will be assigned to the identified segments needs to be articulated and implemented on the institution’s technology infrastructure. This process should also describe how often the customer segments will be refreshed (due to addition of new customers, products, etc.) and the process to assign existing segments to new customers.
Validating Suspicious Transaction Monitoring Systems – Combining Anti-Money Laundering Expertise and Data Analytics

**Issue**

More and more financial institutions rely primarily, if not solely, on information technology systems to monitor their customers’ transactional activity for potential money laundering and terrorist financing. Transaction monitoring (TM) systems that leverage appropriately designed scenarios and thresholds can improve a financial institution’s capability to detect suspicious activity quickly and more effectively. However, significant issues can result if there are errors with the completeness and accuracy of the TM system’s data integration and scenario processing. The AML scenarios within a TM system can be susceptible to multiple issues, including but not limited to invalid threshold settings, errors in scenario logic, data integrity issues, and unknown types of transactions that are omitted from the TM system. These issues could lead to increased false positives, false negatives (i.e., instances of money laundering that are not detected), higher staffing costs, and ultimately, potential regulatory violations and fines. To protect against these potential issues, the TM system must be subject to a comprehensive validation program.

**Challenges and Opportunities**

Financial institutions face multiple challenges with respect to the initial and ongoing validation of their TM systems and, more specifically, of the deployed monitoring scenarios used to detect potentially unusual activity. Some challenges include:

- **Data** – As the scenario logic is directly dependent on transactional and customer master data, lack of validation controls around database structure, contents and metadata leads to incorrect usage of data which, when processed by the TM system, results either in the existence of ineffective alerts (i.e., false positives) or absence of required alerts (i.e., false negatives).
- **Scenario logic validation methodology** – The logic of a deployed scenario is the key driver behind a successful alert generation cycle. Due to inadequate testing at the time of deployment, weak configuration management control or source data changes, scenarios could become defective and generate invalid alerts.
• **Thresholds** – As the customer base of the financial institution grows or changes, the initial thresholds identified based on the transaction data of the historical customer base may no longer be relevant. Stagnant thresholds could result in thresholds that are not aligned with the institution’s risk profile and potentially suspicious activity could go undetected.

• **Independence** – Even if a financial institution follows a typical software development lifecycle, the institution may not have an independent team that can verify the deployed scenario logic and data sources and determine the accuracy of the deployed scenarios. Regulatory guidance, such as the Office of the Comptroller of the Currency’s and the Federal Reserve’s Guidance on Model Risk Management (OCC Bulletin 200-16 AND FRB SR 11-7), emphasizes the importance of validation being performed by staff members who were not involved in the model development and do not have a stake in whether the model is determined to be valid.

• **Lack of documentation** – Inadequate or outdated documentation around TM scenarios and data sources could leave a financial institution unsure of what transactions are or are not being monitored by the TM system. Lack of appropriate documentation typically increases the volume of discrepancies identified in the validation due to unknown data inputs and scenario definitions.

A systematic and independent TM system validation process, supported by individuals with AML subject-matter and data-analytics expertise, enables the institution to overcome the above-listed challenges and presents various opportunities, such as:

• **Meeting regulatory requirements** – By implementing a systematic TM system validation methodology, a financial institution is in a much better position to respond to regulators’ queries about the institution’s scenario validation approach and whether it meets regulatory guidance.

• **Improved TM system performance** – Existence of a disciplined validation methodology and evidence of its successful execution can produce more effective alerts that result in a high percentage of SARs. By generating more effective alerts, compliance personnel can spend less time on clearing false positives and more time on investigating suspicious activity.

• **Acting proactively vs. acting reactively** – The data analytics resulting from the review will allow the institution to adjust its detection scenarios in a timely manner and in line with any modifications to its money laundering risk profile caused by changes to the institution’s customer base, products and services, and geographic footprint. This, in turn, will result in a robust system that does not rely on reacting/responding to external events, such as regulatory violations or law enforcement investigations of the institution, to initiate the needed adjustments.

• **Knowledge sharing** – With an independent team responsible for validating the various aspects of the monitoring system, the knowledge and understanding of the workings of the TM system will not be confined to the implementation team, thus avoiding resource constraints (e.g., “key person” unavailability). This will ensure the ongoing tuning efforts are sustainable.
Our Point of View

An effective model validation methodology is one that will help ensure the TM system is complete, effective and sustainable. A financial institution should consider several critical areas, such as those identified in the accompanying graphic, to develop a successful TM system validation methodology. For each area, we have listed some of the key questions that should be addressed.

