HOW AUDIT DEPARTMENTS CAN DEVELOP
AN EFFECTIVE AML PROGRAM

By Thomas Alessandro, CAMS

The views expressed in this paper are those of the author, and the author alone. The author is not necessarily representing the views or opinions of JPMorgan Chase
Executive Summary

When someone in the Banking community asks you what you do for a living, do you find yourself whispering, “I audit my firm’s AML controls?” We have all seen the head lines:

‘The Cost of AML Fines Soars to Over US $1 Billion in the Last Decade’¹,

‘HSBC Judge Approves $1.9 Billion Drug-Money Laundering Accord’²,

‘UK fines Standard Bank for lax anti-money laundering controls’³,

‘N.J. bank fined $8.2 million over federal money-laundering violations’⁴,

With headlines like that, one can understand the hesitation. Public opinion of large banks is very low these days and headlines announcing multi-million dollar fines for AML (Anti Money Laundering) violations do not help the cause.

With a growing global terrorist and organized crime threat, regulators are focused on AML and related topics such as USA Patriot Act, Bank Secrecy Act and OFAC (Office of Foreign Assets Control). Firms around the world have increased their resources to protect against money laundering and terrorist financing. In a 2013 study conducted by Veris Consulting⁵, nearly 66% of the survey’s 284 respondents (72% Bank, 12% Broker/Dealer, 16% other) reported that their AML and OFAC compliance budgets have increased over the last three years. The majority of resources have been appropriated to the control processes in the lines of business and compliance departments. Firms should also recognize that Audit is the last line of defense that provides an independent review of the control environment against various AML/OFAC risks.

Even with the increases of money used to protect firms against money laundering, firms still receive heavy scrutiny from Regulators. When weak AML controls are identified by the Regulators, the question arises as to what were the recent audit results within that area. Audit Departments are not spared regulatory criticism. In June 2013, when the US Department of Treasury’s Office of Comptroller of the Currency (US DOT OCC) cited need improvements for BSA/AML independent testing against TIAA-CREF Trust Company, FSB of St. Louis (2013-071)⁶. In January 2013, the OCC dedicated an entire section of the AML Consent Order (2013-02)⁷ against JPMorgan Chase Bank (JPMC) to independent testing (Internal Audit Department) stating JPMC needs to maintain an effective plan to audit AML. Similarly, the OCC cited deficiencies with independent testing against Citibank, N.A. in a 2012 AML Consent Order (2013-052)⁸. These firms have spent a considerable amount of money to improve their BSA/AML independent testing functions to address the OCC’s concerns and other firms have taken notice.

Regulatory expectations and pressures will continue to mount on Audit Departments to monitor the anti money laundering controls to ensure compliance with the regulations. There are steps that can be taken by an Audit department to implement an effective AML Audit Program and help keep the regulators at bay.
Solution:

Put in place an AML Audit Program

A coordinated effort across the Audit teams in the form of an AML Audit program is needed to keep pace with the increasing risk and regulatory expectations. In correlation to the size of the organization, each Audit department should have a clearly defined AML Audit program that falls in line with and runs parallel to the overall Audit program and guidance. While compatible with the overall Audit program requirements, the AML Audit program should clearly define specific criteria related to the expectations of AML coverage and be headed by an experienced AML subject matter expert.

The AML Audit program should also have objectives that are clearly defined and meet Regulatory requirements. The AML Audit program should align itself accordingly to the size of the firm. There are several key components to an AML Audit program that need to be in place to ensure the Audit department is prepared and capable of properly auditing AML risk. The overall approach to AML coverage, while risk based, needs to be comprehensive, thoughtful and based upon the same principles across all areas of the firm. Audit teams need to clearly demonstrate how a risk based approach was used to develop their annual Audit plan.

