Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-38-2008
May 16, 2008

Bank Secrecy Act

Provision for Independent Testing for BSA/AML Compliance

Summary: The independent test of the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Compliance Program can improve the efficiency and reduce the burden of the examination process.

Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
BSA Compliance Office

Related Topics:
Bank Secrecy Act/Anti-Money Laundering Programs

Attachment:
Independent Testing text from the *2007 FFIEC BSA/AML Examination Manual*

Contact:
Review Examiner Heather L. Basnett
SASFIL@FDIC.gov or (202) 898-3673

Note:
FDIC Financial Institution Letters (FILs) may be accessed from the FDIC's Web site at http://www.fdic.gov/news/news/financial/2008/index.html

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC FILs may be obtained through the FDIC's Public Information Center, 3501 N. Fairfax Drive, Room E 1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

The importance of an effective independent review, an original component of the BSA/AML Compliance Program, cannot be overstated.

- An effective audit is valued by regulators in identifying and monitoring a bank's specific risks and by assessing how those risks are managed and controlled. Effective audits will assist examiners in determining the BSA/AML examination scope and in identifying areas requiring less review.

- The *FFIEC BSA/AML Examination Manual* provides details regarding the BSA/AML Compliance Program, states minimum areas to be covered by the independent audit, and addresses limiting transaction testing to the independent review.

- Independent testing (audit) assists the bank's board of directors and senior management by identifying areas of weakness or matters requiring stronger controls. The audit should be risk-based and will vary depending on the bank's size, complexity, risk profile, quality of control functions, geographic diversity, and use of technology. By incorporating the bank's *BSA/AML Risk Assessment* into the independent testing process, the audit program can be more effectively tailored to cover all of the bank's activities.
  - Independent testing of the BSA/AML Compliance Program should be conducted by the internal audit department, outside auditors, consultants, or other qualified persons that are independent of the BSA/AML function.
  - If the audit is being performed by an outside party, a contract or engagement letter should be agreed upon that outlines responsibilities and duties. Contracts typically include provisions stating that audit reports are property of the bank, authorized employees will have reasonable and timely access to workpapers, and that the bank will be provided copies of related workpapers, as the bank deems necessary. Further, such agreements should grant examiners access to all workpapers and other materials prepared in the course of the audit.

The following is from the *2007 FFIEC BSA/AML Examination Manual*.

Independent Testing

Independent testing (audit) should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. While the frequency of audit is not specifically defined in any statute, a sound practice is for the bank to conduct independent testing generally every 12 to 18 months, commensurate with the BSA/AML risk profile of the bank. Banks that do not employ outside auditors or consultants or have internal audit departments may comply with this requirement by using qualified persons who are not involved in the function being tested. The persons conducting the BSA/AML testing should report directly to the board of directors or to a designated board committee comprised primarily or completely of outside directors.

Those persons responsible for conducting an objective independent evaluation of the written BSA/AML compliance program should perform testing for specific compliance with the BSA, and evaluate pertinent management information systems (MIS). The audit should be risk based[1] and evaluate the quality of risk management for all banking operations, departments, and subsidiaries. Risk-based audit programs will vary depending on the bank's size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology. An effective risk-based auditing program will cover all of the bank's activities. The frequency and depth of each activity's audit will vary according to the activity's risk assessment. Risk-based auditing enables the board of directors and auditors to use the bank's risk assessment to focus the audit scope on the areas of greatest concern. The testing should assist the board of directors and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

Independent testing should, at a minimum, include:

- An evaluation of the overall integrity and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes.
- A review of the bank's risk assessment for reasonableness given the bank's risk profile (products, services, customers, entities, and geographic locations).
- Appropriate risk-based transaction testing to verify the bank's adherence to the BSA recordkeeping and reporting requirements (e.g., CIP, SARs, CTRs and CTR exemptions, and information sharing requests).
- An evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if applicable.
- A review of staff training for adequacy, accuracy, and completeness.
- A review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for BSA/AML compliance. Related reports may include, but are not limited to:
    - Suspicious activity monitoring reports.

[1] Refer to Appendix J ("Quantity of Risk Matrix") for guidance.

  - Large currency aggregation reports.
  - Monetary instrument records.
  - Funds transfer records.
  - Nonsufficient funds (NSF) reports.
  - Large balance fluctuation reports.
  - Account relationship reports.
- An assessment of the overall process for identifying and reporting suspicious activity, including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness of the bank's policy.
- An assessment of the integrity and accuracy of management information systems (MIS) used in the BSA/AML compliance program. MIS includes reports used to identify large currency transactions, aggregate daily currency transactions, funds transfer transactions, monetary instrument sales transactions, and analytical and trend reports.

Auditors should document the audit scope, procedures performed, transaction testing completed, and findings of the review. All audit documentation and workpapers should be available for examiner review. Any violations, policy or procedures exceptions, or other deficiencies noted during the audit should be included in an audit report and reported to the board of directors or a designated committee in a timely manner. The board or designated committee and the audit staff should track audit deficiencies and document corrective actions.