Dynamic Risk Classification for Anti-Money Laundering

SAS® Anti-Money Laundering enables financial institutions to meet expanded requirements for due diligence

Table of Contents

The primary content provider for this white paper was Cameron Jones, Chief Compliance Advisor at SAS.

Executive Summary

Financial institutions are finding it necessary to strengthen their anti-money laundering (AML) platforms to stem the tide of illicit financial transactions and meet new regulatory mandates. For enterprises with moderate to high risk exposures, this calls for a rigorous automated system based on dynamic risk assessment.

Financial institutions need a way to adapt rules, parameters and scenarios to match the risk profile for any given account or individual in order to monitor differentially based on risk. This requires being able to:

- Integrate a customer's initial "on-board" risk classification into ongoing transaction monitoring.
- Automatically reassess risk rating and support a risk-based monitoring process.
- Adjust scenarios and risk factors to minimize the incidence of false positives.
- Combine multiple scenarios and risk factors to generate high-quality alerts.
- Identify cases that are significant, rather than chasing all simple alerts.
- Identify the highest priority cases to be investigated, based on a customer's risk classification.

SAS Anti-Money Laundering provides all of these capabilities. Institutions can create an enterprisewide view of customer relationships and risks, monitor activity using multiple detection methods, adapt that monitoring as appropriate for each customer's risk classification, investigate and document suspicious cases, and produce required regulatory reports – all within an integrated solution built on award-winning SAS data management and analytic capabilities.

■ The risk assessment process provides the ability to identify relationships as low, medium or high risk – and to stratify scenarios to focus on those high-risk relationships.

Toward a Broader Definition of 'Due Diligence'

Criminals and terrorists have been resourceful and persistent with their money laundering activities – accounting for an estimated US$500 billion to $1 trillion a year – globally. Although most laundered money stems from drug trafficking and organized crime, the events of 9/11 put the spotlight on funding for terrorist activities, which has traditionally been much more difficult to detect.

The Patriot Act expanded the requirements for detecting and reporting suspicious activities that could indicate money laundering or terrorist financing. So did equivalent AML regulations around the world, such as the Third European Union Money Laundering Directive. Implemented in 2007, the directive creates a uniform regime of compliance that expands the definition of "client due diligence," broadens requirements for client/account monitoring and raises the expectations for banks to adopt risk-based management approaches.

Many AML systems apply a rigid, limited set of if/then rules to try to identify potentially suspicious transactions. Over time, compliance officers and regulators often discover these rules are overly broad or not reflective of the institution's real money laundering risks. High-risk entities can escape scrutiny. Legitimate accounts and transactions are often flagged for investigation, creating unproductive busy work for compliance staff.

To resolve these concerns, institutions need a more accurate, holistic and dynamic view of an entity's behavior across all products, businesses, channels and risk factors. Checking transaction data against simple rules is not enough, because what is normal for one customer might be very indicative of risk for another. What is perfectly acceptable behavior for one customer might signal money laundering activity for another.

"Most firms have now placed financial crime and associated compliance requirements very highly on their corporate agendas," states a Chartis Research Ltd. report (*Financial Crime Risk Management Systems 2009*, February 2009). "The key trend has been the adoption of a risk-based approach to managing fraud and money laundering. This has led to policies, procedures and systems that proactively identify, alert, assess and monitor the risk of such events."

Chartis forecasts that by 2012, financial institutions worldwide will spend as much as $3.75 billion on financial crime risk management technology at a compound annual growth rate of 13.1 percent.

■ With typical AML systems, compliance analysts are doing well to just detect basic trends and simple matches against known illegal activities. Few organizations can correlate potentially suspicious behaviors across disparate systems and a multitude of risk factors.

A Risk-Based Approach to Anti-Money Laundering

The foundation of any AML solution, manual or automated, is to identify transactions and actions that signal the risk of illegal activity – such as overlapping account demographics, unusually high-volume transactions or suspicious connections among accounts. A risk-based AML program goes further by looking at groups of customers in different ways depending on their ever-changing, overall risk profile.

