BSA Exams/ Audits Made Easy

AuditLink

15 Ingredients to Ensure Success!

Introduction

Authored by: Jim Vilker, VP of Professional Services, CAMS, NCCO

Successful BSA Audits are a critical component of your credit union's operations, but to prepare for your BSA Exam/Audit can be overwhelming. You may begin with concerns about what's at stake if you don't pass your audit. You may have trepidation when you look at the final implications, including the reputation risk with your peer groups, your board, and, even worse, your members. You may have staff members or managers who are at the beginning stages of learning your policies, procedures, and best practices and are not yet familiar with the examination process.

Do not begin your exam with a deep sense of anxiety. The "Preparing for Your BSA Exam/Audits Made Easy" booklet takes all the worry out of preparing for next exam.

AuditLink has teamed up with the best BSA auditors in the country, Lillie and Company to ensure you will always be ready for an external audit or exam. Our partnership combines our expertise of CU*BASE (reports and best practices) with their track record providing credit unions with auditing and consulting services exclusively designed for credit unions across the country.

We share the passion that a BSA exam/audit should be as much an educational experience as forming an opinion on the credit union's BSA program. This booklet ensures you ready, educated, and confident when the auditor or examiner sends their checklist.

Revision date: November 9, 2022

\

CONTENTS

ACRONYMS USED IN THIS DOCUMENT

Below are several acronyms used in this document

AML	Anti-Money Laundering
BSA	Bank Secrecy Act
CDD	Customer Due Diligence
CIP	Customer Identification Program
CTR	Currency Transaction Report
DOB	Date of Birth
DOEP	Designation of Exempt Person
EDD	Enhanced Due Diligence
FFIEC	Federal Financial Institutions Examination Council
FINCEN	Financial Crimes Enforcement Network
FOM	Field of Membership
HIDTA	High Intensity Drug Trafficking Areas
HIFCA	High Intensity Financial Crime Areas
ISO	Independent Service Organization
MRB	Marijuana-related Business
MSB	Money Services Business
ML/TF	Money Laundering/Terrorist Financing
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Persons
SAR	Suspicious Activity Report
SSN	Social Security Number

Additionally, the following terms are used interchangeably:

- Bank, Banks, Savings Associations, Credit Unions
- Customer, Member

RISK ASSESSMENT

PURPOSE

A well-developed BSA/OFAC Risk Assessment is the cornerstone of an effective BSA program and identifies the credit union's institutional risk profile.

A risk assessment enables your management to better manage and mitigate gaps in operational controls. It drives policies, procedures, and internal controls. The risk assessment should be shared across all business lines within the credit union and all business line leaders should be actively involved in the process.

It is used by auditors and examiners to scope out the review of your BSA program. A poorly done risk assessment can lead to a more exhaustive third-party review and will not provide the BSA officer with winning arguments relative to the credit union's program.

EXPECTATIONS

The risk assessment should include qualitative and quantitative analysis which will drive your risk classifications. Having a data analyst or data-driven reports at the table will provide you with the data needed to help you understand the different components of your assessment. Additionally, this will help you win arguments relative to the quality of your program or need to invest in additional loss mitigation controls.

At least annually and prior to audit or examination, review the risk assessment to ensure that it assesses risk based on your unique credit union profile. Structure the assessment process to include the inherent risk of each area reviewed. Once the inherent risks are defined, include all loss mitigation controls in place and then define the residual risk remaining. Remember, the loss mitigation controls serve as the checklists which third parties will use to test the effectiveness of your program.

The primary components of a good risk assessment should follow FFIEC guidelines and include the following:

- Demographics (FOM, member composition, communities served (e.g. low income)).

- Geography
    - Branch locations (location, HIDTA, HIFCA, near one of those areas).
    - Member presence. (Are many domiciled in other areas of the country or foreign nations?)
- Staff
    - An overview of turnover, expertise, culture of compliance, and training frequency.
- Member Profiles
    - Types of accounts, concentration, high risk, PEPs, Non-U.S. citizens, etc.

- Products and Services
    - The embedded/inherent risk of relative products and services offered as it relates to BSA compliance and OFAC compliance; for example, the risk of ATMs.
    - External threats to the program:
        - 3rd party systems relied upon.
        - Regulatory changes, pressures.
        - Geopolitical or socio-economic unrest.
        - Any other threats to program.

Then update risk assessment whenever the following occurs:

- New products and services are implemented.
- The credit union grows in assets or membership.
- The credit union provides more complex financial products.
- When any of the current categories assumes more risk (FOM expansion, mergers, etc.).

Following is a link to a presentation outlining the risk assessment process along with tools to use in CU*BASE which will give you the data you need to understand your membership, products and services, and geographical presentation.

https://auditlinksuite.com/wp-content/uploads/BSA-Risk-Assessment-Presentation-v3-with-KD-tools-1.pdf

AUDIT PROCEDURES

Review the Risk Assessment to ensure:

- Risk was properly assessed, and level of risk is identified in each of the major areas explained above.
- Mitigations are presented that lower the inherent risk.
- The risk assessment is reasonably commensurate with the credit union's profile.
- Procedures and internal controls are developed from the risk assessment.
- The risk assessment is current and approved by the Board of Directors.

DOCUMENTS REQUESTED

☐ Risk Assessment

☐ Board Minutes reflecting Risk Assessment review/approval

POLICIES AND WRITTEN PROCEDURES

PURPOSE

A well-documented program serves as the basis for all BSA functions. Sound policies and procedures demonstrate the credit union's understanding of a compliant BSA program and helps ensure continuity. Policies are not written for the auditor or examiner. They are written to set clear expectations and to document the expectations of FinCEN and the credit union board.

Effective anti-money laundering and countering the financing of terrorism programs safeguard national security and generate significant public benefits by preventing the flow of illicit funds in the financial system and by assisting law enforcement and national security agencies with the identification and prosecution of persons attempting to launder money and undertake other illicit activity through the financial system.

Anti-money laundering and countering the financing of terrorism programs should be:

A. Reasonably designed to assure and monitor compliance with the requirements of the governing BSA laws and regulations; and

B. Risk-based, including ensuring that more attention and resources of financial institutions should be directed toward higher-risk customers and activities, consistent with the risk profile of a financial institution, rather than toward lower-risk customers and activities.

GOVERNING LAWS AND REGULATIONS:

The following regulations comprise the major BSA/AML/CIP/OFAC legislation promulgated over the years. These are the essential components that should be included in the written policies and procedures that, collectively, document the program.

A. 31 U.S.C. 5318(h)(1): In order to guard against money laundering and the financing of terrorism through financial institutions, each financial institutions shall establish anti-money laundering and countering the financing of terrorism programs.

B. 31 CFR 1020.210(a)(2)– Anti-Money Laundering Program Requirements for Banks[1]

- A system of internal controls to assure ongoing compliance.
- Independent testing for compliance to be conducted by financial institution personnel or by an outside party.
- Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance.

[1] A bank regulated by a Federal regulator, including banks, savings associations, and credit union.

- Training for appropriate personnel; and
- Appropriate risk-based procedures for conducting ongoing customer due diligence, to include but not limited to:
    - Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
    - Conducting ongoing monitoring to identify and report suspicious transactions, and on a risk basis, to maintain and update customer information. For purposes of this paragraph, customer information shall include information regarding the beneficial owners of legal entity customers.

