The Role of an Effective Independent Review of Your Institution's Anti-Money Laundering (AML) Program

by Stephen J. Lurie
PricewaterhouseCoopers LLP
June 3, 2008

PRICEWATERHOUSECOOPERS

Agenda/Contents

- USA PATRIOT Act Requirements and Financial Institutions Covered
- Recent Regulatory Findings
- Elements of a Strong AML Independent Review Program:
- Audit Planning, Scoping and Resources to be Utilized
  - Risk Assessments – Customers/Investors, Products and Geographic Locations
  - Enterprise Wide Approach – All legal entities and business lines
  - Audit Test Plans, Sampling and Test Results
  - Expected versus Actual Activity
  - AML and OFAC Monitoring Systems
  - Documentation:
    - Assumptions and Work Papers
    - Report Preparation and Reporting to Senior Management and Board
  - Reporting, Continued Follow-Up, and Escalation
    - Updating the Independent Review Program

USA PATRIOT Act

Section 352 Anti-Money Laundering Programs:

In order to guard against money laundering through financial institutions, each financial institution shall establish anti-money laundering programs, including, at a minimum—

(A) the development of internal policies, procedures, and controls;

(B) the designation of a compliance officer;

(C) an ongoing employee training program; and

(D) an independent audit function to test programs

“An Independent Audit Function to Test Programs”

- Testing of the program is not a best practice, but a regulatory requirement of the Act;
- Independent
  - Of those implementing the AML program (i.e., Compliance); and
  - Of those who are implementing the internal controls of the program
- The Audit, can be performed by
  - Internal Audit; or
  - An independent consultant
- Test Programs (i.e.,
  - For compliance with all the requirements of BSA, USA PATRIOT Act, OFAC and their regulations; and
  - Testing the internal controls of the program for coverage and effectiveness

Recent Regulatory Findings

- Audit scope
  - Not performed or enterprise wide; and
  - Not tailored to business lines
- Audit staff for Independent Review
  - Not sufficiently trained in AML controls and requirements; and
  - Not truly independent of Compliance or Business units – Conflicts of Interest
- In 2007, 51 of the 122 AML enforcement actions issued for banks (nearly 42%) cited either inadequate or nonexistent audit procedures

Source: Money Laundering Alert, May 2008; Fortent Inform information service.

Recent Regulatory Findings

- Testing of compliance and controls
  - Inadequate testing to gauge the sufficiency of the AML program;
  - AML system not sufficiently tested, including data integrity and system updates and controls;
  - Inadequate testing of transaction and account monitoring procedures; and
  - Failure to detect deficiencies in key AML requirements (e.g., CIP)
- Independent review findings
  - Results and findings not reported to senior management and Board of Directors or a Committee to the Board;
  - Ineffective tracking and follow up;
  - Not sufficiently documented, including testing results;
  - Lack of an effective action plan to close findings; and
  - Results not available to the regulators

Conclusion from Exam Findings:

- Poor independent reviews continued to be one of the top three key factors for AML violations;
- The less the regulator can rely on the independent review, the longer the AML examination will take; and
- If systemic violations are found in the AML program, the independent review will probably also be cited.

Elements of a Strong AML Independent Review Program:

- Audit Scoping, Planning and Resources to be Utilized
  - Scoping
    - Comprehensive coverage of AML regulatory requirements;
    - Risk based - emphasizing the specific money laundering risks of the institution
  - Planning
    - Annually must re-assess the money laundering risks as business (products, customers, geography) continually changes;
    - Obtain prior
      - Regulatory examination
      - AML Independent Review
      - Changes in the business focus and infrastructure (controls)

Scoping & Planning – Comprehensive Coverage

- Documented AML and OFAC Policies and Procedures
- Risk Assessments (AML and OFAC)
- Designation of an AML Compliance Officer
- Senior management/Board approval of AML Program
- Customer Identification Program (CIP)
- KYC/CDD and EDD
- OFAC
- Cash/Monetary Instruments
- Foreign correspondent and private banking accounts
- Suspicious activity monitoring, escalation & reporting (SAR);
- AML system controls and data integrity
- BSA reporting (CTR, FBAR, CMIR, Travel Rule)
- On-going AML Training
- Record keeping/retention
- 314 (a) and (b)
- Special Measures
- Concentration Accounts
- Confidential reporting & employee conduct

Scoping & Planning – Risk Based

- Determining AML risks specific to your institution
  - Documentation to be reviewed:
    - Institution's latest BSA/AML and OFAC risk assessments
    - Last regulatory examination report for BSA/AML and OFAC related findings
    - Prior year's BSA/AML/OFAC independent review
    - AML/OFAC issues brought before the Board/Audit Committee/Senior Management Committee
    - Strategy and business plans for the organization (i.e., new customer segments, products, geographic expansion)
    - Structure, staffing, allocation of responsibilities in the BSA/AML department
    - Institution organizational chart by businesses and entities
    - Structure, changes and flow of AML/OFAC controls
      - Departments, people and systems

