Managing AML Audit Expectations

By Laura H. Goldzung

Getting ready for any examination brings about the initial cringe – followed by the thought of all the documents to produce, interviews to go through, findings to read, responses to write – it's like having that yearly physical we all try to avoid – the lab work, tests, appointments, waiting time, results, and, finally the examination! And then it starts all over again next year.

I haven't met an AML compliance officer yet who enjoys the AML audit process, but nearly all those whom I have had the pleasure to meet or know take it very seriously. We all know why it is serious business, as recent headlines have shown. AML inadequacies and some outright failures have produced myriad enforcement actions, civil penalties, censures, exorbitant fines, and enough case studies to review for years to come.

So how can you best manage expectations for your next or any AML audit? My first and best advice is to always be in a state of audit readiness. Following are explanations around specific key areas and expectations with respect to them. The requirement is to have an "independent audit function to test programs."[1] For purposes of this discussion, the words audit, review and independent test are interchangeable.

The Pivotal Pillar

The AML regulation promulgates the four minimum requirements for an AML compliance program including (1) policies, procedures and internal controls, (2) designation of compliance officer, (3) training for appropriate employees, and (4) an independent audit function to test program. Of the "four pillars" requirements for AML compliance programs, audit is perhaps the most important, simply because it provides reasonable evidence that the program is either working or has flaws. Is any AML program perfect? Of course not, and that's why the regulators leave it up to you to design your own risk-based program. There is no "operators' manual," as only the firm knows its business best and can therefore apply appropriate measures to comply with the requirements.

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.

A Key Driver

Let's begin with the key driver of your AML program – the risk assessment. This discussion of risk assessment is important because many institutions, including broker-dealers, don't have one. The AML risk assessment is not required by law or regulation, but it is a regulatory expectation and indeed a best practice in order to establish a risk-based compliance program. How else would you measure risk if you didn't take an exhaustive inventory of your products and services, customers and the geographies where you conduct business? It only makes good business sense, and so it follows that the AML risk assessment informs the overall risk management[2] program of the entire firm.

The AML risk assessment provides the roadmap to develop the internal controls needed to protect the firm from money laundering and terrorist financing risk. It lays the foundation, no different than cement blocks forming the foundation for a structure. Just as you begin to lay the building blocks for the structure, so, too, do you layer the policies and procedures that will become your AML compliance program. Simply having the four pillars in place does not an effective compliance program make. Surely, painting the exterior of your cement structure to look attractive doesn't mean that it's structurally sound.

So how can you best manage expectations for your next or any AML audit?

You've built your structure, but now you need effective tools and skilled craftsmen to operate them to build out the interiors. You also need to install various utilities and meet specified building codes, and municipal officials need to check the work to ensure that it was done properly.

The AML compliance program is no different really, beginning with the foundational risk assessment, the development of the program elements, and the implementation using the talent and tools to achieve its effectiveness. Now comes the examination of its efficacy, and therein lies the AML audit, that extra key step included in the Bank Secrecy Act ("BSA"), and fully described in the FFIEC Examination Manual,[3] viewed as the gold standard guide for BSA/AML audit.

The AML audit function is meant to review and test whether the program elements are operating sufficiently in accordance with the firm's risk assessment, policies, procedures and internal controls. It's a reconciliation of sorts – ensuring that program elements are adequate and that what you say you do is in fact what you do.

Risk Assessment

The first thing the auditor reviews is the risk assessment – to establish whether it's reasonably designed to inform your policies and procedures. FINRA, like most regulators, has an expectation that the risk assessment provides for a reasonable approach to the design of the AML compliance program.[4]

> The firm's risk assessment is expected to encompass all business lines across all activities and legal entities. Risk assessment comes in all shapes and sizes and complexities, depending on your firm's size and its business. If the assessment is comprehensive, meaning that it contains a detailed analysis of the data identified to arrive at risk conclusions, is well organized, clearly describes all areas of the firm's risk, and follows with a plan to assess the internal controls on a periodic basis, it will demonstrate its reasonableness to manage the AML risks of the firm and drive the basis for the AML compliance program. There is no "one size fits all" methodology.

It is important to note that if you don't have a risk assessment, the auditor will formulate one on its own. Why? Primarily, it must do so to establish whether the policies and procedures are robust enough and include a system of internal controls to demonstrate the program's adequacy.

Some cited weaknesses in risk assessment have included:

- Policies lacked specified frequency of updates
- Lacked methodology for assigning risk levels to customers
- Failed to consider all major categories of risk
- Policies and procedures weren't commensurate with risk profile of the firm

Not only does the risk assessment form the basis of your program, it also informs your training program, and it drives the frequency of periodic testing of internal controls. Additionally,

the risk assessment informs the independent audit by identifying the system of internal controls that results in the development of the policies and procedures. Let's look at how that plays out.

