Auditing the Second Line of Defense:
The Compliance Monitoring and Testing Function

Genesis Martis, CAMS-FCI
CAMS AUDIT Candidate 2019

Disclaimer: The views expressed in this paper represent the view of the author and not necessarily of any third party.
Contents

Preface ........................................................................................................................................... 3
Introduction ................................................................................................................................... 3
  Overview of the Three Lines of Defense Model ("LOD Model").................................................. 4
  Weaknesses Identified in the LOD Model.................................................................................... 5
  The Need for a Compliance Monitoring and Testing Function.................................................. 6
Section 1. Regulatory Drivers for the Implementation of the Compliance Monitoring and Testing
  Function ........................................................................................................................................ 7
  Federal Reserve Letter 08-8: Compliance Risk Management Programs and Oversight at Large
  Banking Organizations with Complex Compliance Profiles ....................................................... 7
  Basel Committee on Banking Supervision: Compliance and the Compliance Function in Banks.... 7
Section 2. The Role and Responsibilities of the Compliance Monitoring and Testing Function ....... 8
  Independence ............................................................................................................................... 8
  Risk-Based Compliance Monitoring and Testing Program......................................................... 9
  AML Compliance Self-Assessment ............................................................................................ 11
Section 3. Auditing the Effectiveness of the Compliance Monitoring and Testing Function .......... 11
  The Compliance Monitoring and Testing Methodology ............................................................... 11
  AML Risk Assessment ............................................................................................................... 13
  Effective Audit Methodology to Assess the Compliance Monitoring and Testing Function ....... 14
Conclusion ...................................................................................................................................... 18
References .................................................................................................................................... 19
ANNEX 1. Staffing of the Compliance Monitoring and Testing Function ...................................... 20
ANNEX 2. Sample Questions to Develop an AML Compliance Self-Assessment ......................... 22
Preface

Financial Crimes Enforcement Network (FinCEN)\(^1\) published an advisory that emphasized prior warnings from the director that FinCEN "will employ all of the tools at our disposal and hold accountable those institutions and individuals who recklessly allow our financial institutions to be vulnerable to terrorist financing, money laundering, proliferation finance, and other illicit financial activity." This warning ought to be taken seriously, considering regulators are taking more aggressive and frequent enforcement actions against institutions and their management in instances where weak compliance programs lead to illicit activity.

FinCEN's director mentioned during one of the speeches in 2019 that: "To be clear—we take the culture of compliance seriously. This is a national security issue: not something to be taken lightly—and we will not take it lightly." It is imperative that financial institutions invest and develop a strong, comprehensive AML audit process to measure and govern the AML/CFT compliance program in accordance with applicable AML/CFT laws and regulations. Aside from the AML Audit, financial institutions dispose of the compliance monitoring and testing function, which can be a helpful tool in preventing AML-related penalties and fines. This function is also a key in identifying weak areas within the first and second line of defense and provides the necessary training, guidance, and tools to mitigate the AML compliance risks associated with these activities.

This informational white paper will provide guidance on how auditors\(^2\) can develop a tailored audit framework to audit the compliance monitoring and testing function. Such a framework should be developed with the focus of enhancing the quality of testing in the timely identification of weaknesses in compliance-related controls, mitigating AML-related risks, and avoiding AML fines and penalties.

Introduction

An example of a deficient second line of defense is evident in the rogue trading fraud (2008) of nearly $7 billion at Société Générale. This scandal brought forward several questions regarding the effectiveness of the compliance function and risk management. In particular, the compliance monitoring and testing function faced criticism amidst the fact that they failed to detect red flags. The Federal Reserve mentions that “there is still room for improvement in compliance monitoring and testing at many large and complex banking organizations”.\(^3\)

The Institute of Internal auditors (IIA) endorses the three lines of defense model as "an effective way to enhance communications on risk management and control because it clarifies roles and duties in an institution, ensuring the ongoing success of risk management initiatives."\(^4\)

\(^1\) FIN-2014-A007
\(^2\) The word “auditor” used in this paper refers to an auditor from the third line of defense or an external auditor/regulator.
On the other hand, the inefficient implementation of this model may cause negative consequences, evident in the growing number of enforcement actions against institutions in which regulators detected AML deficiencies and violations.