- Are the TM system's scenarios, thresholds and customer segmentation rules producing the intended alerts?
- Is the TM system working as designed?
- Are reports and alerts complete and accurate?

- Is the TM system generating too many false positives or are there false negatives?
- Does the TM system monitor for money laundering red flag scenarios?

- Is the TM system assessing all intended types of transactions and transaction codes?
- Have there been significant changes (e.g., acquisition, new product) that could have impacted data completeness and accuracy?
- What transactions are being excluded from the TM system?

- Do configuration changes (e.g., changes to thresholds) and system changes follow a well-controlled process to avoid changes that negatively impact the TM system?
- Is access to the TM system limited to an individual's job responsibilities?
- Are the AML program and TM system included in the institution's business continuity and disaster recovery plans?
Tuning Suspicious Transaction Monitoring Scenarios: Combining AML Expertise and Data Analytics

Issue

Suspicious transaction monitoring systems enable financial institutions to monitor their customers’ transaction behavior systematically by providing relevant scenarios/rules that analyze the underlying customer transactions and generate automated alerts of activity that may be unusual and indicative of potential money laundering. These alerts are then reviewed by a team of investigators to determine if the activity truly is unusual. Activity that is deemed suspicious will then be escalated and suspicious activity reports (SARs) or similar reports for the relevant regulatory agencies will be filed (e.g., SARs filed with the Financial Crimes Enforcement Network (FinCEN) in the United States or Serious Organised Crime Agency (SOCA) in the United Kingdom).

Some institutions do not re-evaluate the effectiveness of their alerts to determine whether there is a need to tune/adjust current thresholds or develop different monitoring scenarios. This lack of tuning occurs when:

• There is an absence of a feedback loop from the alert investigations phase back into the transaction monitoring system; therefore, the information gathered at the alert investigation level cannot be leveraged by the automated transaction monitoring system to fine tune the deployed scenarios; and,

• There is no repeatable process in place that requires the institution to re-evaluate, on an ongoing basis, the thresholds and scenarios, and to perform an analysis to determine if changes are needed.

The absence of periodic tuning of scenarios often results in numerous false positives, which in turn delay alert investigation and ultimately lead to missed reporting deadlines.

Challenges and Opportunities

In our experience, organizations face multiple challenges with respect to ongoing scenario tuning. These include:

• **Information availability** – The information available at the alert investigation level is not captured for use in subsequent scenario tuning phases. Even if the information is captured at the investigations level, it is not in a data structure that is suitable for data analyses or management information reporting (e.g., alert-to-SAR ratio, type of alerts, alerts closed as false positives, etc.).

• **Tuning methodology** – There is no systematic and, therefore, no repeatable tuning methodology. In instances where the need for scenario tuning is identified, it is primarily focused on the problematic
scenario(s) at hand instead of in-scope scenarios. This results in inconsistent execution of the scenario tuning process and in inconsistent documentary evidence in the event of regulatory scrutiny.

- **Dedicated tuning environment** – The scenario tuning effort is never factored into the initial transaction monitoring system implementation; therefore, there is an absence of a dedicated environment that promotes fine-tuning of scenarios. This inhibits the financial institution from performing data analyses to fine tune the threshold values at which each of the deployed scenarios operate.

- **Collaboration among compliance, business and technology teams** – A successful scenario tuning exercise not only is a result of selection and execution of an effective data analysis approach, but also is dependent on critical inputs provided by the business team about how products are intended to be used by customers, as well as inputs from the compliance team about money laundering red flags/typologies associated with each product. Lack of collaboration among compliance, business and technology teams inhibits an informed scenario tuning process that is based on data and expert judgment of end users and risks.

- **Measuring tuning success/effectiveness** – Not all alerts/cases will result in a SAR filed with the authorities (or a true positive); therefore, it becomes difficult to tune the transaction monitoring system and to measure its overall effectiveness based solely on the alert-to-SAR ratio. Adequate measurements of success must consist of a combination of factors, including red flag coverage and minimal criticism of the transaction monitoring system by auditors and regulators.

A systematic scenario tuning process, coupled with anti-money laundering (AML) subject-matter and data analytics expertise, enables the institution to overcome the above-listed challenges and presents various opportunities, such as:

- **Reduced false positives** – By executing a systematic scenario tuning cycle, the financial institution will be able to determine thresholds that are more targeted, as these values will be derived by leveraging historical information gathered at the investigations level and by conducting advanced data analyses.

