BSA Risk Assessments and Transaction Monitoring Systems: Partners in Crime...Prevention and Detection

Presented by
Lynn English
Lafayette Federal Credit Union
Key Takeaways

• After this webinar, participants should have an understanding of basic risk assessment methodology

• Understand the relationship between the BSA Risk Assessment and automated transaction monitoring

• Understand Examiner Expectations for utilizing an automated monitoring system
Agenda

• What is **risk** and why are risk assessments so important?
• Getting Started
• Who should be involved?
• Risk Categories
• Scoring Methodology
• Static vs. Living Documents
• Manual vs. Automated Transaction Monitoring
• Selecting an Automated Solution
• Programming your Monitoring System
• Examiner Expectations
What is “risk” and why are risk assessments so important?

• Risk is defined by Merriam-Webster as:
  • Possibility of loss or injury: Peril
  • Someone or something that creates a hazard
  • To expose to hazard or danger

• Why is the risk assessment so important?
  • A way to identify whether or not a certain risk is present
  • A way to track identified risks and ways to deal with them
  • A way to assign levels of risk to identified vulnerabilities
  • A way to gain familiarity with all the facets of the organization
  • A way to keep your Board of Directors informed of risks that may impact the organization
  • Serves as the blueprint for your transaction monitoring program or system
  • Because the FFIEC said so...
Poll Question??

• Did your credit union use a 3rd party conduct your initial BSA risk assessment?
  
  • YES
  • NO
Getting Started

The first thing to consider when undertaking the risk assessment project is that each risk assessment will be as unique as the entity completing it. You can’t adopt the risk assessment of another institution because each operates differently.

• Identify who owns the risk assessment: In this case it should be the BSA Officer. With other types of risk assessments, ownership should be assigned according to the type of assessment (IT, ACH, Online Banking).

• Assemble a cross functional team: For a BSA risk assessment, you will be reviewing all aspects of the organization to determine whether or not a BSA risk is present across each line of business your organization maintains.
Who Should be Involved?

Depending on your organization’s size you will need representation from the following areas:

• Operations
• Frontline
  • Branch Services
  • Call Center (if internal)
• Lending
• ACH/Wire
• Compliance
• Internal Audit
• Senior Management
Risk Categories: The risk assessment should take into consideration general categories and any special characteristics applicable to your organization. Here is a list of examples:

- **Membership (Open vs Closed)**
- **Geography**
  - HIDTA-High Intensity Drug Trafficking Area
  - HIFCA-High Intensity Financial Crime Area
  - US vs Overseas Physical Presence
- **Geography (Where are your Members?)**
- **Transactions**
  - Types
  - Movement
  - Volumes
- **Products Offered**
  - Wires
  - ACH
  - Credit/Debit Card
  - Currency Exchange
  - Pouch Services
  - Online banking
  - Cash
  - Shared Branching
  - Mobile Deposit
  - Loans
    - Consumer
    - Commercial
    - Indirect Programs
Risk Categories: The risk assessment should take into consideration some general categories and any special characteristics applicable to your organization.

- **Staffing**
  - Frequency of turnover
  - Rate of Fraud

- **Members**
  - Consumer
  - Commercial
  - High Risk?

- **Branches**
  - Number
  - Location
  - Staffing

- **Compliance Program**
  - Written Program
  - Board Oversight
  - Internal Controls
    - Independence
  - Independent Review (Internal or External Auditors, Consultants)
  - Training
    - Frequency
    - Content
  - Designated Compliance Officer
    - Appropriate staffing
    - Adequate knowledge and education
    - Budget Allocation?
Risk Categories: The risk assessment should take into consideration some general categories and any special characteristics applicable to your organization.

- **Policy & Procedures**
  - Written Program
  - Updated regularly
  - Comprehensive?

- **Regulatory Issues**
  - Audit Findings
  - Enforcement Actions
    - DOR-Document of Resolution
    - Monetary Penalties

- **Transaction Monitoring**
  - Manual (system report reviews)
  - Automated
  - 3rd Party reliance
Static vs. Living Document

• Risk assessments are what is known as “living” documents. Unlike an Executive Summary or Corporate memo that you give to Senior Management once (static document), a risk assessment, once it has been completed will need to be updated when the landscape of the organization changes.

