Paper 107-2013

An Ounce of Prevention is Worth a Pound of Cure: How SAS® Helps Prevent Financial Crimes with an Analytical Approach to Customer Due Diligence

Scott Wilkins, SAS Institute Inc.

ABSTRACT

The increasing regulatory expectations on the risk rating of high-risk clients and the emphasis on identification of foreign relationships with existing customers has driven financial institutions to enhance their Customer Due Diligence (CDD) processes. This paper outlines how organizations leverage SAS® to deploy on-boarding and ongoing Customer Due Diligence programs. It explores analytical techniques for risk ranking customers, best practices for deploying these programs, as well as how the SAS approach incorporates a proactive, analytically driven triggering of new investigations based on detected customer events or behavior. SAS can provide organizations "The Power to Know" their customers and the risk they may represent to their financial institutions.

INTRODUCTION

A robust Know Your Customer and Customer Due Diligence (KYC/CDD) application must be able to perform the following tasks:

- import customer data gathered through the on-boarding process
- provide an environment for validation and enrichment
- check against public and internal watch lists of that data
- provide an initial risk ranking for the customer.

Based on that initial ranking, further due diligence may be required, based on policies and procedures. The system must provide for the creation of a CDD case and applying the appropriate workflow for the type of customer and relationship that you are dealing with. The CDD management interface should allow for potential collection and storage of documents, a complete audit trail of actions taken, and the ability to document, through comments or journal entries, findings along the way.

Ongoing monitoring of behavior and customer attributes is also critical in maintaining a good risk assessment program. The application should provide an alert engine which can apply business rules and potential analytical models to signal risk analysts when a customer may warrant review and possible adjustment to their risk ranking. This alerting capability should also include the ability to alert when, for example, documents are set to expire or, other events that require attention and response.

Finally the administration and reporting within the application is important. The application should be able to provide robust dashboards for various user roles such as analysts and managers. Ad-hoc reporting is also important so that information can easily be extracted from the system to meet requests.

SAS Institute Inc. provides the technology with in the Customer Risk Assessment feature of SAS Anti-Money Laundering and will be releasing an enhanced CDD module for the SAS Financial Crimes Suite this year (2013) to further enable financial institutions to meet all the required goals of a robust and flexible KYC/CDD program.

HISTORY AND PRODUCT ROADMAP

Since 2008, SAS Institute Inc. has provided the ability to administer a robust customer risk ranking monitoring program as well as a tightly integrated use of the customer risk ranking for the application of relative thresholds within the deployed Anti-Money Laundering rules. This is accomplished with the SAS® Anti-Money Laundering Solution. SAS is responding to escalations in the attention given to institutions' KYC/CDD programs. SAS plans to release an enhanced module that is focused on supporting the creation, execution, and evolution of KYC/CDD programs.

SAS Institute is in the process of expanding on the capabilities that are currently delivered within the AML module so that KYC/CDD can be delivered separately (standalone) and where required. SAS also plans to deliver capabilities that are integrated with the SAS® Anti-Money Laundering and other SAS compliance and fraud detection solutions. This leverages the new modular approach inherent in the SAS® Financial Crimes Suite.

Through the deployment of the CDD module, on top of the Financial Crimes Foundation, institutions will be able to rely on a central platform for current needs as well as provide a road-map approach for consolidating other detection and investigation channels into a single enterprise platform.

BUILDING BLOCKS OF THE SAS CDD SYSTEM

The SAS CDD functionality is delivered as a module within the SAS® Financial Crimes Suite and relies on this component framework for the features in the robust and flexible CDD solution.

