FedLinks®
Connecting Policy with Practice
BANK SECRECY ACT/ANTI-MONEY LAUNDERING COMPLIANCE
DECEMBER 2015

Overview

Financial institutions have many areas of focus, including lending, managing interest rate risk, and complying with consumer protection laws and regulations. However, financial institutions cannot afford to ignore BSA/AML compliance due to the reputational risk and large fines and settlements related to BSA/AML program deficiencies. In addition, BSA compliance is a factor reviewed in the application process when mergers and acquisitions are contemplated.

Many community banks find it challenging to keep their BSA/AML program up-to-date because of resource constraints and evolving money laundering trends. Historically, examiners have found that banks that have a thorough understanding of their BSA/AML risks, as documented by a high quality, supportable risk assessment, generally have a strong compliance program and, therefore, may be able to minimize administrative expenses associated with BSA/AML compliance by focusing on the areas of highest risk.

There are many effective methods and formats for completing a BSA/AML risk assessment. This bulletin offers ways in which data can be used to help quantify and analyze a bank's inherent BSA/AML risk, and highlights tools to assist community banks in establishing controls commensurate with their specific BSA/AML risks.

1 See the FFIEC's *Bank Secrecy Act/Anti-Money Laundering Examination Manual* at www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm

2 In the absence of significant changes, banks should reassess their BSA/AML risks at least every 12 to 18 months.

3 See the *BSA/AML Risk Assessment – Overview* section at www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_005.htm.

4 See Appendices I and J of the BSA/AML Examination Manual at www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_109.htm and www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_110.htm, respectively.

Risk Assessment Data Analysis

More and more financial institutions, including community banks, are using data to assess their exposures to different types of risks. Using data to assess interest rate risk, liquidity risk, and credit risk has become second nature. Similar data can be helpful in enabling an institution to draw accurate conclusions about its BSA/AML risk profile.

> *"The inclusion of transactional data can be instrumental in putting these three risk areas (products and services, customers, and geographies) into perspective."*

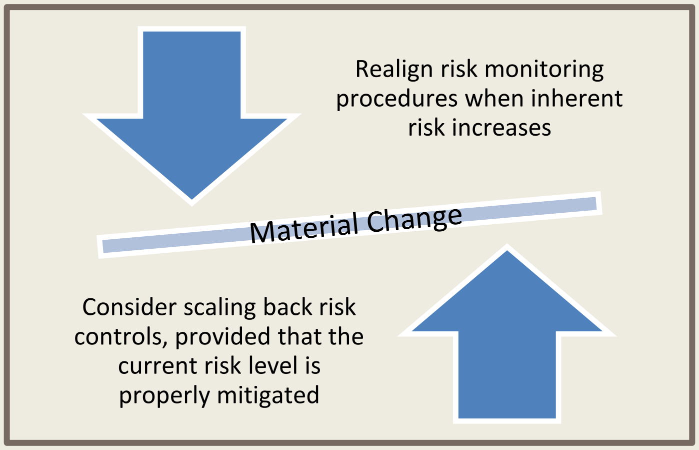
When developing a comprehensive BSA/AML risk assessment, financial institutions should review the Federal Financial Institutions Examination Council (FFIEC) *Bank Secrecy Act/Anti-Money Laundering Examination Manual*,[1] which articulates supervisory expectations concerning the content and frequency of banks' risk assessments.[2] Specifically, the "BSA/AML Risk Assessment – Overview"[3] section, as well as Appendices I and J,[4] of the examination manual highlight the basic elements that should be considered and provide a useful framework to formulate summary conclusions. Still, community banks should remain mindful that as their size, risk, and/or complexity increases, the BSA/AML risk assessment should evolve accordingly (for instance, the level of detail and supporting information may need to increase).

Following are examiner insights on how data can be helpful in supporting the risk assessment process at community banks. These insights consider what data can be analyzed; how it can be generated or gathered, sufficiently measured, and applied to formulate policies and procedures; and, how the process can be repeated in future years.