Policies and Procedures

While regulations form the basis of all requirements, policies are high-level statements that are influenced by the regulations and based on the firm's risk appetite. The procedures set forth the processes for how the firm will implement those policies in order to comply with the regulations, and the internal controls form the framework to controls risks in order to comply with the program.

The audit function will provide for a thorough review of the written program to ensure that the four pillars including policies, procedures and internal controls, the compliance officer and compliance department, independent testing requirements, AML training and frequency are indeed implemented. It will also review management oversight, and regular updating to address recent regulatory updates and guidance. The review will look for a description of the various types of money laundering and compliance with BSA/AML laws and regulations including FINRA Rule 3310.[5] Other considerations will include the CIP/KYC program, identification of higher risk activities, businesses and foreign countries commonly associated with money laundering, description of monitoring systems and tools, BSA reporting, law enforcement requests, Sections 314, record keeping and retention requirements, data recovery and/or business continuity plans. Additionally, the audit function will review third party reliance agreements.

Tip: Ensure that the AML program is aligned with the WSPs. Think of the AML Program as one dish in the stack (of WSPs) and have ready access to it. Always be in a state of audit readiness by verifying that your policies and procedures and internal controls are current and scheduled to be reviewed periodically throughout the year. Ensure that they are approved, and that the approval is dated, by Board/Senior Management.

AML Compliance Officer & Compliance Department

The audit will look at the credentials of AMLCO and other key personnel in the AML process. Does the department have enough staff? Is there a compliance committee? Among items to review are the AML process map including touch points around the firm where controls are implemented or suspicious activity may arise (e.g., receptionist opens mail and receives checks before passing to operations dept.). Further, the auditor will review the tools and resources to manage the day-to-day AML operations and test the tactics used to monitor activities. The auditor will particularly focus on the training of the compliance department personnel in forming a conclusion as to the adequacy of the AML resources as a whole.

Tip: Have a tactical plan for periodic review of various activities, processes and controls. Plan out what critical tasks are managed daily, weekly, monthly and quarterly, how they are documented, who will do each, and how the results will be communicated to senior management.

AML Training

The adequacy of the AML training program ensures that all appropriate employees understand their responsibility for compliance. The comprehensiveness and accuracy of the training is considered to ensure that content is relevant and consistent with requirements, and that it provides context around the business of the firm and the applicable AML risks the firm may encounter in its day-to-day operations. The audit considers this in a number of ways.

An auditor's interviews with key AML personnel will reveal whether they have been properly trained, if they understand the compliance program requirements, and if they understand their responsibilities.

Personnel are expected to be trained in the regulations as well as in the firm's policies, procedures and processes, and the training must be tailored to the job function. The appropriateness of targeted training is expected for specific duties and responsibilities. The compliance officer is expected to have a higher level of training, and the Board/Senior management should be trained on regulatory updates and guidance, and any new developments in the BSA's implementing regulations, as well as any changes to FINRA guidance or expectations regarding AML compliance. The audit function also includes a review of the tracking and monitoring system, to ascertain frequency, method, training dates, and other relevant details. Procedures for managing new hire training with a period

certain for training from date of hire are also reviewed, as well as capturing attestations or sign-in logs and certificates of attendance.

Note to firms that add a couple of slides to the annual compliance meeting presentation and call it AML training: A firm's employees are the first defense in spotting suspicious activity, whether through processes or behaviors, and the better they are trained, the greater the control of AML risk. A good rule of thumb is to provide three training events per year. This could include circulation of the updated compliance manual, an online scenario-based module, and a few slides in the annual compliance meeting or other business meetings. Don't minimize the importance of the AML training!

Tip: If you can't get the attention of senior management or the Board try circulating a copy of some recent cases and suggest that Board training will demonstrate further AML governance. Remind them that AML risk resides with the Board. There have been plenty of enforcement actions[6] citing training and weak governance to use as case studies. Don't allow your firm to become one of them.

Independent Audit & Test

Gone are the days when another person in the firm can perform this independent review, as there is simply too much at stake. FINRA looks at the level of experience and expertise of the provider and the quality and quantity of testing, as all regulators should. Recent cases have identified such testing problems as lack of independence, insufficient testing and results, unidentified root causes, lack of experience, limited scope, and the list goes on.

The AML risk assessment is not required by law or regulation, but it is a regulatory expectation and indeed a best practice in order to establish a risk-based compliance program.

Whether internal audit performs the function or you engage an external specialist, be sure that policies adequately describe the frequency of testing and the requirements for engaging an external provider. Be sure that the individuals conducting the audit have the knowledge, experience and skills to properly plan, scope, review and test all the relevant elements necessary to state whether your program conforms to requirements and is adequate. The audit must be commensurate with the risk profile of the firm, provide sufficient documentation, provide an overall conclusion about the adequacy of the program, and working papers must be made available.

