

BSA/AML Compliance Program — Overview

Objective. *Assess the adequacy of the bank’s BSA/AML compliance program. Determine whether the bank has developed, administered, and maintained an effective program for compliance with the BSA and all of its implementing regulations.*

Review of the bank’s written policies, procedures, and processes is a first step in determining the overall adequacy of the BSA/AML compliance program. The completion of applicable core and, if warranted, expanded examination procedures is necessary to support the overall conclusions regarding the adequacy of the BSA/AML compliance program. Examination findings should be discussed with the bank’s management, and significant findings must be included in the report of examination or supervisory correspondence.

The BSA/AML compliance program³⁰ must be written, approved by the board of directors,³¹ and noted in the board minutes. A bank must have a BSA/AML compliance program commensurate with its respective BSA/AML risk profile. Refer to the core overview section, “BSA/AML Risk Assessment,” page 18, for additional guidance on developing a BSA/AML risk assessment. Refer to Appendix I (“Risk Assessment Link to the BSA/AML Compliance Program”) for a chart depicting the risk assessment’s link to the BSA/AML compliance program. Furthermore, the BSA/AML compliance program must be fully implemented and reasonably designed to meet the BSA requirements.³² Policy statements alone are not sufficient; practices must coincide with the bank’s written policies, procedures, and processes. The BSA/AML compliance program must provide for the following minimum requirements:

- A system of internal controls to ensure ongoing compliance.
- Independent testing of BSA/AML compliance.

³⁰ The Board of Governors of the Federal Reserve System (Federal Reserve) requires Edge and agreement corporations and U.S. branches, agencies, and other offices of foreign banks supervised by the Federal Reserve to establish and maintain procedures reasonably designed to ensure and monitor compliance with the BSA and related regulations (refer to Regulation K, 12 CFR 211.5(m)(1) and 12 CFR 211.24(j)(1)). In addition, because the BSA does not apply extraterritorially, foreign offices of domestic banks are expected to have policies, procedures, and processes in place to protect against risks of money laundering and terrorist financing (12 CFR 208.63 and 12 CFR 326.8).

³¹ The Federal Reserve, the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC), each require the U.S. branches, agencies, and representative offices of the foreign banks they supervise operating in the United States to develop written BSA compliance programs that are approved by their respective bank’s board of directors and noted in the minutes, or that are approved by delegates acting under the express authority of their respective bank’s board of directors to approve the BSA compliance programs. “Express authority” means the head office must be aware of its U.S. AML program requirements and there must be some indication of purposeful delegation. For those U.S. branches, agencies, and representative office of foreign banks that were already in compliance with existing obligations under the BSA (and usual and customary business practices), the BSA compliance program requirement should not impose additional burden. Refer to 71 Fed. Reg. 13936 (March 20, 2006). Refer to expanded overview section, “Foreign Branches and Offices of U.S. Banks,” page 164, for further guidance.

³² Refer to Appendix R (“Enforcement Guidance”), for additional information.

- Designate an individual or individuals responsible for managing BSA compliance (BSA compliance officer).
- Training for appropriate personnel.

In addition, a CIP must be included as part of the BSA/AML compliance program. Refer to the core overview section, “Customer Identification Program,” page 47, for additional guidance.

Internal Controls

The board of directors, acting through senior management, is ultimately responsible for ensuring that the bank maintains an effective BSA/AML internal control structure, including suspicious activity monitoring and reporting. The board of directors and management should create a culture of compliance to ensure staff adherence to the bank’s BSA/AML policies, procedures, and processes. Internal controls are the bank’s policies, procedures, and processes designed to limit and control risks and to achieve compliance with the BSA. The level of sophistication of the internal controls should be commensurate with the size, structure, risks, and complexity of the bank. Large complex banks are more likely to implement departmental internal controls for BSA/AML compliance. Departmental internal controls typically address risks and compliance requirements unique to a particular line of business or department and are part of a comprehensive BSA/AML compliance program.

Internal controls should:

- Identify banking operations (i.e., products, services, customers, entities, and geographic locations) more vulnerable to abuse by money launderers and criminals; provide for periodic updates to the bank’s risk profile; and provide for a BSA/AML compliance program tailored to manage risks.
- Inform the board of directors, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, and corrective action taken, and notify directors and senior management of SARs filed.
- Identify a person or persons responsible for BSA/AML compliance.
- Provide for program continuity despite changes in management or employee composition or structure.
- Meet all regulatory recordkeeping and reporting requirements, meet recommendations for BSA/AML compliance, and provide for timely updates in response to changes in regulations.³³
- Implement risk-based CDD policies, procedures, and processes.
- Identify reportable transactions and accurately file all required reports including SARs, CTRs, and CTR exemptions. (Banks should consider centralizing the review and report-filing functions within the banking organization.)

³³ Refer to Appendix P (“BSA Record Retention Requirements”) for guidance.

