At the core of any financial institution’s anti-money laundering (AML) compliance department is its transaction monitoring system. The system analyzes transactional data against preset rules and generates a list of alerts for users to review. Alerts may be reviewed on a daily, weekly, or monthly basis—but how often are the rules that generate those alerts reviewed?

For many organizations, the only formal review of the rules may occur when the vendor is configuring and installing the system. However, transaction monitoring systems are not simply “set it and forget it” solutions. As the risk appetites of financial institutions change, new customers are added and customer behavior adapts to a changing world, configurations that made sense when the system was installed might not make as much sense now. Useless alerts may be generated in high volumes and—while they may not necessarily prohibit reviewers from identifying suspicious activity—provide unnecessary distraction. The alerts may also bring undesired scrutiny from regulators and auditors.

Considering business intelligence in transaction monitoring threshold-tuning

At the core of any financial institution’s anti-money laundering (AML) compliance department is its transaction monitoring system. The system analyzes transactional data against preset rules and generates a list of alerts for users to review. Alerts may be reviewed on a daily, weekly, or monthly basis—but how often are the rules that generate those alerts reviewed?

For many organizations, the only formal review of the rules may occur when the vendor is configuring and installing the system. However, transaction monitoring systems are not simply “set it and forget it” solutions. As the risk appetites of financial institutions change, new customers are added and customer behavior adapts to a changing world, configurations that made sense when the system was installed might not make as much sense now. Useless alerts may be generated in high volumes and—while they may not necessarily prohibit reviewers from identifying suspicious activity—provide unnecessary distraction. The alerts may also bring undesired scrutiny from regulators and auditors.
With limited resources both in terms of staffing and dollars, AML compliance officers must be diligent about where funds are allocated and how roles are filled. For some, the means of addressing high-alert volumes is to increase staffing resources dedicated to reviewing alerts, when a more effective solution would be to evaluate the rules causing the high-alert volumes.

To optimize threshold values, many financial institutions have elected to evaluate the threshold settings in their transaction monitoring systems and make appropriate changes. Generally, this involves a statistical analysis of transaction data and alert dispositions to identify instances where thresholds can be raised or lowered, new rules may be needed or redundant or non-productive rules can be disabled. This endeavor requires individuals with strong statistical, modeling and systems backgrounds to conduct the initial analysis necessary to make these determinations.

On its own, a quantitative-based approach should provide an improved set of threshold values. However, quantitative analysis should be supplemented by the business intelligence acquired by AML compliance departments through alert reviews, investigations and suspicious activity report (SAR) filings. Therefore, in addition to a quantitative approach to setting rule thresholds, a qualitative review of the impact of threshold changes should be undertaken to ensure both statistical evidence and business intelligence are accounted for in the new threshold settings.

Initial considerations

The following should be taken into account before deciding to conduct an alert-tuning exercise:

• **Rules were made to be broken**—Suspicious activity monitoring rules that were created and enabled during system implementation may no longer be applicable; or, different types of rules may be better suited to identifying significant and possibly suspicious customer activity.

• **Too much of a good thing may be too much**—Failure to identify suspicious activity may be caused by being too conservative with threshold levels. Transaction monitoring systems exist to point reviewers toward possible suspicious activity, and should be optimized to that end.

• **Understand data availability and limitations**—The effectiveness of transaction monitoring and investigations is driven by the quality of data being fed into the system, as well as the data available to reviewers.

• **Nothing in life is free**—Conducting a tuning exercise, whether performed in-house or by an outside firm, costs time and money. If done internally, it may require hiring additional resources with the requisite statistical and modeling backgrounds, or specialized knowledge in system installation, testing and enhancement.

For many organizations, the only formal review of the rules may occur when the vendor is configuring and installing the system.

Putting threshold-setting and tuning in perspective

In the larger scheme of transaction monitoring system implementation and enhancement, the process of threshold-setting or tuning is third in a series of steps, commencing with the identification of possible scenarios, to deployment in production.

• **Scenario identification**—At the outset, the organization needs to identify the types of scenarios or rules it needs. Consulting regulatory guidance on “red flags” and money laundering typologies, white papers, and the knowledge and experience of AML compliance staff are all useful resources in identifying the kinds of activity the organization needs to capture in its transaction monitoring system.