It is important to remember that internal audit has a responsibility to provide the audit function for the whole firm and their remit encompasses all other regulatory audits as well. Therefore, it is important that internal audit personnel are adequately trained on BSA/AML obligations. It is not uncommon for policies to call for a periodic specialist to co-source with internal audit.

Tip: Don't buy an audit on price – buy on expertise and value. The provider will be your AML partner in delivering the audit process, not an adversary. This provider can be your lifeline to current AML practices if you don't have in-house expertise. Be sure that your provider has the credentials, experience, current AML knowledge, and provides a proper proposal including scope of work, deliverables, timings, and terms. The cost of audit should be included in your annual budget.

CIP/KYC Program

Strong on-boarding processes are the objective here, and to ensure that the firm is in compliance with the requirement for customer identification requirements and foreign correspondent and/or private banking relationships and related due diligence. The audit program looks to determine whether the CIP is implemented for all new customers and contains the requisite elements, and whether record keeping is in order. If there is reliance on another institution to verify identification requirements, i.e. the clearing firm performs OFAC checks – then that too is examined by reviewing contracts and agreements with third parties. Additionally, auditors will examine any foreign correspondent account relationships to ensure that the firm prohibits shell banks from maintaining correspondent accounts. Private Banking accounts for foreign individuals or politically exposed persons ("PEPs") are another segment that require specific diligence.

Tip: Be sure policies and procedures are robust enough to mitigate higher risk activities and customers. Ensure that records maintained are clear and easily readable, i.e. drivers' licenses/passports.

Customer Due Diligence (CDD/KYC) and Enhanced Due Diligence (EDD)

The audit function will review the firm's policies and procedures for documenting due diligence and for performing enhanced due diligence for higher risk activities and customers. Often firms' conduct these activities but don't document them. Ensure that you have a policy and process to obtain and document any diligence performed in day-to-day operations.

Tip: Be sure to have a policy and procedure for the EDD you will conduct. The plan should identify under what circumstances you will conduct EDD, and how you will continue to monitor or set time limits to discontinue EDD, or exit the relationship, if appropriate.

Monitoring Accounts for Suspicious Activity

This is another place where the risk assessment plays a big role. The audit will look at policies, processes, red flags, controls, disposition of and documenting the closing of alerts, filters, reports and reviews that you have implemented around monitoring, particularly how you monitor higher risk activities and customers. Red flags, expected to be tailored to the business of the firm, must be described along with a clear escalation process. Auditors will ask about the monitoring systems used (automated systems are sometimes implemented through service agreement with the clearing firm) and question your rationale for setting alerts and filters, and fine-tuning. They may ask about regressions testing for your various data feeds, to ensure your screening tools are current, and may even ask for recent IT certifications or validations. You should always have the IT group at the ready and/or the clearing firm alerted, as auditors may ask for specific data to review in an Excel file, allowing them to analyze transactions for potential anomalies. This is then followed up with requests for documentation around specific transactions, to verify if your systems are identifying unusual activities.

Additionally, auditors may look to non-AML reports to identify trends among wash sales, changes of addresses, frequent wire transfers, frequent journals between accounts, trading outside of expected norms and inconsistent with KYC objectives, deposits of unregistered securities, excessive trading in low-priced securities and other activities.

Tip: Expect to discuss your parameters and thresholds for alerts, as well as the disposition of them, the experience level of your AML analysts so they can detect unusual activity. Be prepared to show evidence of documentation around your rationale for closing alerts/investigations.

Section 314 Information Sharing

Information sharing under Section 314[7] of the USA PATRIOT Act consists of information sharing with law enforcement under 314(a) and information sharing with other financial institutions under 314(b). The policies must be fully described and processes monitored to respond to 314(a) requests with provisions for confidentiality. A policy and procedure must also be in place for 314(b) sharing with other financial institutions by certifying annually with FinCEN, and it is done so under the safe harbor rules as set forth in the Act.

Tip: Be sure to have documented processes for each of these elements. Save a copy of the FinCEN certificate when registering for section 314(b) in a confidential file. Be sure that the process for documenting 314(a) aligns with your suspicious activity monitoring, as a positive match may be for someone for whom you have already filed a SAR.

Review of Specific Reports

The audit will examine Suspicious Activity Reports (SARs) to ascertain completeness of narrative (who-what-when-where-why-how) and timely filing, and the confidentiality of such filings and review the underlying investigatory documentation. Case management for non-SAR filings including the rationale for non-filings will also be reviewed.
If the firm accepts currency (most do not), then the Currency Transaction Report (CTR) will be reviewed for completeness and timely filing. Currency and Monetary Instrument Transportation Reports (CMIRs) used to report currency

received or transported in excess of $10,000 are examined, if applicable. Also examined are Reports of Foreign Bank and Financial Accounts (FBARs), which identify if the firm has an interest in or ownership over any foreign institution accounts of $10,000 or more.

