The Infrastructure of Compliance
Building a Bridge to Vendor BSA/AML Solutions

The recent guidance (warning, really) from the FDIC[1] on the need for financial institutions to perform due diligence when selecting anti-money laundering (AML) software puts the proof of compliance burden squarely on the financial institution. It also points to the need for an enterprise solutions architecture, one that builds on existing structures—how things really are—rather than on pushing through a vendor package. While there is no doubt that commercial off-the-shelf (COTS) products play an integral part in AML compliance, there is also no doubt that AML software depends on the quality and uniformity of data supplied by the financial institution. The systems, data, processes and organizational structure of the enterprise form the infrastructure of compliance, and these must be understood and documented to ensure that the COTS "solutions" are just that. If, for example, a bank wanted to institute an automated customer risk scoring system, there would be many questions that needed answers before software could be selected and installed...

Following the well-publicized negative Bank Secrecy Act (BSA)/AML assessments of Riggs, AmSouth, ABN Amro and others, a rapidly growing bank decided that they needed to beef up their BSA Program. The Bank was determined to avoid the reputational risk suffered by these banks. They were also committed to fixing last year's negative OCC citation for failure to implement an account profiling/risk assessment program. Taking the lead, the Bank's Risk Management AML Committee met to design the ultimate Know Your Customer (KYC) and Enhanced Due Diligence (EDD) program, and they determined that "the system" should include a 5-point weighted scale that risk ranked customers on the following criteria:

- Age
- Account class (private banking, corporate, retail, student, employee, etc.)
- NAICS[2] code (type of business), if commercial
- Address
- Product type (checking, savings, etc.)
- Debit card issued
- Credit card issued
- Account relationships (other accounts with Bank)
- Duration with Bank (how long a customer)
- Citizenship
- Employment status
- Source of income
- Source of wealth (if private banking)
- Beneficial ownership on other accounts.
- Homeownership
- Credit score

[1] *Computer Software Due Diligence: Guidance on Developing an Effective Computer Software Evaluation Program to Assure Quality and Regulatory Compliance*, November 16, 2004
[2] North American Industry Classification System

The risk ranking was to be performed as part of the Customer Identification Program (CIP), after OFAC and other watch list screenings, but before account activation. On a scale of 1 to 5, 1 being excellent and 5 being unacceptable, the plan was to decline to open all 5s, and flag accounts ranked 3 or 4 as medium and high risk for increased scrutiny in the transaction monitoring system. They weren't yet sure how they could risk score the existing customer base and how "the system" would handle ongoing risk scoring.

Upon receiving the AML Committee's mandate, other divisions in the Bank were somewhat concerned. While they agreed wholeheartedly in principle with the AML Committee's recommendations, they realized that there were significant roadblocks to overcome. IT needed to do research to determine if all the data fields were captured and stored, and if stored, in which system(s). Retail Banking, Commercial Banking and Private Banking were concerned that account opening would be a problem if too many questions were asked. Deposit Operations, whose daily work consisted of analyzing various reports to determine whether a Suspicious Activity Report (SAR) should be filed, wondered how a customer's risk rating would affect their account/transaction monitoring system as well as their fraud workload. And everyone wanted to know how the risk rating would be updated as customer circumstances changed, and how much a "total solution" would cost.

The ultimate goal of the Bank was to find a "seamless," "turn-key" vendor solution that could solve all the Bank's customer risk scoring needs—from CIP to SARs—and implement "the system" in six months or less. To this end, the Bank formed an implementation Project Team to scope the effort and begin the vendor search. Because of the condensed time frame, they decided to fast track[3] the effort by conducting the vendor search and the internal systems and process architecture assessment simultaneously. The vendor research group analyzed eight AML vendors, looking at enterprise "horizontal" solutions as well as more narrowly focused functional solutions, with a focus on risk scoring. (The Bank already had a good CIP service as well as a transaction monitoring system.) The vendor research group quickly decided that an enterprise solution would be too costly and take too long to implement, leading to the decision to work with the existing internal systems and outside vendors to fashion a solution.