C. 31 CFR 1020.220(a) – Customer Identification Program Requirements for Financial Institutions.

- The CIP must include **risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable**. The procedures must enable the financial institution to form a reasonable belief that it knows the true identity of each customer. Must contain procedures for opening an account that specifies the identifying information that will be obtained from each customer.
    - Minimum identifying information requirements
    - Procedures for opening an account that has applied for, but not received a taxpayer identification number.
    - Procedures for credit card accounts (credit unions require membership; therefore, their account opening procedures should satisfy this requirement.)
    - Member verification and what to do if any of the information cannot be validated within a reasonable period of time.
    - Verification through documents
    - Verification through non-documentary methods
    - Additional verification for certain customers, for example, businesses or other organizations not owned by an individual.
    - Lack of verification procedures
        - When an account should not be opened
        - Terms of how an account may be used while identity is being verified
        - When an account should be closed if verification fails
        - When a Suspicious Activity Report should be filed
    - Recordkeeping
        - Required records
        - Retention
    - Comparison to government lists
    - Customer notice (disclosure)
    - Reliance on another financial institution

- Exemptions

D. 31 CFR 1020.300-320 – Reports Required To Be Made By Financial Institutions

- Reports of Transactions in Currency (CTR)
  - Filing obligations
  - Identification required
  - Aggregation
  - Structured transactions
  - Transactions of exempt person (and all applicable requirements)
  - Retention

- Reports of Suspicious Activity (SAR)
  - Filing procedures
  - Exceptions
  - Retention
  - Confidentiality
    - General rule
    - Rules of construction
    - Prohibition on disclosures by government authorities
  - Limitation of liability
  - Compliance

E. 31 CFR 1020.400-440 Records to be Made and Retained by Financial Institutions

- Funds transfers over $3,000
  - Originators
  - Beneficiaries
  - Retrievability
  - Verification
  - Exceptions
- Original or copy or reproduction of certain documents/transactions. Refer to the regulation (CFR 1020.410(c)
- Purchases of negotiable instruments (CFR 1020.415)
- Certain records to be made and retained by persons having financial interests in foreign financial accounts.
- Retention Period

F. 31 CFR 1020.500-540 Special Information Sharing Procedures To Deter Money Laundering and Terrorist Activity

- Special Information Sharing Procedures (1010.520) – Referred to as 314(a)
  - Information requests
  - Obligations
  - Reports
  - Contact person

        - Use and security of request
    - Voluntary Information Sharing among Financial Institutions (1010.540) – Referred to as 314(b)

G. 31 CFR 1020.600-670
- Special Standards of Diligence; Prohibitions; and Special Measures
    - Refers to Foreign Financial Institutions – most likely will NOT refer to Credit Union. Do not include if this does not apply to the Credit Union.

H. Office of Foreign Assets Control Compliance Program
- Specific legislation of acts under Presidential wartime and national emergency powers
    - Final Rule: November 9, 2009 Economic Sanctions Enforcement Guidelines
    - OFAC Compliance Program (not required by specific regulation; however, regulators will expect an effective, written OFAC compliance program that is commensurate with the institution's risk profile). Refer to the FFIEC BSA/AML InfoBase)
        - OFAC Risk Assessment
        - Internal controls
        - Blocked accounts
        - Prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals
        - OFAC licenses
        - OFAC reporting
        - Updating OFAC lists
        - Screening ACH transactions
        - Independent testing
        - Responsible individual
        - Training

I. Customer Due Diligence Final Rule
- Four core requirements. It requires financial institutions to establish and maintain written policies and procedures reasonably designed to:
    - Identify and verify identity of customers
    - Understand the nature and purpose of customer relationships to develop customer risk profiles
    - Conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information
    - With respect to the requirement to obtain beneficial ownership information, financial institutions will have to identify and verify the identity of any individual who owns

25 percent or more of a legal entity, and an individual who controls the legal entity

EXPECTED POLICIES / PROCEDURES

The following policies, pursuant to the above regulations, should be reviewed, updated, and approved annually by the board of directors. The approval and date should be included in the board of director's meeting minutes and the date should be documented on the policy or other format easily retrievable or identifiable by an examiner or auditor. Policy approval will be verified through the review of board minutes.

These policies and/or procedures must be provided to the examiner and auditor prior to or during the audit.

- BSA/AML
    - Should include **all** requirements of the regulations and rules described above in the Governing Laws section (beginning on page 8).
    - Best practice considerations:
        - Designate and train a back-up BSA Officer. This is critical for continuity.
        - AML: Describe risk-based methods used for detecting and responding to suspicious activity. Consider reports used, analysis criteria, documentation. methods. These methods could be documented in the risk assessment, procedure or policy, as determined by the credit union.
        - Certain financial crimes have heightened awareness and while they may be implied under current codifications, expressly stating these circumstances aids in documenting an awareness of these particular crimes:
            - Elder financial exploitation
            - Human & drug trafficking
            - Unlicensed MSBs
            - Cyber attacks
            - Pandemic and other fraud
            - Ransomware

- OFAC, if separate
    - Should include **all** requirements of the regulations and rules described in the Governing Laws & Regulation section (page 8).
    - Best practices:
        - Non-member OFAC procedures (shared branching or on-us check cashing)
        - Any risk-based procedures. For example, is there a dollar limit for which a party to a transaction is not scanned? This should be evaluated and documented if so.

- CIP, if separate
    - Should include all requirements of the regulations and rules described in the Governing and Laws section on page 8.
    - Best practice considerations
        - Address mismatch procedures
        - How are account beneficiaries handled (relative to screening on government lists?
        - How are minor, elderly, or other individuals who may not have standard ID handled?
- CDD, if separate
    - Should include all requirements of the regulations and rules to also include:
        - Nature and purpose
        - Member risk profiles. Each financial institution can implement risk-based procedures.
        - Who assigns and modifies risk
        - Definition of high risk
        - Are procedures adequate to identify high risk
        - How ongoing monitoring is conducted
        - Enhanced Due Diligence ("EDD") procedures
            - Documents that will be collected
            - Review process
            - Members subject to EDD
        - Beneficial ownership
- Marijuana-related businesses, if separate
    - Develop an MRB policy
    - Include the financial institutions position on and level of service related to MRBs and MRB activity. Senior management should consider the risk and EDD process relating to servicing MRBs. Most institutions use a three-tier approach when determining their level of risk tolerance.
    - Develop strong internal controls, procedures, and EDD processes.
    - Include how businesses and activity will be screened at account opening and ongoing for MRB activity.
    - Include appropriate FinCEN filling requirements.

    Include what the financial institution will do if activity outside of its policy is conducted by an individual or entity.

- Money services businesses, if separate
    - Develop an MSB policy. Include business decision of whether the institution will or will not service MSBs.
    - If financial institution chooses to serve MSBs, be sure to develop strong internal controls and procedures to ensure compliance with FinCEN guidance and rules. (Refer to FIN-2016-G001 for helpful information)
    - Include how businesses and activity will be screened at account opening and ongoing for MSB activity.

    - Include what the financial institution will do if activity outside of its policy is conducted by an individual or entity.
- Other written procedures that supplement the policies

DOCUMENTS REQUESTED

☐Policies

☐Procedures

☐Other documents processes supplementing the program

☐Board minutes reflecting approval

INTERNAL CONTROLS

PURPOSE

One of the 5 BSA pillars is the development of a system of internal controls. A financial institution's system of internal controls is designed to mitigate and manage illicit financial activity risks and comply with BSA regulatory requirements.

Examiners and auditors rely on the FFIEC manual to assist with the preparation of their procedures and guide their focal points. The FFIEC states: "The board of directors, acting through senior management, is ultimately responsible for ensuring that the financial institution maintains a system of internal controls to assure ongoing compliance with BSA regulatory requirements. Internal controls are the financial institution's policies, procedures, and processes designed to mitigate and manage ML/TF and other illicit financial activity risks and to achieve compliance with BSA regulatory requirements. The board of directors plays an important role in establishing and maintaining an appropriate culture that places a priority on compliance, and a structure that provides oversight and holds senior management accountable for implementing the financial institution's BSA/AML internal controls. The system of internal controls, including the level and type, should be commensurate with the financial institution's size or complexity, and organizational structure. Large or more complex financial institutions may implement specific 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, financial institution-wide BSA/AML compliance program."

