Utilizing Internal Audits to Pinpoint Gaps in Your Institution’s AML Program

Mitigating AML Risk Seminar Series
November 30, 2011 – New York
Discussion Topics

• Internal Audit – In the Crosshairs of the Regulators
• Internal Audit’s Role in AML Compliance
• Importance of Risk-Based Independent AML Auditing
• Planning and Executing a Risk-Based AML Audit
• Commonly Cited Internal Audit-Related Deficiencies
• Credentializing Internal Audit to Avoid Regulatory Criticism
• Q & A
Internal Audit - “In the Crosshairs”

• “…the internal audit function did not adequately evaluate and test the Bank’s suspicious activity monitoring system and related reporting procedures…the internal audit function also did not track adverse compliance findings by supervisory authorities…”

• “…the Bank’s program for independent testing was materially deficient…the scope of the audit function was insufficient to assess the adequacy of the AML program on an enterprise-wide basis…”
Internal Audit - “In the Crosshairs” continued

• “materially deficient internal audit process that failed to
detect [AML] inadequacies…no accounts were
independently sampled or tested for suspicious activity…”

• “…the knowledge and training of the Internal Audit staff
did not appear sufficient in regards to BSA / AML
compliance…certain areas were not correctly defined within
audit scope memos and were not properly
reviewed…critical gaps were noted, including: inadequate
audit coverage of client transaction testing, a lack of
adequate post-implementation review of monitoring
software, and numerous data integrity concerns…”
Case Study – Citibank Japan

Background:

• Between 1997 and 2003, Citibank Japan increased the number of private banking customers from 600 to 6,000.
• The Japan unit was delivering the most robust profit growth of all of Citigroup's private bank locations.
• Successively higher net-income goals imposed on this unit by Head Office in NY.

Warning Signs or “Red Flags”

• In August 2001, Japan's Financial Services Authority (FSA) flagged Citibank Japan’s private bank for 30 infractions, including selling securities without prior authorization.
• These problems were never remediated.
• June 2003, a private banker structured a deal in which six private-banking customers extended to a Tokyo school what amounted to a one-year loan of about $7 million at an effective interest rate of 26%.
Findings from the FSA’s Inspection:

• “Law-evading” system being operated – culture where “client development and securing profits given unduly heavy importance.”
• Poor due diligence – bank “virtually skipped” advance reviews of customers and transactions and failed to investigate the intended use of funds.
• Bank “promoted transactions” with a customer even though another overseas Citibank branch had filed a SAR on that client.
• Financing offered to “aid customers with their wrongdoing.” A number of improper transactions were “used to manipulate accounting records and defer loss recognition.”

Results:

• In September of 2004, FSA orders Citibank’s Private Banking division in Japan to stop accepting new customers and to discontinue operations by September 2005.
• Six local officers and three senior executives in NY were dismissed.
• Sweeping reforms to be undertaken by Citibank, including changes to their internal audit function.
Thomas W. Jones, one of the three top Citigroup Inc. executives dismissed last month, accused his former employer of unfairly holding him accountable for a private-banking scandal in Japan. "Do I feel there's anything more I could have done?" asked Mr. Jones, former chief executive of Citigroup investment and asset-management units, in reference to the private-banking problems in Japan. "The answer is 'no.'"

In an interview, Mr. Jones, dressed in a dark, pin-striped suit, attributed the regulatory actions in Japan to problems that stretched across business lines, and said that Citigroup auditors in New York had failed to flag the problems for him and other executives at the financial-services firm's Park Avenue headquarters. "Given the responsibilities and seniority of the three individuals, it was appropriate for each of them to leave the company," a Citigroup spokeswoman responded. "The decision was made after a thorough and thoughtful review that was supported by, among other things, the work of an independent, outside adviser." She declined to comment further on Mr. Jones's comments.

In September, Japanese regulators yanked Citigroup's private-banking license and charged the company with violations ranging from failure to implement safeguards against money laundering to misleading customers about the risks of investments. The then-head of Citigroup's global private bank, Peter Scaturro, reported to Mr. Jones.

