BANK SECRECY ACT: OVERVIEW AND PROCEDURES FOR ASSESSING THE BSA/AML COMPLIANCE PROGRAM

OVERVIEW

The BSA/AML examination is intended to assess the effectiveness of the credit union’s BSA/AML compliance program and compliance with the regulatory requirements, including a review of risk management practices.

Whenever possible, the scoping and planning process should be completed before entering the credit union. During this process, it may be helpful to discuss BSA/AML matters with management, including the BSA compliance officer, either in person or by telephone. The scoping and planning process generally begins with an analysis of:

- Off-site monitoring information.
- Prior examination reports and workpapers.
- Request letter items completed by credit union management.
- The credit union’s BSA/AML risk assessment.
- The credit union’s written compliance program.
- Independent reviews or audits.

Review of the Credit Union’s BSA/AML Risk Assessment

The scoping and planning process should be guided by the examiner’s review of the credit union’s BSA/AML risk assessment. Information gained from the examiner’s review of the risk assessment will assist the scoping and planning process as well as the evaluation of the adequacy of the BSA/AML compliance program. If the credit union has not developed a risk assessment, this fact should be discussed with management. For the purposes of the examination, whenever the credit union has not completed a risk assessment, or the risk assessment is inadequate, the examiner must complete a risk assessment.

Independent Testing

As part of the scoping and planning process, examiners should obtain and evaluate the supporting documents of the independent testing of the credit union’s BSA/AML compliance program. The scope and quality of the audit may provide examiners with a sense of particular risks in the credit union, how these risks are being managed and controlled, and the status of compliance with the BSA. The independent testing scope and workpapers can assist examiners in understanding the audit coverage and the

---

1 This overview is excerpted from the Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Moneylaundering Examination Manual and is adapted to apply to credit unions.
quality and quantity of transaction testing. This knowledge will assist the examiner in determining the examination scope, identifying areas requiring greater (or lesser) scrutiny, and identifying when expanded examination procedures may be necessary.

**Examination Plan**

At a minimum, examiners should conduct the examination procedures to ensure that the credit union has an adequate BSA/AML compliance program commensurate with its risk profile.

As part of the scoping and planning procedures, examiners must review the credit union’s OFAC risk assessment and independent testing to determine the extent to which a review of the credit union’s OFAC compliance program should be conducted during the examination.

The examiner should develop and document an initial examination plan commensurate with the overall BSA/AML risk profile of the credit union. This plan may change during the examination as a result of on-site findings, and any changes to the plan should likewise be documented. On the basis of the risk profile, quality of audit, previous examination findings, and initial examination work, examiners should complete additional core and expanded examination procedures, as appropriate. The examiner must include an evaluation of the BSA/AML compliance program within the supervisory plan or cycle.

**Transaction Testing**

Examiners perform transaction testing to evaluate the adequacy of the credit union’s compliance with regulatory requirements, determine the effectiveness of its policies, procedures, and processes, and evaluate suspicious activity monitoring systems. Transaction testing is an important factor in forming conclusions about the integrity of the credit union’s overall controls and risk management processes. Transaction testing must be performed at each examination and should be risk-based. Transaction testing can be performed either through conducting the transaction testing procedures within the independent testing (audit) section (refer to the core examination procedures, “BSA/AML Compliance Program,” Examiner’s Manual pages 38 to 43, for further guidance) or completing the transaction testing procedures contained elsewhere within the core or expanded sections.

The extent of transaction testing and activities conducted is based on various factors including the examiner’s judgment of risks, controls, and the adequacy of the independent testing. Once on-site, the scope of the transaction testing can be expanded to address any issues or concerns identified during the examination. Examiners should document their decision regarding the extent of transaction testing to conduct, the activities for which it is to be performed, and the rationale for any changes to the scope of transaction testing that occur during the examination.
Information Available From BSA-Reporting Database

Examination planning should also include an analysis of the Suspicious Activity Reports (SARs), Currency Transaction Reports (CTR), and CTR exemptions that the credit union has filed. FinCEN Form 104 is the CTR report.

The examiners should:

- Identify high-volume currency customers.
- Assist in selecting accounts for transaction testing.
- Identify the number and characteristics of SARs filed.
- Identify the number and nature of exemptions.

Identification of Specific Risk Categories

The first step of the risk assessment process is to identify the specific products, services, customers, entities, and geographic locations unique to the credit union. Although attempts to launder money, finance terrorism, or conduct other illegal activities through a credit union can emanate from many different sources, certain products, services, customers, entities, and geographic locations may be more vulnerable or have been historically abused by money launderers and criminals. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered when the credit union prepares its risk assessment. The differences in the way a credit union interacts with the customer (face-to-face contact versus electronic banking) also should be considered. Because of these factors, risks will vary from one credit union to another. In reviewing the credit union’s risk assessment, examiners should determine whether management has developed an accurate risk assessment that identifies the significant risks to the credit union.