FedLinks is intended to highlight the purpose of supervisory policy and guidance for community banking organizations. FedLinks does not replace, modify, or establish new supervisory policy or guidance.

What Data Is Important

The strong BSA/AML risk assessment process should include an evaluation of a bank's transaction data associated with three specific risk categories – products and services, customers, and geographies – that a bank's BSA/AML staff can use to assess and highlight the areas of highest risk. Banks should also use data to identify changes and trends to the bank's inherent risk profile from the prior risk assessment cycle. If material changes exist, BSA/AML staff can review the changes in detail to determine if they are connected to a particular customer or segment of customers, geographic location, product, service, or a change in law or regulation. By analyzing changes and underlying factors, the bank can ensure that its procedures are appropriately aligned with the risks present at the institution. Conversely, if there are no material changes, the bank can justify keeping the same internal controls and procedures. Lastly, if there are continued declines in risk levels, the bank could justify scaling back controls, provided that the current risk level is mitigated and there is continued compliance with all BSA-related laws and regulations. The figure below illustrates how a bank may align its risk assessment procedures depending on material changes in transaction data.



Products and Services Comparing cash, domestic wire, international wire, Automated Clearing House (ACH), International ACH Transaction (IAT), and other significant transaction activity to overall transaction activity over an appropriate time frame gives BSA/AML staff the ability to quantify the significance of BSA/AML risk of most products and services offered. BSA/AML staff may consider comparing the total number of transactions to the total dollar amounts for the different types of credit and debit activities. If the data analysis reveals material changes from the prior risk assessment cycle, staff should adjust the bank's BSA/AML policies or internal controls to address the change in risk. Transaction data can also identify risks which may affect other departments (for instance, information technology, operations, marketing, and lending).

Customers Customer risk can be evaluated by reviewing several different data points, such as customer and due diligence information, allowing the bank to determine the risk-rating of its customer relationships. The bank should first identify all higher-risk customer relationships by way of an effective BSA/AML customer risk-rating methodology. Customer risk-rating is also essential for purposes of identifying changes to a customer's expected transaction profile during the periodic customer due diligence review process, as well as to ensure the appropriate level of suspicious activity monitoring is applied.

Generally, community banks do not have an excessive number of BSA/AML higher-risk customers; nonetheless, the transactions associated with higher-risk customers could be significant. Higher-risk customer transaction data could be used to identify the scope of the BSA/AML risk posed by a bank's customer base. By quantifying the volume of higher-risk customers and their transaction values and volumes, a bank's BSA/AML staff can focus efforts on having proper due diligence and suspicious activity monitoring processes in place, as well as ensuring that these processes evolve with the nature of the changing transactional profile of its higher-risk customers. Additionally, if there is an increase in the number of higher-risk customers or the volume of transactional activities, then the risk assessment process may reveal bigger-picture strategies that impact the overall BSA/AML risk of the organization. *Note: If a bank cannot differentiate customer totals in its data analysis, the bank can use account totals as a viable alternative as long as it looks consistently across risks and from year-to-year.* Banks should also identify concentrations of customer types and corresponding changes from the prior risk assessment cycle. For example, a bank may track the following:

- Total personal customers;
- Total business customers;

- Total money services business (MSB), cash-intensive business, and other high-risk business customers; and,
- Top five concentrations by customer type, transaction volume, and transaction value, irrespective of customer risk rating.

Geographies Community banks generally associate geographic risks with High Intensity Drug Trafficking Areas (HIDTA)[5] and High Intensity Financial Crimes Areas (HIFCA).[6] It may be helpful for risk assessments to include diagrams or a narrative answering basic questions such as: *Does our institution have branches in HIDTA/HIFCA? Does our institution have customers residing in HIDTA/HIFCA? What percentage of our institution's transactions are sent to or received from HIDTA/HIFCA?*

> *"Aside from location in or near HIDTA/HIFCA, there are other geographical risks that should be considered when assessing geographical risks..."*

A bank should also consider the types of jurisdictions where customers conduct transactions (for example, international jurisdictions or jurisdictions outside of the bank's market area) when assessing the overall level of geographic risk. In addition, a bank may need to consider customers/transactions involving states or jurisdictions where marijuana has been legalized for medical or recreational purposes. For international customers/transactions, the Financial Action Task Force (FATF) List of High-Risk Non-cooperative Countries[7] and the United States Department of State International Narcotics Control Strategy Report[8] are useful resources in determining higher-risk geographic regions. Although there are a variety of methods to measure a bank's geographic risks, the bank's market area is usually the basis for assessing this type of risk. Comparing two or more consecutive years of data can be an effective measure of risk trends.