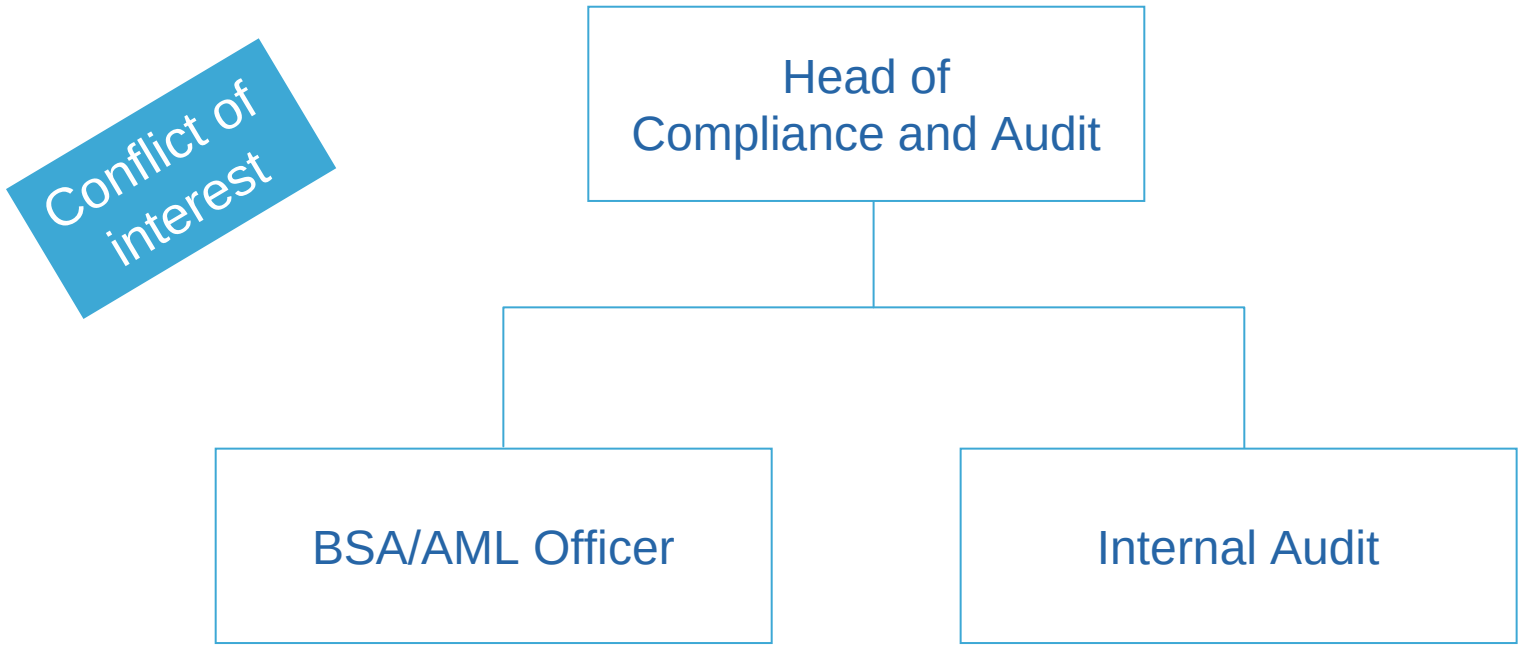
Scoping & Planning – Risk Based (continued)

- Management to be initially interviewed
  - BSA/AML Officer
  - Within major business lines and support units - key executives for awareness and responsibilities in the AML control process
    - Front office management for AML procedures at customer on boarding
    - Operational heads applying AML/OFAC controls
    - IT head for AML/OFAC and operational systems feeding transactional and customer information to AML monitoring systems and processes
  - AML/Compliance Committee and members
- Scoping must ensure
  - Coverage of entire AML/OFAC program; while also being
  - Risk based to allocate the independent reviewer's time and staff resources to areas of greater risk and heavier testing of internal controls

