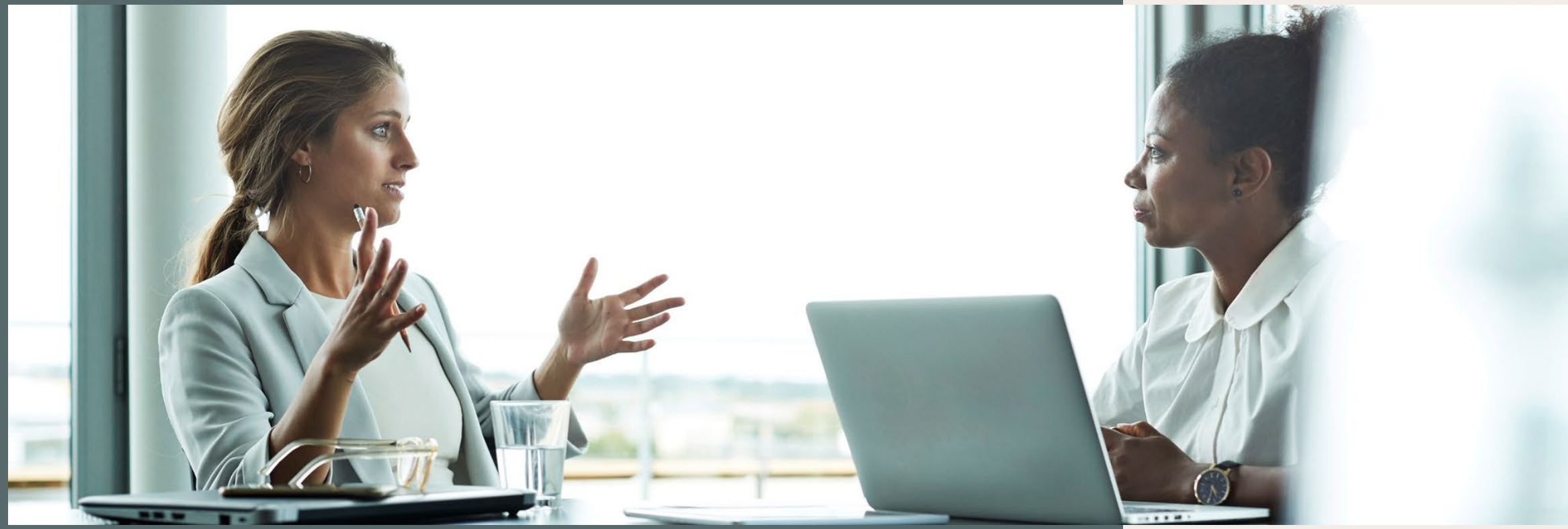


BSA Exams/Audits Made Easy

Ingredients to Ensure Success!

JIM VILKER

VP of Professional Services, CAMS, NCCO

AuditLink

Introduction

- Successful BSA Audits are a critical component of your credit union's operations.
- Preparing for BSA Exams/Audits can be overwhelming.
- AuditLink has teamed up with Lillie and Company to ensure you will always be ready for an external audit or exam.
- Our partnership combines the expertise of CU*BASE with Lillie and Company's proven track record in providing auditing and consulting services exclusively designed for credit unions across the country.

Topics for Today's Presentation

- Common Acronyms
- Risk Assessment
- Policies and Written Procedures
- Internal Controls
- Training
- CIP and OFAC Review and Testing
- CDD Member Risk Profile
- CTR Exemptions
- Suspicious Activity Monitoring and SARs
- Monetary Instrument Sales
- Information Sharing Testing
- Record Retention Testing
- Unsecured Loan Testing

Common Acronyms

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	Financial Federal Institutions Examination Council
FINCEN	Financial Crimes Enforcement Network

FOM	Field of Membership
HIDTA	High Intensity Drug Trafficking Areas
HIFCA	High Intensity Financial Crime Area
ISO	Independent Service Organization
MRB	Marijuana-related Business
MSB	Money Services Business
ML/TF	Money Laundering/Terrorist Finanacing
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:

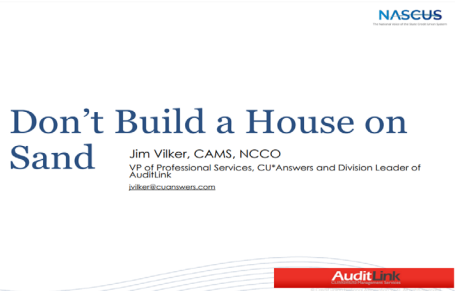
- Bank, Banks, Savings Associations, Credit Unions
- Customer, Member

Risk Assessment

Purpose

- A well-developed BSA/OFAC Risk Assessment is the cornerstone of an effective BSA program.
- Enables you to better manage and mitigate risks in operational controls.
- Should be shared across business lines within the credit union.
- Used by examiners for scope out the review of your BSA program.