- **Improved alert scoring** – The scoring of alerts is performed to promote efficient alert assignment to investigators. A fine-tuned scenario process will have a higher likelihood of generating true positives and, therefore, will promote effective scoring of alerts.

- **Identification of redundant scenarios** – By requiring a continuous information feedback loop from the investigation phase, the financial institution will be able to identify scenarios that are redundant and, consequently, ineffective. Further, this analysis will provide factual data for removing nonproductive scenarios from the production environment.

- **Measuring success** – Having a formal tuning process that takes risk management into consideration allows institutions to present success factors other than escalated cases and SARs filed. These factors include being able to articulate clearly which known money laundering risks (red flags) are mitigated by the scenarios that were implemented, preemptively identifying activity that may later be referred to by law enforcement, and the ability to present a robust tuning methodology (inclusive of change control documentation and rationale for tuning) that is not criticized by regulators.

**Our Point of View**

An effective scenario tuning methodology will help ensure the transaction monitoring system is effective and sustainable by combining both an analytics and an expert judgment approach. Based on our experience, we have identified several key considerations that financial institutions should address to implement an effective scenario tuning methodology successfully.

**Analytics Approach**

- **Above-/below-line testing** – In this step, the threshold values are adjusted in a tuning environment and an alert generation cycle is executed such that the alerts can be reviewed by end users and compared with red flags and SARs filed. Adjustments to thresholds can be made using statistical analysis of the customers’ transactions, moving them above or below predetermined multiples of the standard deviation.
- **Pseudo investigations** – In this phase, a thorough investigation of alerts generated in a testing (pilot) environment allows investigators/compliance professionals to assess the alerts being generated by the implemented scenarios. The key consideration points are the ratio of good versus bad alerts, operational impacts (alert volumes and staffing levels), and most importantly, whether any existing SARs were missed due to the adjustment of existing thresholds.

The following exhibit depicts a high-level process flow of a scenario tuning cycle in a dedicated tuning environment.

---

**Expert Judgment Approach**

- **Red flag gap analysis** – In this step, the products and services are identified and known money laundering red flags are paired with each. An analysis is performed to identify any current controls (manual or automated) in place to mitigate the money laundering risks. The next step is to determine whether a scenario could be used to monitor activity associated with the red flags. Depending on time and money, institutions could choose to take a risk-based approach to deploy certain scenarios prior to others.

- **Ongoing risk assessment and tuning** – There are always new trends and money laundering schemes arising in attempts to circumvent controls for existing products and services. Furthermore, there may be new regulatory reporting requirements that an institution’s customers may try to circumvent. Compliance teams should be aware of new schemes and regulatory requirements. They should assess any monitoring gaps that exist and devise plans to create new scenarios or fine-tune existing ones to detect such activity. In addition, compliance teams should maintain a close link with the business teams to understand any new products or services that will be offered (e.g., remote deposit capture, virtual currencies, prepaid access) in order to assess the associated risks and mitigate them with updated scenarios.
The Importance of a Strong AML Transaction Monitoring Governance Framework in Today’s Regulatory Environment

**Issue**

Expectations for transaction monitoring (TM) governance are quickly evolving due to the complexity of detection systems, the demand for additional operational oversight, increased regulatory scrutiny, and the need for an adequate control framework to guarantee proper risk management. As a result, compliance officers/AML officers/money laundering reporting officers (collectively, MLROs), along with other affected financial institution personnel, are finding it increasingly difficult to manage their existing responsibilities amid the heightened scrutiny and expectations regulators have regarding transaction monitoring systems and the end-to-end (E2E) processes tied to them (e.g., vendor selection, tuning rationale, model validation requirements, backlogs, etc.).

**Challenges and Opportunities**

In our experience, organizations face multiple challenges with respect to designing a strong TM governance control framework. These include:

- **Managing regulatory expectations** – In addition to overseeing the day-to-day operations of clearing alerts and performing investigations, regulators expect institutions nowadays to ensure the integrity of the data, tune/enhance monitoring scenarios, and validate the effectiveness of the systems on an ongoing basis.

- **Tuning methodology and know-how** – Some institutions may lack the expertise in this area to develop scenarios effectively, fine-tune them, and ensure they are designed to cover known money laundering red flags. In some cases, this may be due to the fact that institutions relied on vendors/consultants to implement the TM systems, and never retained the knowledge within the organization. When presented with questions by auditors/regulators, MLROs may be unable to respond with the level of knowledge or detail that is expected.