An AML Audit program should include a strong governance model that clearly articulates the evaluation of the Auditors AML audit experience, governance committee structure, required training, requirements of an internal risk assessment, tracking of key metrics, responsibilities of the AML Officer and completion of a quality assurance program. The execution of the AML Audit program should be consistent, where appropriate, across the firm including testing programs and escalation processes. In addition, an effective AML Audit program promotes the sharing of best practices and lessons learned (internal and external) across the LoBs.

Key components of a strong AML Audit Program

Several key components need to be considered when creating a strong AML Audit program. The program needs to be nimble and appropriate for the size and risk of the firm. There is no one right answer as every firm has its own unique obstacles; however, all firms need to consider their governance, execution and reporting components.

1. Governance

All successful AML programs need to have the proper governance structure. Tone from the top is essential for any successful program and that includes an AML Audit program. A clear message from Management on the importance of AML to the Audit department helps to prioritize the actions of the
Audit team. This message from management should include support for training, escalation of issues, key meetings and documented quality assurance standards.

A. Evaluation of the AML Audit Team

An analysis of the current staffs AML knowledge allows Management to identify gaps that may be present. This analysis should include the specific criteria within AML that the Auditor has experience such as Know Your Customer (KYC) or Suspicious Activity Reporting (SARs). Gaps that are identified can be addressed through additional resources, targeted training or management involvement.

Layering onto the known knowledge of the Audit staff is an understanding of the level of AML knowledge required to complete the audit plan. Managers should constantly review their plan to understand the risks within their area for the next 6 months to a year. Aligning the audit team’s knowledge with the risks covered will boost confidence that the AML risks are being properly audited. In addition, the hours and timing to complete Audits that have AML coverage should be reviewed against the availability of the staff with the specific AML knowledge required.

Understanding the specific and level of expertise that each employee has within AML can improve Audits coverage and have a positive impact to the firm as a whole. This goes beyond just putting a strong KYC Auditor on a KYC Audit. This also includes understanding which tests within the scope of the Audit will be completed by each Auditor. While functioning like this puts the Auditor in a successful position, some thought needs to be given to those Auditors that are growing their knowledge and ability within a certain area of AML. Challenging Auditors to take on AML Audit tests that are a slight stretch makes sense in order to expand the team’s knowledge as long as proper supervision is in place.

A capacity analysis should be conducted to ensure that enough Audit resources are available to complete the AML Audit program. This capacity analysis should be reviewed at least on a quarterly basis and updated as key changes to the audit plan or Audit team occur. Opportunities to use resources with the appropriate AML skills that may normally cover other similar risks and controls may be identified. This can add value to the Audit team’s coverage as well as value to the Auditor by expanding their experiences. The importance of a thoughtful capacity analysis for the coverage of AML risk can not be underestimated.

B. Audit AML Governance Committee

The Corporate or central AML Audit team should hold a standard meeting periodically with the LoB Audit teams. This meeting should include key AML topics and provide an opportunity for audit teams to share best practices across the LoBs. Significant issues identified by the audit teams should be discussed to determine cross LoB applicability. Similarly, industry news should be reviewed to ensure the Audit team stays current with the challenges of other institutions and gain an understanding of the applicability into their institution.

Other discussion topics should include upcoming audit coverage to allow for a coordinated approach to business processes that cross multiple LoB Audit teams. For instance, Foreign Politically Exposed
Persons (PEPs), although present in multiple LoBs, may be better covered by audit from a subject standpoint rather than audited separately by each LoB. The Audit AML Governance Committee should help drive the conversation as to the key topics for consideration in the firm’s horizontal audit coverage. This committee should review key metrics and analyze their impact to the AML Audit program. Finally, any significant changes to the Audit AML program should be discussed in this forum to ensure agreement, awareness and applicability to the audit teams.

C. Training:

The AML Audit training program needs to be comprehensive and stay current. The size of the firm may have a significant impact on the depth of AML training provided. The first piece of a successful AML training program is to have a comprehensive list of classes that cover the various AML risks found within the firm. The AML Audit Governance sub-committee or representative members of this group should be involved in identifying the list of potential classes to be taken by the AML audit teams.