The risk assessment process is a structured approach for assigning customers to different risk categories depending on specific attributes or behaviors. The customer or account is then monitored and managed according to the risk classification. Naturally, the institution would examine the behavior of high-risk customers more closely than low-risk ones. Parameters and scenarios could be applied differently to customers based on the potential risk they represent.

For example, a customer deemed to be high risk might have a much lower threshold for wire transfers before the activity triggers an alert in the AML system. A customer deemed to be low risk – or one that has been "white-listed" as trustworthy – would have a much higher limit for wire transactions in the eyes of the AML system. Stratifying customers based on risk classification enables AML scenarios to be run with different parameter thresholds that more closely match the risk represented by each unique customer.

Most institutions will assess their customers' risk classifications annually, but classification can be updated on intervals determined by the institution, such as biannually, quarterly or, at the lowest level, monthly. Typically once a month, the institution will run active risk classifiers against customer data to make sure the risk classification model itself is still relevant and accurate in a changing risk ecosystem.

A risk-based monitoring and investigation system is a vital component of an effective and compliant AML program. Financial institutions now have a proven way to detect and track suspicious patterns of behavior relative to their unique risks, instead of just one-size-fits-all rules and account name lookups.

Risk Classification and Scenario Stratification with SAS®

SAS Anti-Money Laundering offers a complete environment for detecting, investigating and reporting potentially suspicious activities. The software application integrates the following functions:

- Captures and organizes all customer activity across disparate data sources.
- Monitors that activity against multiple rules, scenarios and risk factors.
- Accurately alerts compliance staff to potentially suspicious activity.
- Provides a structured environment for investigating and documenting alerts.
- Generates required regulatory reports and supporting documentation.

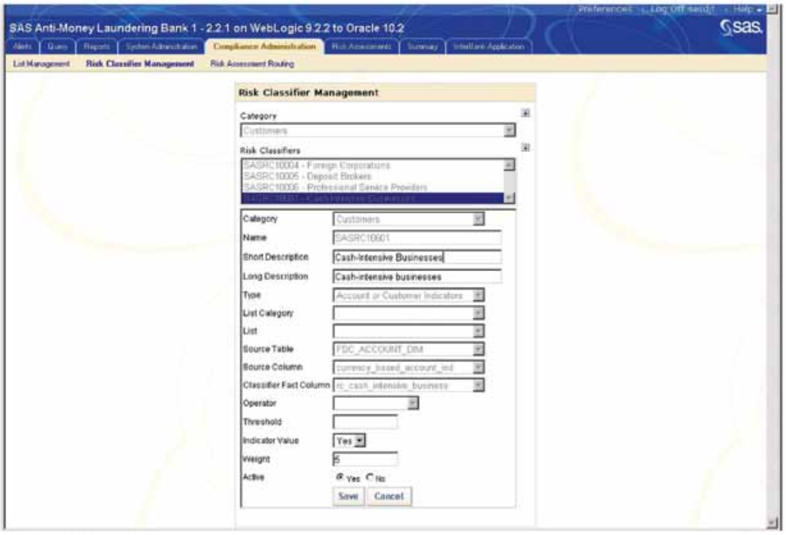
Driven by the European Union "Third Directive," SAS has expanded the due diligence features in the latest release of this AML software, adding even stronger capabilities for risk classification and differentiated monitoring based on risk categories.

Risk Classification – Identifying a Customer's Potential for Illicit Activity

The risk classification process begins with defining risk classifiers – the rules used to categorize customers into risk categories. Classifiers can include attributes of high-risk products, customer types, services and geographies. Some sample risk classifiers are built into SAS Anti-Money Laundering; others are created and managed by the institution's compliance administrators.

Account/Customer Description	Basic Customer Risk
Resident Consumer Account (DDA, Savings and Certificates of Deposit)	Low
Nonresident Alien Consumer Accounts	Low
Small Commercial and Franchise Businesses	Medium
Consumer Wealth Creation	Medium
Nonresident Alien Offshore Investor	High
High Net Worth Individuals (Private Banking)	High
Multiple Tiered Accounts (Money Managers, Financial Advisors, Payable Through Accounts)	High
Offshore and Corporations	High

Table 1: Sample types of customers/accounts and risk classifications.



