





# Anti-Money Laundering:

## Reporting to Senior Management and the Board

by Alan Abel

**FOR ANTI-MONEY LAUNDERING (AML)** as well as for other domains of risk and regulatory compliance, regulators expect to see compelling evidence that bank and non-bank financial institutions govern themselves well. A critical dimension of AML good governance is a Senior Management Team (SMT) and a Board of Directors that is well informed about key aspects of AML compliance, risk management and events that may require SMT and Board attention, policy and program decisions, and other actions.

SMTs and Boards should not be unpleasantly surprised by learning of events either outside the four walls of the institution or from an employee, that could adversely affect the institution's, the SMT's, and the Board's reputations (let this be your "acid-test" for deciding what to report and not to report to the SMT and Board!) Also, SMTs and Boards should be kept sufficiently well informed of AML compliance and risk management matters—beyond core responsibility, members may be independently contacted by regulators and law enforcement and will be expected to be well versed and knowledgeable. Finally, SMTs and Board members are potentially, criminally liable for serious compliance deficiencies that may result in enforcement actions—greatly expanding the boundaries of "need-to-know." At the same time, SMTs and Boards should not be bombarded or overwhelmed

with large volumes of detailed reports that could cloud key points and impair clear thinking on policy, program and other actions. Information should be sufficiently high-level and meaningful.

Boards vary considerably among institutions, particularly in respect of size, constitution, and committee structure. It is not necessary for all Board Directors to be equally well-informed and well-versed in all AML matters—Boards increasingly need to differentiate functions, and more often than not, Boards assign Audit or Risk Management Committees oversight of AML compliance and risk management programs. However, periodically the designated SMT AML oversight committee (which should be a steering committee of executives who "champion" the AML program for their respective business units and support areas of consequence) and the appointed



AML Compliance Officer should make meaningful presentations on the state of AML compliance and risk management and significant matters to the full Board.

Here's a modest checklist of AML governance "TO-DOs" and reportable matters for you to consider:

- At least once a year, or as frequently as changes are made or are required, the full Board, at the direction of the AML Officer, the SMT and the designated AML oversight committee (again, usually audit or risk management) should review, update and re-approve a written AML policy framework, at a minimum:<sup>1</sup>
    - AML policy, including statements that articulate the institutions' AML risk tolerance, (e.g. what are the criteria and thresholds for **not** accepting new customers—where do you draw the line?), 1) addressing core AML risk criteria—all four compliance, reputational, operational, and strategic risk areas; and 2) customer, product, geographic, and distribution channel risk dimensions, and associated account opening policies.<sup>2</sup>
    - USA PATRIOT (PATRIOT) Act compliance policy
    - Bank Secrecy Act (BSA) compliance policy (as amended by the USA PATRIOT Act), including a policy on Suspicious Activity Reporting (SAR)
    - OFAC (Office of Foreign Assets Control, economic sanction and national interdiction laws) compliance policy
    - Anti-terrorist/anti-terrorist financing policy
    - Policy on checking for, accepting and providing services to "PEPs" (Politically Exposed Persons), and also checking (other) government "control" lists
    - KnowYourCustomer (KYC) strategy and policy
    - Customer Identification Program (CIP) compliance policy, including policy on conducting background checks and independent, third-party verification of identity
    - Policy on information-sharing with the government
    - Policy on information sharing with other businesses and trade associations (this policy should be considered in view of your privacy compliance and policies as well)
    - Policy on AML risk assessment and performing risk-based, Enhanced Due Diligence (EDD) and Enhanced Scrutiny (ES)
    - Corporate Code of Ethics – statement of AML policy and responsibility
  - The Board should, at least annually, review and reaffirm the position and job description of the AML/BSA Officer and the appointee.
  - The Board should periodically review and revise its strategic plan that assesses AML strategic risk in the customer base, geographies, jurisdictions, products and services, distribution channels, service providers, mergers and acquisitions, strategic alliances, and deployment of new technologies. The Board needs to get clear and meaningful business and customer profile information so that it clearly understands and demonstrates understanding of the customer base and segments, channels and jurisdictions of operation (lots of pie-charts), particularly highlighting higher risk customers, areas, and issues.
  - Counsel, Compliance Management, and Risk Management should periodically report to SMT and the Board on risk and potential institutional and individual potential criminal liability, and important cases.
- The Board (and /or the designated oversight committee) should be kept informed about:
- AML reputational events immediately upon their occurrence, e.g. negative press about a customer, counterparty, or an employee
  - Reputational and compliance events, and law enforcement actions made public, adversely affecting other institutions ("Look what happened over at \_\_\_\_\_. Could that happen to us?").
  - Any subpoenas and significant regulator and law enforcement requests or inquiries made; requests made by U.S. Attorneys to keep accounts open
  - Any communications with regulators and law enforcement about AML, terrorists or suspected terrorists, OFAC Specially Designated Nationals (SDNs) and other government control list "hits," and PEPs
  - Any penalties assessed resulting from compliance failures or alleged compliance deficiencies
  - Periodic reports on cases and number of cases (investigations) in the works
  - Account closures or pending account closures
  - SARs in progress and reports filed to authorities (the written SARs themselves, by the way, should never leave the four walls except for filing with law enforcement)
  - Any other reportable conditions
  - Volumes of CTRs and other BSA reports filed



- New account activity
- Legal, regulatory, and administrative changes, notices of proposed rule making of consequence, and periodic reports on complying with and implementing new laws and rules. Also, direct or professional association participating comments and correspondence
- The status of AML training among employees, employee certifications (the Board itself is required to undertake periodic AML training and awareness sessions)
- OFAC hits, blocks, and other reportable OFAC events
- AML risk assessment activities and their results
- Significant AML compliance program activities or changes, e.g. program expansion, terminations and new hires, new or changes to business processes or systems and anticipated impact
- AML related examination activities and findings, matters requiring follow-up action and remediation, action item plans and progress on remediation action items; accounts of meaningful examiner discussions and examiner / supervisor correspondence. Also, periodic updates on the status of the continuous examination management plan.
- The results of AML and BSA compliance reviews and management responses, including remediation plans
- The results of AML and BSA audits (independent testing) and management responses, including remediation plans

- The results of customer data quality assessments and remediation activities
- Periodic update on the status of KYC responsibilities embedded in employee job descriptions and how employee compliance performance is assessed and compensated

SMT and Board meeting agendas should be circulated in advance and clearly highlight any AML matters slated for presentation and discussion, and minutes of these meetings should clearly indicate that discussions took place and document their outcomes and action items. (Examiners will review these minutes carefully, and ask for evidence that action items were followed up on.) Directors should have the opportunity to review and accept the minutes of these discussions.

1 The AML policy-framework “frames” the entire AML program. This framework is separate and distinct from two other critical written compliance program components, i.e. AML enterprise-wide guidance and standards, and AML detailed, implementing, operating policies and procedures. The written AML compliance program should never get or appear to be stale.

2 SMTs and Boards need to be well informed about and well engaged in discussions about AML risk criteria, risk thresholds, and risk tolerance. These discussions should be well documented – your supervisors (examiners) will be keenly interested in the SMT’s and the Board’s understanding and articulating AML risk and defining and accepting responsibility for AML risk tolerance setting.

---

For questions on anti-money laundering, please contact Alan Abel in Washington, D.C. at (202) 312-7547 or [alan.abel@us.pwc.com](mailto:alan.abel@us.pwc.com).

---