Auditors should be required to complete a minimum number of courses every year, with emphasis on topics geared towards the areas the individual expects to audit. In addition, when an audit on a particular AML topic is in the planning stage, the audit team should consider training on that topic. Specifically, if an upcoming audit will cover SARs, then the Audit team should identify an enhanced SAR training course from the AML training curriculum.

Auditors covering AML should be rated beginner, intermediate or expert based on knowledge and experience to help identify the appropriateness of current and future class curriculum. Each level should have a defined, but flexible training map. For instance, a beginner may be required to take 10 classes throughout the year with five of them pre-selected. The remaining five would be chosen by the Auditor. While an intermediate may be required to take 3 specific classes with 7 classes more targeted at a specific area within AML to gain the knowledge of a specialty area.

Auditors should focus part of their training efforts on products and services that are present in their Line of Business. In addition to the background information included in this focused training, a section of the training should include how to audit the specific topics. A successful technique within the training should be specific case studies so the trainee can draw upon real world situations to see the application of the auditing techniques.

D. Risk Assessment

Audit’s risk assessment should include a dedicated section to AML. The level at which the AML risk assessments should be assessed need to be in line with the institutions legal or auditable entities. While AML will only be one component of risk for each entity, a detailed depiction of the impact of AML controls within each area should be clearly understood and documented. The AML risks and controls should also be depicted at a level that allows a cross LoB view for certain high risk product or client types. This can be accomplished by identifying which Legal Entities or Auditable Entities has exposure to high risk products or client types.
The AML section of the audit risk assessment should have a similar methodology as the overall Risk Assessment by including identified issues, metrics, key initiatives, significant changes, Audit and regulatory findings. The information used to draw the conclusions should be both qualitative and quantitative. There are several other factors that should be considered such as the businesses AML risk assessment. Specifically to AML risk, the factors that should be closely reviewed include the risk levels of the clients, geographies in which they live and the types of products that are used. In addition, the reliance of central utilities, such as a corporate screening group and previous Audit and regulatory results should be taken into consideration when completing the entities risk assessment.

The AML section of the risk assessment should be broken out at a granular level that allows for clear identification of high risk areas. The supporting rationale should be descriptive and thoughtful and include detailed evaluations. Coverage of AML high risk areas should be considered for annual Audit coverage. An understanding of the prior audit coverage and of any changes within the space can also help decide the timing and necessity of these reviews. The risk assessment should be reviewed at least semi-annually to ensure the risks identified are accurate and confirm if a change in the audit schedule is necessary. This can be accomplished by a clear mapping of identified AML risk to Audit coverage.

E. Metrics

In order to understand how the Audit AML program is working, key audit metrics should be maintained. The metrics should be discussed, reviewed and analyzed at the AML Audit Governance Committee. Audit metrics can provide valuable information on specific areas within AML such as training, Know Your Customer (KYC), Suspicious Activity Reports (SARs), areas where audit issues have been identified and areas where there are gaps in coverage.

One of the most important Audit metric that should be reviewed is a mapping of the AML audit coverage against the AML high risk areas as defined in the audit AML risk assessment. As the risk assessment guides the audit coverage, tracking that coverage throughout the year given the changes to the audit plan will maintain managements focus to ensure the audit coverage is risk based and appropriate. Layering the capacity analysis and auditor expertise into these key metrics can help identify the optimal audit approach given the current expertise.

In addition, the progress and completion of action plans relating to Regulator, Audit and Business identified issues should be tracked. Understanding what the business is doing to resolve issues and the progress they are making against the action plans is important in evaluating the current control environment. Audit should be reviewing this on, at least, a monthly basis.