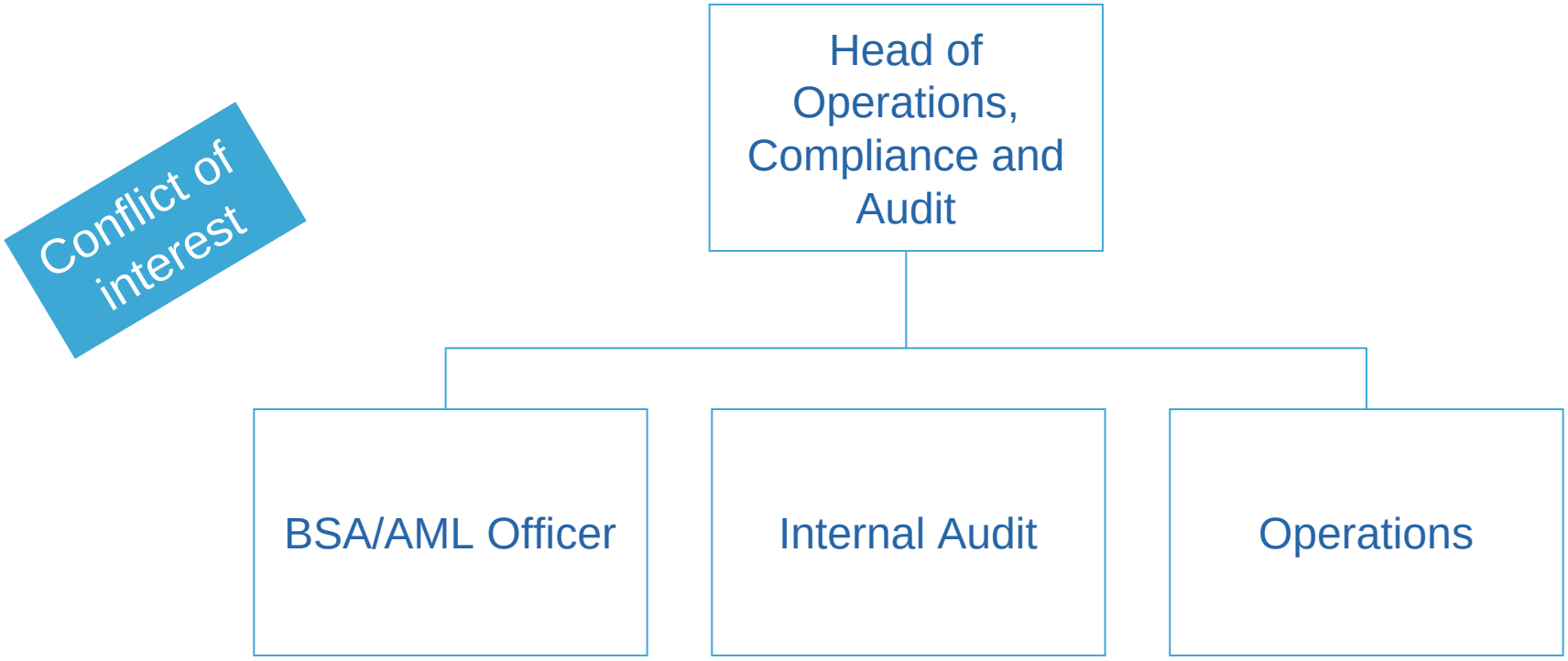
Independence & Resourcing

- Individual(s) performing the review must be independent of
  - Compliance management;
  - Any unit who performs a control(s) in the AML program;
  - Compliance, internal audit, units performing AML control functions should not report to the same executive; and
  - Limited exceptions for small broker-dealers (FINRA (NASD) Notice to Members 06-07)

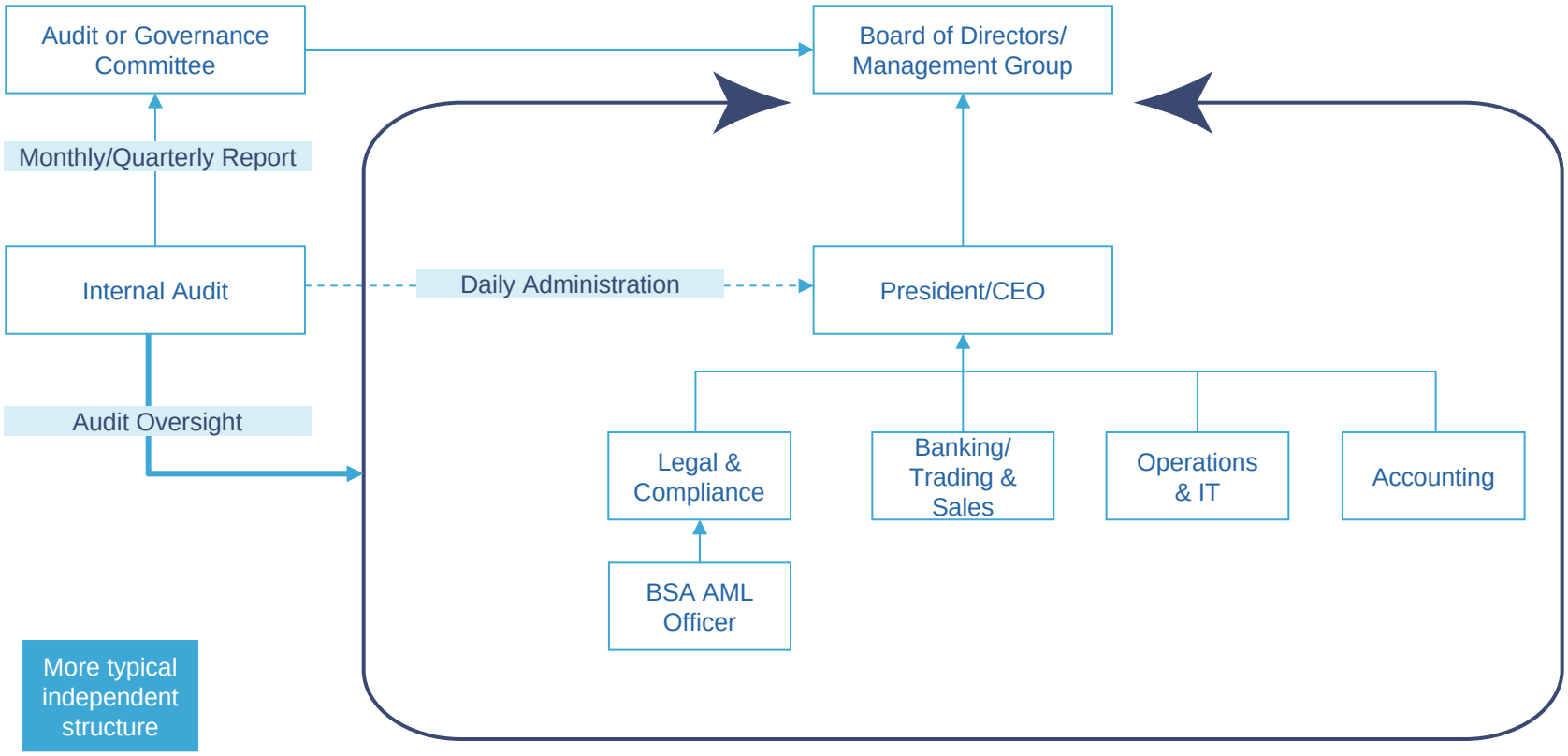
Independence & Resourcing (continued)



