

SAS® Professional Services® for AML

Analytical Services for Optimizing AML Coverage and Program Efficiency



The SAS Anti-Money Laundering Analytics delivery team (part of SAS Professional Services and Delivery) is a group of highly skilled analytics professionals with deep experience working with Bank Secrecy Act compliance. Many of our professionals have worked at Tier 1 banking institutions with roles in AML analytics, optimization and investigations. The team has vast experience solving many of the most challenging issues BSA compliance departments face today, plus extensive expertise in award-winning SAS Analytics tools and solutions. We have one goal in mind: to help our customers solve their most challenging problems and institute efficient AML monitoring programs with optimal coverage.

Benefits

- Proven methodology and documentation to support your bank's regulatory needs.
- Improved coverage and productivity rates and reduced false positives.
- Reduction in alert volumes allows for realigning personnel.
- A detailed documentation package that captures the analysis, results and final recommendations for use with audits and regulatory exams.

Services Offered

Customer/Account Segmentation Model Development

Segmentation is the grouping of customers and accounts that have similar customer attributes, risk characteristics and transactional behaviors to set risk-based thresholds that are appropriate for each particular segment defined within the model. The

process allows for enhanced monitoring of those segments deemed riskiest per your bank's risk assessment.

Segmentation is the primary foundation for setting risk-based scenario thresholds, and the quality of the segmentation model directly affects the ability of your transaction monitoring system to perform in an effective and efficient manner. Implementing a quality segmentation model usually results in greater alert coverage throughout the customer/account population, greater alert productivity (lower false positive rates) and reduced alert volumes. It generally focuses on segmenting customers based on historical transactional activity and customer risk attributes, and allows conservative transaction monitoring of high-risk customers.

The results of this service are:

- Segmentation recommendations.
- A detailed segmentation report.
- Exploratory reports for future analysis.

Optionally, SAS can also provide your bank with the information, training and materials needed to assist in creating your own AML segmentation model(s).

In addition to the delivery methodologies stated later for all services, this service also uses:

- Data profiling to validate and ensure business assumptions.
- Generated party and account summary tables and party and account analysis tables.
- Comprehensive analysis and review of recommended segments.

Initial Threshold Setting (ITS)

When performing initial threshold setting – as with all model development, tuning and verification projects – SAS provides detailed documentation for the recommendations made and the analysis that led to them, which your bank's senior management, model validation group and regulators can review.

ITS initially sets scenario threshold values based on a combination of alert quality, alert volume, internal consistency of thresholds and segments, threshold distributional characteristics and bank experience. It's used when either the segmentation model changes significantly or a new scenario is implemented, and is often referred to as an estimate to be used until sufficient production alert dispositions are available to allow for the scenario threshold tuning process to be performed.

By setting scenarios' tunable parameter threshold values, you can register the scenarios and start generating alerts. ITS is generally only performed in three situations:

- Your bank is changing the transaction monitoring system.
- Your bank is implementing new scenario(s), so historical alert experience doesn't exist.

- Your bank is segmenting the customer/account population so that the historical alert experience will no longer apply.

With this service, your bank will also receive comprehensive documentation for initial threshold settings.

The results of this service are:

- ITS recommendations.
- A detailed ITS report.
- Exploratory reports for future analysis.

In addition to the delivery methodologies stated later for all services, this service also uses:

- Selection of minimum threshold values to generate distribution reports.
- Selection of target range and sampling of potential alerts.
- Customer analyst review and dispositioning of sampled alerts.
- Comprehensive analysis and review of recommended threshold values.

Scenario Threshold Tuning and Model Verification

Tuning is the process of evaluating current monitoring scenarios and their current threshold values to determine if there is statistical evidence the tunable parameters

should be adjusted. Tuning of scenarios should be done on a periodic basis, which is documented within your financial institution's model risk governance procedures.

The process maximizes the effectiveness and efficiency of models and/or scenarios that form the basis of the transaction monitoring system. It consists of segmentation model verification (if applicable), scenario verification, scenario effectiveness, distributional analysis, above-the-line analysis, below-the-line testing, threshold impact analysis and post-alert generation model verification (if applicable). And it's generally conducted every 12 to 24 months, depending on your bank's policies and procedures.