Regulatory Reporting Regulatory filings are also important pieces of data to consider. Reviewing suspicious activity reports (SARs), currency transaction reports (CTRs), Designation of Exempt Persons reports, and other regulatory filings can aid a bank in understanding filing trends compared to risks associated with a product, service, customer, and geography. If there are significant changes in the volume or types of regulatory filings over a period of two or more years, including a decrease in filings when BSA/AML risks have increased, a bank should assess the cause of the change and determine whether the bank should adjust internal controls, resource allocation, or training, or make other adjustments.

Data Sources

Some community banks invest in automated BSA/AML software, which makes extracting transaction and customer data easier. However, many community banks do not have an automated BSA/AML system and are reliant on various core internal systems to gather the data discussed in the prior section. If a bank does not have an automated BSA/AML system, locating the necessary data is the first step and likely the biggest hurdle in the process. BSA/AML staff may want to partner with 1) the bank's operations manager or personnel, 2) the bank's information technology manager or personnel, and/or 3) the banks' core system vendors, to identify and locate the data types and sources that can be used for the risk assessment. The table on page 4 offers various sources of data that can be considered from which to gather information.

5 For more information on HIDTAs, see: www.whitehouse.gov/ondcp/high-intensity-drug-trafficking-areas-program.

6 For more information on HIFCAs, see: www.fincen.gov/law_enforcement/hifca/.

7 View high-risk and non-cooperative jurisdictions publications at www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/.

8 View the Department of State's International Narcotics Control Strategy Report at www.state.gov/j/inl/rls/nrcrpt/.

Product and Service Data

- Product, service, and transaction data is typically derived from a bank's core systems or platforms (for example, teller, wire, ACH, and online banking). Because much of this information is available in daily, weekly, or monthly reports, a bank may be able to work with its internal staff or external vendors to generate annual volumes for different debit and credit transaction types, including international and domestic wires, ACH, IAT, cash, mobile banking, and automatic teller machines. Furthermore, internal reports that may be used to track other products and services, such as remote deposit capture and IATs, can often be exported from the system into a spreadsheet application and manipulated to get the desired results.

Customer Data

- Customer data is generally held within a bank's core systems in the format of customer information files (CIF). Higher-risk customer profiles are typically maintained by the BSA department. Higher-risk customer volumes can be compared to the general customer base. Furthermore, it may be possible to "flag" these higher-risk customers by their unique coding (for example, account number or customer number) and attain transactional information, similar to bank-wide transactions, specific to that higher-risk customer segment. As noted previously, if a bank has difficulty attaining customer totals, it is possible to utilize account number totals as long as the methodology is applied consistently year-over-year.

Geographic Data

- Geographic data generally consists of branch locations and proximity in or near designated higher-risk areas. After receiving branch information, BSA staff can compare a bank's geographical footprint to locations that may pose higher-risk, including HIDTA, HIFCA, permissible medical/recreational marijuana, international, and out-of-market-area geographies by referencing applicable and reputable websites. Measuring transactions that occur outside a bank's market area can give some perspective on a bank's geographic exposure, but this is likely the most difficult geographical data to generate. This type of data may be obtained by identifying incoming funds transfers, or funds leaving the institution to geographies outside of a bank's market area (city, state, or zip code). International activity from the product/service/transaction analysis can also be leveraged to identify any potential international geographic risk exposures.