**Overview of the Three Lines of Defense Model ("LOD Model")**

In the context of AML/CFT compliance, the business units (e.g., front office, customer-facing activity) are the first line of defense. They are ultimately responsible for identifying, assessing, and controlling the risks of their business. The second line of defense includes the compliance function. The internal audit function acts as the third line of defense.

**First Line of Defense**

The first line of defense owns and manages risks. It consists of business units, which include the customer-facing functions. The managers of these functions identify, assess, and mitigate the risks of the business. Furthermore, they are responsible for the implementation of corrective actions resulting from identified issues during compliance testing and/or audit. The business units oversee the daily execution of the strategies and business objectives and therefore own and manage compliance risks associated with these services. In order to effectively manage the risks, applicable policies and procedures should be clearly documented in writing and communicated to all personnel. They should contain a clear description of the obligation of the employees and guidance on how to keep the activity of the bank in compliance with regulations and internal policy and standards. A tailored AML/CFT training program is crucial to keeping the employees up to date with current AML trends and developments.

**Second Line of Defense**

In a perfect world, only the first line would suffice for proper risk management. However, as seen in the current environment, it is crucial to have a well-established and strong compliance function to provide oversight of the first line of defense. The head of compliance is responsible for, among other things, the ongoing monitoring of the fulfillment of AML/CFT-related duties by the institution. Notwithstanding, additional responsibilities include the development and updating of the AML risk assessment, AML/CFT and sanctions compliance program, ongoing training, policies and procedures, transaction monitoring, (ongoing) customer due diligence, investigations, suspicious or unusual transaction monitoring, and reporting and sanctions screening. Furthermore, financial institutions should develop a risk-based compliance monitoring and testing program to assess business and other functions' adherence to the AML risk assessment. The compliance function provides compliance advice to the board, senior management, and business units. The second line compliance function utilizes a risk-based approach to evaluate the effectiveness of compliance controls through ongoing monitoring and planned testing.

**Third Line of Defense**

The third line of defense comprises internal audit function, which is responsible for, among other things, the development of a risk-based audit program to assess the effectiveness of risk
management and to test controls across the institution, and to grant an independent assurance that these are designed adequately and operating effectively, as intended.

Assurance is provided to the organization's board of directors and senior management. This assurance specifies how effectively the organization assesses and manages its risks and will validate the effectiveness of the first and second lines of defense.\(^5\)

**Weaknesses Identified in the LOD Model**

Despite the successful implementation of the LOD model in numerous institutions, we still see a series of enforcements related to AML breaches and violations. These breaches ultimately led to a substantial amount of financial losses, reputational damages, and, in some cases, even bankruptcy. This suggests that there was a series of failures within the internal control system. Knowing these weaknesses and taking them into consideration may assist the auditor in developing an effective audit plan to properly identify the weaknesses and provide recommendations for remediation.

**First Line: Driven by Revenue vs Driven by Risk Mitigation**

The LOD model regards the first line of defense as the major control point. Nowadays, the business units are driven by revenue, and their remuneration is based on how much they have generated rather than a combination of this and proper mitigation of risks. In relation to control duties, lack of familiarity with the workflow and insufficient awareness of risk and control procedures remain the main issue that institutions must deal with.\(^6\)

**Second Line: Lack of Skills, Knowledge, and Independence**

Experience has shown that in some financial institutions, the second line is disposed of insufficient skills and expertise to effectively conduct testing on practices and controls in the first line. Consider the example of XYZ Bank, located in the Dutch Caribbean. The compliance unit in charge of testing CDD/EDD on opened accounts failed to identify several red flags related to money laundering, misuse of accounts, and fraud. The reason was not an unsuccessful implementation of monitoring systems or failed testing plans, but that the personnel was insufficiently trained in detecting red flags related to money laundering and have insufficient knowledge of laws and regulations related to financial institutions, trust service providers, and designated nonfinancial businesses and professionals (DNFBPs). While conducting monitoring, the personnel lacked background knowledge of normal patterns/behavior for a certain group of customer type and failed to detect unusual behavior.

The second line of defense serves a vital purpose but cannot truly offer an independent analysis to management regarding risk management and internal controls. The reason is that the reporting lines and communication lines for the compliance function are more up to senior.