EXPECTATIONS

Explicit in their comments is the expectation that the board of directors has ultimate accountability for internal controls. Their responsibility is to ensure the following, among others:

- A comprehensive risk assessment is developed, and policies and procedures are developed to mitigate and control illicit criminal activity risk
- Culture of compliance exists
- Program continuity despite personnel changes
- Corrective actions are made from previous deficiencies
- There is adequate time and resources to administer an effective program
- Identify and establish specific BSA compliance responsibilities for personnel and provide oversight for execution of those responsibilities, as appropriate.
- Sufficient knowledge and expertise of those responsible for BSA administration
- Systems and technology sources are functioning appropriately
- Dual control processes

- System accesses and least privilege controls exist
- Storage of documents are confidential and secure

AUDIT PROCEDURES

- Auditors and examiners will evaluate the following:
- The board of directors, through senior management, creates a culture of compliance including staff adherence to policies, procedures, and processes
- The board of directors, through senior management, adequately addresses and responds to previously identified compliance deficiencies in a timely manner
- The board of directors has identified a person or persons responsible for BSA compliance (board-appointed BSA Officer)
- The board of directors, through senior management, provides adequate time and resources to effectively administer and oversee the BSA program
- The board of directors, through senior management, provides sufficient controls and systems for proper and timely filing of FinCEN reports (CTRs and SARs)
- The board of directors, through senior management, provides sufficient controls and systems for proper and timely review of and response to comparison of government block lists (OFAC)
- The board of directors, through senior management, incorporates a requirement for all staff to be aware of the responsibilities to BSA requirements, including annual training
- The board of directors, through senior management, provides sufficient controls and monitoring systems for timely detection and reporting of suspicious activity or abnormal account behavior
- BSA systems (SARs/CTRs, 3rd party software, etc) are restricted to "least required privilege" to prevent unauthorized access to SARs and ability to change member risk profiles
- Remediation of weaknesses
- Overall effectiveness of program

DOCUMENTS REQUESTED OR OTHER VALIDATIONS

☐BSA Officer job description
☐Most recent exam report
☐Most recent audit report
☐Discussions with general staff
☐Discussions with BSA Officer
☐Observations
☐SOC 2 (SSAE 16) report for core processing system and third-party processor
☐Completed questionnaire for auditor/examiner
☐Board minutes for the entire review period

TRAINING

PURPOSE

Training is a core requirement of a satisfactory Bank Secrecy Act and Anti-Money Laundering (BSA/AML) compliance program. At a minimum, a BSA/AML training program must provide training for all personnel whose duties require knowledge of the BSA (generally all employees). While BSA/AML training is required, credit unions have flexibility in the way they design the training program. Effective training programs provide employees with a clear understanding how BSA/AML and OFAC regulations affect their specific jobs. Training is also required for the board of directors. Enhanced training should be provided to the BSA Officer and backup, as applicable.

EXPECTATIONS

- Training should be commensurate with job function and should be well-documented.
- New hires should receive training upon employment
- Employees and the board should receive ongoing training. Industry standard is annually or if BSA requirements change.
- Training should include not only BSA requirements, but also scenarios, examples, typologies of criminal behavior, and a reinforcement of the importance of the BSA.

AUDIT PROCEDURES

- Confirm the credit union trained all employees and board members/volunteers on the BSA responsibilities
- Confirm the BSA Officer and back up BSA Officer received extended training during the audit period
- Confirm the BSA Officer and back up BSA Officer possess sufficient knowledge and skill to administer the program
- Confirm training is tailored to job function
- Evaluate appropriateness of training materials

DOCUMENTS AND VALIDATION METHODS REQUESTED

☐Employee and board listing (names & positions, if possible).

☐Evidence of extended training attended by BSA Officer/back up BSA Officer during the year (e.g.: agenda, certificate, email confirmation, etc.).

☐Method of training provided to employees/ board members during the year.

☐Sign in sheets/certificates/roster of employee/board attendance. Board minutes of board training, if applicable.

☐ Training materials. Note: If using TLC (The Learning Campus), please provide training records. If number of employees exceeds 15, a selection will be made.

☐Discussions with BSA Officer

☐Observations

CLASSES AVAILABLE THROUGH CU*ANSWERS

CIP AND OFAC REVIEW AND TESTING

PURPOSE

Your customer information policy and related program should be tailored to those risks identified in your risk assessment as it relates to membership. It should contain the words "form a reasonable belief that you know the true identity of a member." A credit union who is SEG-based will have a mostly simplistic CIP program vs. one that has legal entity accounts and who opens accounts for members in high drug trafficking or criminal geographies. According to the manual it should include the risks associated with the assessment including:

- The types of accounts maintained by the credit union
- The credit unions methods of opening accounts
- The types of identifying information available
- The credit unions size, location, and customer base

Reference:
https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/01

GOVERNING REGULATIONS

31 CFR 1010.220 requires that credit unions comply with minimum regulatory and specific customer identification program requirements to verify and document the identity of new customers.

31 CFR 1010.230 requires that certain financial institutions obtain, verify, and record information about the beneficial owners of legal entity customers. Legal entity is defined as corporations, limited liability companies, or other entity that is created by a filing of a public document with the Secretary of State or similar office, a general partnership, and any similar business entity formed in the US or a foreign country. **Legal entity does not include sole proprietorships, unincorporated associations, or natural person opening an account on their own behalf.**

Beneficial owners are: (1) Each individual, if any, who owns, directly or indirectly, 25 percent or more of the equity interests of the legal entity customer (e.g., each natural person that owns 25 percent or more of the shares of a corporation; and (2) An individual with significant responsibility for managing the legal entity customer (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer).

EXPECTATIONS

Expect third party auditors and examiners to concentrate on these risks described above and build your justification for the size, complexity, and requirements of your policy and programs based upon these variables.

The FFIEC is also very clear on the methods used to identify risks associated with types of accounts the credit union opens. Credit unions are required to ask two questions when opening an account. Those being the nature and purpose of the account. Additional customer due diligence is not required

unless there are unique risk factors which would dictate such. The guidance that came out in December 2021 should be appended to the CIP policy and fully understood by management and utilized if an auditor or an examiner request the credit union create elaborate risk ratings schemas for natural purpose member accounts. https://www.ncua.gov/files/press-releases-news/introduction-customers.pdf

Generally, CIP programs do not require asking the occupation of the member, but the FFIEC has identified high risk occupations such as doctors, attorneys, real estate agents, etc. However, there is no requirement to ask the question. If your state has legalized cannabis this is no longer something that can be avoided as most credit unions have a section in their BSA policy if they will bank these members and if that is the case the examiner or auditor will begin asking how you are managing this policy.

The auditor/examiner will ask for a sampling of new accounts opened since the prior audit/examination. Credit unions will most likely either use **Tool #548** ***New Account Report*** or the examiner will choose from the AIRES files those accounts to test. Based upon the credit union's CIP policy expect the examiner to ask for evidence of:

- Signature card
- Government issued ID; ID cannot be expired at the time the account was opened.
- Results of OFAC scan at the time of account opening
- Risk rating in the event the credit union has a risk rating requirement by policy
- The beneficial ownership form for legal entities, along with procedures for ongoing monitoring against OFAC lists. Use **Tool #523** ***Member Designation Configuration*** and update joint owner to controlling agent (abbreviate it). Change miscellaneous owners to beneficiaries. This will guarantee that the OFAC scan will be run on the names weekly. The beneficial ownership form for legal entities, along with procedures for ongoing monitoring against OFAC lists. Use **Tool #523** ***Member Designation Configuration*** and update joint owner to controlling agent (abbreviate it). Change miscellaneous owners to beneficiaries. This will guarantee that the OFAC scan will be run on the names weekly.
- For accounts opened virtually, the procedures for reviewing accounts opened virtually and secondary validation model results.
- A sample of signature cards of closed accounts dating back five years to test record retention compliance.