Independence & Resourcing (continued)



Independence & Resourcing (continued)



Independence & Resourcing (continued)

- Resources for the independent review:
  - Staff well versed of AML laws, rules and implementing regulations - training required
  - Understand potential money laundering risks across business lines
  - Staffing and time required to perform the independent review has been more than initially expected. Items affecting staff required:
    - Risk assessment
    - Number of business lines and products
    - Geography
    - Transactional volumes for appropriate sampling
    - New customer segments and IT AML systems

Risk Assessments

- Starting Point: Institution's latest BSA/AML and OFAC risk assessments:
  - Prepared by management; or
  - If assessments by management are either inadequate or do not exist, they will need to be developed by the Independent Review Team
  - Assessments need to cover:
    - Products
    - Customer types
    - Geographies
    - Controls in place to mitigate money laundering
    - A consolidated risk for institution; and a separate
    - Assessment for OFAC risks

Risk Assessments (continued):

- Management's risk assessments should be challenged by the auditor to ensure independent factors and other view points have been considered for the assessment
- Will guide the auditor to what management believes are the higher money laundering risk products, customers and geographic areas

Risk Assessments (continued)

Products	Customers	Geographies
• Complete coverage across all business lines – Consumer/Retail – Corporate/Institutional – Capital Markets/Treasury – Trust – Securities – Insurance	• Coverage of all customers regardless of business line or entity	• Overseas: • Special Measures • Offices • Volumes • Higher risks jurisdictions • FATF/NCCTs • OFAC sanctioned • State Dept-INCSR • Transparency Intl
• Channel of delivery: – Branches – Internet – Wires – ACH – Electronic cards – Pouch	• Ability to differentiate between customer groups on risk categorization: high (EDD), medium & low (CDD/KYC) • Customer focus and environs of the institution	• Domestic: • HIFCA • HIDTA

Risk Assessments (continued)

Products	Customers	Geographies
• Cash/Currency • Product convertibility – Monetary instruments • Length of term and ease of access/control • Speed and Transparency – Wire • New products or systems	• Higher risk segments, e.g.: – Shell Cos., PICs, Trusts – Cash intensive, Charities – PEPs, NRAs – MSBs, casas de cambio – High net worth individuals – Hedge funds	• OFAC – History of violations or Licenses for Sanction Programs
• AML controls established – CIP – CDD/KYC/EDD – Adverse data search – P&Ps – OFAC Checking – Monitoring		

Risk Assessments (continued)

- Products
  - Factors considered to risk rate each product:
    - Speed on transfers by product;
    - Restrictions on transfers;
    - Delivery channel(s) product is offered through
  - Internal controls may be mitigating factors to reduce, but not eliminate, gross product risk
    - CIP;
    - KYC/CDD;
    - Control procedures in place;
    - OFAC checking on product transactions;
    - On-going monitoring of the product
  - Some controls though may provide more limited comfort:
    - Manual controls
    - Newly implemented systems

Risk Assessments (continued)

- Customers
  - Risk scoring should be applied to customer types in order to differentiate high risk customers from the remaining part of the lower risk customer population
  - Will be needed to determine which customers must be subjected to enhanced due diligence requirements
  - No risk assessment ➔ no determination of high risk customers ➔ no EDD applied
  - Examples of higher risk customer segments
    - Non-resident aliens (NRAs)
    - High net worth individuals
    - Cash intensive businesses and MSBs
    - Entities in off-shore tax havens
    - Non-regulated financial institutions (e.g., hedge funds)
    - Trusts

Risk Assessments (continued)

  - All customers, across the institution, need to be risk rated, regardless of type (individual, corporate, institutional, partnerships, government entity, trusts, etc.)
  - An overall customer risk rating can be determined from the number of customers within each segment
- Geography
  - Where are transactions received from and sent to (both number and US dollar volume)
  - Compare to independent resources on risk of countries, including:
    - OFAC
    - FATF
    - US State Dept's INCSR Annual Report
    - Transparency Intl. Annual Corruption Index