- **Liaising with multiple parties** – TM programs depend on critical inputs provided by the business team about how products are intended to be used by customers, as well as on inputs from the compliance team about money laundering red flags/typologies associated with each product. Lack of collaboration between compliance, business and technology teams inhibits an informed scenario-tuning process that is based on data and the expert judgment of end users and risks.

- **Achieving global consistency** – For larger institutions with a global footprint, ensuring each region has hired the right people, implemented adequate detection scenarios and instituted strong controls to manage the end-to-end TM process has become a significant challenge. This is due to geographical distance...
from the head office, differences in regulatory requirements, and misinterpretation of regulations and/or internal policies and procedures.

- **Managing the alert investigation team** – The teams involved in the alert review process may be growing quickly, making it difficult to ensure that everyone on the team has the required skill set and expertise to review the output of the TM systems (alerts). It also may be difficult within a rapidly growing unit to manage the quality of the rationale used by investigators to close an alert or to escalate it and document suspicion. Some larger institutions may offshore the alert review process, which adds to the difficulties in providing oversight, guidance and timely feedback.

- **Measuring success/effectiveness** – Traditional numbers-based metrics do not show the full picture when it comes to TM efforts. Many institutions struggle with determining how best to measure success since efficiency benchmarks alone do not guarantee effectiveness.

A strong TM governance control framework enables the institution to overcome the above challenges and presents various opportunities, such as:

- **TM E2E operating model** – Designing an end-to-end operating model provides financial institutions the opportunity to create a roadmap for how they want the TM process to function, including policy and procedure design, system selection, scenario calibration/tuning, alert review, suspicious activity report (SAR) filing and management information reporting. The model will also help in designing the control framework and an ongoing review process to ensure there are continuous enhancements to the overall process.

- **Creating a separate TM unit** – Designating a TM officer and allowing a separate unit to manage the end-to-end transaction monitoring process will allow the financial institution to understand clearly and manage all risks associated with this process, as well as have clear accountability of the function. A separate TM unit will also be better able to retain the proper skills needed to manage the people, process and technology side of transaction monitoring. In addition, a separate unit will allow for clearer lines of communication among different areas of the financial institution (i.e., IT, business and compliance).

- **Applying global minimum standards** – When looking to achieve global consistency, developing minimum TM standards that take regulatory requirements and industry leading practices into consideration and adopting them throughout the different regions will ensure the group is operating at a known base level and managing money laundering risk consistently and effectively.

- **Measuring success** – Having a strong TM program that takes risk management into consideration allows institutions to present to senior management actual success factors and not just escalated cases and SARs filed. Success should be represented by a combination of the alert-to-SAR ratio and the following factors:
  - Being able to articulate clearly which known money laundering risks (red flags) are mitigated by the scenarios that were implemented;
  - Generating effective scenarios that highlight unusual activity, to assist in preemptively identifying activity that may later be flagged and referred to by law enforcement;
  - Documenting a robust tuning methodology (inclusive of change control documentation and rationale for tuning) that is acceptable to regulators; and
  - Having adequate policies and procedures and experienced personnel to investigate the alerts generated by the TM system.

## Our Point of View

In order for financial institutions to meet current regulatory expectations, they should develop a strong TM program – one that has a proper governance framework and oversight with effective, sustainable and repeatable processes and controls. This can be achieved by implementing a comprehensive operating model that covers the E2E process (i.e., system selection, scenario selection, tuning, alert review, SAR filing,
management information reporting, and continuous review/validation and enhancement) to ensure adequate money laundering risk management.

Based on our experience, it is often useful for MLROs to assess the time and effort required to lead a strong TM program and determine whether the organization would benefit from creating a separate function to manage these responsibilities. Normally, larger financial institutions are more inclined to do this; however, some smaller institutions may also see benefits in having a separate unit and officer responsible for the process.

Successfully managing the TM program also consists of understanding risk. Some products or business lines may pose minimal risk – for example, those with low volumes and values of transactions, those with strong controls around transaction limits, or those where customers cannot easily initiate transfers. A proper risk assessment should be performed to determine which products, services or regions pose the highest risk and do, in fact, require automated monitoring and more attention.

Lastly, to achieve global consistency, larger institutions with a global footprint should design and implement a set of minimum TM standards that should be adopted by each region. The regional units should only deviate from the adopted minimum standards in order to increase their controls to meet more stringent local requirements.