If the AIRES file is used, you will need to use **Tool #122** ***AIRES Create Files*** to create the file and **Tool #1375** ***Data Transfer (Upload or Download)*** to download it. Not all individuals in the credit union are authorized to download data and the credit union's CEO must authorize that through the Client Services department by filling out a form.

In the event the AIRES file is not used, you will need to create a trial balance using **Tool #487** ***Mbr Trial Balance Listing – Select Info***. The only selection that will be necessary is the date range for the account opening field which will be equivalent to the audit period. This should be sent to the credit union's instant printer queue which then can be saved as a PDF and supplied to the auditor.

For proof of the OFAC scan being done at the time of account opening, the primary member's scan will be stored in the member's audit tracker. These are stored for 7 years. To prove that the scan was completed, simply click on

the tracker go button from a general inquiry and view the audit tracker type. The original scan will be equivalent to the open date. For memberships opened through the automated membership opening process (MOP) the original scan will be found on the report produced by Experian and can be found in the Experian website. For proof of the joint owner (non-member scan) use **Tool #559** ***OFAC Non-Member Scan History*** and enter the joint owner's name or social security number. See the link below for more on OFAC scans. This link is a good reference document for your examiner/auditor in helping to understand how OFAC is run and what it is run against such as wires, corporate checks, IATs, and coborrowers. https://www.cuanswers.com/wp-content/uploads/UsingtheCUBASEDataMatchSystemforOFACCompliance.pdf

For the ongoing scans of members and non-members, those scans are run every Saturday against the most current lists and a report is generated and saved in your CU*Spy archive. The report name is **LOFAC** and can be accessed by using **Tool #329** ***CU*Spy Daily Reports*** and searching on OFAC. It is recommended that this report be viewed weekly and for those potential hits a record the research performed by either adding a note to the report or updating the tracker record. This will be proof to the auditor/examiner that you are working the hits.

Auditors will also ask you to prove potential hits that occur are worked or responded to in workflow processes such as opening an account, adding a joint owner, issuing a corporate draft, etc. This can be proven by printing a tracker report **Tool #664** ***Print Member Trackers*** and inputting the Tracker Type **AT** and the Memo Type of **OO** (OFAC override). To verify that action was taken the tracker should contain a response from the employee who overrode the potential hit. **A blank record with no verbiage is *not* what you want to see.** This report should be run each month by the BSA officer.

AUDIT PROCEDURES

- Ensure the following for personal membership accounts:
  - The credit union collected the name of the member and all joint members
  - The credit union collected the physical address(es), SSNs, DOBs for all signers on the account
  - The credit union verified the physical mailing address with either a government issued photo ID or other method, per policy or procedure
  - The credit union collected the occupations for all individuals on the account
  - The credit union verified OFAC for all signers on the account
  - The credit union completed a CDD profile for all members on the account
  - The credit union collects and retains all documents required in policy or procedure

- The credit union collected all information required for business membership accounts
  - The credit union collected the required business entity documents per policy or procedure
  - The credit union identified the nature of the business

- The credit union identified all signers on the account using CIP processes
- The credit union collected the beneficial ownership information on a certification form acceptable to the regulation
- The credit union collected CIP information for all beneficial owners using CIP-like procedures
- The credit union performed OFAC for the business and all signers and beneficial owners (if different) on the account
- The credit union collects and retains all organizational or other documents required by policy or procedure

- The credit union conducts routine membership scrubs against OFAC in a manner that would allow it to properly respond to a match after an OFAC update

- The credit union conducts OFAC verification for transactions that may involve non-members prior to the completion of the transaction (e.g.: on-us check cashing, monetary instruments purchased and made payable to a non-member, etc.)

The auditor may review the AIRES file to ensure that all TINs appear to be complete or are legitimate, and may test for other CIP information within the AIRES, such as adequate address collection

DOCUMENTS REQUESTED

☐New member listing. The auditor/examiner will select a sample of members

☐Share AIRES file

☐Member files for the selected accounts. The following information will be examined:

- Account card
- Proof of OFAC on all parties: primary owner, joint owner(s), business name, beneficiaries
- Proof of CDD (or other means identified in Risk Assessment)
- ID
- Organizational documents
- Beneficial owner certification

☐Documentation for the OFAC scan on entire membership (system logs) for the last 3 months of the review period

☐Evidence of non-member OFAC verifications made at the time of the transaction

TOOLS

Tool #329 *CU*Spy Daily Reports* (To review the report of weekly scans. Report name **OFAC**)

Tool #559 ***OFAC Non-Member Scan History*** (To prove joint owners are getting scanned as well as other non-members utilizing credit union services)

Tool #778 ***Scan a Single Name Through OFAC*** (Used when performing incoming wire scans and performing check cashing services for non-members)

Tool #122 ***AIRES Create Files*** and **Tool #1375** ***Data Transfer (Upload or Download*** (To create an AIRES files and download it)

Tool #487 ***Mbr Trial Balance Listing - Select Info*** (To create a list of all member records)

Tool #664 ***Print Member Trackers*** (To generate a list of trackers created relative to OFAC)

ProDOC Vault icon (To garner any proof of identity documents outside of the one scanned into CU*BASE from the inquiry screen)

Tool #523 ***Member Designation Configuration*** and update joint owner to controlling agent (abbreviate it). Change miscellaneous owners to beneficiaries. This will guarantee that the OFAC scan will be run on the names weekly.

Tool #559 ***OFAC Non-Member Scan History*** and enter the joint owner's name or social security number (for proof of the joint owner (non-member scan)

Tool #329 ***CU*Spy Daily Reports*** and searching on OFAC (for the ongoing scans of members and non-members those scans are run every Saturday against the most current lists and a report is generated and saved in your CU*Spy archive. The report name is **LOFAC**.)

Tool #664 ***Print Member Trackers*** and inputting the Tracker Type **AT** and the Memo Type of **OO** (OFAC override) to prove to auditors potential hits that occur are worked or responded to in workflow processes such as opening an account, adding a joint owner, issuing a corporate draft, etc.

CDD MEMBER RISK PROFILE

PURPOSE

A cornerstone of a strong BSA/AML compliance program is the adoption and implementation of risk-based CDD policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing. The objective of CDD is to enable the financial institution to understand the nature and purpose of customer relationships, which may include understanding the types of transactions in which a customer is likely to engage. These processes assist the financial institution in determining when transactions are potentially suspicious.

Effective CDD policies, procedures, and processes provide the critical framework that enables the financial institution to comply with regulatory requirements including monitoring for and reporting of suspicious activity.

CDD policies, procedures, and processes are critical to the financial institution because they can aid in:

- Detecting and reporting unusual or suspicious activity that potentially exposes the bank to financial loss, increased expenses, or other risks.
- Avoiding criminal exposure from persons who use or attempt to use the bank's products and services for illicit purposes.
- Adhering to safe and sound banking practices.

CID and CPP work together to establish **risk** policies

EXPECTATIONS

In determining a customer's risk profile, the financial institution should consider risk categories, such as the following, as they relate to the customer relationship:

- Products and services
- Customers and entities
- Geographic locations
- Other high-risk criteria that should be explicitly defined

The financial institution's procedures should establish criteria for when and by whom customer relationships will be reviewed, including updating customer information and reassessing the customer's risk profile. The procedures should indicate who in the organization is authorized to change a customer's risk profile. A number of factors may be relevant in determining when it is appropriate to review a customer relationship including, but not limited to:

- Significant and unexplained changes in account activity
- Changes in employment or business operation
- Changes in ownership of a business entity
- Red flags identified through suspicious activity monitoring

- Receipt of law enforcement inquiries and requests such as criminal subpoenas, National Security Letters (NSL), and section 314(a) requests
- Results of negative media search programs
- Length of time since customer information was gathered and the customer risk profile assessed

Procedures should be documented that explains the CDD program and how and when Enhanced Due Diligence will be performed. CDD/EDD can be performed through questionnaires, risk matrices, CIP information, or other documents that aid in the CDD process, among others. There is no specific format a financial institution has to follow when establishing risk profiles and it may use a combination of multiple sources or criteria to develop an understanding/profile of a member. **The key is to document in policy and procedure how these profiles are determined.**

Significant to the CDD program is the identification and monitoring of high-risk accounts. At the same time, activity that is considered high risk should be defined.

