AML Independent Audit: Independent Verification and Validation

By Laura H. Goldzung, CAMS, CFE, CFCS, CCRP and David DeMartino, CCRP

Laura H. Goldzung, CFE, CAMS is President and Founder of AML Audit Services, LLC, an anti-money laundering and fraud boutique consultancy specializing in independent testing and compliance consulting services to financial and nonbank financial institutions. Additional expertise includes domestic and international training, design and development of BSA/AML compliance programs, risk assessment and analysis, remediation and corrective action programs, expert witness testimony, and CFPB compliance benchmark assessments.

David DeMartino, CCRP, is an independent consultant with more than 30 years of industry experience. In his former role as equity partner and co-founder of Prime Associates, Inc., he helped to pioneer the regulatory compliance technology space by designing and deploying AML, EDD, and OFAC technology in 1999 and became the leading provider of USA PATRIOT Act technology for a US client base of over 600 banks, brokers, insurance companies and credit unions located in the US and globally. In 2005, Mr. DeMartino engineered the sale of Prime Associates to Metavante Corporation.

Anti-money laundering programs require an audit function to test the efficacy of the program under the regulations; this is one of the four pillars of AML compliance.[1] Some important components of AML audit are review of the firm's management information systems, review of monitoring reports, and review of the techniques and tactics applied to monitoring activity and reporting. When it comes to asking important questions about your firm's technology, independent auditors will expect you to know the answers.

Transaction monitoring systems (TMS) improve a firm's capability to identify suspicious activity more effectively than manual monitoring. Many broker-dealers, along with most financial institutions, use AML monitoring systems that provide transaction monitoring, enterprise risk assessment, customer risk rating, and alert/case scoring. Smaller firms perform manual monitoring using reports furnished by the clearing firm along with other tactics.

The use of surveillance monitoring software presents a risk if the system is not working as designed or is configured incorrectly. Thus, the independent review may have a less than favorable outcome. Therefore, systems must be correctly configured and periodically adjusted. Employing a third party provider to conduct a system verification and validation is a best practice financial institutions undertake periodically, usually on an annual basis.

Guidance from the OCC

In April 2011, the Office of the Comptroller of the Currency (OCC) published supervisory guidelines on Model Risk Management,[2] offering comprehensive guidance around sound model risk management processes including governance, inventory, development, implementation, and use, tuning, and validation. Simply put, the guidance suggests a roadmap to ensure that risk models

are properly developed, documented, tested, implemented and used. Firms might be inclined to say this guidance is just for banks. However, large, complex broker-dealers are already following this guidance to some extent, and other broker-dealers that are mid-sized or smaller are looking at following the guidance to the extent practicable for their firms. Regardless of who you are regulated by, this guidance is a good tool

FFIEC

The Federal Financial Institutions Examination Council (FFIEC), established in 1979, is a formal interagency body empowered to proscribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions.[3] The Council publishes an examination manual, known as the Bank Secrecy Act/Anti-Money Laundering Examination Manual ("the FFIEC Manual") which is considered the gold standard from which regulators pattern their AML examinations and from which audit professionals draw from for independent AML audits. It serves as a good reference for compliance managers to understand the methodology of an AML examination.

Important components of AML audit are review of the firm's management information systems, review of monitoring reports, and review of the techniques and tactics applied to monitoring activity and reporting.

The Council also publishes the FFIEC IT Examination Handbook InfoBase providing delivery of introductory, reference, and educational training material on specific topics of interest to IT professionals in the AML compliance arena. The IT Handbooks are updated and maintained electronically using InfoBase.[4] There is an audit handbook available which provides good guidelines in conducting IT audit.

Reliance on Clearing Firms

Most or all introducing firms rely on the clearing firms' AML resources to assist them in managing their AML programs, by providing tools including exception reports, alerts, and various processes applied to transaction activity. That reliance does not relieve the broker-dealer of the ultimate responsibility for conforming to requirements under the Bank Secrecy Act (BSA); the firm is ultimately responsible for the design, maintenance and adequacy of its AML program.

Independent Verification and Validation (IVV) for AML Compliance

Conducting a third party IT audit requires attention to the detail, just as it does when employing a specialist to conduct the AML compliance audit. It is paramount to ensure that your firm's technology system is configured correctly prior to relying on it for combating money laundering and/or terrorist financing. If AML software is implemented incorrectly and/or ineffectively, then suspicious activity monitoring and reporting can be totally inaccurate. The goal is to determine if all critical pieces of data that would affect the monitoring processes or risk profiles of the system are correctly flowing into the system.