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



Expectations

- Risk assessment should include qualitative and quantitative analysis which will drive your risk classifications.
- Review risk assessment at least once annually and prior to an audit/examination.
- A good risk assessment should follow FFIEC guidelines and should include:
    - Demographics
    - Geography
    - Staff
    - Member Profiles

Policies and Written Procedures

Purpose

- Effective anti-money laundering and countering the financing of terrorism programs safeguard national security and generate public benefits.
- Prevent the flow of illicit funds in the financial system, assist law enforcement and national security agencies.
- Anti-money laundering and countering of financing terrorism programs should be:

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

    B. Risk-based, ensuring that more attention and resources be directed toward higher-risk customers and activities and tailored from your risk assessment.

Let's have a conversation on using templates

Internal Controls

Purpose

- One of the 5 BSA Pillars is the development of a system of internal controls.
- Examiners and auditors rely on the FFIEC manual to assist with the preparation of their procedures and guide their focal points.

Expectations

- The board of directors has ultimate accountability for internal controls. Their responsibility is to ensure the following, among others:
    - Comprehensive risk assessment is developed, policies and procedures to mitigate and control illicit activity risk.
    - Culture of compliance exists.
    - Program continuity despite personnel changes.
    - Corrective actions are made from previous deficiencies.
    - Adequate time and resources to administer an effective program.
    - Specify BSA compliance responsibilities for personnel, provide oversight for execution.
    - Sufficient knowledge and expertise of those responsible for BSA administration.
    - Systems and technology sources functioning appropriately.
    - Dual controls process.

Internal Controls

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 BSA/AML compliance program.
- Credit unions have flexibility in how they design the program.
- Effective programs provide employees with a clear understanding of how BSA/AML and OFAC regulations affect their specific jobs.
- Training is also required for the board of directors.

Expectations

- Training should be commensurate with job function, should be well-documented.
- New hires should receive training upon employment.
- Employees and board members should receive ongoing training – annually, or if BSA requirements change.
- Training should include BSA requirements as well as scenarios, examples, typologies of criminal behavior, and a reinforcement of the importance of the BSA.

Training

Classes Available through CU*Answers

- Bank Secrecy Act
- BSA for Frontline Staff
- BSA for Volunteers and Senior Management
- The USA Patriot Act
- BSA for Electronic Services
- BSA for Lending Operations

CIP and OFAC Review and Testing

Purpose

- Customer information policy and related program should be tailored to risks identified in your risk assessment as it relates to membership.
- Credit unions who are 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.
- Should include risks associated with assessment including:
    - Types of accounts maintained by CU
    - The CUs methods of opening accounts
    - Types of identifying information available
    - CU size, location, and customer base

CIP and OFAC Review and Testing

Expectations

- Expect third party auditors and examiners to concentrate on the risks described, 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 the types of accounts a CU opens. CUs must ask questions regarding the nature and the purpose of the account.
- The FFIEC has identified high risk occupations such as doctors, attorneys, real estate agents, etc. However, asking about an occupation is not required.

CIP and OFAC Review and Testing

Expectations

- Auditor/examiner will ask for a sampling of new accounts opened since the prior audit/examination. Based on the credit union's CIP policy, expect the examiner to request evidence of:
    - Signature card – Tool 329 CU*Spy
    - Government issued ID - Tool 329 CU*Spy
    - Results for OFAC scan at the time of account opening – Snip of member audit tracker for primary. For joint owners tool 559 OFAC Non-member Scan History
    - Risk rating (if required by CU policy)
    - Beneficial ownership form for legal entities, along with procedures for ongoing monitoring against OFAC lists. – Snip of member trackers for controlling agent and tool 559 for beneficial owners
    - For accounts opened virtually, the procedures for reviewing these accounts and secondary validation model results. Contact Experian if using Precise ID
    - A sample of signature cards of closed accounts dating back 5 years to test record retention compliance. – For sampling use tool 487

Let's have a conversation on risk rating

CIP and OFAC Review and Testing

Expectations

- For ongoing scans of members and non-members, these scans are run every Saturday against the most current lists. A report is generated and saved in your CU*Spy archive.
- 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.

