Powerful Insights.
Proven Delivery.®

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.

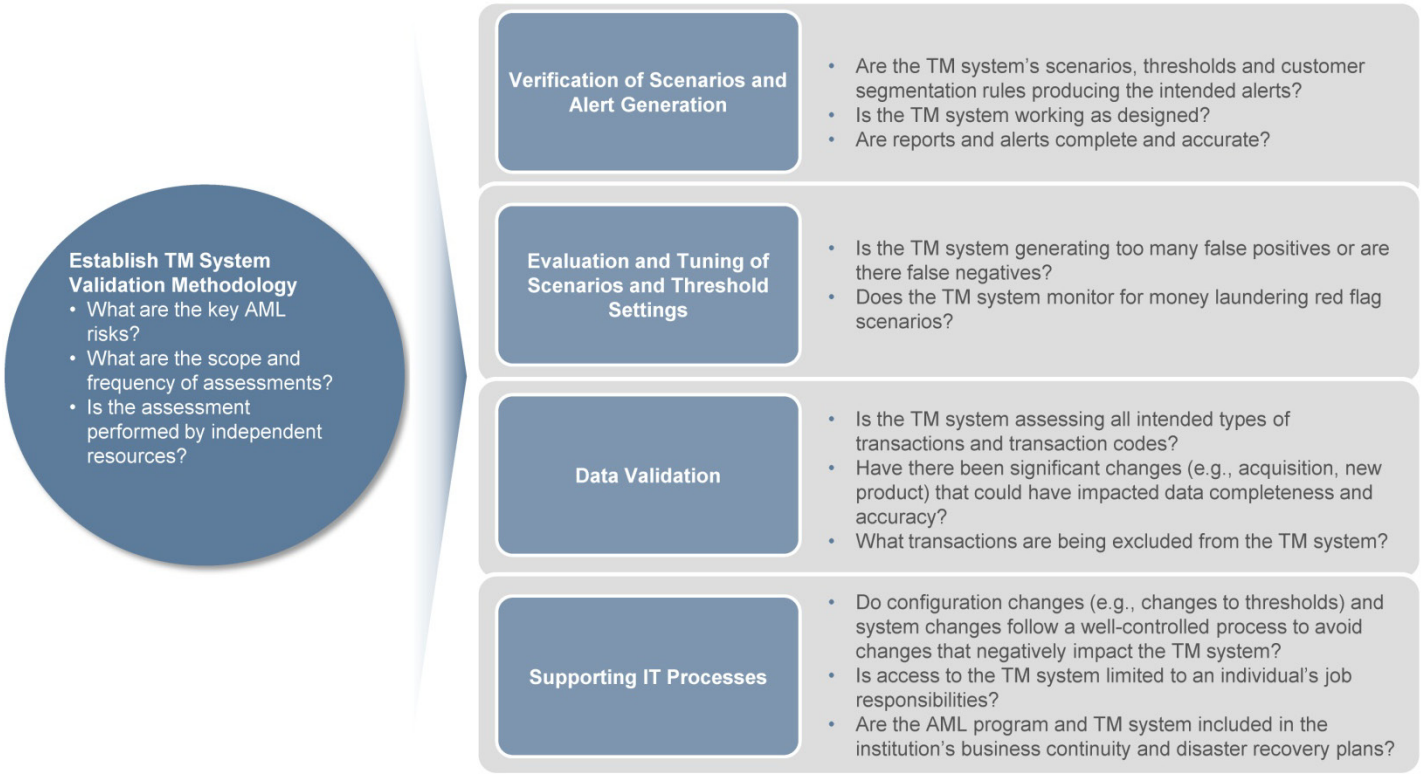
- **Lack of documentation** – Inadequate or outdated documentation around TM scenarios and data sources could leave a financial institution unsure of the transactions that are or are not being monitored by the TM system. Lack of appropriate documentation typically increases the volume of discrepancies 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.
- **Proactive versus reactive** – 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** – As there will be 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.



How We Help Companies Succeed

Our AML professionals, teaming up with the experts from our modeling team, who include Ph.D.-level professionals with deep quantitative skills, can help your institution articulate and maintain a sound and robust AML TM system validation program. Collectively, we assist financial institutions in implementing and executing their AML TM system validation strategy. We have experience with a number of AML TM systems on various platforms, including but not limited to Actimize, Detica NetReveal AML (Norkom), Mantas and SAS AML, as well as a number of homegrown systems. Our AML TM validation services include the following:

- Developing an effective and efficient model validation methodology and approach
- Conducting validations in the following areas as part of a validation approach:
    - Verification of scenarios and alerts
    - Evaluation and tuning of scenarios and thresholds
    - Data validation
    - Customer segmentation
    - AML red flag gap analysis
    - Worst-case scenario analysis
- Assessing the existing model validation process
- Improving the current tuning methodology, approach and documentation, and transferring knowledge for the financial institution to use on an ongoing basis

Examples

- **A regional bank sought our assistance 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 its configuration management process to help avoid future threshold issues. Additionally, we created a detailed data sourcing document that describes the existing data extraction and loading processes, which the bank previously did not have. Through our efforts, the bank resolved gaps in its monitoring scenarios and adjusted its thresholds to reduce false positives.

- **A large regional bank engaged Protiviti to assess its current TM system scenario thresholds**. Our AML and modeling personnel worked with the bank 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.

Contacts

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

Shaheen Dil
Managing Director
+1.212.603.8378
shaheen.dil@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

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

protiviti®
Risk & Business Consulting.
Internal Audit.