---

\(^5\) Chartered Institute of Internal auditor: Governance of risk: Three lines of defense. (2019)

management than to the board. A way to approach this issue is to present a more extensive report of identified compliance issues and activities to senior management and provide the board with a more comprehensive report on the testing activities accompanied by corrective action measures performed on the first and second line.

**Third Line: Inadequate Risk Assessment and Lack of AML Knowledge/Expertise**

It is imperative that auditors identify deficiencies and ensure that financial institutions maintain a sound AML/CFT compliance risk management program in relation to supervisory requirements and expectations. An effective audit is the result of an audit plan based on comprehensive annual risk assessment, covering all applicable laws, regulations, and internal policies and procedures.

Consider the example of ABC Bank, located in the Dutch Caribbean. One of its subsidiaries received an AML audit report based on an AML compliance audit performed by its internal audit department. However, the results were inconclusive. Based on the dismissal of various issues identified by the compliance function, it was visible that the auditor did not have extensive knowledge of the compliance framework and the laws and regulation applicable to the jurisdiction. The auditor failed to comprehend that the bank's risk appetite gave space to spread certain compliance responsibilities on the first and second line.

Another example is from Buy Your House Real Estate, located in the Dutch Caribbean, which received an AML audit performed by an external auditor. The external auditor failed to comprehend that the local laws and regulations state that each real estate should complete an AML risk assessment and develop its own compliance framework. The compliance framework should be tailored to their specific risk appetites, rather than compliance policies and procedures that are one-size-fits-all.

In another case, an external auditor failed to comprehend that the laws and regulations applicable for a nonfinancial institution are different than those regarded in the United States of America and provided wrongful recommendations that were based on a financial institution's perspective.

These cases clearly demonstrate some important factors in performing an AML audit:

- the auditor should have a comprehensive AML compliance background;
- the auditor must be included in the process of the development of the AML audit program;
- the auditor should be involved in recommendations and reporting phase of the audit.

**The Need for a Compliance Monitoring and Testing Function**

The previous paragraph identified the weaknesses that may exist in the first line and second line. This gives an opportunity for the compliance monitoring and testing function to serve as an internal control system prior to reaching the controls performed by (internal) audit. The objective of the compliance monitoring and testing function is to assess the effectiveness of controls
designed to ensure compliance with regulatory requirements, the internal policies and procedures, and management of the compliance program.

Monitoring and testing are often considered an ongoing health check on the AML/CFT compliance program. Without this so-called "ongoing health check," it would be nearly impossible to timely identify weaknesses within the program, communicate and escalate these, and plan the respective corrective actions. This function is essential to validating key assumptions, data sources, and procedures utilized in measuring and monitoring compliance risk to assure that they can be relied upon on an ongoing basis (in the case of transaction testing, that controls are working as intended). If working properly, the monitoring and testing function will assist in maintaining an effective internal control framework.7

Section 1. Regulatory Drivers for the Implementation of the Compliance Monitoring and Testing Function

Regulators view testing and monitoring activities as a financial institution's commitment to ethics and compliance. Moreover, testing and monitoring programs are a regulatory requirement, and in cases of noncompliance, institutions can receive penalties and fines.

Federal Reserve Letter 08-88: Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles

In October 2008, the Federal Reserve published a letter titled, Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles, which highlighted its view related to several compliance areas, for which guidance has been requested.

With regards to monitoring and testing, the guidance indicates that: "Robust compliance monitoring and testing play a key role in identifying weaknesses in existing compliance risk management controls and are, therefore, critical components of an effective firm-wide compliance risk management program."

Basel Committee on Banking Supervision: Compliance and the Compliance Function in Banks9

In its published guidance on compliance and the compliance function within banks, the Basel Committee encouraged institutions to perform "sufficient and representative compliance testing." The results of this exercise should be reported up through the reporting line drafted in the internal procedure of the institution. In addition, the Basel Committee advised that the report should include "the compliance risk assessment that has taken place during the reporting period,

---

7 FRB: Supervisory Letter: SR 08-8 (October 2008)
8 FRB: Supervisory Letter: SR 08-8 (October 2008)
9 Basel Committee on Banking Supervision Compliance and the Compliance Function in Banks. (April, 2005)
including any changes in the compliance risk profile based on relevant measurements (such as performance indicators), summarize any identified breaches and/or deficiencies and the corrective measures recommended to address them, and report on corrective measures already taken.  