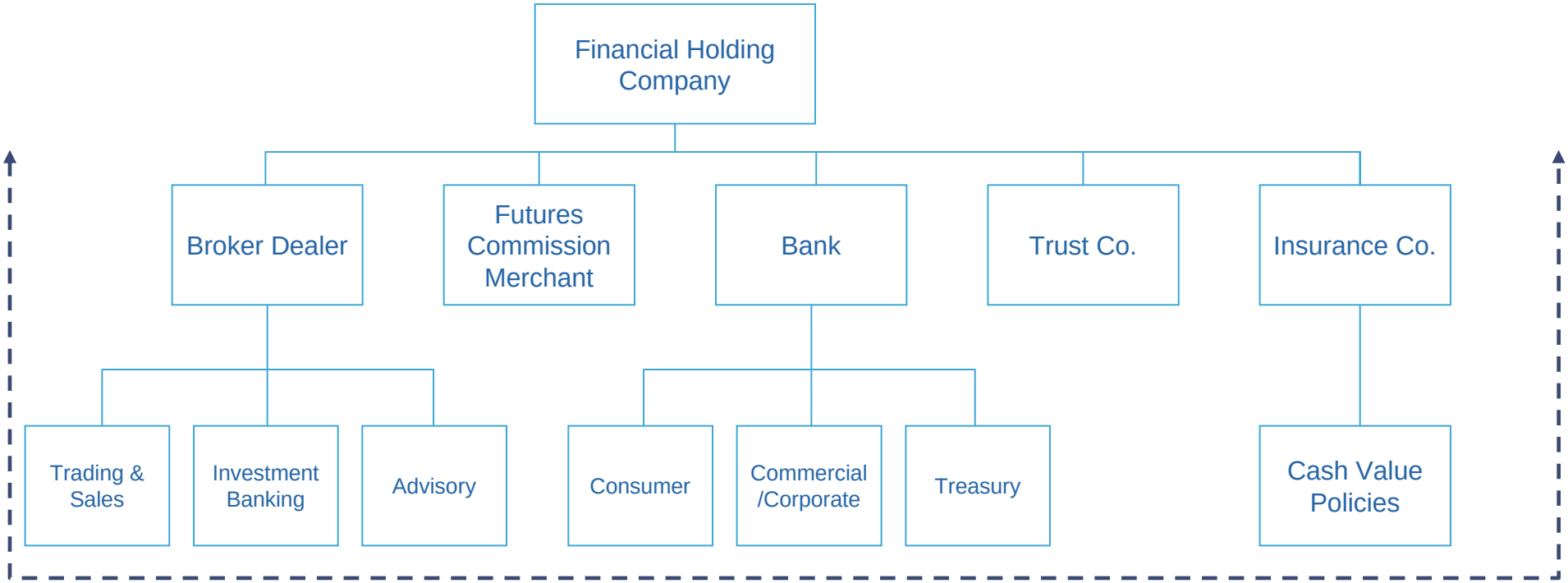
Risk Assessments (continued)

- Consolidated AML Risk Assessment
  - Products
  - Customers
  - Geographies
- A scale for the level of AML risk should be included and each level of risk defined
- Are levels of risk assigned appropriate to regulatory or industry guidance?
- Methodology, analysis and assumptions for each risk area/segment needs to be documented and auditable (road map)
  - Including any quantitative work performed, that underlies the conclusion
- Conclusion needs to be reached on the level of risk faced by the institution
- Similarly, OFAC risk assessment must also reach a conclusion
- Senior management should review and approve the assessments

Enterprise Wide Approach

- Independent review must examine AML and OFAC program and controls across the organization
- While regulators may be interested in the AML and OFAC programs of their specific regulated legal entity, the review must be able to cover all entities to ensure the entire AML and OFAC programs are reviewed
- Customers, products, systems and internal controls cutting across “silos” must be covered

Enterprise Wide Approach (continued)



AML Controls Across the Organization

Enterprise Wide Approach (continued)

- Allows AML audit team to
  - Report on enterprise wide trends
  - Potential AML violations, control weaknesses or suspicious activities that may lie within one entity or cut across the entire organization
- Risk of cross-entity AML control support
  - AML control(s) of one unit being outsourced to another
  - Independent review should examine that if any division/unit provides AML control support to another division/unit
  - The unit receiving the support should periodically ensure its quality
    - Testing of any Service Level Agreement

Audit Test Plans, Sampling and Test Results

- Comprehensive AML/OFAC program coverage and Risk Assessments will begin to guide the review team on allocation of man hours for the review
  - Check list for covering all requirements
  - Risk based for focusing on greater AML/OFAC risks to the organization
- As regulators will be the *primary* readers of these documents, the key audit requirement is
  - Document – Assumptions/Criteria
  - Document – Sample selection reasoning
  - Document – Testing results, findings and any reasons for overturning exceptions
  - If ever in doubt, Document

Audit Test Plans, Sampling and Test Results (continued)