Institutions should consider the following points when developing minimum standards:

- Vendor selection (minimum automated system requirements)
- Product, transaction and customer coverage based on red flags
- Data inclusions/exclusions
- Minimum risk-based scenario set (taking CDD information into consideration), scenario selection, tuning processes and documentation
- Training standards customized for each role in the end-to-end process
- Investigation standards, including maintenance of supporting documentation and timeframes for completing reviews and filing SARs
- Metrics for generating management information reports that can be used to measure performance and risk, and identify enhancement opportunities
- Ongoing validation of the TM system (including recalibration of scenarios based on lessons learned from SARs filed) and the end-to-end process
Examples of Protiviti’s Work With AML Transaction Monitoring Systems

Transaction Monitoring System Selection

A large regional bank engaged Protiviti to assist with its TM system selection process. We worked with the bank to develop and execute a TM system selection approach, assembling a working group that included company stakeholders from project management, compliance, operations, technology and internal audit. As part of the project, we helped our client develop technology and business requirements, vendor scorecards and demonstration scripts and evaluations, and we assisted through the process of final vendor evaluation and selection.

Customer Segmentation

A large global bank sought our assistance to comply with the requirements of its regulators following an independent review related to enhancing its current AML transaction monitoring systems. As part of the project, the bank also sought our assistance in implementing a new transaction monitoring system for its capital markets division, as well as in tuning existing systems for its retail, private banking and wealth services divisions. During the course of the project, it was noted that effective thresholds and scenarios could not be implemented due to poor customer segmentation. Together with the client, we developed a strategy and implemented a methodology for initially and continuously segmenting the customer base. This was achieved by:

- Grouping of transactions (cleaning up transaction codes)
- Developing a segmentation model using existing KYC and transaction channel activity data
- Enhancing the system architecture to be able to filter/group customers based on similar customer data (occupation, annual turnover, size of entity, etc.)
- Ensuring the segmentation model could be easily customized when future KYC data or industry knowledge became available

We were able to use the transactional analyses and available KYC data to segment the customer base in a meaningful manner. Once segmented, we set effective thresholds and design scenarios for capturing outliers that were representative of potentially unusual activity. Through our efforts, the bank was able to demonstrate to its regulators that it was taking corrective action in implementing strong AML controls with respect to its transaction monitoring systems.

AML System Validation

A regional bank requested Protiviti’s expertise in performing an end-to-end independent validation of its AML TM system. The validation consisted of comparing existing scenarios to money laundering red flags and validating data inputs, scenarios and thresholds, as well as assessing the configuration management process.
We worked together with the bank’s business and technology personnel to obtain a clear understanding of existing processes and collected relevant data sets to perform an in-depth validation of deployed TM scenarios and supporting data processes. Upon conclusion of our review, we provided recommendations to add scenarios to monitor activity that was previously not monitored, modify thresholds to align better with the bank’s risk profile, and improve the configuration management process to help avoid future threshold issues. Additionally, we created a detailed data sourcing document, which the bank previously did not have, that describes the existing data extraction and loading processes. Through our efforts, the bank resolved gaps in its monitoring scenarios and adjusted its thresholds to reduce false positives.

Threshold Tuning

A large regional bank engaged Protiviti to assess its current TM system scenario thresholds. Our AML and modeling experts worked with the client to develop a statistical approach that evaluated the effectiveness of each threshold based on quality alerts. Each potential threshold change was tested to verify the intended activity was captured with the new threshold. In addition, the bank’s risk assessment results were used to help determine adequate threshold levels. Prior to changing the thresholds in the production environment, management tested the new thresholds in parallel for a period of time. With the recommended threshold changes, the bank was able to reduce false positive alerts.

AML TM Governance

A large global bank sought Protiviti’s help to enhance its current AML transaction monitoring systems and functions. This involved assessing the current organizational structure and control framework, designing a target operating model, developing policies and procedures, and evaluating and enhancing detection scenarios. Together with our client, we developed a strategy and implemented a methodology for performing initial and continuous assessment of the institution’s risk. Specifically, we identified source systems and transaction codes, ensured accurate data feeds, selected scenarios aligned to the institution’s risks, performed quantitative analysis to calibrate the systems, used the analyses and available KYC data to segment the customer base in a meaningful manner, and tested the output and effectiveness of the generated alerts to drive further recalibration of the thresholds and scenarios. Furthermore, we deployed the target operating model we had developed with the client to ensure the entire group was managing its money laundering risk in a consistent and effective manner.
About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