Section 2. The Role and Responsibilities of the Compliance Monitoring and Testing Function

The compliance monitoring and testing program not only aids in the identification of potential issues or required enhancement prior to independent testing or regulatory examination, but also provides valuable insights into the overall health of compliance framework. The results of a well-implemented monitoring and testing exercise can be used to provide information to the head of compliance and senior management of the operation of the controls across the institution, the provision of evidence that supports the effectiveness of the control system. Most importantly, it provides senior management with an assessment of how well the institution meets AML compliance regulatory expectations.

The monitoring aspect of the compliance function should focus on the ongoing assessment of adherence to the policies and procedures governing activities that pose compliance risk to the business and assist in effectively managing risks on an ongoing basis. The main activities of a monitoring program are ongoing monitoring, review, analysis of key business performance, and risk indicators that allow the organization to identify potential noncompliance.

The testing aspect consists of a periodic selection and review of a sample of a certain product, services, and/or other areas to ensure the effectiveness of compliance controls and compliance with policies and procedures. This process is risk-based and independent, and the results should be reported to senior management. When implemented correctly, the results/findings can be processed into metrics that can assess the effectiveness of the program design and that of the operations.

Independence

To an extent, the function is conducting similar activities as the internal audit function, but most are not considered as such. The reporting line of the monitoring and testing function is directly towards the compliance function and senior management. There may be instances where the internal audit function may rely on the work conducted by the monitoring and testing function, but this should be exercised with care. A good cooperation between the internal audit function and the monitoring and testing function is of vital importance to avoid duplication of activities. This is achieved by communicating on the audit and testing scope, testing plan, audit program, objectives, and the timetable to conduct the activities. The benefit of this approach is that the

---

10 Basel Committee on Banking Supervision Compliance and the Compliance Function in Banks. (April, 2005)

11 Overall, the activities should consider whether internal controls are designed appropriately and operate effectively.
testing activities performed by the second and third line are aligned at all stages (planning, execution, reporting, and remediation).\textsuperscript{12}

With reference to the compliance function itself, the monitoring and testing function should be considered the independent testing arm of the compliance function. The annual monitoring and testing program should be reviewed and updated alongside the AML/CFT compliance program. When drafting the annual monitoring and testing plan, the compliance function may provide additional areas that need testing. However, the monitoring and testing function should independently develop the monitoring and testing plan and remain responsible for the execution and results. To ensure the independence of the unit itself within the compliance function, the institution must clearly define the roles, responsibilities, and segregation of duties. These should be clearly documented within the policies and procedures related to the monitoring and testing function. Controls should be put in place to validate that these are operating effectively. The individuals conducting the testing activities should not be the compliance officers exercising the controls within the second line of defense. The members of this unit should be independent enough to conduct testing on the activities performed by the members of the compliance unit of the organization.\textsuperscript{13}

Risk Assessment

The process to establish an effective AML/CFT compliance program commences with the development of an AML risk assessment. This enables the institution to assess which money laundering and terrorist financing risks threaten it, in which ways, and to what extent. The documentation of these risks will help the institution simultaneously determine the level of controls necessary to mitigate the identified risks. It should always be properly documented, maintained, and communicated to relevant personnel within the institution. A risk-based monitoring and testing program will target specific areas of risks, including the organization's highest risks or emerging risks. In addition, the scope and frequency of the activities should be based on the compliance risk associated with a specific business activity, product, or customer type.

Risk-Based Compliance Monitoring and Testing Program

The compliance testing and monitoring program consists of the following elements:

- Development of a risk-based monitoring and testing program
- Execution of the program
- Management reporting
- Tracking of agreed remediation actions

\textsuperscript{12} E.g., if internal audit is planning to assess a particular risk and/or area, then the compliance monitoring and testing team can evaluate to deprioritize the same risk and add this to the following year scope.

\textsuperscript{13} This should be clearly indicated in the mandate of each team member.
• Validation of remediation actions to confirm that the identified issues have been remediated
• Assessment of quality
• Review and update of the AML compliance risk assessment

Monitoring and testing should be able to help an institution move from a "paper-based compliance program" to a dynamic program that is "implemented, reviewed and revised as appropriate, in an effective manner. The compliance monitoring and testing plan covers all aspects of the compliance program." Furthermore, the testing plan should capture high-risk compliance elements identified in the risk assessment.