In the meantime, the systems and process architecture group was at work evaluating the Bank's existing AML capabilities. What they discovered is represented in the Table below. The gaps in the ideal solution were quickly apparent based on the "Sometimes," "No," "If Provided," and "Sort of" responses. They immediately saw that some of the data they considered integral to assessing risk was not available. Type of business, for example, was captured only sometimes for business accounts, and it turned out that this wasn't a database issue, but a procedural one. They resolved to fix that through their Policies and Procedures immediately, because they were aware of the recent problem

[3] A project management method of compressing the project schedule by overlapping activities that would normally be done in sequence, such as design and construction.

with an ice cream store in Brooklyn and the large bank that failed to detect suspicious activity.[4]

They also immediately noticed a problem: If the goal was to risk score new customers, they needed to capture all relevant information at account opening. If the goal was also to perform ongoing risk scoring of existing customers, not only did they need all the same information, they also needed a logical method of updating, storing and using the risk rating.

Account Risk Scoring Criteria ***Availability of Data***					
	How Obtained		***Where Stored***		
Risk Scoring Criteria	At Account Opening (Bank)	Account Opening (Vendor)	Deposits	CRM	Existing Transaction Monitoring System
Age (DOB)	Yes	Yes	Yes	Yes	Yes
Address	Yes	Yes	Yes	Yes	Zip code
Account class	Yes	Yes	Yes	Yes	Yes
Type of business	Sometimes	No	If provided	If provided	If provided
Product type	Yes	N/A	Yes	Yes	Yes
Debit card	Yes	N/A	Yes	Yes	Yes
Credit card	Yes		Yes	Yes	Yes
~~**Account relationships**~~	Yes	N/A	No	Yes	No
~~**Duration with Bank**~~	Yes	N/A	No	Yes	No
Citizenship	Yes	Yes	Yes	Yes	Yes
~~**Employment status**~~	Sometimes	Sometimes	No	If provided	No
Source of income	Sometimes	Sometimes	No	If provided	If provided
Source of wealth	Sometimes	Sometimes	No	If provided	If provided
Beneficial owners	Yes	No	Yes	Yes	No
Homeownership	N/A	Yes	No	Sometimes	No
Credit score	N/A	Yes	No	Yes	No
Derived Risk Score	N/A	Maybe	N/A	No	Sort of

[4] Ref the lead Wall St. Journal article of December 30, 2004: *As Investigations Proliferate Big Banks Feel Under the Gun.*

For account opening/CIP the Bank currently used a well-known data aggregation and credit scoring service that worked well. It performed OFAC and other watch list screening, and it was constantly adding new sources to its database. It also performed sophisticated fraud pattern analyses against its databases using advanced analytics from the intelligence community. What it didn't provide was a Derived Risk Score using the Bank's criteria and weighting system. This was easily solved, and the risk scoring was simplified. Upon further reflection of what constitutes a risk defining criterion, the AML Committee decided to eliminate Account Relationships, Duration with Bank, and Employment Status from the mix. (Represented on the Table with strikethroughs) The Bank also persuaded the vendor to return risk scores based on the Bank's criteria. The risk score would then be "attached" to the account database in the Deposit system using a previously unused field in that system. The risk score would also be made part of each transaction so it could be used by the transaction monitoring system. Understanding that customer non-transactional profiles change, the Bank decided that the entire customer database would be run through a modified CIP analysis on an annual basis. That left the biggest gap the inability of the transaction monitoring system to store and use the derived risk score.

The Bank's transaction monitoring system was a stand-alone system that took daily feeds from the deposit accounts. Its method of analysis was to look at current transaction activity against a system-created profile based on historical activity. If a customer's transactions suddenly looked out-of-profile, an alert would be issued for follow up. It did not have the ability to automatically create a risk score based on the criteria the Bank wanted, but it did have a field that could be used to store a previously defined score. The Bank was able to work with the vendor to create a customized approach. The risk score would be added to the database and the vendor would modify the system to create a new method of transaction analysis and profiling.

With the implementation of a new procedure to capture the type of business (NAICS) at account opening, the modification negotiated with the external service to return the risk scoring method they desired, and the vendor's software changes to the transaction monitoring system, the Bank felt that they had an effective, risk-based anti-money laundering program. Through the project management technique of fast tracking, they met the Bank's AML mandate on time and within budget.

Unfortunately for the Bank, though, the story doesn't end happily. While they conducted admirable due diligence on the functional capabilities of every vendor in their price range, and designed and clearly documented the architecture of the AML solution, they neglected the vendor management side of due diligence. Had they read *Money Laundering Alert,* the *Wall St. Journal*, etc., they would have discovered that their chosen vendor, EnterpriseAML, was about to be acquired by one of the very expensive "total solution" AML companies who would soon be phasing out the product the Bank had painstakingly customized. They had to go back to the drawing board, but this time they knew exactly how all required BSA/AML elements mapped to their own systems.