- Ensure population selections cover the entire enterprise, e.g.,
  - CIP and KYC/CDD
    - All business lines and entities of their customer bases
  - CTRs and Monetary Instruments
    - All branches and entities transacting in cash or monetary instruments
  - Travel Rule
    - Sampling of wires
  - Review of Transactions in AML Monitoring System
    - Coverage of all businesses
    - Rule Algorithms/Parameters and threshold levels established
    - Review of alerts generated and resolved
    - Additional transactional testing if rules/parameters don't match the risks
  - 314(a)
    - All 314(a) requests over the audit period

Audit Test Plans, Sampling and Test Results (continued)

- When a program element's population is determined the sample size to be selected for testing will be influenced by
  - Frequency of the control being applied
  - Size of the overall population the sample will be selected from
  - Risk based assessment to the organization of the AML control failing
  - Automated or manual control being tested
  - Is the control new since the last review or already established?
  - Is the control being applied to new products, customer groups or locations?
- A consistent approach to the sample selection process should be maintained throughout the testing process of the review
- Inconsistency can undermine the testing results creating uncertainty as to whether relevant risks were properly and sufficiently tested

Audit Test Plans, Sampling and Test Results (continued)

- This does not mean the sampling approach must be exactly the same for each control tested
  - Approaches can be modified based upon the previous factors, but consistency in how changes in sample approach are made must be documented in detail
- Test Plan should include:
  - Population
    - Actual size and information on what was included and excluded (if any)
  - Sample Size
    - Methodology/logic utilized for testing to be applied
    - Not just saying “10% of the total population”, but why was the percentage chosen, what was the risk based reasoning for the selection of the sample
    - Ensure sample covers entire population
  - Describe Control and How It Is Being Tested
    - Frequency of the control and how applied (manual or automated)
    - Describe the test’s questions in detail; what is the auditor looking for in the test?

Audit Test Plans, Sampling and Test Results (continued):

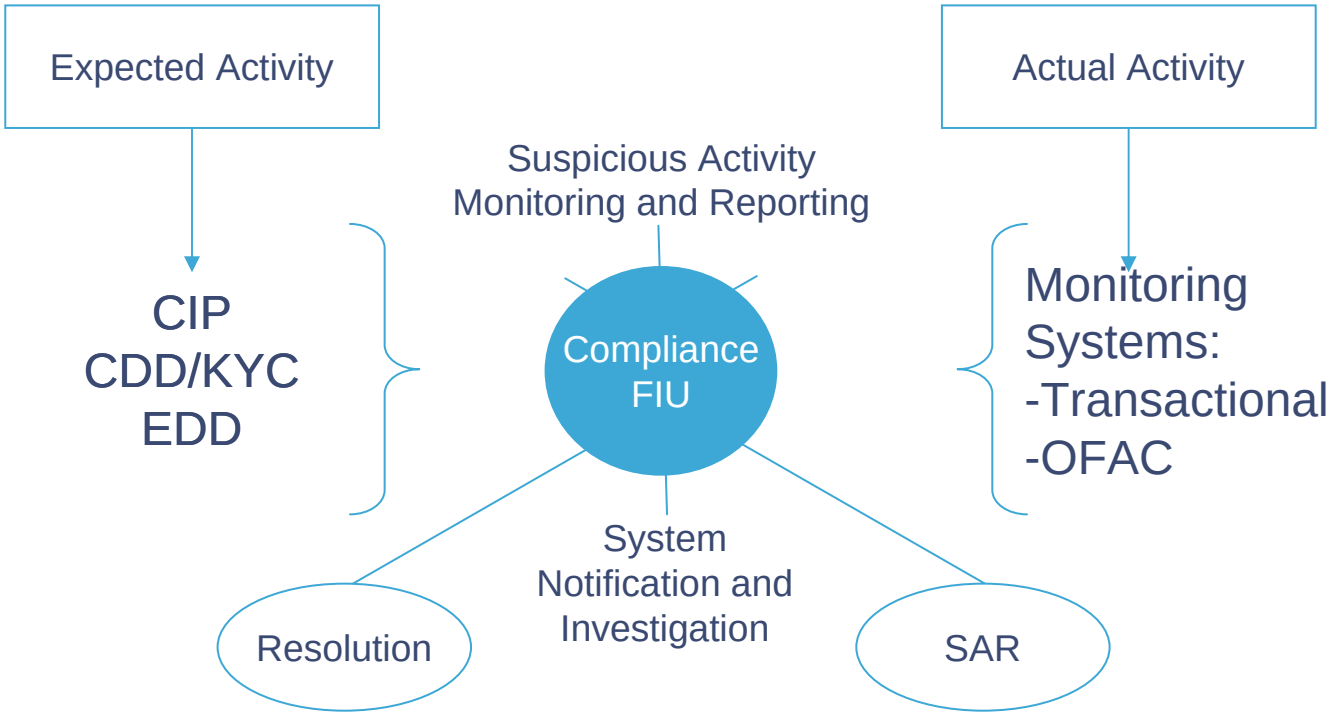
- May be testing not only what did get reported, but also what should have been and was not e.g.,:
  - BSA Reporting (e.g., SARs, CTRs, CMIRs, FBARs)
  - CTR Exemptions
  - Monetary Instruments
- Test Results
  - Detailed, and easily followed for reviewers (i.e., audit management and regulator)
  - Extreme caution should be applied for attempting to “explain away” a sample that fails a control
  - Based on results, determine whether sampling needs to be expanded and document conclusion
    - Are exceptions isolated or a systemic breakdown?