A compliance monitoring and testing program contains schedules, plans, scopes, reviews of compliance processes, policies, procedures, guidance, and standards, as well as validations of certain systems to ensure the established compliance program is complied with and to identify potential issues or recommended enhancements prior to the internal and external audit and regulatory examination.

**Compliance Testing Plan**

Compliance testing is used to assess whether the compliance program is effective and efficiently reduces compliance risks to an acceptable level for the organization. The results of a testing exercise should include identified weaknesses and corrective actions. All review steps should be adequately documented and reported to the board or related committees.

**Scope**

The scope of testing should be risk-based, including specific pillars of the compliance program in conjunction with the results of previous testing, audit findings, self-identified issues, issues raised by previous regulatory examination, incidents, and other areas identified as high risk. Another approach may be to test the effectiveness of controls related to each specific pillar of the compliance program. The plan should cover compliance-related activities of the first line of defense, and the activities of the compliance function in the second line of defense.

Example of scope:

• Customer due diligence/enhanced due diligence
• Investigations and suspicious activity reporting
• Law enforcement requests
• Sanctions screening
• Bribery and corruption

**Frequency**

---

The frequency of the testing activities should be derived from the AML compliance risk assessment. The testing plan should be scheduled based on resources, availability, and multi-year planning to avoid duplication of testing areas.

**AML Compliance Self-Assessment**

The AML compliance self-assessment is an exercise an institution can do to grade itself on its AML compliance program, including the current compliance testing processes and procedures. The oversight and reporting can be assigned to the compliance monitoring and testing function. This exercise will enable the institution to identify gaps/improvement areas in AML control designs, resulting in a better understanding of the number of efforts required to remediate those gaps. The obtained results can be processed into a heatmap, which displays the level of compliance against each core requirement and automatically rates its level of compliance; e.g. high, medium, or low risk.

By striving to use and invest in automated systems and artificial intelligence, institutions can transform the compliance functions into proactive (real-time) teams enabled to anticipate risks rather than react (post-event) to risks, and prevent noncompliance incidents while supporting the strategic business goals. The current regulatory landscape of both the U.S. and jurisdictions of the Dutch Caribbean do not formally require the completion of a (yearly) AML compliance self-assessment, but completing this exercise and including this in the testing plan may indicate efforts to create a compliant culture within the organization and a strong commitment to mitigate AML risks.¹⁵

**Section 3. Auditing the Effectiveness of the Compliance Monitoring and Testing Function**

**The Compliance Monitoring and Testing Methodology**

**Data Gathering: A Key Activity Prior to Commencement of the Compliance Testing Process**

Prior to initiating the compliance testing process, the following documents should be requested and reviewed prior to the on/off-site visit/testing:

- Risk assessment: AML/CFT and OFAC sanctions
- Relevant laws, regulations, and guidelines (including changes or newly implemented laws, regulations, etc.)
- AML compliance program: approved by senior management
  1. Policies
  2. Procedures

¹⁵ Refer to Annex 2 for a series of questions that can be included in the development of this self-assessment exercise.
3. Internal controls

- Annual AML training program
- Annual compliance testing plan
- Results of conducted compliance testing (based on a selected period)
- Minutes of meetings conducted between the first line and testing function after the conducted testing activities
- Reports to senior management and board
- Prior regulatory exam reports, exceptions, responses
- Prior audit issues identified by either external or internal audit
- Prior self-identified issues
- Prior issues identified in a previous compliance testing report

Policies and Procedures Related to the Monitoring and Testing Function

Regulatory guidance indicates that policies and procedures are the foundation of the AML/CFT compliance program. The testing program should be documented in a separate policies and procedures (or manual) to test the effectiveness of the testing program’s implementation and execution of its requirements. Such a separate manual is necessary to create a structure within the unit and for organizational discipline.

The activities performed by this function are to test the controls and effectiveness related to internal policies and procedures, which on their turn are derived from applicable laws, regulations, and best practices. This can be documented within a monitoring and testing policy. The policy should clearly state that this unit’s overall objective is to determine adherence to requirements of the regulators and supervising entities. Moreover, it should highlight that the monitoring and testing function works independently within the compliance function and should establish the communication line to the head of compliance and senior management.