High Risk Accounts

Examiners and auditors will review and test not only your ongoing review of identified high-risk accounts but also processes to uncover high-risk activity which may lead to categorizing them as a high-risk account. This is generally done at account opening, when evaluating potential illegal activity, or when running the abnormal activity monitoring tools. The expectation and exam and audit checklists include a question regarding your ongoing monitoring of high-risk activity.

Examiners and auditors will also review "High Risk" accounts procedures and practices to verify the credit union is identifying and monitoring accounts that have characteristics of elevated risk of money laundering or other criminal activity. They will ensure review of these accounts is being regularly conducted in a timely manner and that enhanced due diligence is performed, as appropriate. **It is imperative that these reviews be documented.**

Enhanced due diligence flags can be configured in **Tool #247** ***Configure Due Diligence Codes***. Up to **9 codes** can be used to generalize the types of activity you are monitoring for. An important item to remember is that they generally dictate the frequency of your review as well. Adding a due diligence code to a member record does require someone with file maintenance authority and ability to use **Tool #20** ***Update Account Information*** to update the member account.

Currently the only method to get a complete list of all members with a due diligence code is the use of a query report. The evidence of periodic reviews will be in the reports run through **Tool 402** ***Insider Audit/Due Diligence Report*** (4 reports will general) – or **Tool #537** ***Monitor Abnormal Transaction Activity*** (abnormal monitoring report). Each of these two tools has functionality to generate a report. Procedurally these should be run on a frequency of your choice and then saved in the credit union's archive for evidence it was ran. Findings from running these reports should be included in the member audit tracker. It is recommended that **Memo Type of AB** (using **Tool #260** ***Configure Memo Type Codes for Trackers***) be used so you can print and supply the auditor of proof that you completed the work.

AUDIT PROCEDURES

- Review the policies and procedures developed by the financial institution and:
    - Ensure that effective processes exist to develop a risk profile.
    - Confirm procedures are risk-based and adequate to the risk profile and appetite of the Credit Union
    - Ensure a process for Enhanced Due Diligence exists
    - Obtain documentation of how risk profiles are developed
    - Test a sample of new members and business accounts to ensure that the financial institution performed CDD according to its policies and procedures, and the CDD was documented.
    - Confirm High Risk members are reviewed, and results are documented
    - Ensure CDD and EDD is used during the suspicious activity case management process

Auditors and Examiners will most likely have follow-up questions after the audit has begun and these documents are reviewed. Be prepared for questions.

DOCUMENTS REQUESTED

☐Copy of CDD matrices, if available or used

☐Copy of electronic or manual "questionnaire" used to collect information, if used

☐Documentation of member risk profile. If the profile is based on inherently low risk criteria (savings account only, no high-risk demographic or personal attributes), the low-risk criteria should be detailed in the risk assessment.

☐High Risk Account Listing with evidence of last review or when EDD was performed

☐Query on members with a due diligence flag not equal to 0, configured in **Tool #247** ***Configure Due Diligence Codes*** The evidence of periodic reviews will be in the reports run through **Tool #402** ***Insider Audit/Due Diligence Report*** (4 reports will general) – or **Tool #537** ***Monitor Abnormal Transaction Activity***. (abnormal monitoring report). Please generate report.

TOOLS

Tool #101 ***Abnormal Activity Monitoring Config*** to configure abnormal activity monitoring codes.

Tool #247 ***Configure Due Diligence Codes*** to configure enhanced due diligence flags can be configured in. Up to **9 codes** can be used to generalize the types of activity you are monitoring for. An important item to remember is that they generally dictate the frequency of your review as well.

Tool #20 ***Update Account Information*** to update the member account by adding a due diligence code to the member record (does require someone with file maintenance authority).

Tool 402 ***Insider Audit/Due Diligence Report*** (4 reports will generate) – or **Tool #537** ***Monitor Abnormal Transaction Activity*** (abnormal monitoring report). Only method to get a complete list of all members with a due diligence code is a query report.

Tool #260 ***Configure Memo Type Codes for Trackers*** so you can print and supply the auditor with proof that you completed the work. It is recommended that **Memo Type of AB** be used.

MONEY SERVICES BUSINESSES

PURPOSE & RISKS

Money Services Businesses (MSBs) fill a need, especially among the unbanked and underbanked populations. MSBs offer quick and opaque services to move monies domestically and internationally. MSBs also transact in large volumes of cash, which is untraceable for the credit unions which service them. Due to their risky nature, a lot of banks and credit unions refuse service to MSBs in order to minimize risk. However, MSBs can offer a solid source of income, if managed appropriately.

MSBs are subject to a threshold of greater than $1,000 per person per day in one or more transactions. MSBs include currency dealer/exchanges, check cashers, issuers of traveler's checks, money orders, or stored value, seller/redeemer of traveler's checks, money orders, or stored value, and/or money transmitters.

The Credit Union is expected to assess the risks posted by each individual MSB on a case-by-case basis, monitor and report any unusual activities, and implement documented & appropriate controls to manage the risk exposure.

EXPECTATIONS:

Your auditor will request a due diligence packet that you have compiled for the MSB. This packet should include, at a minimum, evidence of site visits, a copy of the MSB's BSA policy, a copy of the MSB's independent audit report, documentation of frequent and routine membership reviews, evidence of the MSB's Department of the Treasury registration, evidence of annual training received by the MSB's staff, and an assessment of the credit union's risks for servicing the MSB. The credit union should assess the diverse products and services as well as the MSB's member base, the minimal or lack of ID requirements, the lack of ongoing customer relationships, the limited recordkeeping, the frequency of cash transactions, and the frequent change of product mix, location, and operations.

AUDIT PROCEDURES

The examiner and auditor will ensure:

- The credit union has a documented policy and procedures for banking MSBs
- The credit union is aware of accounts that are transactional businesses (check casers, prepaid card providers, foreign currency dealers, money transmitters, money order/travelers check issuers, etc.)
- The credit union identifies businesses that show characteristics of an MSB when reviewing reports, such as the large cash reports
- The credit union has conducted site visits for MSBs and businesses which show characteristics of MSBs to verify business is not an MSB
- The credit union documents the results of the site visit
- The credit union conducts ongoing EDD for its MSB members

- The credit union collects additional documents from the MSB, including a copy of the MBS's BSA Policy, BSA training for staff, independent audit, and any other relevant documents
- The credit union assesses the diverse products and services provided to the MSB customer base
- The credit union assesses the MSB's member base
- The credit union assesses the minimal or lack of ID required by the MSB
- The credit union assesses the MSB's lack of ongoing customer relationships
- The credit union assesses the MSB's limited recordkeeping
- The credit union assesses the MSB's currency transaction frequency
- The credit union assesses the MBS's change of product mix, locations, and/or operations
- The credit union verifies the MSB is registered with the Department of the Treasury
- The credit union has filed a SAR if an MSB is not registered with the Department of the Treasury
- The credit union reviews MSB activity regularly for legitimate and unusual or suspicious transactions
- Risk-based OFAC procedures are implemented

DOCUMENTS REQUESTED

☐ MSB files

☐ All Member Due Diligence

☐ Annual reviews that evaluate activity for suspicious transactions

☐ ATM Due Diligence documents (ISOs) of the MSB

☐ Proof of Independent Audit by the MSB

☐ Registration Renewals

TOOLS

Tool #101 ***Abnormal Activity Monitoring Config*** to configure abnormal activity monitoring codes.

Tool #247 ***Configure Due Diligence Codes*** to configure enhanced due diligence flags can be configured in. Up to **9 codes** can be used to generalize the types of activity you are monitoring for. An important item to remember is that they generally dictate the frequency of your review as well.