• **Scenario development**—Once identified, scenarios need to be developed. In many cases, the transaction monitoring system utilized by the organization will be equipped with an array of scenarios, such as velocity, dollar threshold, transaction volume and geographic-oriented scenarios. Others have the ability to create custom scenarios or offer features such as peer and historical activity threshold analyses.

• **Threshold-setting and tuning**—Quantitative analysis and qualitative tuning occur. Quantitative analysis leverages statistical techniques on the transaction dataset to identify appropriate thresholds for given scenarios. The qualitative tuning involves the evaluation of alerts generated based on the thresholds derived from quantitative analysis.

• **Quality assurance (QA) testing**—Once thresholds are set, testing needs to be conducted to ensure system settings and configurations—as well as data feeds and alert outputs—are accurate. This testing is performed before the threshold value changes are deployed in production and therefore does not focus on the post-deployment testing aspects whose primary focus is to determine whether the configurations changes are appropriate in the production environment.
• Production deployment—The threshold changes are implemented in the production environment.

Threshold-setting and tuning: Quantitative analysis

Traditionally, financial institutions and outside firms have utilized a quantitative-driven approach to evaluating transaction monitoring rules and thresholds. This involves a number of methods of statistical analysis, including:
• Distributional analysis
• Clustering
• Stability analysis
• Above- and below-the-line testing

These analyses are integral to helping to define threshold settings. However, relying solely on quantitative analysis is inadequate. While one of the biggest draws to quantitative analysis is that it is unbiased, this is also one of its limitations. On its own, quantitative analysis fails to capture the years of knowledge and skill possessed and utilized by alert reviewers, which may result in less than ideal threshold settings.

The purpose of qualitative tuning

An effective way to capture business intelligence in the tuning process is to perform qualitative analysis of alerts generated due to the quantitatively-derived threshold values to ascertain whether the proposed settings are appropriate. Qualitative analysis serves to supplement the quantitative tuning and serves to validate the proposed settings or create a business case for either modifying or rejecting the proposed threshold change. Combining quantitative and qualitative analysis ensures mathematical results are balanced appropriately with real-world business experience and judgment.

Unlike reviewing alerts in a production environment, the goal in reviewing alerts as part of a tuning exercise is to determine whether the alerts being generated by the quantitatively derived threshold settings are productive; meaning, they are generally of the type that could ultimately result in investigations or SAR filings. In addition, qualitative tuning can identify instances of the following:
• False positives—These are alerts generated by a transaction monitoring system that do not relate conceptually to the rule parameters under which an alert should be generated. For example, an alert requiring ATM withdrawals above a certain value is generated for non-ATM transaction types.
• Redundant or ineffective scenarios—Through the review of alert-to-case information and SARs, an institution can identify current rules or scenarios that are not yielding productive alerts. The institution can then use this information to detect redundant or ineffective scenarios and make a case for retiring them.

Qualitative tuning checklist

The qualitative tuning phase begins after the initial threshold values have been determined quantitatively. The following steps are necessary to conduct effective qualitative tuning:
• Sandbox environment—The organization should create a dedicated sandbox environment where the qualitative tuning exercise can take place. The sandbox environment should include data as it would appear in the production environment; doing so will enable the reviewer to obtain a real picture of how the alerts will appear when they are actually deployed in production. The sandbox environment also should be able to execute multiple alert generation cycles (days, weeks or months, depending on scenarios), which would allow for multiple iterations of alert investigations.
• Alert sampling—Alerts generated in the sandbox environment should be sampled for investigation. A statistically valid sample should be extracted from the alert population. If the organization leverages customer segmentation or risk levels, then a stratified sample should be extracted such that alerts are sampled from each of the customer segments or risk levels.
• “Investigations Lite”—This is a key phase of qualitative tuning. Each sampled alert is reviewed by experienced investigators to determine whether the new thresholds are effective, as discussed in the following section.

Investigations Lite

The standard of review utilized in the Investigations Lite phase is to determine whether the alerts being reviewed under a given scenario are productive, unproductive or false positives.