CIP and OFAC Review and Testing

Audit Procedures

- The CU ensured the following for personal membership accounts:
    - Collected the name of the member and all joint members
    - Collected the physical address(es), SSNs, DOBs for all signers on the account
    - Verified the physical mailing address with either a government issued photo ID or other method
    - Collected the occupations for all individuals on the account
    - Verified OFAC for additional signers on the account
    - Completed a CDD profile for all members on the account
    - The CU collects and retains all documents required in policy or procedure
- The CU collected all information required for business membership accounts:
    - Collected required business entity documents
    - Identified the nature of the business
    - Identified all signers on the account using CIP processes
    - Collected the beneficial ownership information on a certification form acceptable to the regulation
    - Collected CIP information for all beneficial owners using CIP-like procedures
    - Performed OFAC for the business and all singers and beneficial owners (if different) on the account
    - The CU collects and retains all organizational or other documents required by policy or procedure

CIP and OFAC Review and Testing

Documents Requested

- New member listing. Auditor/examiner will select a sample or members. Tool 487 for member trial balance
- Shares AIRES file Tool 122 Create Aires file and tool 1375 to download data
- Member files for the selected accounts. The following information will be examined:
    - Account card
    - Proof of OFAC on all parties
    - 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. Tool 329 CU*Spy and search for OFAC
- Evidence of non-member OFAC verifications made at the same time of the transaction. Snip of member tracker for scan such as a corporate check recipient.

CIP and OFAC Review and Testing

Tools

- Tool #329: *CU*Spy Daily Reports*
- Tool #559: *OFAC Non-Member Scan History – for non-members*
- Tool #778: *Scan a Single Name Through OFAC*
- Tool #122: *AIRES Create Files* and Tool #1375: *Data Transfer (Upload or Download)*
- Tool #487: *Mbr Trial Balance Listing – Select Info*
- Tool #664: *Print Member Trackers*
- Tool #523: *Member Designation Configuration*
- Tool #559: *OFAC Non-Member Scan History*
- Tool #329: *CU*Spy Daily Reports*

Provide your auditor the following

Using the CU*BASE Data Match System for OFAC Compliance

https://www.cuanswers.com/wp-content/uploads/UsingtheCUBASEDataMatchSystemforOFACCompliance.pdf

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.
- Effective CDD policies, procedures, and processes provide critical framework that enable financial institutions to comply with regulatory requirements including monitoring for and reporting suspicious activity.
- CDD policies, procedures, and processes are critical to the financial institution because they can aid in:
    - Detecting & reporting unusual/suspicious activity that potentially exposes the credit union to financial loss, increased expenses, or other risks.
    - Avoiding criminal exposure from persons who attempt to use the bank's products & services for illicit purposes.
    - Adhering to safe & sound banking practices.
- CID and CPP work together to establish risk policies.

CDD Member Risk Profile

Expectations

- In determining a customer's risk profile, the financial institution should consider the following risk categories:
    - Products & services
    - Customers & entities
    - Geographic locations
    - Other high-risk criteria that should be explicitly defined
- Financial institutions should establish criteria for when and by whom customer relationships will be reviewed. Factors that may be relevant in determining when it is appropriate to review a customer relationship:
    - 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
    - Results of negative media search programs
    - Length in time since customer information was gathered and customer risk profile assessed

CDD Member Risk Profile

Expectations

- Procedures should be documented to explain the CDD program and how/when Enhanced Due Diligence will be performed.
    - There is no specific format a financial institution must follow when establishing risk profiles; 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 us considered high risk should be defined.

CDD Member Risk Profile

High Risk Accounts

- Examiners and auditors will review and test not only your ongoing review of 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.
- Examiners/auditors will also review "high risk" accounts procedures and practices to verify the CU is identifying and monitoring accounts that have characteristics of elevated risk of money laundering or other criminal activity. It is imperative that these reviews be documented.
- Enhanced due diligence flags can be configured in Tool #427: *Configure Due Diligence Codes*. Up to 9 codes can be used to generalize the types of activity you are monitoring for.
- 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* or Tool #537: *Monitor Abnormal Transaction Activity*.

CDD Member Risk Profile

Audit Procedures

- Review the policies & procedures developed by the financial institution and :
    - Ensure that effective process exist to develop a risk profile
    - Confirm procedures are risk-based and adequate to the risk profile and appetite of the CU
    - 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 is policies and procedures, and the CDD was documented
    - Confirm high risk members are reviewed and the 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.

CDD Member Risk Profile

Documents Requested

- Copy of CDD matrices, if available of 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* or Tool #537: *Monitor Abnormal Transaction Activity*. Please generate report.

CDD Member Risk Profile

Tools

- Tool #101: *Abnormal Activity Monitoring Config*
- Tool #247: *Configure Due Diligence*
- Tool #20: *Update Account Information*
- Tool #402: *Insider Audit/Due Diligence Report* or Tool #537: *Monitor Abnormal Transaction Activity*.
- Tool #260: *Configure Member Type Codes for Trackers*

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.