Tool #20 ***Update Account Information*** to update the member account by adding a due diligence code to the member record (does require someone with file maintenance authority).

Tool 402 ***Insider Audit/Due Diligence Report*** (4 reports will generate) – or **Tool #537** ***Monitor Abnormal Transaction Activity*** (abnormal monitoring report). Only method to get a complete list of all members with a due diligence code is a query report.

Tool #260 ***Configure Memo Type Codes for Trackers*** so you can print and supply the auditor with proof that you completed the work. It is recommended that **Memo Type of AB** be used.

CTRs and Large Currency Reports

Purpose

Currency Transaction Reports (CTRs) are the original reporting document of the BSA and have been around since 1970. CTRs are filed whenever currency transactions over $10,000 are conducted singularly or in aggregate on any one business day by or on behalf of an individual.

Failure to file CTRs accurately could result in a fine of up to $500 for each violation. Similarly, fines for unfiled CTRs can top out at $10,000 per report per day it is late.

To support proper CTR filing, credit unions must review daily large cash aggregates to determine if currency transactions require reporting. The credit union should easily be able to determine which individuals or businesses should be included in the filing, the amounts and types of cash transactions involved, any conductors, and CIP information for all related parties.

Expectations

Your auditor will request access to your daily large cash reports, the core system, and the filed CTRs. The auditor will test transactions from the daily large cash report to ensure CTRs were filed when they were required. Additionally, the auditor will ensure that any joint owners or conductors are identified and included appropriately. The auditor will also reconcile the core system's transactions for all related accounts and individuals to the transactions included on the CTR. In this way, the auditor gains a comfort level of ensuring CTRs are filed correctly, completely, and timely.

Audit Procedures

The examiner and auditor will ensure:

- The credit union files CTRs for transactions that report on the large currency report
- The large currency report aggregates ATM transactions which are CTR reportable
- The large currency report aggregates shared branching transactions which are CTR reportable
- The large currency report aggregates all accounts with currency associated by TIN
- The large currency report aggregates all joint owners on accounts with CTR reportable transactions
- The credit union has mitigating tools in place for any weaknesses in the large currency report

CTRs will be tested for the following Items

- Timeliness
- Correct federal regulator
- RSSD entered in all fields (corporate and branch)

- All applicable parties are included
- The conductor and beneficiary relationship are correctly reflected
- All checkboxes are appropriately marked (multiple transactions, aggregated transactions, ATM, night drop, shared branching, etc.)
- All listed parties have complete information including occupation and ID (ID for businesses include the document number of the articles of incorporation or other identifying document)
- Transactions are reported with the correct party and account number
- The transaction types and amounts are correctly reported. For example, cash withdrawal, negotiable instrument purchase, etc.

DOCUMENTS REQUESTED PRIOR TO THE AUDIT

☐ FinCEN e-filing "Track Organization Status" report exported to .CSV, for "Show All" for the review period

☐ Excessive cash transaction reports for a selection of dates during the review period. In CU*Spy this is the LBKSC3 report. Combine these for the period requested and save to a PDF. Also, you can schedule monthly cash logs using **Tool #1990 Print *BSA/SAR Structuring Report*** and **Tool #759 *Report Automation: Standard Reports***. Always choose member currently served to aggregate activity on accounts the member is primary on as well as joint. This way the auditor will only get fewer reports containing more activity.

DOCUMENTS REQUESTED AT THE TIME OF THE AUDIT

☐ CTRs and supporting documentation of underlying transactions will be made at the time of the audit.

TOOLS

Tool #984 *Work Daily BSA/CTR Activity* to mark the items as "verified" as you check them against the Currency Transaction Report and/or Suspicious Activity Reports your credit union is required to file.

Tool #991 *Work with CTR Forms* to view all CTR forms generated by your credit union over the past three months, displayed in order by date (most current at the top), then by SSN/TIN.

Tool #1990 Print *BSA/SAR Structuring Report* and **Tool #759 *Report Automation: Standard Reports*** to schedule monthly cash logs.

NOTE: The system only stores CTRs for 90 days. They must be stored off system if you have elected to have CU*Answers batch file for you to FinCEN.

CTR EXEMPTIONS

PURPOSE

In some instances, CTR filing for business members can become burdensome to credit unions because of excessive cash transactions. In these cases, credit unions may exempt certain business members from CTR filing. In order to exempt members, the credit union must verify the eligibility of the member under either Phase I or Phase II.

Credit unions should take care to ensure they fully understand the requirements of CTR exemption under each phase and adequately review the member initially as well as annually to ensure the member qualifies for exemption.

For exhaustive information on CTR exemption, reference the FFIEC Exam Manual.

EXPECTATIONS

Your auditor will request a listing of exempt members to make a selection. The testing will review the initial exemption as well as current review for continued exemption, if applicable.

AUDIT PROCEDURES

The Examiner and Auditor will look for the following:

The credit union has filed the Designation of Exempt Person (DOEP) with the correct exemption type (Phase I, II)

- The credit union has maintained a copy of the DOEP filing
- The credit union has conducted an annual review of the exempt member to ensure continued eligibility
- The DOEP is accurate
- Evidence the credit union has continued to monitor the exempt member for suspicious activity

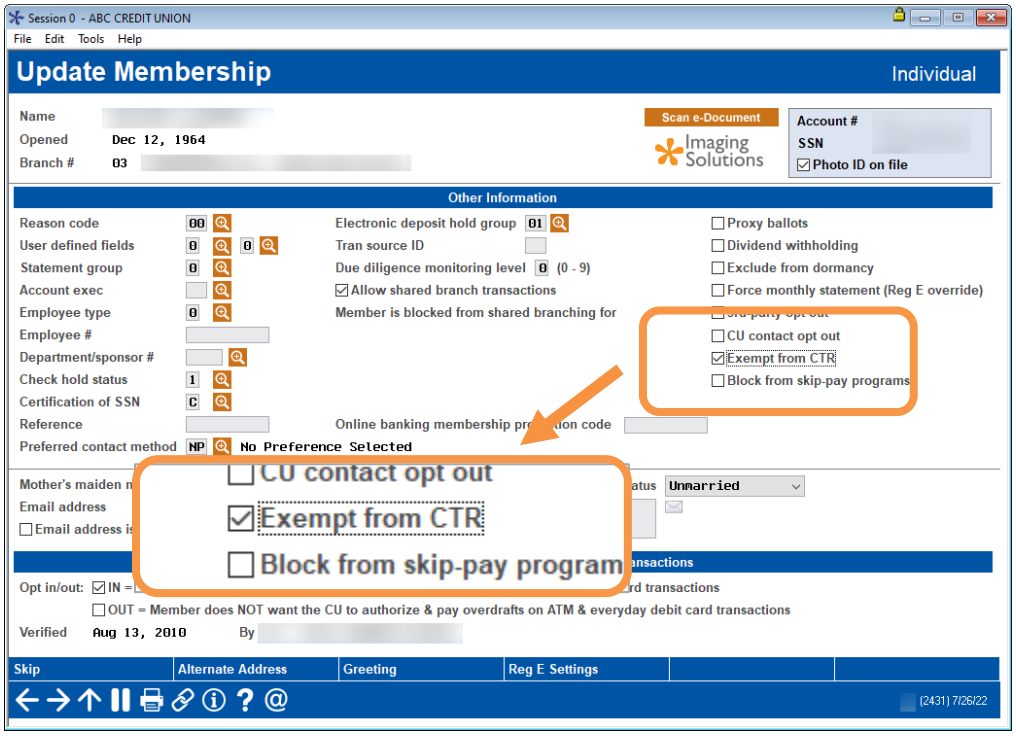
DOCUMENTS REQUESTED PRIOR TO THE AUDIT

☐ Listing of any CTR Exempt members with exemption date

DOCUMENTS REQUESTED AT THE TIME OF THE AUDIT

☐ DOEP with most recent annual review selections will be made at the time of the audit

Tool #15 *Update Membership Information*, then check *Exempt from CTR* to exempt the membership from CTR reporting



SUSPICIOUS ACTIVITY MONITORING AND SARS

PURPOSE & RISKS

Suspicious Activity Reports (SARs) are an important tool to helping law enforcement investigate and prosecute money laundering and other financial crimes. Credit unions play a vital role in stemming the flow of illegal money.