It is advised to develop a manual that provides a substance to the monitoring and testing policy. This manual will be the main document that forms the basis for the audit methodology on the compliance monitoring and testing function.

A few indications for the content of the proposed manual are:

- Policy statement indicating that it is derived from the risk assessment
- Mission statement
- The objective of the function
- Expectation on maintaining independence within the compliance function
- Regulatory expectations of the first and second line
- Operational activities
- Coordination of the communication between the first, second, and third line of defenses
• Qualifications for a monitoring and testing team member\textsuperscript{16}
• Training for the team members
• Testing methodology (basic framework)
• Testing Standards\textsuperscript{17}
• Process for communication with senior management
• Process for escalating issues

\textbf{Compliance Testing Process}

• Determine the testing area(s) based on the risk-based approach
• Determine the testing objective and the testing scope
• Obtain input from the head of compliance, head of compliance monitoring, and testing
• If the testing will be performed in other areas, obtain the input from the local compliance officers. The team should discuss the testing plan with the local compliance officers to understand the coverage and applicable laws and regulations
• Gather data related to the business/testing area
• Gather results of previously conducted audit/testing, self-identified issues, regulatory examination issues, and or any third-party review issues
• Create a risk-based testing plan (based on the AML risk assessment)
• Conduct the testing activity
• Review and report the results
• Create the report and submit this to the management of the business, head of compliance, and head of monitoring and testing function
• Provide remediation actions for identified issues
• Provide a timeline to close the identified issues
• Track Issues
• Provide validation of remediation actions to confirm issues identified have been remediated

Afterwards, conduct quality assurance and adapt the testing plan for the next year where necessary.

\textbf{AML Risk Assessment}

\textbf{Perspective: Compliance Testing}

Throughout the compliance testing process, the AML risk assessment should be used as a guidance to develop a compliance testing scope and objective. Based on the AML risk

\textsuperscript{16} Basic qualifications for the function within the monitoring and testing unit, e.g., skillset and knowledge that a monitoring and testing officer must possess

\textsuperscript{17} Testing standards are needed to establish a consistency in the minimum requirements related to planning, executing, and reporting in support of the AML/CFT compliance program.
assessment, the team should choose the areas on which testing will be performed and which entities are subject for the testing. The testing plan should strive to include all areas identified within the risk assessment and test the controls that are implemented to mitigate said risks. Simply put, the compliance testing plan should be visibly derived from the AML risk assessment.

If not all areas can be covered within that specific testing, it may be decided to move certain testing areas to the next year's testing plan.

**Perspective: Audit**

The audit has a different perspective on the risk assessment. Audit looks at the risk assessment, as to how compliance testing performs risk assessment in order to determine which entities or AML compliance functions are in the scope of the test (e.g., by using the risk-based approach), how the scope is determined, and whether the scope is appropriate and provides appropriate coverage. Furthermore, it looks at the sufficiency of staffing and knowledge of staff performing compliance testing (their external trainings, etc.), whether the approach to performing compliance testing is appropriate, the documentation of compliance testing's testing, how the issues are distributed and followed up to ensure that remediation is completed, and that the issues remain closed.

**Effective Audit Methodology to Assess the Compliance Monitoring and Testing Function**

**Components of the Audit Methodology**

A comprehensive audit methodology to provide assurance on the effectiveness of the monitoring and testing function would entail the following:

- Risk assessment
- Audit scope
- Assess the coverage of the testing scope
- Policies and procedures related to the function itself
- Assessment of the knowledge and skillset of the team members
- Training
- Issue management
- Record retention

The audit process consists of the following components:
Policies and Procedures

The monitoring and testing function conducts testing on observance and compliance with implemented policies and procedures related to AML/CFT within certain units of the financial institution. During the audit testing, assurance must be provided if there is a process in place to address changes in the regulatory landscape and that these are being taken into the testing plan on the first line. It is suggested that the regulatory compliance function (or equivalent function in the institution) provides this information to compliance monitoring and testing function.

It is important that the auditor validifies whether the monitoring and testing function periodically assesses whether the policies and procedures implemented in the first line are working at the same pace as the regulatory developments.