An alert would be deemed productive if it is of a nature that could, in a production environment, give rise to an investigation or SAR filing. An alert would be deemed unproductive if, in a production environment, there would be a low likelihood that alerts of this kind would result in an investigation or SAR filing. An alert would be deemed a false positive if it were found to be the result of underlying bad data, such as duplicate transactions or an incorrect country code.
Note that the extent of analysis being conducted in qualitative tuning is not intended to identify suspicious activity. Rather, it is focused on evaluating whether the alerting activity could lead an experienced investigator to believe that further review, such as an investigation, could be warranted for the kind of activity being reviewed. Where *prima facie* evidence of suspicious activity is identified, proper care should be taken to notify the institution’s AML compliance officer, so appropriate actions may be taken.

Investigators need the following to perform their analyses effectively:

- **Customer data**—Access to the customer data attributes is necessary to understand the customer's background and business or banking activities. Available data may vary based on customer type (e.g., individual, business, financial institution), but should include name, address, occupation or industry, entity type and income.

- **Account data**—Access to account data is necessary to understand the nature of the account, as well as the identities of individuals or entities who/that have access to, influence over or an interest in the account. Available data should include the account type, the date the account was opened, average account activity, related accounts, authorized signatories and beneficial owners.

- **Transaction data**—Access to transaction data is necessary in order to understand the nature of the transactions being reviewed. The data should include a minimum of six months prior to the period covered by the alerts and it should include the transaction type, as well as the originator, beneficiary and intermediary details.

- **Prior SARs**—Knowledge of prior SAR filings in relation to the customer or a customer’s account will aid in determining the effectiveness of alerts being reviewed by investigators. Alerts of customers or accounts with previous SAR filings may be viewed as more effective than alerts for customers or accounts with no such previous filings.

- **Prior alerts**—An understanding of prior alerting activity and alert dispositions will aid in understanding the kinds of activity that have been subject to previous review, and will assist in determining the effectiveness of alerts being reviewed by investigators. Recurring alerts for repeated, non-suspicious activity may be viewed as less effective than the alerts for different and potentially suspicious behaviors.

Results should be documented to allow proper analysis of data generated by the qualitative analysis. This will also serve to “memorialize” the exercise.

### Interpreting and analyzing results

Analysis should then be conducted for each scenario to determine how many of the alerts reviewed were deemed productive. Based on this review, stakeholders can determine which thresholds should be accepted. If stakeholders believe the number of productive alerts for a given scenario is too low relative to the number of unproductive or erroneous alerts, then they may choose to keep the existing thresholds or could elect to “sunset” the scenario. In such a circumstance, further review should be conducted to determine if a different kind of scenario needs to be employed, or if the scenario can be disabled without leaving a gap in coverage for a transaction type.

### Implementing changes

Once changes are finalized and approved by appropriate stakeholders, the threshold changes will be implemented and communicated to investigators. Policy and procedure documentation should be updated to reflect the threshold changes, and training materials amended. If necessary, training should be conducted to ensure investigators have a firm understanding of the scenarios in production.

Tuning should be built into compliance plans and completed on a periodic basis to ensure thresholds remain appropriate for the life cycle of the transaction monitoring system.

### Summary

Transaction monitoring systems are only as effective as the rules they employ. Over time, thresholds need to be adjusted to capture current customer behavior and economic trends adequately. Quantitative analysis is a significant piece of the tuning puzzle, but it does not take into account the business intelligence of AML compliance officers and their investigators, who have unique insight into the nuances of their institution’s clientele and activity.

By including qualitative assessment as part of the tuning process, AML compliance officers can increase the value of generated alerts and improve investigation and SAR ratios. They can also be confident that business intelligence is accounted for sufficiently and that the right rules and thresholds are utilized.

---

**Brendan Mulvey, CAMS, manager, risk and compliance group, Protiviti, New York, NY, USA, brendan.mulvey@protiviti.com**

**Chetan Shah, CAMS, director, risk and compliance group, Protiviti, Charlotte, NC, USA, chetan.shah@protiviti.com**