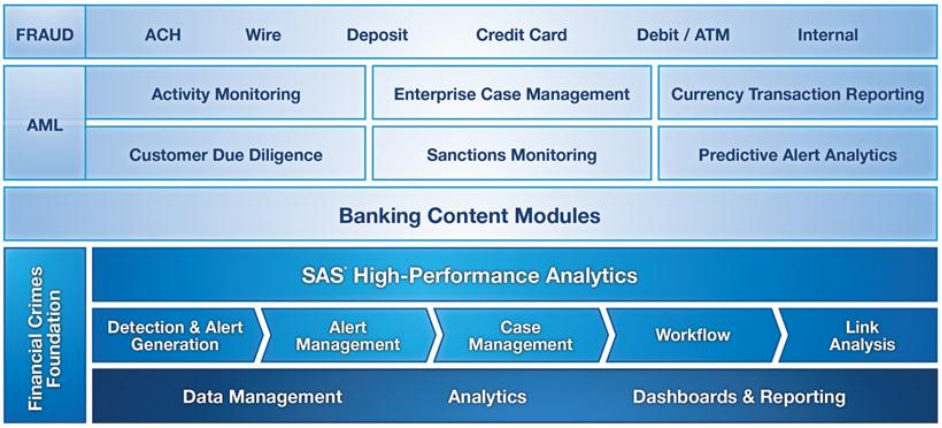


Figure 1. The SAS Financial Crimes Suite

These core features include:

- data management and data quality
- analytics
- detection & alert generation
- alert/case management and workflow
- dashboards & reports

Within the Alert and Case Management function, core objects offer the ability to define the incident, case, and subject of an investigation. Within these object definitions, data fields, comments, and

attachments are used to present, collect, and organize information in support of CDD processes and procedures. The following core objects are used within the Alert and Case Management function:

SUBJECTS

This object allows for the definition of an entity, internal or external to your organization. For example, it could be; an individual customer, a business, or an organization. Custom subject screen definitions can easily be created to store all needed information for the subject. Comments and attachments can also be associated at the subject level.

INCIDENTS

The Incident Object (sometimes referred to as an alert) allows for the definition of various events or alerts that an analyst needs in order to be aware of to establish a risk ranking for a subject. Comments and attachments are also able to be associated at the incident level. For example, incidents can represent unusual or suspicious behavior, periodic review indicators, expiration of required documentation, or negative news hits for a subject.

CASES

The Case Object allows for the definition of various types of CDD investigations. The case object has a corresponding workflow definition associated to it. When a new case is created, or an existing case activated, the system also instantiates or activates the associated workflow and links the two together. Comments and attachments can also be associated at the case level.

Cases can have zero or more incidents linked to them as well as zero or more subjects linked. So, for example, a case may have all the owners of a business linked along with any associated incidents on that business or the individual owners.

A simple example process could flow as follows:

1. The alert engine detects something that breaks a rule threshold such as unexpected wire transactions for a customer or maybe, a soon to expire required document for a business customer.
2. An alert is fired and is placed in an analyst's queue as an incident.
3. After reviewing, the analyst may determine that the incident should be referred for further investigation as part of a CDD case.
4. The incident and the associated subject are used to create and populate a new case. Or, if there is already a relevant existing case, the incident can be joined to that case.
5. The new or existing case progresses through its assigned workflow until it reaches its final state.

WORKFLOW

Workflows are created and managed with the SAS Workflow Studio™. This graphical user interface provides a drag and drop interface for creating, modifying, and managing, (through check-in and check-out) the workflows used in the CDD case management interface.

CDD case types can be as dictated by business requirements. In addition, a dedicated, custom workflow for that CDD case type can be associated to drive the prescribed steps.

The workflow administrator can control which roles (that are defined in the system) can execute which activities, using the swim lane feature. A role is associated to a swim lane and activities inside that swim lane are actionable only by users defined in the associated role. For example, you can define a manager

review activity inside a swim lane associated to the manager role and when the workflow progresses to that activity, the case will show up only in managers' work queues.