SAS Anti-Money Laundering Bank 1 - 2.2.1 on WebLogic 9.2.2 to Oracle 10.2

Risk Classifier Management

Category: Customers

Risk Classifiers:
SASRC10004 - Foreign Corporations
SASRC10005 - Deposit Brokers
SASRC10006 - Professional Service Providers
[illegible]

Category: Customers
Name: SASRC10601
Short Description: Cash-Intensive Businesses
Long Description: Cash-intensive businesses
Type: Account or Customer Indicators
List Category:
List:
Source Table: FDC_ACCOUNT_DIM
Source Column: currency_based_account_ind
Classifier Fact Column: rc_cash_intensive_business
Operator:
Threshold:
Indicator Value: Yes
Weight: 5
Active: ● Yes ○ No

Figure 1: Sample risk classification screen.

In this example, any customer with a cash intensive business flag in the data model will receive a risk weight of 5 on a scale of 1-10.

The SAS solution checks a customer's demographics, transactions and other information from internal and external data sources to look for the presence of any risk classifier. Each classifier carries a unique weight depending on the severity of the classifier. Combining these values and attributes in a multidimensional analysis, the system arrives at a proposed risk classification for the account: low, medium or high.

Risk Classification Process

1. System collects H/M/L risk classifications from external processes.
2. System manages lists of risk classifiers that describe ML risk.
3. System captures transactional and list-based classifiers on monthly basis.
4. System automates periodic review and suggestion of new risk classification for the customer during assessment process.

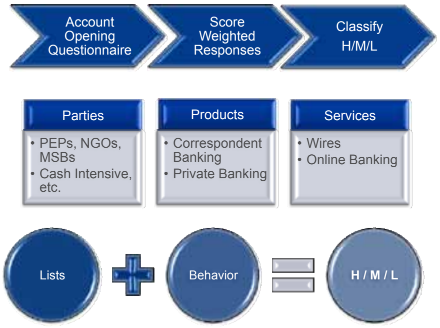


Figure 2: Risk classifications are based on a combination of information from lists and behaviors.

A detail screen displays all the risk classifiers that contributed to the customer's overall risk classification. This transparency provides valuable information to show regulators why a particular case was investigated with more stringency than another with similar transaction patterns.

Here are some sample cases:

- **Sustain a certain risk classification.** The institution has created a list of high-risk customers that should always be classified as high risk. Risk analysts can assign more points to certain classifiers to ensure that these customers are automatically assigned a high-risk classification whenever the assessment is redone.
- **Focus on cash transactions.** Suppose the institution wants to classify any business account with more than 50 percent cash transactions as high risk. The Cash-Intensive Business risk classification can be used and adjusted up or down based on the volume of cash transactions in the previous evaluation period.
- **Look closely at private banking customers.** An institution could have a list of client accounts that fall into the Private Banking (International/Domestic) risk classifier. For product line account numbers that meet this classifier, the system derives the corresponding party number and assigns a high-risk classification.
- **Watch deposit broker activity.** The institution can create a list of account types that correspond to its internal designation of clients considered to be "deposit brokers." Accounts that match this list would fall under the Deposit Broker risk classifier. For these accounts, the system would look at product type, then update the risk classification for the account number of the primary owner.
- **Assess risk from transaction patterns.** The institution can create a risk classifier, such as Large Number of International Wire Transfers, that assesses the number of matching transactions and scores the account based on this number, relative to predefined thresholds.

SAS Anti-Money Laundering enables institutions to integrate customer risk profiles collected during the account opening process with their ongoing transaction monitoring system. During the risk assessment process, the system suggests the customer's actual risk classification based on a combination of static and behavioral factors.

Risk Segmentation – Differential Treatment for Customers by Risk Classification

Once risk classifications have been assigned, customers can be segmented or stratified based on their specific risk groups. Based on summary profiles of historical transactions, the SAS solution can calculate expected behavior. The system then applies scenarios and risk factors to monitor variances against normal or expected behavior.