- Provide for dual controls and the segregation of duties to the extent possible. For example, employees that complete the reporting forms (such as SARs, CTRs, and CTR exemptions) generally should not also be responsible for the decision to file the reports or grant the exemptions.
- Provide sufficient controls and systems for filing CTRs and CTR exemptions.
- Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity.
- Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations.
- Incorporate BSA compliance into the job descriptions and performance evaluations of bank personnel, as appropriate.
- Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines.

The above list is not designed to be all-inclusive and should be tailored to reflect the bank's BSA/AML risk profile. Additional policy guidance for specific risk areas is provided in the expanded sections of this 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. Banks that employ outside auditors or consultants should ensure that qualified persons doing the BSA/AML testing are not involved in other BSA functions such as training or developing policies and procedures that may present a conflict or lack of independence.

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 and evaluate the quality of risk management for all banking operations, departments, and subsidiaries. Risk-based audit programs 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 covers all of the bank's activities. The frequency and depth of each activity's audit varies 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 adequacy and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes. Typically, this evaluation includes an explicit statement about the BSA/AML compliance program's overall adequacy and effectiveness and compliance with applicable regulatory requirements. At the very least, the audit should contain sufficient information for the reviewer (e.g., an examiner, review auditor, or BSA officer) to reach a conclusion about the overall quality of the BSA/AML compliance program.
- 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.
 - 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 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.

BSA Compliance Officer

The bank's board of directors must designate a qualified individual to serve as the BSA compliance officer.³⁴ The BSA compliance officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance. The BSA compliance officer is also charged with managing all aspects of the BSA/AML compliance program and with managing the bank's adherence to the BSA and its implementing regulations; however, the board of directors is ultimately responsible for the bank's BSA/AML compliance.

While the title of the individual responsible for overall BSA/AML compliance is not important, his or her level of authority and responsibility within the bank is critical. The BSA compliance officer may delegate BSA/AML duties to other employees, but the officer should be responsible for overall BSA/AML compliance. The board of directors is responsible for ensuring that the BSA compliance officer has sufficient authority and resources (monetary, physical, and personnel) to administer an effective BSA/AML compliance program based on the bank's risk profile.

The BSA compliance officer should be fully knowledgeable of the BSA and all related regulations. The BSA compliance officer should also understand the bank's products, services, customers, entities, and geographic locations, and the potential money laundering and terrorist financing risks associated with those activities. The appointment of a BSA compliance officer is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority, or time to satisfactorily complete the job.

The line of communication should allow the BSA compliance officer to regularly apprise the board of directors and senior management of ongoing compliance with the BSA. Pertinent BSA-related information, including the reporting of SARs filed with FinCEN, should be reported to the board of directors or an appropriate board committee so that these individuals can make informed decisions about overall BSA/AML compliance. The BSA compliance officer is responsible for carrying out the direction of the board and ensuring that employees adhere to the bank's BSA/AML policies, procedures, and processes.

Training

Banks must ensure that appropriate personnel are trained in applicable aspects of the BSA. Training should include regulatory requirements and the bank's internal BSA/AML policies,

³⁴ The bank must designate one or more persons to coordinate and monitor day-to-day compliance. This requirement is detailed in the federal banking agencies' BSA compliance program regulations: 12 CFR 208.63, 12 CFR 211.5(m), and 12 CFR 211.24(j) (Federal Reserve); 12 CFR 326.8 (FDIC); 12 CFR 748.2 (NCUA); 12 CFR 21.21 (OCC).

procedures, and processes. At a minimum, the bank's training program must provide training for all personnel whose duties require knowledge of the BSA. The training should be tailored to the person's specific responsibilities. In addition, an overview of the BSA/AML requirements typically should be given to new staff during employee orientation. Training should encompass information related to applicable business lines, such as trust services, international, and private banking. The BSA compliance officer should receive periodic training that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall BSA/AML risk profile of the bank.

The board of directors and senior management should be informed of changes and new developments in the BSA, its implementing regulations and directives, and the federal banking agencies' regulations. While the board of directors may not require the same degree of training as banking operations personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the bank. Without a general understanding of the BSA, the board of directors cannot adequately provide BSA/AML oversight; approve BSA/AML policies, procedures, and processes; or provide sufficient BSA/AML resources.

Training should be ongoing and incorporate current developments and changes to the BSA and any related regulations. Changes to internal policies, procedures, processes, and monitoring systems should also be covered during training. The training program should reinforce the importance that the board and senior management place on the bank's compliance with the BSA and ensure that all employees understand their role in maintaining an effective BSA/AML compliance program.

Examples of money laundering activity and suspicious activity monitoring and reporting can and should be tailored to each individual audience. For example, training for tellers should focus on examples involving large currency transactions or other suspicious activities; training for the loan department should provide examples involving money laundering through lending arrangements.

Banks should document their training programs. Training and testing materials, the dates of training sessions, and attendance records should be maintained by the bank and be available for examiner review.