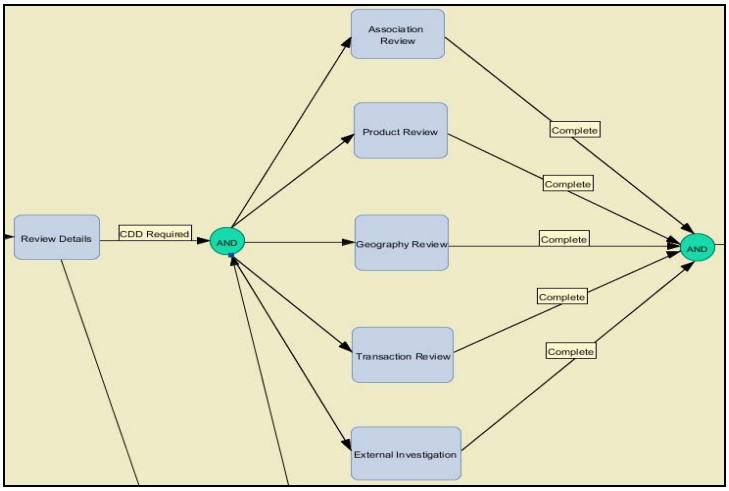


Figure 2. CDD Workflow Section

Notification and escalation can be controlled via the event and policy features of the workflow engine. Activities have normal events such as process-started or process-ended as well as specifically defined events such as timer-expired. These events can be responded to by actions called policies. For example, a timer-expired event can be responded to by a send-email action or policy. In this situation, you could have an email sent to someone if a workflow has remained in a specific activity longer than desired.

Here is a policy that is configured as described above.

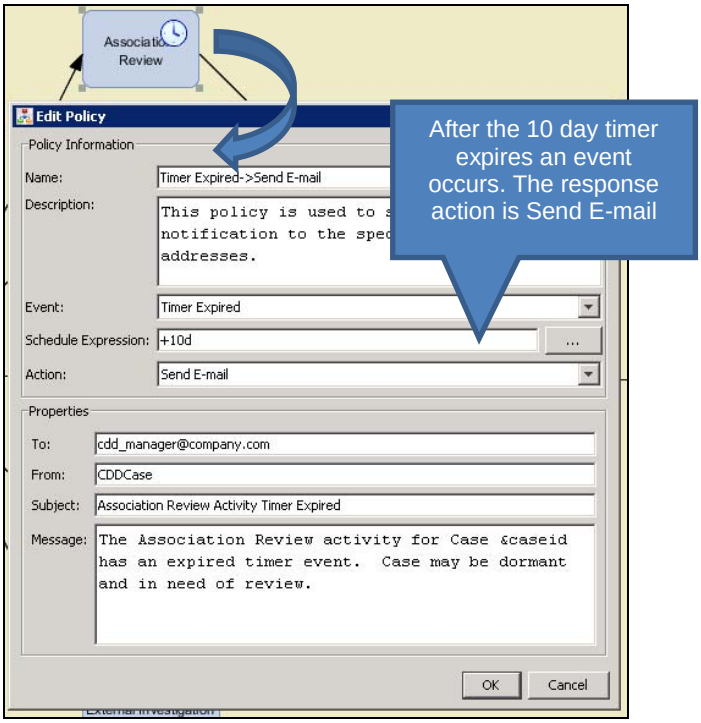


Figure 3. Sending Email When Timer Expires

Some examples of other policies that can be used to respond to workflow events are:

- HTTP request
- invoke SAS code
- invoke web service
- notify participant
- remove status from process
- schedule process
- send e-mail (illustrated above)
- send notification by data object
- send notification by workflow role
- send workflow group notification

Events that can be monitored from within the workflow are:

- process finished
- status addition
- data object updated
- process started
- participants updated
- timer expired (illustrated above)
- status removal

The workflow administrator and work flow engine make it easy for users to create and manage very robust workflows to help facilitate efficient, repeatable, and auditable procedures as various CDD case type investigations are executed.

ANALYTICS

Initially, your on-boarding system will facilitate customer identification in accordance with the policies stipulated in the Customer Identification Program (CIP). The main goal here is to collect sufficient information in order to establish a reasonable assurance that the person or persons trying to establish a relationship are who they say they are. It is also important to initially verify that these identified entities are not on a sanctions or other watch list (external or internal) as stipulated by the CIP policies.

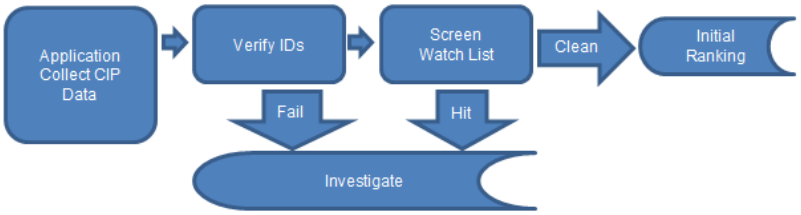


Figure 4. New Customer Initial Screening Process

Generally, initial-money-laundering and terror-financing-customer-risk rankings are based on three primary characteristics of the customer relationship. These factors are based on country, industry, and products. There are of course variations, other factors that can be considered, and extensions to this model that can also be accommodated within the flow.