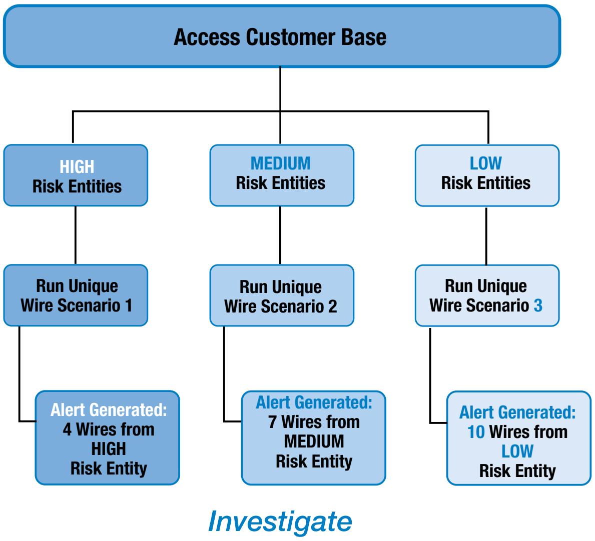

Access Customer Base
HIGH Risk Entities
MEDIUM Risk Entities
LOW Risk Entities
Run Unique Wire Scenario 1
Run Unique Wire Scenario 2
Run Unique Wire Scenario 3
Alert Generated: 4 Wires from HIGH Risk Entity
Alert Generated: 7 Wires from MEDIUM Risk Entity
Alert Generated: 10 Wires from LOW Risk Entity
Investigate

Figure 3: An institution might choose to monitor high-risk customers more closely for variances in their outgoing wire activity versus a medium- or low-risk customer.

Any parameters and thresholds – such as dollar amounts for transactions, volumes of certain types of transactions, or other definitions of normal and abnormal for demographic or behavioral rules – can all be tailored to match a customer's risk classification.

Examples include dormancy, velocity of funds transfers, increased activity or higher-than-normal transaction value. Is this a business that is expected to engage in one type of activity, but now is demonstrating entirely another pattern? Has the business deviated greatly from expected deposits or transaction value per month, or from past trends?

The ability to apply scenarios differently for different risk classifications dramatically reduces the number of false negatives and false positives, because normal ranges and potentially suspicious levels of activity can mirror the customer's potential to engage in illicit behavior.

Know Your Customer regulations have required institutions to collect information on expected activity, citizenship, source of funds and other risk indicators at account opening. Risk scores based on this information should also be used to differentiate how the institution monitors a customer's behavior over time.

Risk Assessment – Dynamic Rescoring to Match Changing Conditions

AML is a fast-moving target. Criminals are constantly probing AML systems to discover new techniques to move their funds. Risks also change as a bank expands into new markets or adds products and services, and as regulators increase their expectations. As a result, the AML system should allow easy modification of the data model, rules, risk classifiers and reports to reflect changing conditions.

Furthermore, the system should reassess risk classifications whenever necessary. The customer's risk profile at account opening might change as the customer seeks new ways to circumvent controls or undergoes a change in circumstances.

In addition to routine, periodic risk reassessments, the system may alert you to new conditions that call for a party's risk assessment to be reevaluated. Perhaps a scenario was run against the customer's data that shows high-risk activity that calls for revisiting the customer's risk classification. If the analysis dictates a change in the customer's current risk classification, a manual risk assessment may be entered with supporting documentation.

Summary reports are provided to illustrate metrics on high-risk customers, subsequent alerts and regulatory submissions.

- The risk assessment process, run at automatic intervals, enables the institution to uniquely monitor customer segments based on an up-to-date risk profile.

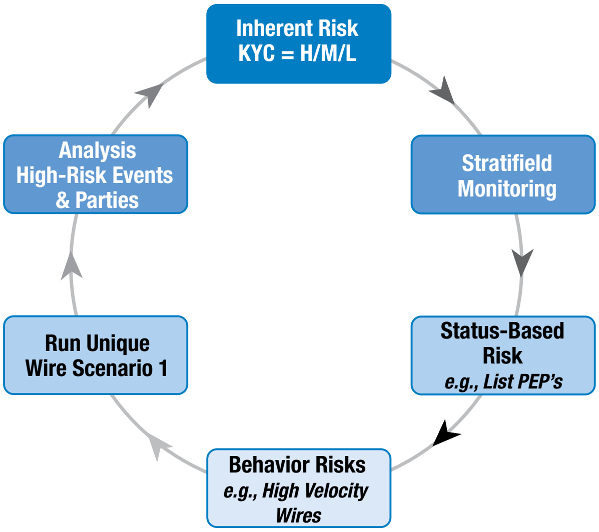


Figure 4: SAS Anti-Money Laundering incorporates risk classification and scenario stratification in a continuously self-learning process.