Tip: Some failures in SAR reporting have included taking too much time to determine whether activity is suspicious resulting in delayed reporting, poor narratives lacking in why the activity is suspicious, and failure to take follow-up action. Be sure you have a policy and procedure in place following a SAR filing to place customers on watch list with more frequent monitoring and documenting that monitoring and its outcomes as evidence of enhanced due diligence. Multiple SAR filings must be monitored with consideration given to when law enforcement is notified and/or the relationship is exited. Following the 2nd filing, you should be looking to limit activities of the customer.

Recordkeeping

The audit will verify that certain records are maintained for the required periods; these include Funds Transmittals of $3,000 or more, Monetary Instruments where applicable, all of the above referenced reports, and other records regarding the extension of credit will also be tested.

Tip: Ensure that you have a record retention plan as well as a data recovery plan in place. Auditors will frequently ask to review it. Records should be made available within 24 hours of initial request.

Monitoring Employee Conduct

KYE is no different than KYC. Ensure that policies and procedures are in place for employees to carry accounts with the firm and to confidentially report non-compliance with the AML program.

Tip: Many smaller firms do not properly screen employees as thoroughly as they do a customer. Remember that knowing your employee can reduce a broad array of risk not just in the AML program but also in other aspects such as financial, occupational, operational and reputational risk.

Regulatory Examinations

Whether FINRA, the State, SEC or other functional regulator, the examiner will often identify scenarios consistent with your business and perform lots of diligence around it. They know plenty about you before they walk in the door. They will know how many SARs or other BSA-related reports you have filed. They do their homework and you must do yours. Be sure you have a corrective action tracking plan for any and all items revealed by a regulatory exam and all recommendations or deficiencies brought about from independent audits. The tracking plan will demonstrate your compliance with outcomes and provide documentation and activities for resolution and closing of items.

Tip: You may elect *not* to implement recommendations made by the independent audit provider, but best practices dictate that you document the reasons the firm is willing to accept the risk of not doing so. Addressing deficiencies or weaknesses in controls and implementing corrections followed by documented self-testing will avoid a citation by FINRA.

OFAC Review & Testing

OFAC regulations are not technically a part of the legal framework of BSA/AML, however, they are linked to BSA/AML for purposes of regulatory examination. Therefore, most independent testing engagements will include a review and test of OFAC unless specifically out of the scope of work (some larger firm will conduct a separate audit of OFAC requirements). OFAC screening is generally conducted at the time of customer onboarding, and at such times that cash management processes are undertaken, e.g., wire transfers, check disbursements, etc. The independent test will include a review of OFAC policies, procedures and the risk assessment, where applicable, processes for screening, if any reliance agreements are in place with third parties to perform the screening, and testing will be conducted. This is done by reviewing proof of acknowledgement of screening as part of the client file. Also included will be a review of controls for rejecting and blocking transactions when a positive match is confirmed, and that reporting is conducted in accordance with requirements. The test may also include documentation review as to how frequently you update SND and sanctions lists.

Tip: Avoid a common OFAC error – failing to use updated and complete lists. The FINRA OFAC tool is excellent. If you are using a third party provider to screen OFAC, be sure they are utilizing the most current and up-to-date lists. The firm is ultimately responsible for ensuring that third parties are effective in their delivery. Please note that the FINRA OFAC tool does not include PEPs (Politically Exposed Persons) screening.

While not an exhaustive list, these items reflect some of the key auditable elements you can expect in the AML audit. Remember that the goal of the audit process is to identify problems and help the firm to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance in its compliance processes. The audit identifies and highlights AML compliance weaknesses before they become examination issues or targeted areas for enforcement actions. It does so by providing an independent, objective assurance designed to add value and improve your compliance.

Finally, pay attention to recent enforcement actions and take the appropriate action to avoid becoming one of them!

ENDNOTES

1 Some covered sectors refer to the fourth pillar as independent review or test.

2 http://en.wikipedia.org/wiki/Risk_management

3 The FFIEC (Federal Financial Institutions Examinations Council) Examination Manual is viewed as the gold standard of AML examinations among AML professionals: http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_007.htm

4 FINRA begins its AML guidance with the topic of risk assessment: http://www.finra.org/Industry/Issues/AML/P011419

5 FINRA Rule 3310: http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=8656

6 Pamrapo Savings was cited for not having a formalized training program. Commerzbank failed to provide appropriate training to all staff regarding BSA/AML requirements. TCF Bank was cited for failure to provide periodic evaluations of employee knowledge. Biremis Corp. was cited by FINRA for failing to provide adequate AML training for employees.

7 USA PATRIOT Act Section 314(a) and (b): http://www.fincen.gov/statutes_regs/patriot/index.html?r=1&id=314#314