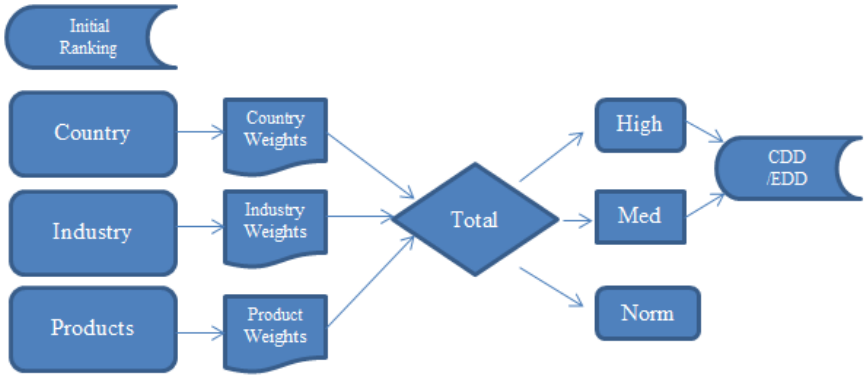


Figure 5. New Customer Initial Risk Ranking

Regulatory bodies provide various degrees of guidance on what financial institutions should consider as important risk factors when establishing the initial risk ranking of their customers. Given this guidance, and the expectation that the institution considers their inherent risk (as outlined in their internal risk assessment), the base-line process is very prescriptive in nature. This means that a rules-based approach is most typically used for establishing base-line money-laundering and terror-financing-risk for a customer.

This is not to say that an institution could or should not consider an additional, analytical approach to integrate the rules-based approach or to complement the rules-based approach.

Generally speaking, if a clear target population can be established (customers who are by definition, behavior, or investigation considered high-risk), then analytical techniques can be used to create predictive models to score the general population.

Perhaps the most analogues predictive scoring model to the typical customer risk ranking process is that of the Decision Tree Model that Tom Bohannon points out in his Blog post on decision trees:

> *" An important characteristic of decision trees is that they are easy to use and simple to explain"*

This characteristic is very important in a regulatory environment. Decision trees can also be displayed graphically with nodes and branches that are similar to an organization chart. This visual nature of the process also helps explain how scores are derived. Figure 6 shows a simple decision tree diagram.

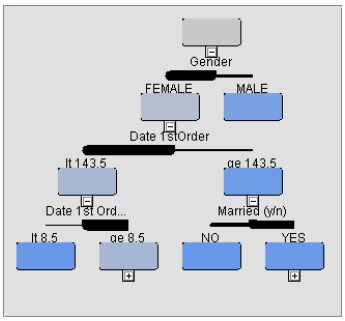


Figure 6. Example Decision Tree Chart

Other options that you can consider with your SAS consultants or your organization's quantitative analysts are regression and neural networks that are based predictive models. Also, data mining efforts can be useful when incorporated into the customer risk scoring process. These data miming efforts are focused around variable correlation and have a goal of uncovering the most likely predictors of a customers' degree of risk to the organization. AML/BSA risk ranking of customers is important for regulatory compliance and proper monitoring. However, it is just one component to enterprise customer risk. A best practice is to take into consideration how the AML/BSA risk is derived as well as how it fits into the overall picture of the enterprise risk in areas such as credit and lending, that the customer may represent. Figure 7 depicts some of the components that should be considered as well as where rules, models, and network (association) analysis play the largest roles. For example, network analysis can be a powerful tool for detecting potential, unsecured credit-bust-out-fraud networks. However, they typically are not used to establish a credit score.

