

BSA/AML INDEPENDENT TESTING

Objective: *Assess the adequacy of the bank's independent testing program.*

The purpose of independent testing (audit) is to assess the bank's compliance with BSA regulatory requirements, relative to its risk profile, and assess the overall adequacy of the BSA/AML compliance program. Independent testing should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties.¹

Banks that do not employ outside auditors or consultants or do not have internal audit departments may comply with this requirement by using qualified bank staff who are not involved in the function being tested. Banks engaging outside auditors or consultants should ensure that the persons conducting the BSA/AML independent testing are not involved in other BSA-related functions at the bank that may present a conflict of interest or lack of independence, such as training or developing policies and procedures. Regardless of who performs the independent testing, the party conducting the BSA/AML independent testing should report directly to the board of directors or to a designated board committee comprised primarily, or completely, of outside directors. Banks with a community focus, less complex operations, and lower-risk profiles for ML/TF and other illicit financial activities may consider utilizing a shared resource as part of a collaborative arrangement to conduct independent testing.²

There is no regulatory requirement establishing BSA/AML independent testing frequency. Independent testing, including the frequency, should be commensurate with the ML/TF and other illicit financial activity risk profile of the bank and the bank's overall risk management strategy. The bank may conduct independent testing over periodic intervals (for example, every 12-18 months) and/or when there are significant changes in the bank's risk profile, systems, compliance staff, or processes. More frequent independent testing may be appropriate when errors or deficiencies in some aspect of the BSA/AML compliance program have been identified or to verify or validate mitigating or remedial actions.

Independent testing of specific BSA requirements should be risk-based and evaluate the quality of risk management related to ML/TF and other illicit financial activity risks for significant banking operations across the organization. Risk-based independent testing focuses on the bank's risk assessment to tailor independent testing to the areas identified as being of greatest risk and concern. Risk-based independent testing programs vary depending on the bank's size or complexity, organizational structure, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology. Risk-based independent testing should include evaluating pertinent internal controls and information technology sources, systems, and processes used to support the BSA/AML compliance program. Consideration should also be given to the expansion into new product lines, services, customer types, and geographic locations through organic growth or merger activity.

¹ 12 CFR 208.63(c)(2) (Federal Reserve); 12 CFR 326.8(c)(2) (FDIC); 12 CFR 748.2(c)(2) (NCUA); 12 CFR 21.21(d)(2) (OCC)

² For detailed information on collaborative arrangements see "[Interagency Statement on Sharing Bank Secrecy Act Resources](#)," issued by Federal Reserve, FDIC, FinCEN, NCUA, and OCC, October 3, 2018.

The independent testing should evaluate the overall adequacy of the bank's BSA/AML compliance program and the bank's compliance with BSA regulatory requirements. This evaluation helps inform the board of directors and senior management of weakness, or areas in need of enhancements or stronger controls. Typically, this evaluation includes an explicit statement in the report(s) about the bank's overall compliance with BSA regulatory requirements. At a minimum, the independent testing should contain sufficient information for the reviewer (e.g., board of directors, senior management, BSA compliance officer, review auditor, or an examiner) to reach a conclusion about the overall adequacy of the BSA/AML compliance program.

To contain sufficient information to reach this conclusion, independent testing of the BSA/AML compliance program and BSA regulatory requirements may include a risk-based review of whether:

- The bank's BSA/AML risk assessment aligns with the bank's risk profile (products, services, customers, and geographic locations).
- The bank's policies, procedures, and processes for BSA compliance align with the bank's risk profile.
- The bank adheres to its policies, procedures, and processes for BSA compliance.
- The bank complies with BSA recordkeeping and reporting requirements (e.g., customer information program (CIP), customer due diligence (CDD), beneficial ownership, suspicious activity reports (SARs), currency transaction reports (CTRs) and CTR exemptions, and information sharing requests).
- The bank's overall process for identifying and reporting suspicious activity is adequate. This review may include evaluating filed or prepared SARs to determine their accuracy, timeliness, completeness, and conformance to the bank's policies, procedures, and processes.
- The bank's information technology sources, systems, and processes used to support the BSA/AML compliance program are complete and accurate. These may include reports or automated programs used to: identify large currency transactions, aggregate daily currency transactions, record monetary instrument sales and funds transfer transactions, and provide analytical and trend reports.
- Training is provided for appropriate personnel, tailored to specific functions and positions, and includes supporting documentation.
- Management took appropriate and timely action to address any violations and other deficiencies noted in previous independent testing and regulatory examinations, including progress in addressing outstanding supervisory enforcement actions, if applicable.

Auditors should document the independent testing scope, procedures performed, transaction testing completed, and any findings. All independent testing documentation and supporting workpapers should be available for examiner review. Violations; exceptions to bank policies, procedures, or processes; or other deficiencies noted during the independent testing should be documented and reported to the board of directors or a designated board committee in a timely

manner. The board of directors, or a designated board committee, and appropriate staff should track deficiencies and document progress implementing corrective actions.

Examiners should review relevant documents such as the auditor's report(s), scope, and supporting workpapers, as needed. Examiners should determine whether there is an explicit statement in the report(s) about the bank's overall compliance with BSA regulatory requirements or, at a minimum, sufficient information to reach a conclusion about the overall adequacy of the BSA/AML compliance program. Examiners should determine whether the testing was conducted in an independent manner. Examiners may also evaluate, as applicable,³ the subject matter expertise, qualifications and independence of the person or persons performing the independent testing. Examiners should determine whether the independent testing sufficiently covers ML/TF and other illicit financial activity risks within the bank's operations and whether the frequency is commensurate with the bank's risk profile. Examiners should also review whether violations; exceptions to policies, procedures, or processes; or other deficiencies are reported to the board of directors or a designated board committee in a timely manner, whether they are tracked, and whether corrective actions are documented.

[Return to Contents](#)

³ For more information, *see e.g.*, OCC Safety and Soundness Standards, 12 C.F.R. Part 30 App. D, II.L.