Audit Test Plans, Sampling and Test Results (continued)

- Recommendations by Audit
  - Must address the exceptions noted from the findings
  - Specific as possible, without selecting any one alternative
- Management Responses must
  - Address audit recommendations made, including:
    - Remediation plans to address the control weakness(es)
    - Responsible party(ies) to implement the new control. Management must ensure split responsibilities are addressed
    - Specific timeframe by which the finding(s) will be remediated

Expected versus Actual Activity

- Cornerstone of AML process:



Expected versus Actual Activity (continued):

- As noted in the FFIEC BSA Examination Manual, an independent review must test the accuracy of CDD/EDD information so that it can be used as a baseline for comparing actual activity
- The testing of actual transactional activity against CDD/EDD information, on a sample of customers, across customer classes and products is designed to determine whether that KYC information is accurate
  - Will unusual activity be captured in the monitoring?

Expected versus Actual Activity (continued)

- CDD/KYC:
  - Procedure exists and testing of documented information on:
    - Customer type (e.g., individual, partnership, trust)
    - How will the customer be using the accounts opened and products offered by the institution?
    - Financial information on the customer
    - Amount of information and how gathered will vary depending upon complexity and variety of products, services and transactions the customer plans to do:
      - Checking account only for monthly salary and bills
      - Checking, lending, L/Cs, international wire transfers
    - Reach a conclusion in order to assign a risk rating to the customer
    - Reviewing, approving, editing dated CDD/KYC information

Expected versus Actual Activity (continued)

  - Consistency on information gathered
  - How are exceptions handled by management
  - Updated to reflect changes in the customer
- EDD
  - Procedures in place for documenting additional due diligence information to be obtained on higher risk customers
  - Increased risk ➔ increased documentation/verification
  - Issue: No high risk customers or no additional documentation/verification

Expected versus Actual Activity (continued)

- Inconsistency in actual activity to KYC information could be due to one or a combination of factors, including:
  - Insufficient or outdated CDD/EDD information on the customer
  - Unfocused filtering or rule settings in the AML monitoring system
  - Missing transactional activity not being reviewed by the AML monitoring system
  - Insufficient manual review and analysis of warnings coming out of the AML monitoring system
- If a control gap is identified in the CDD/EDD process, additional testing may be required to determine how deep and broad the control lapse is across the institution (i.e., isolated or systemic)
- Were certain suspicious transactions missed as the CDD/EDD process and information was not effective and KYC information inaccurate?

Expected versus Actual Activity (continued)

- Monitoring Actual Activity
  - Procedures for creation and modifications to monitoring reports, including review and approvals
  - Monitoring reports should cover all customers, products and geographies
  - Alerts generated should have documented review by monitoring staff and management
    - Guidelines for required elements for a review and resolution of an alert (including KYC information)
    - Only initialing of a monitoring report containing alerts is not sufficient as no audit trail produced for the reasoning for each alert's resolution
    - Explanation for false positives, if frequent revision to rule thresholds

Expected versus Actual Activity (continued)

- Escalation and Reporting
  - Escalation of an alert into a case for investigation will need to have a documented trail, whether for a:
    - SAR; or
    - For a resolution of a case
  - Documentation to support the case should be maintained with investigator's write up of the case and its conclusion, including management review
  - Examiners have requested financial institutions to report AML statistics up to senior management or management committees, e.g.,:
    - Alerts generated by business area;
    - Number of cases opened/resolved by business area;
    - SARs filed

Expected versus Actual Activity (continued)

- Sample and Test
  - Alerts generated and review how resolved or escalated with reasoning and review approvals;
  - Why activity does not generate alerts based upon actual activity vs. expected activity?
  - Cases created from alerts that are subsequently either resolved or SARed reviewing documented reasoning for resolution or SARing
  - What and how is information reported and reviewed (with evidence) by senior management

AML and OFAC Monitoring Systems

- AML Systems
  - Monitoring systems are only as good as the data entered and the rules developed to generate alerts
  - Systems must not be set up on “generic vendor rules”. The system needs to be customized to the institution’s potential money laundering risks from its products, customers and business locations
  - AML Independent Review will need to include
    - An evaluation of the methodology of the system (and subsequent updates) and what it is designed to identify
    - An assessment of whether the system is capturing and evaluating all of the customers and activities that it should be capturing (i.e., data leakages)
    - Testing of the system to determine whether it is identifying or capturing reportable events or suspicious activities as intended:
      - Sampling of customer accounts (activity) to test the quality of alerts

AML and OFAC Monitoring Systems (continued)

  - Sample of accounts that are reasonably representative of the population (may wish to increase based on risk)
  - Statistical analyses can be used to comparing alerts generated to SARs filed, as well as to compare alert algorithms for their effectiveness and usefulness
- Is the information from KYC data passed correctly into the monitoring system for accurate comparisons to actual activity?
- A review of change management procedures (test and production environments) and user access controls
- An evaluation of the process in place to follow-up on identified items (i.e., alerts)
- A review of the documented reasoning for the rules developed in the AML system. Rule development should tie back to the risks (a mapping) in the AML risk assessment
- Documented reasons and approvals for creation, deletion and changes to all rules within the AML system