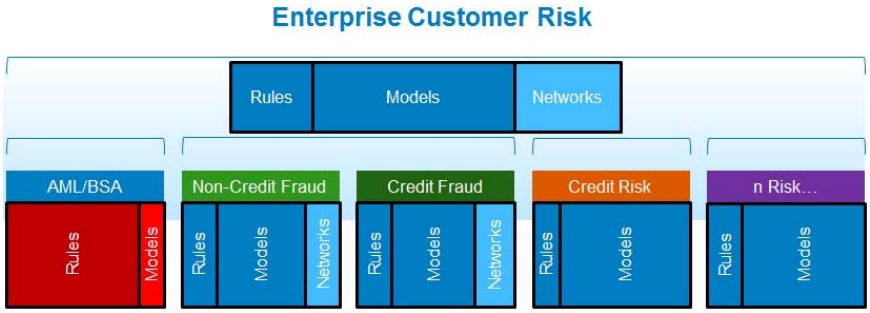


Figure 7. Components of Enterprise Customer Risk

CASE NETWORK ANALYSIS

Important initially, as well as during the life of the customer relationship, is the ability to assess internal relationships between customers. The CDD case management system provides the investigator with the ability to visually examine a subject's relationships that could have some impact on the due-diligence process. It is important to uncover these relationships in order to quantify the level of suspicion or risk that is represented. For example, if spouses share phone and address information, that would be expected. However, if seemingly unrelated subjects shared such information, then it might warrant a closer look and better understanding.

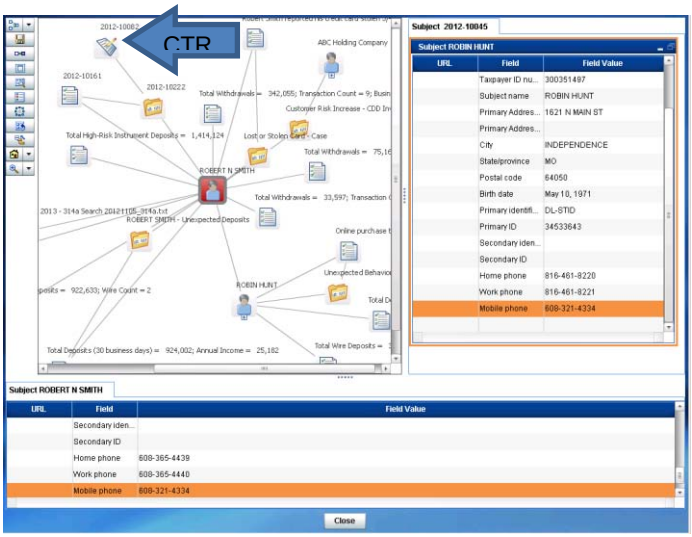


Figure 8. Case Network Analysis

The Case Network Analysis feature of the system allows the investigator to quickly visualize subjects that are related through sharing demographic information or by being common subjects on alerts or case investigations. Furthermore, if the data is available, as in the case where SAS Anti-Money Laundering™ is integrated, then interesting facts such as regulatory report filings are quickly uncovered as well. In the network below, you can see that Robert Smith was also the subject of a Cash Transaction Report (CTR) regulatory filing.

In the network you can also see that Robert Smith is related to ABC Holding Company by virtue of being common subjects on a case investigation. You can also see Robert's relationship to Robin Hunt by virtue of sharing the same mobile phone number. Within the interface, hovering over the link between the nodes reveals the nature and extent of the relationship. You can also open the details of the subject nodes to view their information side-by-side.

CASE SCREEN DEFINITIONS

The CDD case management system enables you to easily define screens with the required data fields present in order to support your information gathering and storage requirements. Within these screens, extensive data validation and conditional logic can be applied. For example, phone number formats can be validated and flagged if in error. Or, drop down menus can be related to each other so that selecting a country will direct the population of the following State or Providence drop-down menu.

A standard component that is used in the case screen definitions is the Activities component. This allows for the visualization of the connection between the case and its' associated workflow. The Activities component shows the current actions that will be taken on the case as well as completed actions. It also indicates if the activity has been assigned, due to swim lane roles, to another user or group.

Also useful, is a component that is included to help track to-do items. This Reminder component enables you to set reminders that notify you, after some period of time, to follow-up or take some action that is relative to the case.

Figure 9 shows a screen that uses the Activities and the Reminders component and is organized on a tab named Activities.