F. AML Officer

Having a qualified AML Officer is considered one of the pillars to a strong AML Program. Auditing the qualifications and training of the AML Officer is imperative for the Audit function to provide an independent view of the appropriateness of that individual for that function. While qualifications
should match the size and complexity of the firm, training should also be in scale with the risk level of the firm. As part of Audit’s annual assessment of the overall AML program, testing of the AML Officer should be conducted to help provide a complete view of the program.

G. Quality Assurance

Quality Assurance (QA) of AML Audit work should be completed on an appropriate basis. Similar to other aspects of the AML Audit program, the timing of QA reviews depends on the size and amount of AML risk associated with the firm. Audit QA should consist of a review of an Audit’s work papers including the Governance related activities. There needs to be an Audit QA program in place with an AML component to ensure comprehensiveness and consistency for all AML reviews completed. AML Continuous Auditing documentation should also be considered for a quality assurance review. These reviews should be conducted by AML knowledgeable Auditors that are independent of the work being evaluated.

The QA program should ensure that all LoBs are periodically included for review within the program in proportion of the AML work they complete and the risk associated with the businesses they cover. The QA program should be maintained by an AML specialist to ensure the key items are included in the review. The AML Audit QA review should be consistent with the Audit QA approach but more specifically to certain questions to ensure the AML coverage has been completed appropriately. The checklist of items to be reviewed during the QA should be developed by an AML specialist.

Similar to a standard Audit QA program, AML reviews should result in a report listing the identified issues with action plans developed to focus on remediation of the issues. Issues that have been identified in one business should be shared and evaluated by the Audit AML Governance Committee. Results of the AML QA review should also be escalated to the Audit Management Team and where appropriate, the Audit Committee.

2. Execution

A. Standard Testing Program: Method of ensuring consistent coverage

To promote consistency of Audit testing across LoBs, a standard testing program should be developed based on key topics and areas. An inventory of topics should be developed that covers the key areas with AML risk. The topics should include program functions (i.e., governance, training) as well as testing plans for certain product types, geographies, etc (Remote Deposit Capture, Correspondent Banks). The inventory should be reconciled to the risk assessments (business and Audits) and the Federal Financial Institutions Examination Council (FFIEC) Manual. The inventory should be reviewed for updates on an annual basis.

Once the inventory is determined, each standard testing program needs to be developed using the Audit team’s experience, prior work completed and a review of the FFIEC manual. An example of an area that would warrant a testing program is the LoBs risk assessment. On an annual basis, all LoB audit teams
should evaluate the completeness and accuracy of the business’ risk assessment. Therefore, in order to provide consistency across the LoB Audit teams, a standard testing program should be created that includes key risks, controls and Audit test steps that define what the Audit teams could review when testing the area. While the test steps should vary from engagement to engagement, the basis for a full scoped audit of that area should be included in this standard testing program and the decision on what to include should occur during the planning stage of each audit.

The use of the standard testing program should be clear in any pre-planning documentation. Also important is the rationale for excluding any of the risks included in the standard testing program. The rationale should be clear, reasonable and documented. The standard testing programs should be flexible as various LoBs may have wide ranging differences that would appropriately warrant a change in test steps.

Another way to promote consistency and comprehensive AML coverage is to establish an AML Sampling guideline that can be used by all LoBs. This will ensure that, at minimum, each LoB is reviewing a sample using similar criteria. The sample guideline should be risk based and have applicability to most AML samples across the LoBs. As an example, for a sample of Know Your Customer (KYC) files, a certain number of files selected based upon the sample’s population should be high risk, medium risk and a certain number should be low risk customers.