AML and OFAC Monitoring Systems (continued)

  - Where the testing of the AML technology determines that the AML controls provided by the technology are weak or inadequate, additional transactional testing may need to be performed
- OFAC Systems
  - Documentation on methodology of how OFAC systems are checking transactional names and countries against OFAC lists
  - Evidence for testing the following vs. OFAC lists:
    - New customers
    - All customers at the time of revision to the OFAC lists
    - All transactions to/from the institution
  - Be aware of different OFAC list vendors and how the information is provided to your institution on a timely basis
    - More than one vendor across business lines

AML and OFAC Monitoring Systems (continued)

- IT Audit Component
  - Do not underestimate the application of the IT audit practice on AML and OFAC systems
  - Becoming more critical in the eyes of the regulators
    - FFIEC: Audit of IT systems http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#audit
    - SIFMA Best Practice advises: “For automated systems, verify with the IT Audit Department that system tests are routinely conducted and reviewed and that the parameters of such tests are properly established.“

Documentation

- As you might expect
  - Detailed
  - Thorough
  - Easily followed by the regulator (i.e., clear audit trail) from: risk assessment ➔ audit plan ➔ audit programs ➔ population ➔ sample ➔ testing results ➔ findings ➔ recommendations
- Assumptions and Methodologies
  - Completely described with supporting reasons
  - Business lines, products, customers, geographies -receiving the risk-based focus
  - How are populations and sample sizes determined?
    - Not just, “10% of the population was selected”
    - WHY 10%?

Documentation (continued)

- The single page report or a report that indicates that the AML compliance program or its program components are "Adequate" or "Satisfactory" is not sufficient
- Reports need to significantly detail:
  - AML requirements being tested,
  - Provide observations regarding documented policies and procedures,
  - Documented findings from testing results on the effectiveness of the controls tested, and
  - Provide recommendations to address identified gaps in findings.
- If findings are either modified or removed from the review report, provide written details as to why, including appropriate review and approval of such changes
- Recommendations must be focused to the issues uncovered, but allow management the flexibility of alternatives to address the findings outlined
- Timetables and assignment of responsible parties to address all recommendations MUST be in management’s responses

Reporting, Continued Follow-Up, and Escalation

- FFIEC Exam Manual
  - "The findings should be reported directly to the board of directors or an audit committee composed primarily or completely of outside directors."
- NASD (FINRA) Notice to Members 02-21
  - "After a test is complete, the internal testing personnel or qualified outside party should report its findings to senior management or to an internal audit committee, as appropriate."
- Reporting
  - Senior management (i.e., CCO, General Counsel, Chief Risk Officer)
  - Audit Committee to the Board of Directors
  - Minutes of the meeting should be taken documenting comments and follow up actions noted by members
  - Follow-up reporting on all open issues needs to occur until all findings are addressed (i.e., no loose ends)

Reporting, Continued Follow-Up, and Escalation (continued)

- Reporting process is to show regulators that management is
  - aware of issues,
  - taking them seriously and
  - have management address all issues in an expeditious fashion
- A formal issue tracking mechanism or leveraging existing internal audit processes to identify parties responsible for remediation and to track identified issues to resolution.
- Extended delays in closing findings and implementing agreed-upon recommendations should also be reported back to senior management and the Audit Committee so that delays can be addressed in an expedited fashion and have management's focused attention.

Updating the Independent Review Program

- Program must be updated and revised each year as the institution changes:
  - Risk assessment of the institution
    - Products
    - Customers
    - Geographies
  - Organizational structures
  - Infrastructure systems and reporting lines of management
    - Data systems feeding AML/OFAC monitoring systems
    - Changing management responsibilities for AML/OFAC procedures and processes
- Ensure overall coverage of AML and OFAC programs
- Be risk-based, recognizing changing risks of the institution – risk levels are not static
- Include in the new program that all prior findings have been addressed in a timely fashion and remain closed

In Conclusion

- A robust independent review program can help identify and address AML control weaknesses before they become a problem and are identified during a regulatory examination.
- Utilizing the independent review can help to avoid:
  - Regulatory examination findings
  - Public or private written agreements with regulators
  - Fines and costly transactional look-back reviews
  - Reputational risk from AML/OFAC violations
- Leveraging the review will also aid the process of capturing sustainable efficiencies across the organization for the investment made in enterprise wide AML controls
- Identification of AML/OFAC issues in a independent review is always preferable to the same items being found during a regulatory examination. It should be leveraged as much as possible.

Questions

Contact Information

Stephen J. Lurie
Director
FS Regulatory
PricewaterhouseCoopers LLP (pwc.com)
300 Madison Avenue – Room 27112.1
New York, NY 10017
Telephone: +1 646 471 5129
Facsimile: +1 813 329 5442
Mobile: +1 914 980 0319

pwc.com

PRICEWATERHOUSECOOPERS