On an Oct. 19 internal memorandum, Chief Executive Officer Charles Prince said that Messrs. Jones and Scaturro and Vice Chairman Deryck Maughan would leave Citigroup. In announcing the departures, Citigroup said nothing about the involvement of the three executives in the problems in Japan. But people familiar with the dismissals linked the departures to the report on the private-banking problem, which was prepared by former U.S. Comptroller of the Currency Eugene Ludwig.
Basis for AML-Related Audits

- USA PATRIOT Act (Section 352)
- Financial Action Task Force (FATF) Recommendation No. 15 [paragraph (c)]
- Bank for International Settlements / Basel Committee
- International Organization of Securities Commissions (IOSCO)
- Joint Money Laundering Steering Group (JMLSG)
- Individual country legislation, regulations and directives (e.g., UK FSA Handbook)
Key AML / Sanctions Program Components

- Designated AML Compliance Officer
- Internal Policies, Procedures, and Controls
  - Prevention
    - Customer Risk Rating
  - Customer Identification Program (CIP)
    - Customer Due Diligence (CDD)
    - Enhanced Due Diligence (EDD)
  - OFAC Screening and Reporting
  - Suspicious Activity Reporting (SAR)
- Detection
  - Transaction Monitoring
  - Currency Transaction Reporting
  - Surveillance and Case Management
  - Receiving & Responding to Information Requests from the Federal Government
  - Sharing Information with Other Financial Institutions
- Employee Training Program
- Independent Testing of the AML Compliance Program
US Requirements / Expectations (FFI EC BSA/ AML Examination Manual)

• Must be periodic (but how often not specified in law or regulations).
  o Exam Manual says 12 – 18 months or more often as indicated by risk profile (p. 34).

• Must be performed by an independent person, including but not limited to the internal audit department, accountants, or consultants.

• Should be “comprehensive, accurate, adequate, and timely” (p. 40, para. 7).

• Should mirror the regulatory on-site examination.
US Requirements / Expectations continued

• Should be risk based – focus on highest risks faced by financial institution.

• Is one of the first documents reviewed by the examiners

  o Serves as a window into the compliance culture of the financial institution.

• BSA/AML requirements are constantly evolving, not always by intelligent design – care should be taken not only to constantly update internal policies, procedures and controls, but also to verify their effectiveness through an independent audit.

• Don’t be the last one on your block to comply - regulators are never happy with outliers.
Formulating a Risk-Based AML Audit Plan

• Evaluate risk assessment performed by AML Officer

• Alignment of risk appetite to the actual strategy and policies of the financial institution

• Internal Audit may need to conduct its own risk assessment of the various businesses and AML-related functions within its organization; note that the FFIEC Exam Manual and the IRS MSB Manual both require (yes, require) the examiner to prepare a risk assessment if the risk assessment is absent or defective

• Many ways to skin a cat…
Risk Assessment Factors

- Customers / Entities
- Geographies
- Products and Services
- Distribution Channels
- Transaction Flows
- Organizational Structure and Tone
- LOB-Specific Policies and Procedures
- Transaction Monitoring / Surveillance Capabilities
Risk Assessment Factors continued

- Results of Prior Internal Audits and Regulatory Examinations
- AML-Related Projects / Initiatives Currently Being Undertaken
- New Business and/or New Product Development
- SARs Filed
- 314(a) and 314(b) Referrals
- Subpoena Volume
- OFAC Blocking and Rejecting Activity
Conducting Effective AML Audits

AML audits should never be “box checking” exercises; specific skills necessary to ensure quality of execution include:

- Knowledge of regulatory expectations – both those required by law and seen in practice.
- Understanding of evolving regulations.
- Knowledge of market leading AML software solutions and how they work.
- Understanding of the “red flags” unique to the business being audited.
- Ability to distinguish between regulatory violations and industry best practices.
- Appropriate, robust workpapers that are commonly reviewed by regulators upon request.
### Typical Audit Approach

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OBJECTIVE</strong></td>
<td><strong>KEY ACTIVITIES</strong></td>
<td><strong>WORK PRODUCTS</strong></td>
<td><strong>Final Reporting</strong></td>
<td></td>
</tr>
<tr>
<td>- Conduct planning sessions with AML Compliance Officer and other key stakeholders</td>
<td>- Conduct interviews and walkthroughs with key process owners</td>
<td>- Audit Announcement &amp; Kick-Off Meeting</td>
<td>- Produce a written report that outlines audit procedures performed, findings resulting from testing, and recommendations for process and procedure improvements</td>
<td></td>
</tr>
<tr>
<td>- Understand business model (including risks)</td>
<td>- Identify inherent risks and evaluate existing controls to mitigate such risks</td>
<td>- Gap analysis comparing policies/procedures against regulatory requirements, regulatory expectations, and industry best practices</td>
<td>- Produce a written report that includes a conclusion about the overall quality of the AML program</td>
<td></td>
</tr>
<tr>
<td>- Target work effort</td>
<td>- Determine whether policies/procedures are sufficiently documented and address regulatory requirements, expectations, and industry best practices</td>
<td>- Process narratives and flowcharts</td>
<td>- Develop matrix that compiles gaps and deficiencies</td>
<td></td>
</tr>
<tr>
<td>- Finalize audit (testing) scope and approach</td>
<td>- Provide management with an initial gap analysis</td>
<td>- Testing documentation (e.g., sample selection rationale, detailed testing spreadsheets)</td>
<td>- Recommend policy/procedure and control improvements</td>
<td></td>
</tr>
<tr>
<td>- Review risk assessments</td>
<td>- Evaluate AML policies and procedures against regulatory requirements</td>
<td>- Finalize results of work performed</td>
<td>- Findings &amp; Recommendations</td>
<td></td>
</tr>
<tr>
<td>- Review results of prior internal audits, regulatory exams, and other external program assessments</td>
<td>- Prepare gap analysis</td>
<td>- Compile list of findings from process walk throughs and detailed testing</td>
<td>- Final Report</td>
<td></td>
</tr>
</tbody>
</table>

