A Risk-Based Program

BSA Graduate School

January 2018

Consultants to the Financial Industry
Young & Associates, Inc.
121 E. Main Street
P.O. Box 711
Kent, OH 44240
Phone: 330.678.0524
Fax: 330.678.6219
www.younginc.com

Table of Contents

Introduction

A comprehensive Bank Secrecy Act/Anti-Money Laundering (BSA/AML) risk assessment must be completed. This includes a similar risk assessment relating to the institution's Office of Foreign Assets Control (OFAC) compliance program.

The financial institution regulatory agencies (Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and The Consumer Financial Protection Bureau) require banks and thrifts to develop and administer a program to assure compliance with the Bank Secrecy Act and its corresponding regulation.

Our objective in this seminar is to examine the federal examiners' expectations as they relate to a financial institution's assessment of its BSA/AML risk profile. This portion of the manual will include discussion of each of the key risk factors as set forth by the examiners, as well as other suggested factors to be considered in the risk assessment process. While banks have been expected to adopt and approve written BSA/AML compliance programs for some time, the BSA/AML risk profile expectation is an evolutionary change in a risk-based environment. Logically, a risk assessment (or profile) would normally occur prior to the development of policies or procedures.

The aspects relating to an Office of Foreign Assets Control (OFAC) risk assessment will be covered here and in the latter portion of the manual.

Examination Manual Background

The issuance of the uniform Bank Secrecy Act/Anti-Money Laundering (BSA/AML) examination procedures by the Federal Financial Institutions Examination Council (FFIEC) in June 2005 established a formal requirement for financial institutions to perform a BSA/AML risk assessment. The examination manual (exam manual) is used by all of the federal banking agencies for carrying out BSA/AML and OFAC examinations.

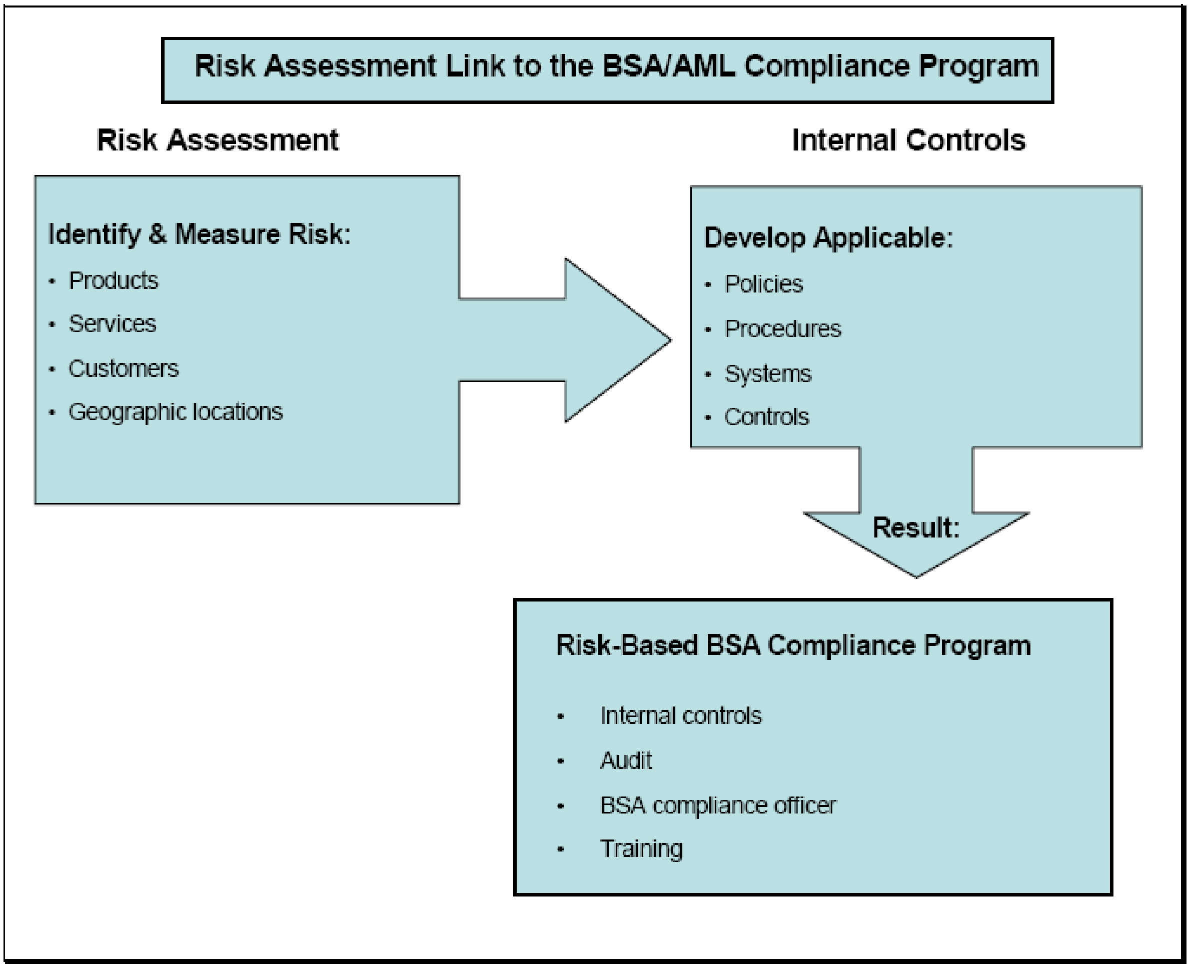
Periodically, the Federal Financial Institutions Examination Council (FFIEC) releases a revised Bank Secrecy Act/Anti-Money Laundering Examination Manual (Exam Manual). The most recent revision was released in 2014. The revisions generally reflect the federal banking agencies and the Financial Crimes Enforcement Network (FinCEN) efforts to provide current and consistent guidance on risk-based policies, procedures, and processes for banking institutions to comply with the BSA. The 2014 version of the Exam Manual may be found at:

https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf

This is the fifth generation of the manual. It is expected that such revisions will continue to occur on a periodic basis. While there were some changes to the exam manual in 2014, most changes were just getting the manual up-to-date with existing guidance such as rules for electronic filing of CTRs and SARs.

Section 2: The BSA Examination Manual Matrices

Each bank must have a BSA program. In order to make decisions regarding the specifics of a bank's program, the regulators have placed a renewed emphasis on the bank's Risk Assessment. The following graphic representation of this interrelationship appeared in the Exam Manual titled the "Quality of Risk Matrix" (Appendix I). It identifies the link between the BSA/AML risk assessment and the BSA/AML compliance program.



As the above diagram illustrates, an effective BSA/AML compliance program is directly linked and is a product of a BSA/AML risk assessment. The results of a risk assessment should have a direct impact on the level of policies and procedures required to maintain compliance. The final result is a risk-based BSA/AML compliance program.

An effective risk-based independent testing program will cover all of a bank's BSA/AML-related activities. Primary objectives of a risk-based independent testing program include:

- Enable the board of directors and auditors to use the bank's risk assessment to focus the intensity of the review.

- Assist the board of directors and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

Regulator Expectations for Risk Assessments

Developing risk-based policies and procedures have become commonplace in the day-to-day management practices of banks. Assessing risk for BSA/AML implications is no exception. Therefore, it was no surprise that the exam manual includes the concept of BSA/AML risk assessments.

The exam manual provides banks with tools to assist in the risk assessment process. We have included some of those tools in the Appendix of this manual and will cover the concepts throughout the presentation. Specifically, the exam manual provides banks and examiners with two key tools to assess the quantity of risk for BSA/AML and OFAC. The matrices are found on the next few pages. Throughout this manual, specific risk factors from the matrices will be reproduced as they relate to the section's topic.