Regulatory Filings

- Regulatory filings are tracked internally by all banks, so this should be readily accessible for risk assessment purposes. Reviewing dollar values may take some work if they are not previously tracked for SARs and CTRs, but identifying volumes and dollar amounts associated with filings and comparing to the general volumes of customers and transactions can be a helpful exercise to ensure controls are keeping pace with increased activity or customer volumes, particularly those related to the higher-risk customer portfolios.

General Bank Data

- Using general bank information, such as the size of a bank's assets, deposits, and loans, to conduct the risk assessment can also be helpful. The risk assessment should comment on significant changes in a bank's structure and size, including occurrences such as acquisitions of assets, banks, and/or subsidiaries, and bank staffing, primarily key staff turnover and continuity of BSA knowledge.

Data Organization and Analysis

Once the appropriate data has been identified and the mechanism to gather this data has been established, BSA/AML staff can decide what software or format to use to organize and analyze the data. BSA/AML staff may choose to use a database program; however, most community banks have found the greatest ease and benefit in working with a spreadsheet program. Once the data has been organized and its accuracy verified, BSA/AML staff can conduct analyses to look for material changes or trends in each of the categories.

Drawing Conclusions

BSA/AML staff completing the risk assessment should consider consulting with staff in the business lines to gain perspective on how the data should be interpreted. For example, BSA/AML staff could have a discussion with the wire department to better understand why certain trends in international and domestic wire activity are occurring within the bank, or with the retail/branch staff to understand why certain new customer trends may have occurred. Business line staff can also help the BSA/AML staff fully understand the business lines' strategies. This type of communication will result in increased BSA/AML knowledge across the organization and aid in promoting a positive compliance culture.

Documenting the Methodology

Initially, banks may experience obstacles in establishing a process to collect data, but once a collection process is in place, data collection should be relatively seamless in future years. It is helpful for a bank to document the methodology/procedures used to generate supporting data reports to aid in making future assessments repeatable and consistent.

> *"Evaluate the BSA/AML risk for your institution's entire portfolio."*

A documented methodology will also enable a third-party reviewer (for example, independent testing function or federal and state bank examiners) to understand the process without requiring a detailed explanation from those directly involved in the development and implementation. The documentation process does not need to be labor-intensive or formal, but it should identify: 1) staff involved in the analysis, 2) systems used to pull the data, 3) systems used to organize the data, and 4) templates used for organizing data.

Board and Management Reporting

As the board sets the risk strategy for the banking organization, it is important that directors and senior management be apprised of significant changes in risk so they can continue to make meaningful decisions and that changes in risk methodology are approved and documented. The information presented to the board and senior management should be concise, but provide enough detail to ensure they are familiar with the institution's risks. In turn, the risk assessment helps the board and senior management have a thorough understanding of the most prominent risks facing the bank. In the end, the data collection and analysis processes should culminate in a risk assessment that summarizes the overall risk profile of the bank, includes basic statistical information to support statements, provides an assessment of the internal control environment, discusses significant changes from previous years, highlights emerging risks, and states whether the results indicate any necessary action from the board or senior management team (including adjusting policies, procedures, training, and human or automated tools) to ensure that the program runs efficiently and effectively in the future.

Summary

Because money laundering can occur at any institution, regardless of size, product and service offerings, customer base profile, or location, it is essential that community banks understand their unique risks in order to appropriately and efficiently align procedures and controls to mitigate those risks. An effective risk assessment should be an on-going process and not a one-time exercise. Having a BSA/AML program that is not tailored to the actual risks of an institution can lead to negative impacts on a bank's bottom line, the overall effectiveness and continuity of its compliance program, and the usefulness of regulatory filings to law enforcement. Data is fundamental to an effective risk-based BSA/AML compliance program because it supports an institution's understanding of its unique risk and the development of a robust risk assessment and internal controls.

FedLinks is published on an ad-hoc basis and is a Federal Reserve resource for community banks. Current and past issues of FedLinks are available at www.cbcfrs.org *or* www.communitybankingconnections.org*. Suggestions, comments, and requests for bulletin topics are welcome in writing (*fedlinks@communitybankingconnections.org*).*