When a credit union fails to adequately monitor for or report suspicious activity, regulators are within their legal authority to levy heavy fines and penalties. In extreme cases, severe and willful negligence or apathy can result in cease & desist orders being given, and the shutdown of financial institutions. As a result, the credit union as a whole, the BSA Officer and/or senior management, and the board of directors can all be held liable for violations of the BSA.

EXPECTATIONS

Your auditor will request access to your monitoring system or activity reports to determine how you review, decision, and disposition of suspicious or unusual activity alerts. Your auditor may have recommendations for alert reviewing and/or rule tuning.

Your auditor will also request a log of the SARs you have filed. This log will be used to make a sample selection for SAR reviews. SARs will be reviewed for filing accuracy and completeness. An evaluation of the effectiveness of the SAR narrative will also be completed.

AUDIT PROCEDURES

- Select and review SARs commensurate with the size and complexity of the credit union
- Review of alert and case management process
- Evaluate 3rd party inter dictum software rules, training, and alert generation

Suspicious activity monitoring will be tested for the following Items

- Timely review of the alerted activity
- Thoroughness of the review
- Reasonableness to determination of suspicious or not suspicious
- Documented determination of the activity (suspicious vs not suspicious)
- Adequate case management of alerts which are escalated into cases for SAR filing
- Continued monitoring for elevated risk due to SAR filing
- Appropriate continued filing procedures

SARs will be tested for the following Items

- Timeliness of filing (≤30 days from date of determination for known suspect or ≤ 60 days from date of determination for unknown suspect)
- Correct federal regulator
- RSSD entered in all fields (corporate and branch)
- All applicable parties are included
- Loss to the credit union completed, if appropriate
- All branches involved are identified
- All listed parties have complete information including occupation and ID (ID for businesses include the document number of the articles of incorporation or other identifying document)
- The SAR does not list any victims in the subject fields
- all listed parties have accurate relationships to the credit union identified with credit union TINs in boxes 24-26
- Dates and amounts are correctly reflected in boxes 29-31
- Suspicious activity checkboxes are noted in boxes 32-42
- Products and services checkboxes are noted in boxes 45-46
- SARs are reported to the board at the next board meeting
- SAR members are considered high risk for activity monitoring or have a clear and reasonable explanation for why they are excluded for high risk (e.g. non-member, closed account, etc.)
- Narratives give a complete, concise picture of the activity involved, including a listing of the transactions or reference to an included attachment See section on SAR narratives.

SAR NARRATIVES

Importance

One of the critical tools law enforcement has in combatting financial crime is the Suspicious Activity Report (SAR). A SAR itself is not direct evidence that a crime has occurred; it is a report that indicates criminal activity may have occurred. SARs are extremely confidential and unauthorized individuals should not have access to or knowledge that one has been filed.

As the single point of filing, FinCEN shares information with law enforcement analysts who review SARs and then disseminate useful information to national and local law enforcement task forces. These task forces or agencies then evaluate whether the event(s) is elevated to a level that warrants further investigation.

The body of the SAR contains the basic information of who participated in the activity, where it occurred, and what occurred. It also provides contact information. However, the meat of the information is in the narrative. That is the data mine where investigators sift to hit criminal gold. Therefore, it is critical that sufficient and detailed information be reported so that the report is useful and effective.

Tips for strong narratives

Paint a complete picture to intrigue law enforcement. You have one or two sentences to capture their attention. If your narrative does not quickly paint a compelling story of why it is worth their time to review further, it is likely to get pushed aside, never to be looked at again. Spend time crafting a story that tells law enforcement what they need to know. Remember, an unread narrative is a wasted narrative.

Include key words. SARs are subject to sorting algorithms that look for specific key words, zip codes, names, amounts, type of activity, etc. Be sure to slip these into your narratives so that you can be sure your SAR gets seen. While we are on this subject, it might even be helpful to paste your narrative into a Word document and run spell check just to make sure you have not misspelled a word, especially if you have included key words, which are likely to get missed if they are misspelled. The other benefit of this is you do not have to worry about losing the information if the site times out or if you inadvertently leave the site.

Include the "5 Ws" and even the "How" if it is applicable or known! These include:

Who conducted the activity and who were all the participants?

What type of instruments were used, such as cash, check, wire, ACH, cryptocurrency, etc.?

Where did the transactions take place?

When did the activity occur? Include the times of day and when you detected the activity.

Why do you believe the activity is suspicious?

How was the activity conducted? Including the subject's normal types of behavior.

Detail the transactions. Include the transactions and list the dates, types, amounts, and known address locations for branches or ATMs. Including this information helps build a picture of how the suspect operates and why the activity may be suspicious. Consider if the subject is visiting multiple branches or ATM locations across the country, or even across the city.

Use an attachment if there are multiple transactions. The SAR form allows the use of an Excel attachment if the transactions are too numerous to list out. Do not be afraid to use the attachment for your benefit and to make sorting the details easier. Be sure to include a statement that an attachment is included.

STRUCTURING VS SUSPICIOUS ACTIVITY

One prominent area of confusion is the difference between structured cash transactions that are from legal activity versus suspected money laundering. Note that structuring cash transactions with the intention of evading Currency Transaction Reporting is a crime that must be reported via a SAR. Structured transactions are made with the intention to avoid having a CTR filed and can be with funds that are from or intended for either legitimate or illegitimate business. On CU*BASE there are 4 very important tools which can be utilized in combination with the due diligence codes configured in

Tool #247 ***Configure Due Diligence Codes*** and assigned the membership update functionality. See the tools section for further clarification.

DOCUMENTS REQUESTED PRIOR TO THE AUDIT

FinCEN e-filing "Track Organization Status" report exported to .CSV, for "Show All" for the review period

Board Minutes reflecting SARs are reported

DOCUMENTS REQUESTED DURING THE AUDIT

☐ Access to suspicious activity monitoring (alerts/reports/run sheets) for a selection of dates during the review period

☐ Access to SARs filed for a selection of SARs during the review period

TOOLS

The amount of functionality on CU*BASE is vast for uncovering suspicious activity and structuring. The tools you will use should be dependent up the credit unions risk profile. At a minimum you should be using the following and will be expected when the auditor and examiner begin their program review.

Tool #1990 ***Print BSA/SAR Structuring Report*** is unique in that it aggregates all cash activity by the day and utilizes the member currently served functionality of the teller platform. This guarantees the individuals performing transaction that they are primary and joint on are aggregated for review.

Tool #247 ***Configure Due Diligence Codes*** allows you to configure up to 9 enhanced due diligence codes based upon the types of activity you want to monitor for. These codes can then be added to the membership record for analysis using other tools.

Tool #402 ***Insider/Audit Due Diligence Report*** to analyze and report activity based upon the due diligence codes you have assigned to suspicious accounts. This tool is also used to analyze internal employee accounts.

