

Validating BSA/AML Technology – No Longer Just Compliance Concerns

For those financial institutions utilizing BSA/AML/OFAC software for various facets of your BSA/AML/OFAC compliance processes, the days of bank examiners focusing on non-IT aspects of your BSA/AML/OFAC program have passed. A new breed of BSA/AML Examiner, skilled in technology and automation, has come on the scene, and they will be asking additional questions that have not been typically asked of BSA/AML personnel in past examinations. What can you do to be prepared?

By Christopher Price
Metavante Regulatory Services
(407) 831-3001

Dateline February 2009

BSA/AML examiners have typically followed a standard workflow pattern for examining financial institutions' BSA/AML/OFAC Compliance Programs. Offsite preparations include reviews of the target institution's BSA/AML/OFAC Risk Assessment, prior Report of Examination, and the most recent independent annual review of the BSA/AML/OFAC Compliance Program. Additionally, examiners will query the FinCEN SAR and CTR databases for reports that have been filed by the target institution. Once the onsite portion of the examination has commenced, examiners will apply the risk-based approach by focusing most of their efforts to areas deemed to be high risk, whether that risk be inherent risk as cited in the BSA/AML/OFAC Risk Assessment, or residual risk due to areas of weak internal controls uncovered from the independent annual review and/or prior examination.

Examiners will continue to apply a risk-based approach and utilize many of the tools and techniques they have conventionally used in past examinations. However, with the explosion of BSA/AML technology that many financial institutions are now using to risk score customers, monitor for customer profile deviations and questionable activity patterns, file regulatory reports and screen for potential OFAC, Section 311 and other sanctioned data party matches, the bar has been raised. Many BSA/AML examiners have been recruited from the ranks of IT examination specialists who are now being cross-trained in BSA/AML in order to keep pace with information technology developments in the world of BSA/AML.

Examiners must be assured of the functional capabilities of compliance automation, and will take steps to determine that functionality meets industry standards, best practices, legal and regulatory requirements, privacy requirements, and basic sound internal controls. With the need to further validate the automation being employed, it is now incumbent upon financial institutions to provide evidence that these concerns are being addressed in their BSA/AML/OFAC automated solutions.

The following list, though not exhaustive, comprises a number of issues that financial institutions should consider in addressing examiner concerns:

1. Validating data integrity – are all of the required data from the core banking system, wire systems, and any other source systems mapped into the AML software?
2. Availability of mapping documents detailing all fields to be mapped from source systems into the AML software, and what fields they are mapped to;

3. Process controls to ensure that required data continues to flow from source systems to the AML software, including evidence of processing schedules;
4. Access rights controls, including segregation of duties and dual controls over various functions in the AML software; and super-user access. Examples include the right to review an alert or case vs. the right to approve an alert or case that the reviewer designates "suspicious," the authority to change a customer's risk classification manually in the system, and the authority to approve an updated customer profile that exceeds the prior period profile by a percentage beyond the user-defined tolerance;
5. Audit features allowing for view-only access by audit and examination personnel;
6. Date and time records for all user-related activities;
7. Evidence of testing the validity of user-defined parameters for automated customer profiles, risk classifications, monitoring rules, alerts and cases, sample filed reports, etc. on a test server;
8. User-defined and vendor-defined (default) parameters for algorithms used to screen customer files and transactions for OFAC, Section 311 and other sanctioned data regulatory requirements;
9. Documented evidence of training conducted on the use of the software by the respective vendor; and
10. Privacy controls compliant with Gramm-Leach-Bliley and Section 314(a) suspect information safeguards.

BSA/AML personnel will need to communicate these concerns with IT personnel, Internal Audit and those responsible for information security/vendor risk management in order to ensure that all related parties are kept informed and are prepared to provide any input required of them.

By considering these and other possible questions, you can provide assurance to your examiner that you are managing both the operational risks that come with AML technology as well as the compliance risk management concerns that are reflected in the use of your AML software.