### Work Products

- Audit Planning Memo
- Final Report
Planning / Scoping for the AML Audit

• Review results of previous audits and any regulatory examination reports.
• Determine whether previously identified issues were addressed and/or remediated.
• Monitor for any negative news or publicity related to lapses in AML-related controls.
• Apply lessons learned from other organizations in the news.
• Identify new products and services and/or establishment of operations in new markets and assess their impact on the organization’s money laundering risk.
• Assess adequacy of the risk assessment – if there is one!
AML Audit Execution - Areas for Assessment

- Oversight and Management of the AML Compliance Program
- Policies, Procedures, and Internal Controls
- Employee Training
- Customer Risk Rating / Scoring Protocols
- Customer Identification Program (CIP)
- Customer Due Diligence (CDD) / Enhanced Due Diligence (EDD)
- Politically Exposed Persons (PEPs)
- Transaction Monitoring / Account Surveillance
- Suspicious Activity Reporting
- Currency Monitoring and Transaction Reporting
- Purchase and Sale of Monetary Instruments
- Foreign Correspondent Accounts
- Funds Transfers
- Information Sharing
- Special Measures
- Office of Foreign Assets Control (OFAC)
- Documentation and Recordkeeping
- Vendor Management
# Evaluating IT-Related Processes & Controls

<table>
<thead>
<tr>
<th>IT Focus Area</th>
<th>Key Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Identification Program (CIP), Customer Due Diligence</td>
<td>• Assess customer identification, profiling, risk rating and investigation capability</td>
</tr>
<tr>
<td>(includes KYC and EDD)</td>
<td></td>
</tr>
<tr>
<td>Transaction Monitoring / Account Surveillance</td>
<td>• Perform pre / post implementation review of monitoring / surveillance tool (also see note below)</td>
</tr>
<tr>
<td>Currency Monitoring and Transaction Reporting</td>
<td>• Assess appropriateness of mechanism used to identify all currency transactions exceeding reporting thresholds</td>
</tr>
<tr>
<td>Funds Transfer</td>
<td>• Validate technology has been implemented to enable compliance with BSA Travel and Recordkeeping rules for EFTs</td>
</tr>
<tr>
<td>Information Sharing</td>
<td>• Evaluate Data Mining capabilities</td>
</tr>
<tr>
<td>Special Measures</td>
<td>• Evaluate Data Mining capabilities</td>
</tr>
<tr>
<td></td>
<td>• Validate technology has been implemented to enable independent searches of information systems or other appropriate records</td>
</tr>
<tr>
<td>OFAC Requirements</td>
<td>• Perform pre / post implementation review of software utilized to facilitate compliance with OFAC requirements (Note 1)</td>
</tr>
<tr>
<td></td>
<td>• Evaluate data capture and screening functionality</td>
</tr>
<tr>
<td>Documentation and Recordkeeping</td>
<td>• Evaluate procedures to track, store and control documents</td>
</tr>
<tr>
<td></td>
<td>• Destruction or disposal of documents reaching their retention control date</td>
</tr>
</tbody>
</table>

*Note: Evaluation of IT general controls supporting the application (logical security, change management, backup and operations) should also be undertaken*
# Why Data Analytics & AML?