In addition to the above tools the credit union may also want to utilize the following:

Tool #101 ***Abnormal Activity Monitoring Config*** *to configure both types of analytical tools. One for the monthly review based upon thresholds and the other more robust tools based upon specific patterns.*

Tool #537 ***Monitor Abnormal Transaction Activity*** *to run the groups you have set up or the patterns you have configured in accordance with the credit union's member activity.*

Request a copy of AuditLink's best practice guide for performing research on suspicious accounts. https://store.cuanswers.com/product/abnormal-activity-monitoring-transaction-patterns-a-guide-for-change-management-and-data-governance/

MONETARY INSTRUMENT SALES

PURPOSE

Monetary instruments can circumvent a layer of transparency for money launderers. Since they can be purchased with cash in amounts below CTR thresholds, they can be used to make funds appear clean. In order to help combat this, 31 CFR 1010.415 of Chapter X requires financial institutions to maintain certain information about the sales of monetary instruments when they are purchased with cash for amounts between $3,000 and $10,000. Credit unions are not necessarily required to keep a log but are required to keep records. Additionally, should law enforcement request records for these sales, the credit union is expected to furnish documentation in a timely manner.

EXPECTATIONS

Your auditor will request your records for monetary instrument sales that were paid for with cash. The auditor will test to make sure the required information is retained in an easily accessible manner.

AUDIT PROCEDURES

Testing will look for the following items:

The credit union maintains records of monetary instruments sold for cash in amounts between $3,000 and $10,000.

The Credit Union Includes Information on the Sale of These Items

- Date of transaction
- Type of instrument sold
- Serial number
- Dollar amount of cash portion of the transaction
- Documentation of identity
- Name
- Account number
- Address
- Date of birth (for shared branching members or non-members)
- SSN (for shared branching members or non-members)

DOCUMENTS REQUESTED PRIOR TO THE AUDIT

☐ Money instrument log / or record of negotiable instruments purchased with cash

DOCUMENTS REQUESTED AT THE TIME OF THE AUDIT

None unless there is a discrepancy or missing document

TOOLS

Tool #260 *Configure Memo Type Codes for Trackers* (to configure Memo Type code MI for monetary instruments)

Tool #664 *Print Member Trackers* (for running the report listing all monetary instruments)

WIRE TESTING

PURPOSE

Wires are a fast and easy means of transferring funds between parties, both domestically and internationally. As an attractive option for money launderers, credit unions must be vigilant in monitoring wire transfers to detect and prevent money laundering. Additionally, wires are governed by "The Travel Rule" which acts as recordkeeping requirements. 31 CFR 1010.410 establishes requirements for information to be kept regarding wire transfers in amounts of $3,000 or more.

Wires are also a prime vehicle for criminals to evade OFAC sanctions and have a history of being a popular vehicle for moving funds. Sound OFAC programs will ensure that all parties, including intermediary institutions, are scrubbed against OFAC prior to sending or crediting a wire.

EXPECTATIONS

Your auditor will request supporting documentation from a sample of wires selected from your wire logs. The auditor will assess if the credit union maintained sufficient documentation to satisfy the Travel Rule requirements, which include:

- Name and address of the originator
- Amount of the payment order
- Date of the payment order
- Any payment instructions
- Identity of the beneficiary's institution
- As many of the following items as are received with the payment order
    - Name and address of the beneficiary
    - Account number of the beneficiary
    - Any other specific identifier of the beneficiary

Your auditor will also request OFAC verification indicating all related parties, including the sender or receiver, any additional beneficiaries, the initiating or receiving institution, and any intermediary institution was scrubbed.

AUDIT PROCEDURES

Testing will look for the following items:

- The credit union collected all applicable information to satisfy the Travel Rule requirements
- The credit union verified OFAC on all related parties in compliance with its policies and procedures
- The credit union retained evidence of the member initiating or requesting outgoing wires
- The credit union practiced dual control in the outgoing wire process

DOCUMENTS REQUESTED PRIOR TO THE AUDIT

☐ Wire logs from the last three months of the review period

DOCUMENTS REQUESTED AT THE TIME OF THE AUDIT

☐ Supporting documents for the wire selections made at the time of the review

TOOLS

Tool #980 ***Wire Transfer Activity Report for a*** list of all wire transfers that have been marked as "Completed" in the CU*BASE Wire Tracking system

Tool #981 ***Wire Transfer Tracking*** to mark a wire transfer that has already been posted to a member account as being completed

INFORMATION SHARING TESTING

PURPOSE

Section 314(a) of the USA PATRIOT Act requires all financial institutions to share information with law enforcement. These requests are generated on a bi-weekly basis with special requests made outside of this normal routine, as necessary. Credit unions have 14 days to respond to positive matches via FinCEN's 314 website.

Section 314(b) allows for financial institutions to share information between themselves to aid in money laundering investigations and allow for more accurate SAR filing. This information sharing is completely voluntary and credit unions must register for participation via FinCEN's 314 website.

Both types of information sharing are vital to law enforcement and SAR investigations. To further prove this point, law enforcement and FinCEN strongly encourage all financial institutions to participate in information sharing and cooperate in information sharing at every opportunity.

EXPECTATIONS

Your auditor will request a log of your FinCEN 314(a) activity via FinCEN's 314 website. This log will then be compared to the member scrubs housed within your core. The auditor will ensure that timely review of these lists is occurring. Additionally, the auditor will review if your credit union has renewed voluntary information sharing registration within the annual timeframe if your credit union has elected to participate in 314(b) information sharing.

AUDIT PROCEDURES

Testing will look for the following items:

- Evidence the credit union reviewed the 314(a) requests in a timely manner
- Evidence the credit union renewed 314(b) registration within the 12-month timeframe, if applicable

DOCUMENTS REQUESTED PRIOR TO THE AUDIT

☐ FinCEN 314(a) SISS report for the entire review period

☐ Documentation of the 314(a) reviews for the entire review period

☐ Most current acknowledgement letters for all applicable employees for 314(b)

DOCUMENTS REQUESTED AT THE TIME OF THE AUDIT

None, unless there's a discrepancy or missing document

TOOLS

Tool #769 *Run FinCEN 314* to generate the FCPERSON and FCBUSINESS reports.

RECORD RETENTION TESTING

PURPOSE

31 CFR Chapter X requires that BSA records are retained for specific periods of time. Most documents are required to be maintained for a period of 5 years. However, there are some exceptions. For an exhaustive list, reference the FFIEC exam manual, Appendix P.

EXPECTATIONS

Your auditor will request documents from within the recordkeeping requirement timeframes to ensure the credit union is maintaining records within the prescribed requirements.

AUDIT PROCEDURES

Testing will look for the following items:

- Evidence the credit union maintains records within the BSA recordkeeping requirements

DOCUMENTS REQUESTED PRIOR TO THE AUDIT

None

DOCUMENTS REQUESTED AT THE TIME OF THE AUDIT

☐ Selections of CTRs, SARs, monetary instrument sales records, or other BSA records within the recordkeeping requirement timeframes

UNSECURED LOANS TESTING

PURPOSE

Extensions of credit are an attractive option for money launderers, as it can often be used for a quick and easy way to make their illicit funds appear to be cleaned. As such, 31 CFR 1010 requires financial institutions to document the purpose of extensions of credit over $10,000 which are not secured by real property.

EXPECTATIONS

Your auditor will test to ensure that the credit union is documenting pertinent information about the extension of credit not secured by real property, including the nature and purpose of the extension.

AUDIT PROCEDURES

Testing will look for the following items:

- Evidence the credit union collects the purpose for unsecured loans granted for amounts over $10,000

DOCUMENTS REQUESTED PRIOR TO THE AUDIT

☐ Unsecured loans listings for a selection of months during the review period

DOCUMENTS REQUESTED AT THE TIME OF THE AUDIT

☐ Selection of loan applications or evidence of purpose of loan made at the time of the review

TOOLS

Tool #778 ***Scan a Single Name Through OFAC*** to run an OFAC scan on a person's name or an organizational name.

CONCLUSION

BSA regulations and audit and exam processes are changing on an annual basis. With that said, so too will the tools of the CU*BASE platform and their best practice use. CU*Answers' partnership with Lillie & Company has proven itself over and over. When you marry those in the field performing audits with the experts in BSA at CU*Answers responsible for being practitioners and designers of functionality it forms a powerful alliance designed to guarantee you will stay one step ahead of the auditors and examiners.