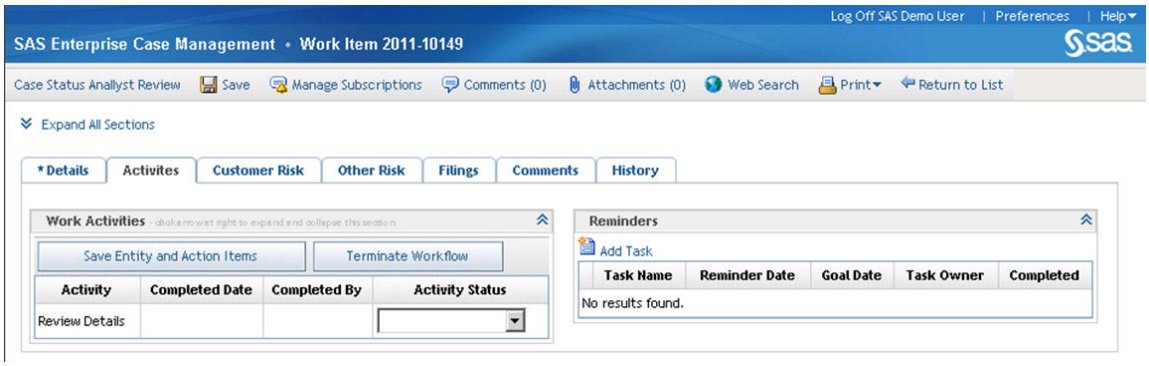
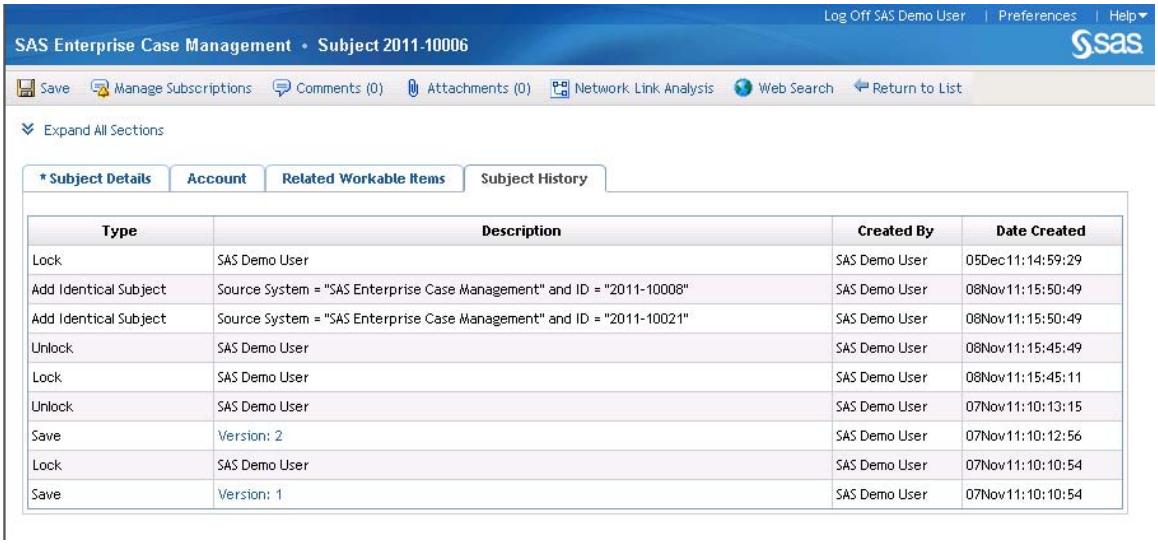


Figure 9. Example of Activities and Reminders Screen Components

Important in any compliance function, is the ability to provide a clear audit trail of actions taken, by whom, and when. This need is supported within the system by the History component. All actions and updates taken on an incident (alert), subject, or case are stored in the data model and then made available for display through the History component that is located in the associated screen definition.

Figure 10 shows a screen definition that is configured with a “Subject History” tab which displays the audit trail for this subject record.