B. Continuous Auditing

An essential part of providing appropriate AML Audit coverage is the activities conducted during continuous auditing. This can include meeting with stakeholders periodically or reviewing metrics. The AML Audit Program should specifically define an AML continuous auditing approach that sets minimum standards and promotes consistency across the various Lines of Business audit teams. When applicable, the minimum standards should include key criteria that all LoBs are required to review, when applicable. The list of minimum criteria metrics should include the below:

Key Criteria:

• KYC Records
  o for aging of new customer files
  o aging of renewals
• AML Transaction Monitoring
  o alerting volumes
  o yield results from scenarios
• Investigations
  o volume
  o aging of investigation (back logs)
  o SAR Filing stats
• Feedback Loop
In addition to reviewing and analyzing the results of the metrics above, AML auditors can conduct test work on a narrowly defined scope than the work completed in a regular audit. This targeted testing if executed correctly can be very effective. For example, using the metrics above, Audit can run a quick automated auditing test (discussed further below) against the names that have been indicated as closed accounts due to increased suspicious activity in the Feedback Loop Metric. The test can confirm if a customer relationship has been closed and that the customer has not re-entered the firm in a different LoB as a new customer. If the test is designed properly, an Audit department can run this test more frequently using fewer resources while obtaining the same results. This test should be completed across the LoBs or at the corporate level to ensure all LoBs are included in the scope to support consistency across the teams that audit AML.

An important outcome of completing Continuous Auditing is the shaping of future audit coverage which could allow for a more comprehensive test. While this may apply to other risks within the firm, this should be noted in the AML Audit Program as a driver of future audit work and as a factor in the overall Audit AML program evaluation. The AML Continuous Audit work results should be clearly documented and part of the quality assurance review process.

C. **AUTOMATED AUDITING**

While not a specific requirement but rather best practice, automated auditing should be included as part of the AML program, embedded in the Standard Testing programs where appropriate and used during Continuous Auditing as discussed above. The testing ability and breadth of the sample and scope can be greatly increased when using automated auditing techniques. These tests can be run more frequently and with greater ease that allows for a quicker and more in depth test of the controls effectiveness.

Automated Auditing can be used for several different tests within AML. As an example, if AML training is included in the scope of the audit, automated auditing can be used to obtain 100% of the population’s training results. These results can be sorted and viewed in such a way that can test the full population for training completion against a specific training as well as completion against training timeframes mandated in the AML policy. This will allow for more efficiency during the audit while covering a larger sample and providing a more accurate assessment of the area’s internal controls. Other important applications of automated auditing within AML are the ability to mine data extracted from a transaction monitoring or case management system.

D. **Validation of completed issues (from Regulators and Internal Audit)**

An AML Audit program needs to be clear on how to address previous AML related issues whether the issues were identified by the Regulators, Audit or self identified. All issues should be validated through testing within a reasonable timeframe from when the action plan is completed. The Audit team should be auditing the specific issue and not the action plan to ensure that the root cause of the issue has been
properly addressed. Performing work in a timely manner is important to allow the business a shortened time period to remediate additional issues that may be found during Audit’s testing.

For issues that are considered significant, the AML Audit teams should handle these as they would handle Regulatory identified issues. As the timing of the validation of AML issues may fall in line with the overall Audit policy for validating issues, the AML identified issues need to go a step further.

The AML Audit Governance Committee should share issues that have been identified in one LoB with all the others to determine if the issue exists elsewhere. This will help inform the overall view of the AML Program. Additional CA work may be completed in order to confirm if the issues are present in other LoBs.

3. Reporting

The AML program should address how the reporting of AML issues is to be completed. AML issues should be properly reported and escalated to Senior Management and under adverse conditions or for significant control break downs, the Audit Committee. The escalation of issues needs to occur swiftly as some issues can lead to violations of law that need immediate attention.

Generally, the reporting of AML issues should follow closely to the reporting of other issues identified by Audit. However, the AML Audit program should clearly define a few nuances that take place for AML Audits. For example, Audit should ensure the AML/BSA Officer receives in a timely way all significant AML issues identified by Audit. A best practice that should be included in the AML Program guidance is that emerging issues should also be escalated to the AML/BSA Officer. This will provide an opportunity for the AML/BSA Officer to ensure an appropriate action is agreed upon to remediate the issue and provides an opportunity for the Officer to evaluate the significance of the issue and determine other LoB impact.