How Protiviti Can Help

Whether your financial institution is implementing an AML transaction monitoring system for the first time, changing vendors and systems, or performing periodic review and maintenance of current systems, Protiviti has the experience and resources to help. Below is a short summary of how we can assist your financial institution in each of the five stages discussed in this white paper.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning</td>
<td>• Review to ensure program is risk based</td>
</tr>
<tr>
<td>Implementation</td>
<td>• Review data feeds and data integrity</td>
</tr>
<tr>
<td></td>
<td>• Assist in the development of rules and parameters</td>
</tr>
<tr>
<td>Pilot testing</td>
<td>• Review to ensure policies and procedures are appropriate</td>
</tr>
<tr>
<td></td>
<td>• Review to ensure management/users have adequate knowledge</td>
</tr>
<tr>
<td></td>
<td>• Provide training to end users and refresher training for management</td>
</tr>
<tr>
<td></td>
<td>• Perform pilot testing to understand whether initial parameters for rules are effective/efficient</td>
</tr>
<tr>
<td>Alert review and trend analysis</td>
<td>• Evaluate system configurations using worst-case scenarios</td>
</tr>
<tr>
<td></td>
<td>• Evaluate system for adequate coverage of financial institution’s profile</td>
</tr>
<tr>
<td></td>
<td>• Provide support to clear accumulated backlogs</td>
</tr>
<tr>
<td>Maintenance of the monitoring program</td>
<td>• Provide recommendations for improving system effectiveness and efficiency based on changes at the financial institution</td>
</tr>
<tr>
<td></td>
<td>• Assist in the validation of risk assessment based on monitoring system trends</td>
</tr>
<tr>
<td></td>
<td>• Perform periodic reviews of the monitoring system</td>
</tr>
</tbody>
</table>

For additional information about the issues reviewed here or Protiviti’s services, please contact:

Carol Beaumier
Managing Director
+1.212.603.8337
carol.beaumier@protiviti.com

Bernadine Reese
Managing Director
+44.20.7024.7589
bernadine.reese@protiviti.co.uk

Carl Hatfield
Director
+1.617.330.4813
carl.hatfield@protiviti.com

John Atkinson
Director
+1.404.926.4347
john.atkinson@protiviti.com

Chetan Shah
Associate Director
+1.704.972.9607
chetan.shah@protiviti.com

Luis Canelon
Senior Manager
+44.20.7024.7509
luis.canelon@protiviti.co.uk

Carol Beaumier
Managing Director
+1.212.603.8337
carol.beaumier@protiviti.com

Carl Hatfield
Director
+1.617.330.4813
carl.hatfield@protiviti.com

Chetan Shah
Associate Director
+1.704.972.9607
chetan.shah@protiviti.com

Luis Canelon
Senior Manager
+44.20.7024.7509
luis.canelon@protiviti.co.uk
# THE AMERICAS

## UNITED STATES
- Alexandria
- Atlanta
- Baltimore
- Boston
- Charlotte
- Chicago
- Cincinnati
- Cleveland
- Dallas
- Denver
- Fort Lauderdale
- Houston

## Argentina*
- Buenos Aires

## Brazil*
- Rio de Janeiro
- São Paulo

## Canada
- Kitchener-Waterloo
- Toronto

# ASIA-PACIFIC

## Australia
- Brisbane
- Canberra
- Melbourne
- Perth
- Sydney

## China
- Beijing
- Hong Kong
- Shanghai
- Shenzhen

## India
- Bangalore
- Mumbai
- New Delhi

## Indonesia**
- Jakarta

## Japan
- Osaka
- Tokyo

## Korea
- Seoul

# EUROPE/MIDDLE EAST/AFRICA

## France
- Paris

## Germany
- Frankfurt
- Munich

## Bahrain*
- Manama

## Kuwait*
- Kuwait City

## Oman*
- Muscat

## Peru*
- Lima

## Venezuela*
- Caracas

## South Africa*
- Johannesburg

## Argentina*
- Buenos Aires

## Brazil*
- Rio de Janeiro
- São Paulo

## Canada
- Kitchener-Waterloo
- Toronto

## Australia
- Brisbane
- Canberra
- Melbourne
- Perth
- Sydney

## China
- Beijing
- Hong Kong
- Shanghai
- Shenzhen

## India
- Bangalore
- Mumbai
- New Delhi

## Indonesia**
- Jakarta

## Japan
- Osaka
- Tokyo

## Korea
- Seoul

# Protiviti

© 2013 Protiviti Inc. An Equal Opportunity Employer. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.