Products and Services

Certain products and services offered by credit unions may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Some of these products and services are listed below, but the list is not all inclusive:
- Electronic funds payment services — electronic cash (e.g., prepaid and payroll cards), funds transfers (domestic and international), payable upon proper identification (PUPID) transactions, third-party payment processors, remittance activity, automated clearing house (ACH) transactions, and automated teller machines (ATM).
- Electronic banking.
- Trust and asset management services.
- Monetary instruments.
- Foreign correspondent accounts (e.g., bulk shipments of currency, pouch activity, payable through accounts (PTA), and U.S. dollar drafts).
- Trade finance.
- Services provided to third party payment processors or senders.
- Foreign exchange.
- Special use or concentration accounts.
- Lending activities, particularly loans secured by cash collateral and marketable securities.
- Nondeposit account services (e.g., nondeposit investment products and insurance).

Customers and Entities

Although any type of account is potentially vulnerable to money laundering or terrorist financing, by the nature of their business, occupation, or anticipated transaction activity, certain customers and entities may pose specific risks. At this stage of the risk assessment process, it is essential that credit unions exercise judgment and neither define nor treat all members of a specific category of customer as posing the same level of risk. In assessing customer risk, credit unions should consider other variables, such as services sought and geographic locations. The expanded sections of the FFIEC manual provide guidance and discussion on specific customers and entities that are detailed below:

- Foreign financial institutions, including banks and foreign money services providers (e.g., casas de cambio, currency exchanges, and money transmitters).
- Nonbank financial institutions (e.g., money services businesses; casinos and card clubs; brokers/dealers in securities; and dealers in precious metals, stones, or jewels).
- Senior foreign political figures and their immediate family members and close associates (collectively known as politically exposed persons (PEP)). Nonresident alien (NRA) and accounts of foreign individuals.
- Foreign corporations and domestic business entities, particularly offshore corporations (such as domestic shell companies and Private Investment Companies (PIC) and international business corporations (IBC) located in higher-risk geographic locations.
Deposit brokers, particularly foreign deposit brokers.
- Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators, and parking garages).
- Nongovernmental organizations and charities (foreign and domestic).
- Professional service providers (e.g., attorneys, accountants, doctors, or real estate brokers).

**Geographic Locations**

Identifying geographic locations that may pose a higher risk is essential to a credit union’s BSA/AML compliance program. Credit unions should understand and evaluate the specific risks associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not necessarily determine a customer’s or transaction’s risk level, either positively or negatively.

Higher-risk geographic locations can be either international or domestic. International higher-risk geographic locations generally include:

- Countries subject to OFAC sanctions, including state sponsors of terrorism.
- Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State.
- Jurisdictions determined to be “of primary money laundering concern” by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the USA PATRIOT Act.
- Jurisdictions or countries monitored for deficiencies in their regimes to combat money laundering and terrorist financing identified as non-cooperative by international entities such as the Financial Action Task Force on Money Laundering (FATF).
- Major money laundering countries and jurisdictions identified in the U.S. Department of State’s annual International Narcotics Control Strategy Report (INCSR), in particular, countries which are identified as jurisdictions of primary concern.
- Offshore financial centers (OFC).
- Other countries identified by the credit union as higher-risk because of its prior experiences or other factors (e.g., legal considerations, or allegations of official corruption).

Domestic higher-risk geographic locations may include, but are not limited to, banking offices doing business within, or having customers located within, a U.S. government–designated higher-risk geographic location. Domestic higher-risk geographic locations include:
- High Intensity Drug Trafficking Areas (HIDTA).
- High Intensity Financial Crime Areas (HIFCA).

**Analysis of Specific Risk Categories**

The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess BSA/AML risk. This step involves evaluating data pertaining to the credit union’s activities (e.g., number of: domestic and international funds transfers; private banking customers; foreign correspondent accounts; PTAs; and domestic and international geographic locations of the credit union’s business area and customer transactions) in relation to Customer Identification Program (CIP) and customer due diligence (CDD) information. The level and sophistication of analysis may vary by credit union. The detailed analysis is important because within any type of product or category of customer there will be accountholders that pose varying levels of risk.

This step in the risk assessment process gives management a better understanding of the credit union’s risk profile in order to develop the appropriate policies, procedures, and processes to mitigate the overall risk. Specifically, the analysis of the data pertaining to the credit union’s activities should consider, as appropriate, the following factors:

- Purpose of the account.
- Actual or anticipated activity in the account.
- Nature of the customer’s business/occupation.
- Customer’s location.
- Types of products and services used by the customer.

The value of a two-step risk assessment process is illustrated in the following example. The data collected in the first step of the risk assessment process reflects that a credit union sends out 100 international funds transfers per day. Further analysis may show that approximately 90 percent of the funds transfers are recurring well-documented transactions for long-term customers. On the other hand, the analysis may show that 90 percent of these transfers are nonrecurring or are for noncustomers. While the numbers are the same for these two examples, the overall risks are different.