<table>
<thead>
<tr>
<th>Why?</th>
<th>Potential Impact</th>
<th>Example</th>
</tr>
</thead>
</table>
| To validate the data quality across customer and transactional data.| • Missing customer fields could cause incorrect profiling or other identification issues  
• Wrong data in fields could cause reporting rules to not catch suspicious activity | • Customers with missing information may be dropped  
• Debit and credit transactions may not be applied to the right product types |
| To validate the processing of transaction monitoring scenarios       | • Current reporting could be incorrectly missing suspicious activity per current rules/scenarios.  
• Data warehouse may be filtering and changing records. The data transport integrity needs to be validated by implementing data quality checks and balances. | • Reporting engine was performing exact matches on key words rather than using fuzzy logic which led to missing suspicious activities  
• Retail broker-dealer X was “householding” home phone numbers but would fail in most instances because the formats were different |
| To benchmark scenarios against leading practices                    | • AML rules may not be sufficient and the risk assessment can be implemented in operations by identifying and defining suspicious activity.  
• Further historical analysis may yield insight into scenario’s not currently identified | • Using historical data, analysts can map out a typical transactions that deviate from a standard transaction and generate models for scenario based testing |
| To help the client develop ongoing monitoring tools & procedures to gauge the performance of its AML system and rules | • Evaluating the AML system at one point in time creates the risk that new money laundering behaviors are not captured by current transaction models.  
• Scenario’s may become non-applicable to business | • Changes to warehouse logic could cause AML reporting to break |
Internal Audit’s Role in the BSA/ AML Exam Process

• Prior to Exam
  • Upon Exam Announcement
• During the Exam
• Upon Exam Completion
Internal Audit’s Role in the BSA/AML Exam Process

- Monitor the situation and apply healthy tension to ensure your institution’s responsiveness
- Separately track examination issues and validate the completion of corrective actions
- Provide separate reports on the status of remediation efforts to your institution’s executive bodies
- Accelerate the timetable for future AML audits
- Conduct limited transaction lookbacks (due to regulatory mandate)
  - Final determination for SAR filings still the responsibility of the AML Compliance Officer or his/her designees
Regulatory Expectations

Independent audits of AML programs have come under increasingly greater scrutiny from regulators. Specifically, regulators expect that a strong independent audit program:

- is risk based and sufficient in scope and frequency
- is sufficiently budgeted in terms of hours and optimal staffing levels
- contains audit work programs that have been tailored to the risks unique to the organization under review
- has workpapers that are adequately documented and that have clear linkages between risk assessments and work programs
- includes sufficient transaction testing (both quantitative and qualitative)
- contains proper follow-up of prior findings/remediation plans
- is executed by competent individuals (individuals who are sufficiently trained, certified in the subject matter, and possess the necessary auditing expertise)

Regulators typically ask for bios/credentials of the audit team
Commonly Cited Audit-Related Deficiencies

• Lack of rigorous risk assessment process.
• Frequency and scope of audits not risk-based.
• Unqualified and/or inexperienced personnel conducting the audits.
• Lack of sufficient transaction testing.
• Little or no follow-up of previously identified issues to ensure appropriate corrective actions were taken.
• Lack of professional skepticism exercised by auditors.
• Sloppy workpapers.
Credentializing Internal Audit to Avoid Regulatory Criticism

- Qualified, skilled, and experienced team.
- Certified Anti-Money Laundering Specialist (CAMS) professionals.
- Prioritization of coverage by risk.
- Enterprise-wide approach (where possible).
- Adequate time allocated to planning / preparing for the audit.
- Transparent process / timely escalation of issues.
- Robust workpapers.
- Appropriate / tailored reporting and issue tracking.
Questions ?
Speaker Bio

Vasilios P. Chrisos, CAMS
Office: +1 212 231 0705
Email: vasilios.chrisos@macquarie.com

Vasilios is the Americas Anti-Money Laundering (AML) and Economic Sanctions Director for Macquarie, Australia’s largest investment bank. He is responsible for managing the company’s AML and sanctions programs across all business groups and legal entities in North and South America. This includes coordinating the completion of risk assessments, developing and implementing policies and procedures, ensuring employees receive periodic AML training, acting as an adviser to stakeholders regarding AML/CTF and sanctions matters, managing investigations, as appropriate, ensuring Suspicious Activity Reports are prepared and filed timely, performing compliance testing, participating in the new business / product approval process, and chairing various AML Working Groups across the region.

Prior to joining Macquarie, Vasilios helped lead Ernst & Young’s AML advisory practice by managing projects / initiatives at large, complex institutions. He assisted and advised financial services institutions in developing comprehensive AML risk assessment frameworks, identifying inherent money laundering vulnerabilities, establishing customer risk ranking protocols, designing AML compliance programs, implementing policies, procedures, and controls, creating AML governance structures, establishing Enhanced Due Diligence (EDD) protocols, and developing transaction monitoring capabilities. Vasilios has worked with financial institutions that were either undergoing or facing regulatory enforcement actions and advised them on the construction of action plans and communication strategies with regulators, including regular updates on the progress of remediation efforts.

Vasilios is a Certified Anti-Money Laundering Specialist (CAMS). He currently serves as the Co-Chair of the ACAMS New York Chapter and is also involved with several ACAMS initiatives, including: the global Chapter Steering Committee and Education, Securities Industry, and Audit task forces.