Closing Thoughts

With risk assessment and stratification capabilities built into SAS Anti-Money Laundering, institutions can:

- Monitor risks across the institution, using data from many legacy systems.
- Allocate resources to the most meaningful cases, while reducing false positives.
- Adapt to keep pace with the changing risk environment, internally and externally.
- Apply knowledge of risk exposures to update the enterprise risk assessment.

All of these capabilities are provided in a comprehensive solution built on award-winning SAS data management and analytic capabilities. The monitoring process is transparent, and the entire platform is adaptable to each institution's unique risk profile. Scenarios and risk factors are driven directly from the institution's AML risk assessment and can be easily changed as risks change for the organization or for the industry as a whole.

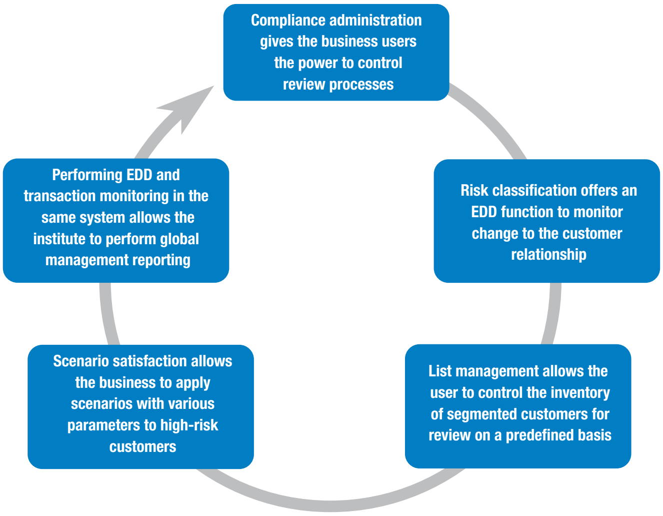

Compliance administration gives the business users the power to control review processes
Risk classification offers an EDD function to monitor change to the customer relationship
List management allows the user to control the inventory of segmented customers for review on a predefined basis
Scenario satisfaction allows the business to apply scenarios with various parameters to high-risk customers
Performing EDD and transaction monitoring in the same system allows the institute to perform global management reporting

Figure 5: Risk classification with scenario stratification adds an extra layer of accuracy, flexibility and control to enhanced due diligence.

The SAS Anti-Money Laundering solution has proven its value for financial institutions on every continent with assets from less than $1 billion to more than $1 trillion, representing all financial sectors.

Because no two financial institutions have the same AML monitoring needs, SAS offers the proven methodology via a choice of avenues:

- ***SAS Anti-Money Laundering*** provides an integrated risk scoring, alert management and reporting platform for Tier I, Tier II and midmarket institutions ($1 billion to more than $100 billion in assets).
- ***SAS Money Laundering Detection*** provides the same robust SAS methodology in a solution tailored for small to midsized financial institutions.
- ***SAS Solutions OnDemand*** gives customers in the Americas the option of having SAS host the AML application as a secure service.

To find out more about how to mitigate risk while reducing the cost of compliance, visit www.sas.com.

> "Chartis considers SAS as one of the leading players in the provision of technology solutions for financial crime risk management. SAS is one of the few technology vendors that has taken a truly platform approach to developing its financial risk management solutions. The SAS financial crime solutions integrate analytics, advanced decisioning capabilities and sophisticated rules into a single enterprise financial crimes platform."
>
> ***Financial Crime Risk Management Systems 2009***
> **Chartis Research Ltd., February 2009**

About SAS

SAS, the leader in business analytics and the largest independent vendor in the business intelligence market, helps customers at 50,000 sites make better decisions faster. SAS' innovative business applications, supported by an enterprise intelligence platform, give customers THE POWER TO KNOW®.

SAS Institute Inc. World Headquarters +1 919 677 8000

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