As illustrated above, the credit union’s CIP and CDD information take on important roles in this process. Refer to the core overview sections, "Customer Identification Program" and "Customer Due Diligence," found in FFIEC Examiner’s Manual for additional guidance.

**BSA/AML Compliance Program**
The BSA/AML compliance program must be written, approved by the board of directors, and noted in the board minutes. Furthermore, the BSA/AML compliance program must be fully implemented and reasonably designed to meet the BSA requirements. Policy statements alone are not sufficient; practices must coincide with the credit union’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.
- 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," in FFIEC Examiner’s Manual, for additional guidance.

**Internal Controls**

The board of directors, acting through senior management, is ultimately responsible for ensuring that the credit union 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 credit union’s BSA/AML policies, procedures, and processes. Internal controls are the 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 credit union. Large credit unions 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 credit union 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 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.
• Implement risk-based CDD policies, procedures, and processes.
• Identify reportable transactions and accurately file all required reports including SARs, CTRs, and CTR exemptions. (Credit unions should consider centralizing the review and report-filing functions.)
• 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 credit union personnel, as appropriate.
• Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines.

Examiner Development of a BSA/AML Risk Assessment

In some situations, credit unions may not have performed or completed an adequate BSA/AML risk assessment and examiners must complete one based on available information. When doing so, examiners do not have to use any particular format. In such instances, documented workpapers should include the credit union’s risk assessment, the deficiencies noted in the risk assessment, and the examiner-prepared risk assessment.

Examiners should ensure that they have a general understanding of the bank’s BSA/AML risks and, at a minimum, document these risks within the examination scoping process. This section provides some general guidance that examiners can use when they are required to complete a BSA/AML risk assessment. In addition, examiners may share this information with bankers to develop or improve their own BSA/AML risk assessment.

The risk assessment developed by examiners generally will not be as comprehensive as one developed by a credit union. However, similar to what is expected in a credit union’s risk assessment, examiners should obtain information on the products,
services, customers, entities, and geographic locations to determine the volume and trend for potentially higher-risk areas. This process can begin with an analysis of:

- Prior examination or inspection reports and workpapers.
- Response to request letter items.
- Discussions with credit union management and appropriate regulatory agency personnel.

Examiners should complete this analysis by reviewing the level and trend of information pertaining to banking activities identified, for example:

- Funds transfers.
- Monetary instrument sales.
- Foreign correspondent accounts and PTAs.
- Branch locations.
- Domestic and international geographic locations of the credit union’s business area.

This information should be evaluated relative to such factors as the credit’s total asset size, customer base, entities, products, services, and geographic locations. Examiners should exercise caution if comparing information between credit unions and use their experience and insight when performing this analysis. Specifically, examiners should avoid comparing the number of SARs filed by a credit union to those filed by another credit union in the same geographic location. Examiners can and should use their knowledge of the risks associated with products, services, customers, entities, and geographic locations to help them determine the credit union’s BSA/AML risk profile. Examiners may refer to the FFIEC Examiner’s Manual Appendix J (“Quantity of Risk Matrix”) when completing this evaluation.

**Examiner Determination of the Credit Union’s BSA/AML Aggregate Risk Profile**

The examiner, during the "Developing Conclusions and Finalizing the Examination" phase of the BSA/AML examination, should assess whether the controls of the credit union’s BSA/AML compliance program are appropriate to manage and mitigate its BSA/AML risks. Through this process the examiner should determine an aggregate risk profile for the credit union. This aggregate risk profile should take into consideration the risk assessment developed either by the credit union or by the examiner and should factor in the adequacy of the BSA/AML compliance program. Examiners should determine whether the credit union’s BSA/AML compliance program is adequate to appropriately mitigate the BSA/AML risks, based on the risk assessment. The existence of BSA/AML risk within the aggregate risk profile should
not be criticized as long as the credit union’s BSA/AML compliance program adequately identifies, measures, monitors, and controls this risk as part of a deliberate risk strategy. When the risks are not appropriately controlled, examiners must communicate to management and the board of directors the need to mitigate BSA/AML risk. Examiners should document deficiencies as directed in the core examination procedures.

Citations:

Bank Secrecy Act of 1970  12 USC 1829b, 12 USC 1951-1959, 31 USC 5311 et seq
Anti-Drug Abuse Act of 1986
Money Laundering Control Act of 1986
Money Laundering Suppression Act (1994)
USA PATRIOT Act (2001) Title III
US Treasury/FinCEN Regulations, 31 CFR Chapter X, Part 1020
NCUA Rules and Regulations 12 CFR 748.2

**FFIEC Examiners Manual**


www.fincen.gov

**EXAMINATION PROCEDURES**

Complete the following AIRES questionnaires:

BSA

OFAC