Appendix J: Quantity of Risk Matrix

Banks and examiners may use the following matrix to formulate summary conclusions. Prior to using this matrix, they should complete the identification and quantification steps detailed in the BSA/AML Risk Assessment Overview section at pages 22 to 30 of this manual.

Low	Moderate	High
Stable, known customer base.	Customer base increasing due to branching, merger, or acquisition.	A large and growing customer base in a wide and diverse geographic area.
No electronic banking (e-banking) or the Web site is informational or nontransactional.	The bank is beginning e-banking and offers limited products and services.	The bank offers a wide array of e-banking products and services (e.g., account transfers, e-bill payment, or accounts opened via the Internet).
On the basis of information received from the BSA-reporting database, there are few or no large currency or structured transactions.	On the basis of information received from the BSA-reporting database, there is a moderate volume of large currency or structured transactions.	On the basis of information received from the BSA-reporting database, there is a significant volume of large currency or structured transactions.
Identified a few higher-risk customers and businesses.	Identified a moderate number of higher-risk customers and businesses.	Identified a large number of higher-risk customers and businesses.
No foreign correspondent financial institution accounts. The bank does not engage in pouch activities, offer special-use accounts, or offer payable through accounts (PTA), or provide U.S. dollar draft services.	The bank has a few foreign correspondent financial institution accounts, but typically with financial institutions with adequate AML policies and procedures from lower-risk countries, and minimal pouch activities, special-use accounts, PTAs, or U.S. dollar draft services.	The bank maintains a large number of foreign correspondent financial institution accounts with financial institutions with inadequate AML policies and procedures, particularly those located in higher-risk jurisdictions, or offers substantial pouch activities, special-use accounts, PTAs, or U.S. dollar draft services.

FFIEC BSA/AML Examination Manual J–1 04/29//2010

Low	Moderate	High
The bank offers limited or no private banking services or trust and asset management products or services.	The bank offers limited domestic private banking services or trust and asset management products or services over which the bank has investment discretion. Strategic plan may be to increase trust business.	The bank offers significant domestic and international private banking or trust and asset management products or services. Private banking or trust and asset management services are growing. Products offered include investment management services, and trust accounts are predominantly nondiscretionary versus where the bank has full investment discretion.
Few international accounts or very low volume of currency activity in the accounts.	Moderate level of international accounts with unexplained currency activity.	Large number of international accounts with unexplained currency activity.
A limited number of funds transfers for customers, noncustomers, limited third-party transactions, and no foreign funds transfers.	A moderate number of funds transfers. A few international funds transfers from personal or business accounts with typically lower-risk countries.	A large number of noncustomer funds transfer transactions and payable upon proper identification (PUPID) transactions. Frequent funds from personal or business accounts to or from higher-risk jurisdictions, and financial secrecy havens or jurisdictions.
The bank is not located in a High Intensity Drug Trafficking Area (HIDTA)[271] or High Intensity Financial Crime Area (HIFCA). No fund transfers or account relationships involve HIDTAs or HIFCAs.	The bank is located in an HIDTA or an HIFCA. Bank has some fund transfers or account relationships that involve HIDTAs or HIFCAs.	Bank is located in an HIDTA and an HIFCA. A large number of fund transfers or account relationships involve HIDTAs or HIFCAs.
No transactions with higher-risk geographic locations.	Minimal transactions with higher-risk geographic locations.	Significant volume of transactions with higher-risk geographic locations.

[271] A list of HIDTAs is available at www.whitehousedrugpolicy.gov/index.html.

Low	Moderate	High
Low turnover of key personnel or frontline personnel (e.g., customer service representatives, tellers, or other branch personnel).	Low turnover of key personnel, but frontline personnel in branches may have changed.	High turnover, especially in key personnel positions.

Appendix M: Quantity of Risk Matrix — OFAC Procedures

Examiners should use the following matrix, as appropriate, when assessing a bank's risk of encountering an OFAC issue.