• The FFIEC BSA Examination Manual dictates that the risk assessment should be updated at least every 12-18 months.

• A good rule to follow would be to update the risk assessment whenever a new product or service is introduced, branch is opened, staffing changes, etc and of course with any regulatory changes that effect the BSA program.

• The Board of Directors should receive an update annually.
Scoring Methodology

• Drafting your assessment doesn’t have to be complicated. An Excel spreadsheet works very well.

• Scoring should be kept simple so that it is easy for the reader to understand. Common methods are as simple as High, Medium and Low or Red, Yellow and Green.

• The basic formula for risk scoring is:
  • Impact X Probability= Risk
  • The values assigned to each rating should make calculating the risk easy.
Risk Assessment Headers (Categories)

• Here is a sample list of recommended column headers for the assessment:
  • Threat
  • Current Practices
  • Risk Category (Compliance, Credit, Reputation, etc)
  • Probability
  • Impact
  • Net Risk (Probability x Impact)
  • Risk Strategy (Mitigate, Avoid, Deflect, Accept)
  • Compensating Control
Poll Question?

• Does your Credit Union use an automated BSA transaction monitoring system?
  • YES
  • NO
The risk assessment should identify the areas of BSA risk your institution faces. Once identified, you can create a program to monitor those risks within the organization. The question now becomes, should we do what has always been done or should we automate the monitoring process? Hmmm...
Manual Monitoring

• If you are still using a manual process, consider the following:

  • Do we have the ability to capture the risks identified in the risk assessment?
  • Is the monitoring consistent across the organization?
  • Can we afford an automated monitoring system?
  • Can we afford to run our BSA program without any type of automated system?
Automated Monitoring

• If using an automated transaction monitoring system, consider the following:

  • Can your monitoring system track the risks identified in the risk assessment?

  • Does the staff know how to use the monitoring system effectively?

  • Do you now need more staff in the department because we automated?
Selecting an Automated System

Selecting an automated solution can be a daunting task, but there are certain things universal to the selection process:

- **Pricing** - Try to consider *value over cost*
- **Features** - Does it do all that you want or need?
- **Training** - Does the Vendor offer training?
- **Ease of Use** - Do you need a PhD to understand it?
- **Support**
  - Is it built in to the contract?
  - Extra cost?
  - Availability
- **Implementation**
  - How long does it take?
  - In house or hosted by Vendor?
  - Is the Vendor familiar with your core processor?
- **References** - Can you speak with other clients?
Programming Your Monitoring System

• An automated solution can come pre-programmed, but rarely will it match the risk assessment for your organization.

• Your risk assessment will serve as the roadmap for your monitoring system.

• The rules or strategy your system uses should be able to address the majority of the risks addressed in your risk assessment.

• Rules should be reviewed periodically to ensure they are still relevant or effective.

• New rules should be added as new threats are identified.
Poll Question??

- Has your Examiner ever asked for a demonstration of your transaction monitoring system?
  - YES
  - NO
Examiner Expectations

Whether you are monitoring manually or using an automated system, your Examiner expects you to be able to demonstrate the following:

• Manual system
  • Clear, consistent methodology
  • Organized record keeping

• Automated System
  • Demonstrated understanding of system features
  • Demonstrated understanding of reports
  • Evidence of Rule updates
  • Management of 3rd parties (if applicable)
  • Appropriate access levels
Summary

• Your risk assessment is critical to a successful BSA monitoring program.
• Whether you are using manual reports or an automated solution, the successful application of either process is based on your ability to monitor risks that were identified in your institution’s risk assessment.
• The expectation is that your credit union can identify the risks that it faces and show that the chosen method of monitoring works for the institution.
Useful Links

• FFIEC BSA/AML Examination Manual: https://www.ffiec.gov/bsa_aml_infobase
Questions?
If you have any questions regarding the presentation you have just seen you may contact me directly.

Lynn M. English
lenglish@lfcu.org