Type	Description	Created By	Date Created
Lock	SAS Demo User	SAS Demo User	05Dec11:14:59:29
Add Identical Subject	Source System = "SAS Enterprise Case Management" and ID = "2011-10008"	SAS Demo User	08Nov11:15:50:49
Add Identical Subject	Source System = "SAS Enterprise Case Management" and ID = "2011-10021"	SAS Demo User	08Nov11:15:50:49
Unlock	SAS Demo User	SAS Demo User	08Nov11:15:45:49
Lock	SAS Demo User	SAS Demo User	08Nov11:15:45:11
Unlock	SAS Demo User	SAS Demo User	07Nov11:10:13:15
Save	Version: 2	SAS Demo User	07Nov11:10:12:56
Lock	SAS Demo User	SAS Demo User	07Nov11:10:10:54
Save	Version: 1	SAS Demo User	07Nov11:10:10:54

Figure 10. Example of the History Screen Component

DASHBOARDS AND REPORTING

Any application is only as valuable as it is easy to use, derive intelligence from, and extract needed information from. The SAS® Financial Crimes Suite, within which the CDD module is deployed, provides access through the foundation layer to the full power and flexibility of the SAS® Business Intelligence Architecture. This allows for the building and deployment of specific role based dashboards and reports in support of the KYC/CDD operational and strategic reporting needs. Figure 11 shows some examples of the type of reports possible.

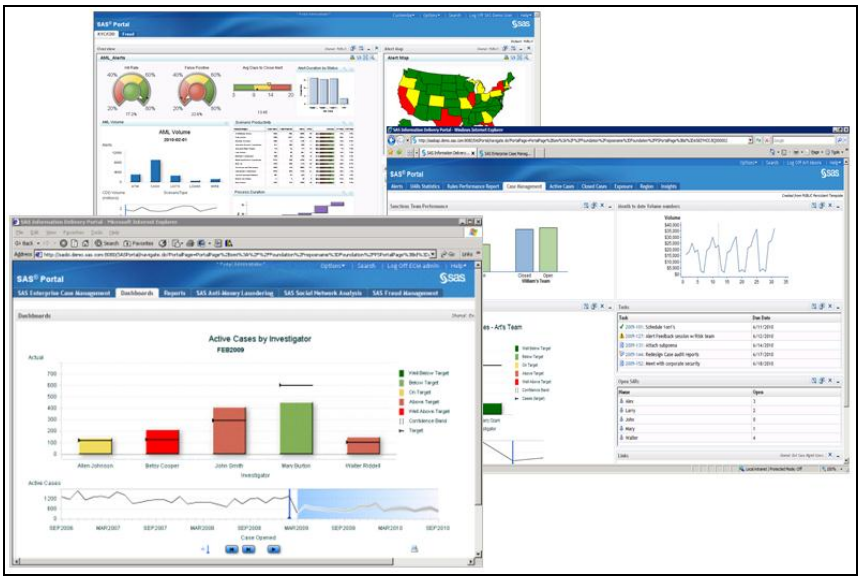


Figure 11. Example Dashboards and Reports

MULTI-CHANNEL ALERT AGGREGATION

Imagine the power of a being able to have multi-channel events consolidated and dispatched into a centralized case management hub. And, what if you could automate brokering-out of the required workflows for the multiple-event generated cases? And in some situations, what if you could use straight-through processing to automatically document and adjust a customer's risk ranking or even generate a required regulatory report?