Low	Moderate	High
Stable, well-known customer base in a localized environment.	Customer base changing due to branching, merger, or acquisition in the domestic market.	A large, fluctuating client base in an international environment.
Few higher-risk customers; these may include nonresident aliens, foreign individuals (including accounts with U.S. powers of attorney), and foreign commercial customers.	A moderate number of higher-risk customers.	A large number of higher-risk customers.
No overseas branches and no correspondent accounts with foreign banks.	Overseas branches or correspondent accounts with foreign banks.	Overseas branches or multiple correspondent accounts with foreign banks.
No electronic banking (e-banking) services offered, or products available are purely informational or nontransactional.	The bank offers limited e-banking products and services.	The bank offers a wide array of e-banking products and services (e.g., account transfers, e-bill payment, or accounts opened via the Internet).
Limited number of funds transfers for customers and noncustomers, limited third-party transactions, and no international funds transfers.	A moderate number of funds transfers, mostly for customers. Possibly, a few international funds transfers from personal or business accounts.	A high number of customer and noncustomer funds transfers, including international funds transfers.
No other types of international transactions, such as trade finance, cross-border ACH, and management of sovereign debt.	Limited other types of international transactions.	A high number of other types of international transactions.

Low	Moderate	High
No history of OFAC actions. No evidence of apparent violation or circumstances that might lead to a violation.	A small number of recent actions (e.g., actions within the last five years) by OFAC, including notice letters, or civil money penalties, with evidence that the bank addressed the issues and is not at risk of similar violations in the future.	Multiple recent actions by OFAC, where the bank has not addressed the issues, thus leading to an increased risk of the bank undertaking similar violations in the future.

Section 3: BSA/AML Risk Assessment Overview

Introduction

The two matrices reproduced above address various risk areas for four key factors: geography, customers and entities, products, and services. The OFAC risk matrix contains similar risk areas for the same factors, but targets OFAC compliance specifically. The following sections of this manual will detail suggested approaches to assess the bank's risk for each factor, including OFAC. Subsequent portions of the manual will include additional areas to be considered in the risk assessment process.

Risk Assessment Basics

In the Exam Manual's Core Overview - BSA/AML Risk Assessment – The Overview section discusses a review of the bank's BSA/AML risk assessment, as follows:

> "Evaluating the BSA/AML risk assessment should be part of scoping and planning the examination, and the inclusion of a section on risk assessment in the manual does not mean the two processes are separate. Rather, risk assessment has been given its own section to emphasize its importance in the examination process and in the bank's design of effective risk-based controls.
>
> The same risk management principles that the bank uses in traditional operational areas should be applied to assessing and managing BSA/AML risk. A well-developed risk assessment will assist in identifying the bank's BSA/AML risk profile. Understanding the risk profile enables the bank to apply appropriate risk management processes to the BSA/AML compliance program to mitigate risk. This risk assessment process enables management to better identify and mitigate gaps in the bank's controls. The risk assessment should provide a comprehensive analysis of the BSA/AML risks in a concise and organized presentation, and should be shared and communicated with all business lines across the bank, board of directors, management, and appropriate staff; as such, it is a sound practice that the risk assessment be reduced to writing.
>
> There are many effective methods and formats used in completing a BSA/AML risk assessment; therefore, examiners should not advocate a particular method or format. Bank management should decide the appropriate method or format, based on the bank's particular risk profile. Whatever format management chooses to use for its risk assessment, it should be easily understood by all appropriate parties.
>
> The development of the BSA/AML risk assessment generally involves two steps: first, identify the specific risk categories (i.e., products, services, customers, entities, transactions, and geographic locations) unique to the bank; and second, conduct a more detailed analysis of the data identified to better assess the risk within these categories. In reviewing the risk assessment during the scoping and planning process, the examiner should determine whether management has considered all products, services, customers, entities, transactions, and geographic locations, and whether management's detailed analysis within these specific risk categories was adequate. If the bank has not developed a risk assessment, this fact should be discussed with management. For the purposes of the examination, whenever the bank has not completed a risk assessment, or the risk assessment is inadequate, the examiner must complete a risk assessment based on available information.