Although this isn't an independent third-party validation, the Scenario Threshold Tuning and Model Verification Report contains key information and analytic analysis that an independent third-party validator will likely want to review and reference in its report.

The results of this service are:

- Potential segmentation adjustment recommendations.
- Exploratory reports for future analysis.
- A comprehensive tuning impact analysis report.

In addition to the delivery methodologies stated later for all services, this service also includes:

- Data profiling to validate and ensure business assumptions.
- Above-the-line analysis, below-the-line testing, distribution analysis, scenario effectiveness and impact analysis.
- Quantitative alignment to the bank's risk assessment and policies.

One goal: to help our customers solve their most challenging problems and institute efficient AML monitoring programs with optimal coverage.

Anomaly Detection and Peer Group Model Development

SAS Anomaly Detection Scenarios allow your bank to monitor anomalous customer activity in terms of transactional activity. The major areas monitored are:

- Total transactional activity over time compared to current activity.
- Primary medium usage over time compared to current usage.
- Customer or account (entity) to peer group comparisons.

The development of the customer peer group model is used by the SAS Anomaly Detection Scenario in generating alerts. Anomaly detection is generally used to provide additional broad monitoring coverage for behaviors that other active rules or models don't specifically cover.

Scenario Emulation Development / Scenario Verification

Scenario emulations are extremely useful when performing testing and tuning, as they are autonomous from the AML transaction monitoring system, and thus are more flexible in terms of modifying your logic, output and threshold values. Since they generally apply different code to arrive at the alerts, they allow independent verification that the underlying scenario is operating as expected. The emulation programs are designed to pull their own preparation data set, and therefore allow testing that the correct data is being sent to the scenario. All tunable threshold parameter variable values and triggering transactions are output by the scenario emulations, along with accounting for the impacts of system suppression.

Customer Risk-Rating Model Development

The SAS AML Analytics team often assists banks in setting up and developing their customer risk-rating models (this must be a joint effort with your bank's BSA officer to ensure that the customer due diligence model aligns to your bank's AML risk assessment appropriately). SAS can assist using the SAS Customer Due Diligence solution (which relies on a weighted risk category model) or by using a statistical modeling technique, such as ordinal logistic regression. When setting up a risk-rating model, it's extremely important to have an accurate target variable to use in the development process. SAS Customer Due Diligence is generally the best choice - unless your bank requires the use of a statistical predictive model in the risk-rating process.

Post-Alert Generation Model Development

Post-alert generation models run after the alert generation process is complete and may be used for alert prioritization, alert hibernation or alert risk scoring. Common approaches include rule-based, binary or ordinal logistic, decision trees or neural network models. While alert prioritization models are used to set the alert queue, you can use risk-scoring and hibernation models to bring in additional information regarding the customer and/or account for scoring and possibly auto-closing or fast tracking the alert to SAR review. These models can be another way of reducing false positive alerts and increasing the overall productivity rate of monitoring, thus improving the efficiency of operations.

What's Included?

Typical Deliverables

- Assessment to review requirements and design.
- Deployment of standard methodology content.
- Data acquisition and data profiling of provided data.
- Data profiling to validate and ensure business assumptions.
- Service-specific components and comprehensive reports.
- Package of reports, results, findings and recommendations.

Delivery Methodology

- Assessment to review requirements and design.
- Deployment of standard methodology content and artifacts.
- Business stakeholder interviews and risk assessment review.
- Data loading and data profiling to confirm business assumptions.
- Iterative review of findings and results with business stakeholders.
- Compilation of final findings and recommendations.

How Do I Find Out More?

For more information on SAS Professional Services for AML, contact your SAS account executive, call 1-800-727-0025 or contact us at sas.com/contact.

To contact your local SAS office, please visit: sas.com/offices



SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries.
® indicates USA registration. Other brand and product names are trademarks of their respective companies. Copyright © 2017 SAS Institute Inc.
All rights reserved. 109068_G60755.0917