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.

CTR Exemptions

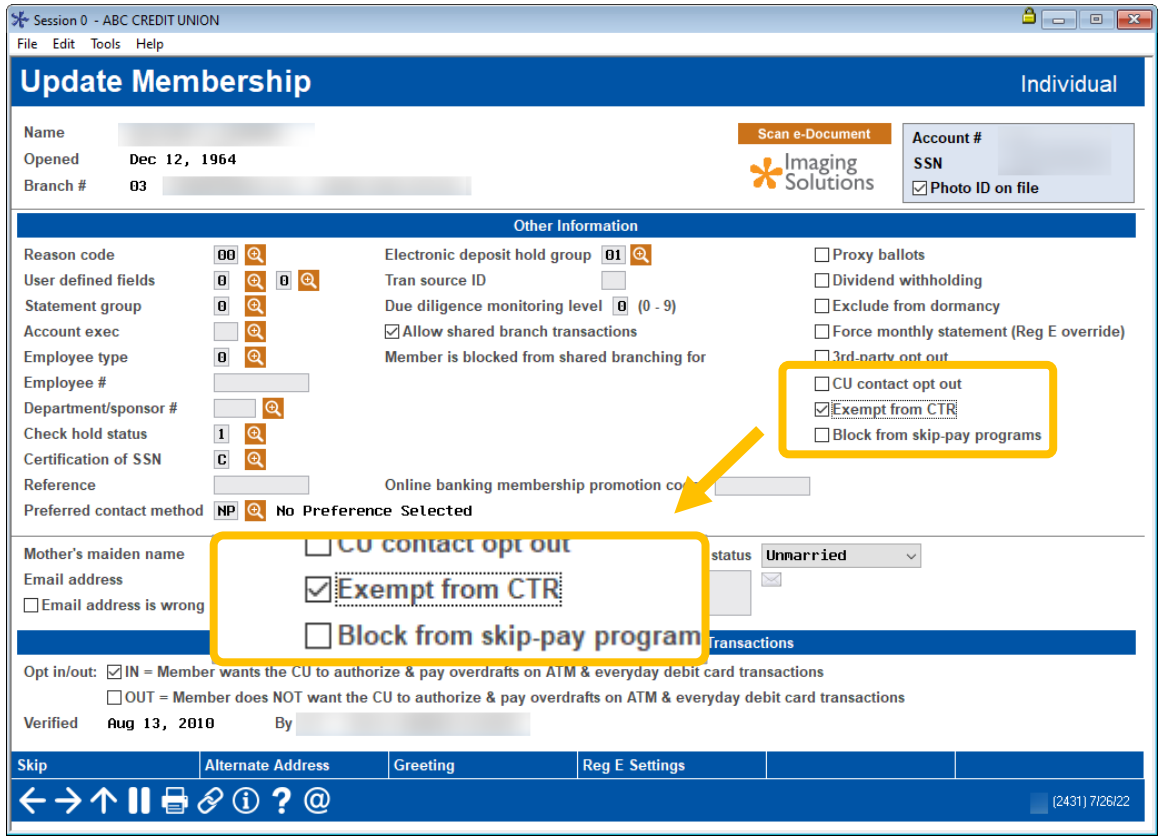
Audit Procedures

- 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.

CTR Exemptions

Tools

- Tool #15: *Update Membership Information*
    - 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.

Suspicious Activity Monitoring and SARs

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.

Suspicious Activity Monitoring and SARs

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 and SARs

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)

Suspicious Activity Monitoring and SARs

SARs will be tested for the following items:

- 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.

Suspicious Activity Monitoring and SARs

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.

Suspicious Activity Monitoring and SARs

Tools

- Tool #1990: *Print BSA/SAR Structuring Report*
- Tool #247: *Configure Due Diligence Codes*
- Tool #402: *Insider/Audit Due Diligence Report*

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

- Tool #101: *Abnormal Activity Monitoring Config*
- Tool #537: *Monitor Abnormal Transaction Activity*

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.

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.

Monetary Instrument Sales

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.

<u>The Credit Union Includes Information on the Sale of These Items:</u>

- 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)

Monetary Instrument Sales

Tools

- Tool #260: *Configure Memo Type Codes for Trackers*
- Tool #664: *Print Member Trackers*

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.

Information Sharing Testing

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.

Information Sharing Testing

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

Information Sharing Testing

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.

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 including last five years audits, sample of CIP documents, wire transfer logs, cash logs, CTR's, and SAR's.

Let's have a conversation on what is and what is not saved in GOLD

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.

Unsecured Loans Testing

Tools

- Tool #788: Selective Loan Information Report to generate a report of unsecured loans

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.

Questions or Comments?