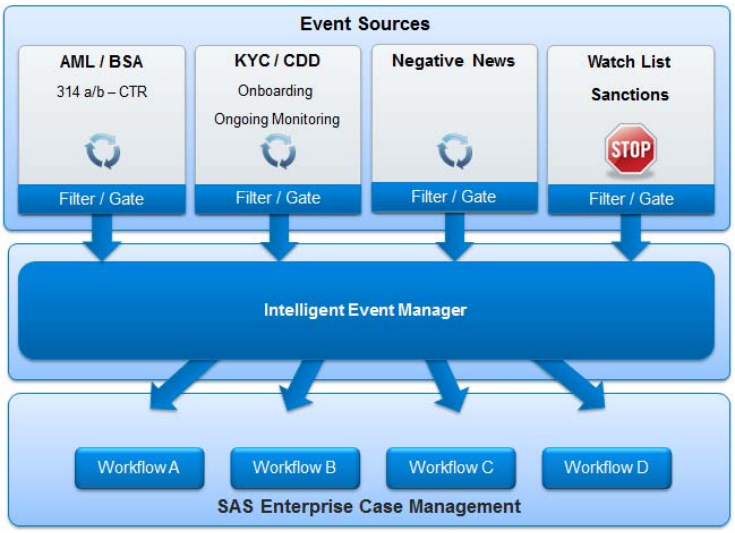


Figure 12. Multi-Channel Event Detection and Processing

With the power of SAS, this can be a reality for organizations striving to reach this level of optimization and efficiency. By using the SAS® Financial Crimes Suite approach, SAS's data integration capabilities, business intelligence based reporting, and robust workflow and case management, the vision depicted in Figure 12 is possible. This represents a strong approach to "knowing your customer" and staying very much in-tune when further due-diligence is needed in the customers' risk rankings. However, it also gives that 360 degree of the customer that is "the nobel goal". This topology could be expanded, providing great customer intelligence to marketing, product development, compliance, risk, and multiple other stake holder departments within the organization.

CONCLUSION

SAS has provided customers with the ability to derive customer intelligence from their information and behavior for over 30 years. The same techniques of data management, data correlation, business rules, and predictive models can be used to combat financial crime; as is used to predict what products customers are most likely to purchase or where they will most likely go on vacation, for example.

SAS is dedicated to providing financial institutions with specific business solutions that address the task of uncovering high-risk relationships by virtue of providing a BSA/AML solution (since 2003) and providing enhanced functionality for customer risk ranking since 2008. Fraud and compliance is specifically stated on the top five focus areas for SAS, year after year. Significant investments are made in this area by SAS R&D each year to keep our fraud and financial crimes offerings modern and relevant to emerging threats and regulatory expectations.

In response to a high market demand that is due to increased focus by regulators on financial institutions, SAS continues to enhance and bring to market powerful supporting technology that is specific to this area. It does this by having a robust and flexible "know your customer" program through proper Customer Due Diligence.

The dedicated Customer Due Diligence solution, with its next enhancement release that is due in mid-2013, will bring together and further enhance an institution's ability to deploy, maintain, and explain the type of program that regulators are coming to expect. The enhanced CDD module will accomplish the following tasks:

- set a high standard in the industry, giving institutions a powerful ability to manage customer data
- perform quick and accurate initial risk ranking
- deploy and manage sophisticated business rules and scoring models
- alert investigators to customer changes in behavior or potential risk classification changes
- drive efficient CDD/EDD investigations and workflows
- close the loop by providing up-to-date customer risk rankings back into the risk-based monitoring program

REFERENCES

Bohannon, tom. "Institutional Research and SAS!" Web Site/Blog - December 20, 2011. Available at: (http://blogs.sas.com/content/academic/2011/12/20/institutional-research-and-sas/).

de Ville, Barry "SAS author's tip: The basics of decision trees" Web Site/Blog - November 8, 2012. Available at: (http://blogs.sas.com/content/publishing/2012/11/08/sas-authors-tip-the-basics-of-decision-trees/).

ACKNOWLEDGMENTS

I would like to thank Mr. Jay Flowe for his consultation in the process of producing this paper.

RECOMMENDED READING

Joint Release: Financial Crimes Enforcement Network, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, Securities and Exchange Commission; Guidance on Obtaining and Retaining Beneficial Ownership Information (March 5, 2010)
www.fincen.gov/statutes_regs/guidance/pdf/fin-2010-g001.pdf
• FinCEN Guidance: Special Due Diligence Programs for Certain Foreign Accounts (March 2009)
www.fincen.gov/news_room/rp/files/Special_Due_Diligence_Program.pdf
• Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act Anti-Money Laundering Examination Manual
www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm
• FinCEN U.S. Money-Laundering Threat Assessment
www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf
• FinCEN Guidance: Potential Money Laundering Risks Related to Shell Companies
www.fincen.gov/AdvisoryOnShells_FINAL.pdf
• FinCEN Guidance: The Role of Domestic Shell Companies in Financial Crime and Money Laundering (November 2006)
www.fincen.gov/LLCAssessment_FINAL.pdf

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Scott Wilkins
SAS Institute Inc.
SAS Campus Drive
Cary NC, 27513
919-531-6935
Scott.Wilkins@sas.com