Evaluating the Bank's BSA/AML Risk Assessment

An examiner must review the bank's BSA/AML compliance program with sufficient knowledge of the bank's BSA/AML risks in order to determine whether the BSA/AML compliance program is adequate and provides the controls necessary to mitigate risks. For example, during the examination scoping and planning process, the examiner may initially determine that the bank has a high-risk profile, but during the examination, the examiner may determine that the bank's BSA/AML compliance program adequately mitigates these risks. Alternatively, the examiner may initially determine that the bank has a low- or moderate-risk profile; however, during the examination, the examiner may determine that the bank's BSA/AML compliance program does not adequately mitigate these risks.

In evaluating the risk assessment, an examiner should not necessarily take any single indicator as determinative of the existence of a lower or higher BSA/AML risk. The assessment of risk factors is bank-specific, and a conclusion regarding the risk profile should be based on a consideration of all pertinent information. Banks may determine that some factors should be weighed more heavily than others. For example, the number of funds transfers is certainly one factor to be considered in assessing risk; however, in order to effectively identify and weigh the risks, the examiner should look at other factors associated with those funds transfers, such as whether they are international or domestic, the dollar amounts involved, and the nature of the customer relationships.

Identification of Specific Risk Categories

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

The expanded sections in this manual provide guidance and discussions on specific lines of business, products, and customers that may present unique challenges and exposures for which banks may need to institute appropriate policies, procedures, and processes. Absent appropriate controls, these lines of business, products, or customers could elevate aggregate BSA/AML risks. The examiner should expect the bank's ongoing risk assessment process to address the varying degrees of risk associated with its products, services, customers, entities, and geographic locations, as applicable.

Analysis of Specific Risk Categories

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

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

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

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

Assigning Responsibility for Performing the Risk Assessment

Determining the person or persons responsible for performing the BSA/AML risk assessment is a management decision. However, it seems logical that the BSA/AML compliance officer, at a minimum, coordinate this effort. This individual should possess the greatest regulatory and operational knowledge of the bank's BSA/AML program and risks. For consistency, this person will be referred to as the "reviewer" throughout this manual.

A team approach is also a likely option, such as a BSA/AML committee. The committee should include staff members directly responsible for BSA/AML functions as they relate to a representative cross-section of the bank's business lines. Using a well-organized BSA/AML team affords greater access to various views for the BSA/AML regulatory requirements. This approach will also allow for a more in-depth analysis of the various risk areas.

Since the bank's BSA/AML risk assessment must be included in the bank's BSA/AML independent review scope, it is not advisable to include a representative from the audit department when assessing the bank's risks. It is this person's responsibility to opine on the effectiveness of the risk assessment itself. Inclusion in the assessment development process removes the independency component.

Relationship to Policies and Procedures

The risk assessment process should generally not consider the procedures or controls in place to mitigate the risks. The risk assessment will outline what the risks are and provide management with relative information on the magnitude of such risks to allow for the development of appropriate policies, procedures, and processes. The bank's adopted BSA/AML policy and procedures should be commensurate with its identified risks. In essence, this means that a thorough evaluation of the bank's policies and procedures be performed following the risk assessment to assure that all identified risks, especially those that are "high," are adequately addressed within the bank's policies and procedures.

Summarizing Your Risk Assessment

Using and analyzing the data you have obtained is the second phase in the risk assessment. Not only will your risk assessment be evaluated, but the analysis process used to reach a risk conclusion will be assessed. Controls that are in place, management's ability and willingness to identify and mitigate risk will be evaluated. A bank need not necessarily consider itself at higher risk because of a large volume of wire transfers if the analysis of the information proves the majority of the transfers were recurring and took place for well-established customers and that transfers, in fact, are only conducted for existing customers. Compare that same volume of funds transfers for non-customers or nonrecurring customers, many transfers being destined for higher risk geographic areas, and the risk analysis outcome will be vastly different.