In reviewing procedures to carry out the activities, the auditor should be able to provide an assurance that the function carries out testing on controls established for monitoring purposes within the first and second lines.

Audit-Planning Process

The audit planning process consists of some important steps:

- Ensure that the audit plan has a visible link to the AML risk assessment and that it is updated.
- Create a schedule based on the audit plan that takes into account the availability of human resources and that the scope is not in conflict with other ongoing audits/testing activities.
- Document the objectives and determine the steps necessary to assisting the audit team to complete its target/assignment.
- Schedule a kickoff meeting with the management of the business owner (auditee) in the order of the audit-planning schedule already established. Explain the scope and planning and the objective of the audit. This meeting should be documented and provided to the head of compliance and head of the monitoring and testing unit.
- Share with the auditee the communication’s protocol, expectations, and deliverables, along with the timelines.
- Commence the data-gathering phase to initiate the audit phase.
• Share with the management of the first line the scope and objectives, respective responsibilities, and other expectations of the audit.
• Inform the auditee of the names of the individuals that are a part of the audit team.
• Schedule travel plans for the audit teams covering the audit (if required).
• Share with the first line the timeline providing dates of the kickoff meeting, periodic status meetings, fieldwork and testing, report writing, and report submission.

Fieldwork and Testing

Auditing Best Practices Related to Monitoring and Testing Activities Performed by the Second Line

• Work with management to identify and make a list of compliance high-risk areas related to operational areas.
• Organize periodic status meetings with key stakeholders during fieldwork to keep them apprised of status, potential observations, issues, roadblocks, and challenges.
• Create a compliance audit plan that will evaluate whether ongoing monitoring and auditing are adequately addressing compliance high-risk areas and prioritizing higher-risk areas.
• The audit plan should include previous findings from compliance audits applicable for the function and regulatory examinations from the past.
• Ensure that the testing plan of the monitoring and testing function covers components, such as customer due diligence, enhanced due diligence, OFAC sanctions screening, filling of suspicious activity reporting, transaction monitoring, and law enforcement requests.
• Conduct audit on the aforementioned areas to provide an assurance of the efficiency and effectiveness of the monitoring and testing activities.
• Determine whether ongoing auditing has addressed the adequacy of the internal controls (e.g., policies and procedures) to reduce likelihood that an unwanted high-risk event will occur.
• Conduct interviews and walkthroughs with key process owners.
• Ensure that the findings are documented according to internal policies and external guidelines, and that these are timely communicated to the key process owners and management.
• Ensure that all identified weaknesses are graded based on a risk-scoring method (e.g., weakness can be scored as low, medium, high, or unacceptable; this will enable the auditee to develop a corrective action plan based on the grade of identified weaknesses).
• Ensure that corrective action plans have been instituted for all deficiencies found within a risk area and verify that the corrective action works as intended.
• Include results of audit as regular agenda items for both the management and board-level compliance committees.
• Place special emphasis on the scope of work for reviewing whether high-risk areas are being properly addressed.
Reporting and Recommendations

According to regulatory guidance, an independent testing should, at a minimum, include:

A review and statement on the overall adequacy and effectiveness of the institutions' AML/CFT compliance programs, including compliance with applicable laws and regulations. The report of the independent testing should also provide enough information for the reviewer/reader, to determine the overall quality of the AML/CFT compliance program.

To create a comprehensive report:

- Finalize the results of work performed.
- Compile a list of findings from process walkthroughs and detailed/substantive testing.
- Schedule a meeting with the head of compliance, head of monitoring and testing, and senior management to review results of work performed.
- Discuss management response as to how compliance will address the issues identified.
- Produce a written report that outlines audit procedures performed, findings resulting from testing, and recommendations for process and procedure improvements.
- The findings may be processed into a matrix (heat map) that grades the severity of the identified weaknesses.
- Include a deadline to receive the corrective action plan and ensure that the auditor keeps a copy.

Corrective Action Tracking

The auditor should track and validate the corrective actions to ensure that proper measures have been taken to address the issues, that the corrective actions are implemented, and that the issues remain closed.