Another consideration when reporting AML issues is the distribution list. There should be a list of individuals within the firm that should be included on certain types of AML audits depending upon its’ exact scope. This contact list should be maintained periodically and shared with the Audit teams to ensure appropriateness. The list will consist of mainly individuals in the corporate sector responsible for functions that cross LoB and regions. For instance, if there is an individual responsible for SARs within the Corporate group, they should be included on all SAR related Audit coverage throughout the firm. The AML Audit program should require this list to be used and maintained appropriately.

Separate from the reporting of Audit issues, the AML Audit team should assess on an annual basis the effectiveness of the overall AML controls for the firm. OFAC/Sanctions should be clearly broken out and reported separately. This report can be delivered to the audit committee or documented within Audit work papers. This process should also be documented in the AML Audit Program.
**Conclusion:**

There is no guarantee that an effective Audit AML program will prevent every money laundering scheme. But given the high stakes and sophisticated efforts by money launderers and terrorist financing to use firms as a way to move or hide money, the independent testing function needs to be strong. Having a coordinated AML Audit program will put the firms Audit practice in a position of strength and hopefully reduce the penalties that regulators impose on offending firms.

While most Audit departments generally have many of the characteristics described, in order to face the challenges of money laundering in the 21st century and avoid gaps in audit coverage, Audit needs to have a comprehensive AML audit program with the following key tenets:

**Governance**

- have a strong governance structure that includes an evaluation of the auditor’s skills that are mapped to current and upcoming work
- setting up an Audit AML Governance Committee to allow for the sharing of information between various audit teams to help coordinate the auditing efforts
- provide a training plan for auditors at all levels that will foster a continued improvement in the audit team’s knowledge of AML
- producing a comprehensive Audit AML risk assessment to help identify the areas of the firm where AML audit coverage is needed based on the risk level of each function
- producing metrics that report on the progress of Audit’s results will identify gaps and escalate issues timely
- Audit’s job of reviewing the AML Officers skills and knowledge to lead a firm should be an important part of Audit testing
- the Audit’s Quality Assurance work over the AML space should be tailored accordingly

**Execution**

- a standard testing program to promote consistent and comprehensive audit coverage throughout the firm
- a strong continuous auditing program that focuses on key metrics produced by the business
- the use of automated auditing to enhance the testing strategies and results for audit
- ensure the timely validation of closed action plans for AML related issues

**Reporting**

- ensure the reporting of AML issues are escalated and given the appropriate attention commensurate with the level of risk associated with the issue

Having an AML Audit program that incorporates the above items will allow the Audit department to perform these functions in a coordinated effort across the LoB Audit teams and provide a consistent and
comprehensive approach to testing AML controls. The presence of a comprehensive AML Audit program will demonstrate the firm’s commitment to fighting money laundering and terrorist financing.

The Head Auditor will have a difficult time defending AML coverage that is not comprehensive and consistent. Audit should identify the controls to be put in place to ensure they have the mechanisms to fulfill their job duties with respect to AML. As much as the businesses may not like when Auditors bother them with questions, they will appreciate issues that are identified by the Audit Department and not by the Regulators in form of a Consent Order.

Don’t waste anymore time trying to patch together AML Audit coverage across a firm, rather develop an AML Audit program that incorporates the components discussed in order to make your firm and the world safer. Don’t let your firm be the next case study in AML training sessions around the world. Develop a comprehensive AML Audit program for your firm and you will not have to whisper that you audit AML controls.
Resources


3 http://uk.reuters.com/article/2014/01/23/uk-standardbank-fine-idUKBREA0M0LF20140123


6 http://www.bankersonline.com/security/bsapenaltylist.html


8 http://www.bankersonline.com/security/bsapenaltylist.html