A key method with which firms can confirm that their systems are configured correctly is through an outsourced system verification and validation. As with any outsourced engagement, the firm must determine if the scope of the outside review is adequate. Since the scope of any type of AML review can dramatically differ from one provider to another, making sure the scope is comprehensive is essential. The scope should consist of the following elements:

- Transaction Code Mapping Verification verifies that all transaction codes from the core system (the firm's management information systems) are properly mapped and coded to the AML system.
- Transaction Coverage Verification involves the extraction of a sample of core transaction data and automated monitoring system transaction. The data from the core system is reconciled to corresponding period automated monitoring system data to determine if there are any

significant gaps. Ensuring that the sample selection is comprehensive in size will assist in the effectiveness of the validation process.

- Alert Processing Validation is an analysis of the configuration of the automated systems alert engine. A sample of alerts is selected in which the firm will replicate the parameters of the alerts and compare the results against the system to determine if output is accurate.

Other Considerations

Regardless of whether you are implementing a new system, it is important to consider any of the following as possible reasons to enlist a third party IT audit to verify and validate your system:

Many broker-dealers, along with most financial institutions, use AML monitoring systems that provide transaction monitoring, enterprise risk assessment, customer risk rating, and alert/case scoring.

- How often do you recalibrate your AML technology?
- Are you keeping up with the latest versions released by the vendor?
- Have you activated critical new detection methodologies based on the new releases?
- How thorough is your internal testing when you integrate new financial instruments into your AML technology?
- Is your internal audit staff skilled enough to understand the functionality of your AML technology in order to conduct a proper audit?
- How are you addressing your false positive rate ?
- Have you verified that the data mapping is accurate and consistent from your core systems into your AML technology?
- Do your systems parallel your peer group's systems and follow industry best practices?
- Have you checked that your systems are protected against cyber security attacks?

Converting Systems and Processes

When converting from a manual system to an automated system, it is a best practice to conduct a parallel monitoring exercise. This ensures coverage until the new system is verified and validated.

The adequacy of alerts and thresholds generated by the system is subject to periodic review by the firm. Sometimes too many alerts will dilute the overall effectiveness of the monitoring process which can be as bad as too few alerts. The objective of the review is to validate and support the assumptions implemented in the monitoring process to ensure they remain consistent with the transaction population. Maintaining an adequate monitoring system will provide a strong foundation for generating alerts and exceptions from which to identify unusual and suspicious activity, and this ensures that suspected money laundering and terrorist financing activities are timely reported to authorities.

It is critical to understand that the regulators are very focused on technology validations. Examiners commonly comment on this subject, focusing on recalibration of the technology, data analytics, and now even cyber security that must be maintained to address the ever-changing risks of the financial institution. One of the most critical elements is upgrading your technology when upgrades become available. Keep in mind that 90% of vendor upgrades have to do with creating better ways of detecting suspicious activity.

Finally, it is very important to select a proper provider to perform your validation. You need to look for a provider that is knowledgeable about the technology, compliance, the process, and your business, and that has strong model validation methodology.

Failure to maintain the firm's AML technology by not having a independent verification and validation performed could put your firm at an unnecessary risk where you end up hoping that the examiners will not be thorough in their review of your firm's technology. In this regulatory environment, this is not a recommended position for any firm.

Conclusion

The goal of an AML audit is to determine if all the critical pieces of the program are reasonably designed and operating effectively. An effective AML compliance program requires people, processes and technology to work together.

Optimizing your AML systems will reduce the risk of potential transaction lookbacks, reduce costs by reducing false-positive alerts, and give you more assurance that AML systems are more accurately capturing the right surveillance data.

Regardless of the level of automation your firm employs to manage its AML compliance, conducting verification and validation will ensure that systems are working efficiently and effectively, confirming that the AML program will continue to effectively identify potentially suspicious activity for analysis and reporting.

ENDNOTES

1 FinCEN regulations codify the four current core requirements of a required financial institution's AML program and are often referred to as the "four pillars."
2 See OCC 2011-12 http://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf
3 http://www.ffiec.gov/about.htm
4 http://ithandbook.ffiec.gov