Powerful Insights.
Proven Delivery.®

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 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 and 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, closed alerts 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 eventually is not supported by consistent 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 based solely on the alert-to-SAR ratio and to measure its overall effectiveness. Adequate measurements of success must consist of a combination of factors, including red flag coverage and minimal criticisms 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 for 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

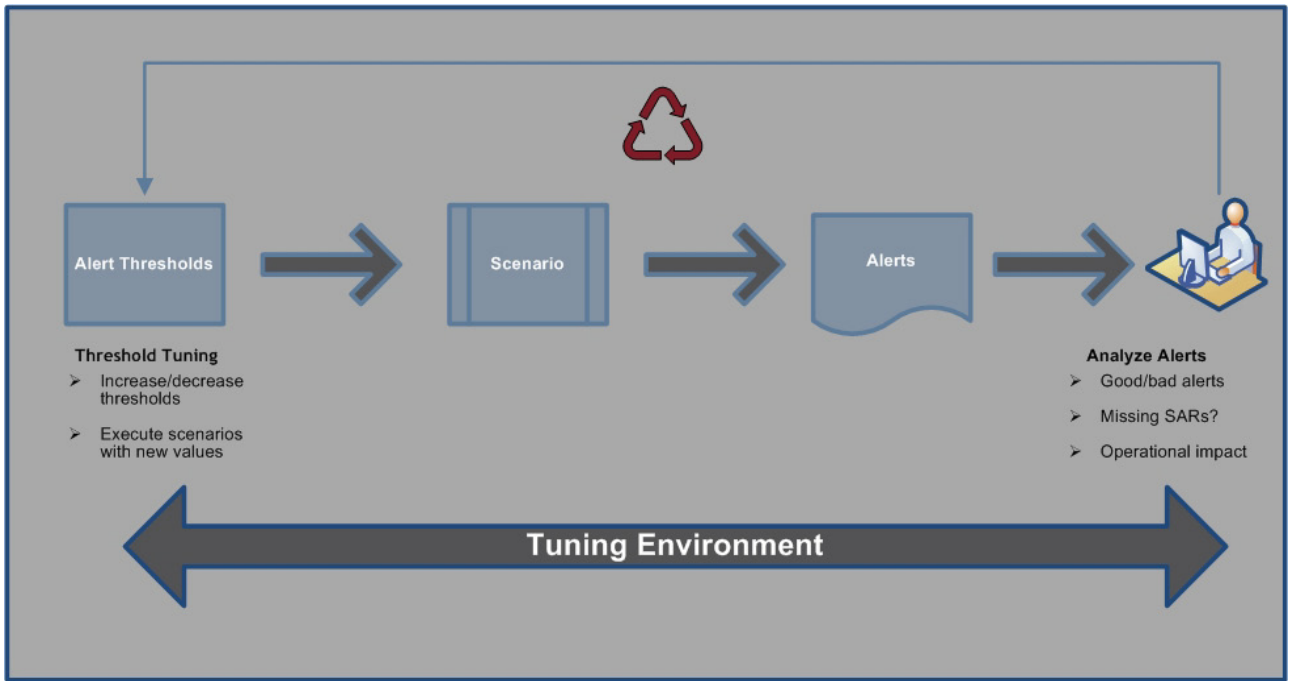
An effective scenario tuning methodology will help ensure the transaction monitoring system is effective and sustainable by combining both an analytics and an expert judgment approach. Based on our experience, we have identified several key considerations that financial institutions should address to 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 to circumvent controls for existing products and services. Furthermore, there may be new regulatory reporting requirements that an institution's customers try to circumvent. During this phase, compliance teams should be wary 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 risks and mitigate them with updated scenarios.

How We Help Companies Succeed

Our Risk and Compliance professionals focusing on AML technology, teaming up with our model risk experts who include Ph.D.-level professionals with deep quantitative skills, can help your institution articulate and maintain a sound and robust AML transaction monitoring scenario tuning process. We have experience with a number of AML transaction monitoring systems on various platforms including, but not limited to, Actimize, Detica NetReveal AML (Norkom), Mantas and SAS AML, FISERV, as well as a number of homegrown systems.

Our AML transaction monitoring technology services include:

- Developing and executing a sound and efficient scenario tuning methodology and approach
- Performing any or all of the following tasks by acting as an independent team:
    - AML red flag gap analysis
    - Worst-case scenario analysis
    - Data validation
    - Scenario logic validation
    - Threshold values validation
- Performing customer segmentation
- Recommending improvements to scenarios/thresholds

Example

A regional bank sought our assistance in performing the threshold tuning of its AML transaction monitoring system. The effort consisted of selecting representative scenarios and validating the logic and tuning of the threshold values. As part of the solution, we articulated the tuning methodology to tune scenario thresholds systematically. Additionally, we wrote relevant tuning scripts that performed statistical data analyses to identify new threshold values. Through our efforts, the bank was able to re-evaluate the threshold values in a systematic manner and deploy a repeatable tuning process.

About Protiviti Inc.

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.

Contacts

Carol Beaumier
+1.212.603.8337
carol.beaumier@protiviti.com

Shaheen Dil
+1.212.603.8378
shaheen.dil@protiviti.com

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

Carl Hatfield
+1.617.330.4813
carl.hatfield@protiviti.com

Priyantha Perera
+1.212.708.6346
priyantha.perera@protiviti.com

Chetan Shah
+1.704.972.9607
chetan.shah@protiviti.com

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

protiviti®
Risk & Business Consulting.
Internal Audit.