Validating Your AML Monitoring System

The FFIEC BSA/AML Examination Manual defines suspicious activity reporting as the “cornerstone” of the Bank Secrecy Act reporting system. It further notes that one of the key components to an effective suspicious activity monitoring and reporting system is being able to identify unusual activity. Financial institutions have multiple processes for identifying unusual activity. For many companies, one of the most important is an automated monitoring system for analyzing transaction data.

Issue
An automated monitoring system is a key component of an effective anti-money laundering (AML) program because of its ability to analyze large amounts of transaction data for anomalies or “red flags” that may indicate unusual or suspicious activity. These systems require more than a “plug and play” approach. Once installed and in production, an automated monitoring system must be managed actively to maintain its effectiveness. One of the most important issues to consider in keeping AML software properly fine-tuned is the regulatory expectation, outlined in the FFIEC BSA/AML Examination Manual, that a monitoring system’s programming methodology and algorithms should be validated independently to ensure the models are detecting potentially suspicious activity.

Challenges and Opportunities
Validation of AML monitoring software presents several challenges for financial institutions, including finding qualified staff to perform the validation testing, determining whether the system is configured appropriately for the institution – which requires accessing detailed descriptions of algorithms – and identifying data integrity issues. Additionally, there is very little regulatory guidance on the scope and frequency of validation testing.

Despite these challenges, successful validation testing provides assurance that monitoring software is producing reliable results in support of an institution’s AML program. It also identifies opportunities to improve the quality of the output and maximize the usefulness of alerts. However, financial institutions should be mindful of common problems that can occur with monitoring system methodologies. These include:

- **Reasonableness.** In accordance with regulatory guidance, monitoring thresholds and rules should be assessed periodically for reasonableness given the institution’s risk profile. Financial institutions should structure and document the assessment to demonstrate an objective approach fully supported by available data.

- **Date Range.** Monitoring system rules for activity over a specified date range should state the date ranges as clearly as possible. For example, detection of accounts with excessive aggregate activity in a single month can be interpreted in two ways: activity in 30 consecutive days or a calendar month. In the case of the latter, transactions that occurred on consecutive days but different months would not be flagged. Thus, while the software correctly detects all accounts within the criteria, it may not provide the results anticipated.

- **Date of Execution.** Business processes indicate the day that a process should be executed. For certain AML flags, enough time should be allotted for all transactions to occur and for data sources to be updated.

- **Change in Account Type.** Generally, AML detection rules are specific to account type – business, personal, etc. For various reasons, account types may be converted from one type to another; however, account conversion may not be detected by the AML software, resulting in alert errors.

- **Naming Conventions.** Inconsistent naming conventions within an institution (often the result of multiple legacy systems) can undermine the accurate production of alerts. Additionally, the inability to employ “fuzzy logic” to identify common originators and beneficiaries can inhibit the generation of important alerts.

- **Country Risk.** Wire transfers are a source of AML risk. AML software typically monitors this risk based on transactional-level data and a user input country risk table. Change control procedures should ensure the most up-to-date table is implemented.
Our Point of View

Periodic validation of AML software systems not only complies with regulatory expectations but also is a vital control in an AML program. Validation testing provides assurance that automated monitoring is performing as expected, identifies opportunities to improve the accuracy of system-generated alerts and brings management’s attention to potential gaps where suspicious activity may go undetected.

When planning for validation testing, there are several important considerations to keep in mind:

1. Staff conducting validation testing should have the necessary technical expertise and regulatory knowledge.
2. Spot gaps where monitoring software may not cover risk exposures.
3. Staff should have access to the technical tools and automated support needed to conduct the testing efficiently and accurately.
4. Data integrity testing should be an integral part of the validation testing.
5. Data to be tested should be chosen carefully to provide independent replication of the production environment and complete coverage through specification of sufficient date ranges.
6. Complete and thorough documentation should be maintained.

PROVEN DELIVERY

How We Help Companies Succeed

For AML software validation testing, Protiviti’s AML professionals, including former regulators and industry managers, team up with the experts from our modeling team, which includes Ph.D.-level professionals with deep quantitative skills. This combination brings together the skill sets needed to conduct objective, rigorous and well-documented testing and analyze the results to bring the most value to our clients’ AML programs. We help financial institutions:

- Ensure monitoring system algorithms are producing accurate results.
- Refine rules for accuracy and effective risk management, and identify opportunities to eliminate duplicative rules.
- Identify data integrity issues that could affect outputs.
- Spot gaps where monitoring software may not cover risk exposures.

Example

In response to regulatory criticism regarding the need to validate its AML monitoring system, our client, an international bank in a high-risk jurisdiction, requested that we perform validation testing. We assembled a cross-functional team of AML and modeling experts to build an independent replica model using a separate programming language to test the accuracy of flags generated by the client’s system. Our review identified eight separate issues, ranging from date anomalies to inconsistent naming conventions, that affected the accuracy of the system’s alert output. In addressing these issues, our client improved the quality of the system’s output and increased the likelihood that alerts identify suspicious activity.

Contacts

Carol Beaumier  
+1.212.603.8337  
carol.beaumier@protiviti.com

John Atkinson  
+1.404.926.4347  
john.atkinson@protiviti.com

Shaun Creegan  
+1.212.708.6362  
shaun.creegan@protiviti.com

About Protiviti

Protiviti (www.protiviti.com) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. The firm helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Protiviti’s highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.