Best practices on corrective action tracking and corrective action validation are:

- Schedule a meeting with the head of compliance and the head of monitoring and testing to review and verify the implementation of the respective action to rectify the key control gaps on a quarterly basis.
- Communicate the progress of the corrective action plan on a periodic basis to the board, compliance committee, and senior management on the progress on a quarterly basis.
- These updates should also be reflected simultaneously in the AML risk assessment model.
- Consolidated reporting of corrective actions and validation is provided to management and leadership for awareness and escalation.
- Maintain high visibility throughout the corrective action implementation and validation.

---

18 This may vary upon the organizational structure of the institution.
Conclusion

Despite successful implementation of the three lines of defense model and advancements in developing robust compliance programs, there is still an increase in AML-related penalties and fines for violations of AML/CFT compliance programs. A method to mitigate this risk is leveraging on a monitoring and testing program. This paper provided information and audit practices for the audit function to provide assurance and recommendations to secure effective and efficient monitoring and testing activity.

The compliance monitoring and testing function aids in shifting the AML/CFT compliance program into a dynamic program that is flexible enough to adequately handle AML/CFT compliance risk in a timely manner, in "real-time." A robust monitoring and testing program will benefit a financial building in numerous ways. It enables the building to gather critical information on weaknesses in the AML/CFT compliance program. While working optimally, it provides advanced warning of any looming problems before they become significant and potentially damaging, resulting in AML-related fines.

The fight against money laundering and terrorist financing never ends, especially when criminals are constantly developing new methods and techniques to launder their funds. The compliance monitoring and testing function serves a critical part, as vulnerable areas of the first and second lines of defense are working effectively. Consequently, performing the appropriate scope of testing and validation, coordinating with the third line of defense, and developing remediation plans to close gaps and identify issues are the main activities of this function, and will aid the function to effectively test adherence within the first and second line.
References

ANNEX 1. Staffing of the Compliance Monitoring and Testing Function

A centralized unit that conducts compliance monitoring and testing will result in a more robust governance and compliance oversight, which will result in better quality of test results and comprehensive data analytics. Most importantly, it will demonstrate to regulators a more consistent approach across the institution. The compliance function itself will benefit by being able to quickly identify emerging risks and regulatory changes and integrate identified trends within the annual testing plan.

See below a guidance to create a monitoring and testing team.19

Compliance Officer With Specific Subject Matter Expertise/Specialization

Profile:

- Subject matter expertise on one or several areas of compliance
- Thorough compliance knowledge and experience

Responsibilities:

- Conduct risk assessment and define scope of the testing plan
- Choose testing areas based on his/her expertise
- Conduct testing based on his/her area of expertise or in high-risk areas
- Management reporting

Compliance Officer With Audit or Testing Background

Profile:

- Audit background
- Subject matter expertise on one or several areas of compliance
- Thorough compliance knowledge and experience

Responsibilities:

- Develop testing areas and create a testing methodology in conjunction with the compliance officer with specific subject matter expertise
- Coordinate and lead the testing activities across the business functions and compliance function
- Provide assurance of the controls based on the findings of the testing activities
- Support corrective action tracking and issue management activities

Monitoring and Testing Officer

Profile:

- Basic knowledge of conducting testing

---

19 To make sure that this setup will work effectively, institutions must focus on striving to enhance the data available to the team.
• Compliance knowledge

Responsibilities:

• Prepare test scripts
• Execute testing in conjunction with the roles
• Document testing results
• Prepare report
• Organize meeting
ANNEX 2. Sample Questions to Develop an AML Compliance Self-Assessment

Refer to a sample of questions that institutions can include in the self-assessment exercise:

- Do we have a compliance testing unit independent of the operating units that test the processes and procedures?
- Is our compliance testing function engaged with the internal audit?
- Is our compliance testing program controls-based?
- Does our compliance testing program leverage technology, or do we have a realistic plan to do so?
- Do we have the in-house capabilities and bandwidth to drive innovation, including technology advancements?
- Do the compliance testing and monitoring function perform testing on adherence of account-opening procedures?
- If yes, based on the reports and corrective actions, did we see a decrease in noncompliant account opening files?
- Does the compliance testing and monitoring function provide advice to the compliance-training team on areas for improvement or high-risk areas/activities?

If one or more of the answers to these questions is "No," then it is advised to develop a remediation plan to quickly close the identified gaps.