At the conclusion of completing the risk profile for your institution, the results must be reviewed and analyzed to determine whether the existing policies and procedures remain adequate. In addition, the risk profile should be summarized to inform both management and the board of directors of the bank's overall BSA/AML risks.

In general, it is recommended that the data you have obtained through the risk profile be summarized into a narrative document that briefly discusses each risk factor. The summary document should be written not only from a perspective where risks are evident but it should also highlight areas of the bank's operations that are not as prone to risks. Those conducting a risk assessment may not consider for inclusion factors that are not applicable to the bank. Excluding what does not apply may give the appearance that the issues were not taken into consideration. For example, if your institution is not located within or near an HIDTA, the risk profile summary should make note of this fact. In proving the validity of a self-assessed lower risk rating to a higher risk area such as funds transfers, the institution could include the fact that the that wires are conducted for customers only, the majority of wires are for long established customers, any monitoring processes in place, and that all names associated with a wire are compared to the current OFAC list as well as the country and bank when conducting an international transfer.

Updating the Risk Assessment

Any risk profile is not static and should be considered a "living" document, which will change over time as a result of changes to an institution's customer or product base, expansion through mergers or acquisitions, or geographical influences. It is recommended that a bank perform a risk assessment at least every 12 to 18 months, or as specific factors arise.

Consolidated BSA/AML Compliance Risk Assessment

As stated in the *Exam Manual*, "Banks that implement a consolidated or partially consolidated BSA/AML compliance program should assess risk both individually within business lines and across all activities and legal entities. Aggregating BSA/AML risks on a consolidated basis for larger or more complex organizations may enable an organization to better identify risks and risk exposures within and across specific lines of business or product categories. Consolidated information also assists senior management and the board of directors in understanding and appropriately mitigating risks across the organization. To avoid having an outdated understanding of the BSA/AML risk exposures, the banking organization should continually reassess its BSA/AML risks and communicate with business units, functions, and legal entities. The identification of a BSA/AML risk or deficiency in one area of business may indicate concerns elsewhere in the organization, which management should identify and control."

Section 4: Risk Assessment Factors – An Overview

As discussed above, there are four key factors that a bank must assess as part of its BSA/AML risk assessment. These include:

- Geographic locations
- Customers and entities
- Products
- Services

Geographic Locations

When assessing the geographic location factor, institutions should consider risk associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations. Higher-risk geographic locations can be either "international" or "domestic." While some institutions may not have any presence internationally, these higher-risk areas should be considered for operations such as wire transfers (i.e., originators and beneficiaries). The exam manual provides banks and examiners with a listing of identified international and domestic higher-risk geographies. These are covered in the next section.

Customers and Entities

Certain customers and entities may pose special money laundering risks, depending on the nature of their business, occupation, or anticipated account activity. As a result, institutions must not treat all members of a specific category of customer as posing the same level of risk. Multiple factors, such as services sought, source of funds, and geographic location, should be considered when assessing a particular customer's risks. The exam manual includes a listing of the inherently higher risk types of customers. These are covered in Section 6.

Products and Services

While not all products or services present the same level of risk, there are some that may pose a higher risk of money laundering or terrorist financing. A sample listing of potentially higher risk products or services is included in the exam manual and will be covered in Section 7.

Other Risk Factors

In addition to the four assessment factors and the OFAC risk assessment factors expected by examiners, banks should also focus on some operational areas. This portion of the risk assessment will likely vary from bank to bank, but should consider, at a minimum, the following:

- Characteristics of the bank's profile, such as asset size, market area, etc.
- Available BSA/AML resources of the bank, such as information technology systems, etc.
- Operational concerns, such as recordkeeping and reporting compliance

Discussion of these factors will be covered in Section 8.

Section 5: Geography Risk Profile

Introduction

The geography portion of the risk assessment will focus on a number of factors and is likely the most time consuming part of the assessment. The geography risk assessment must consider the following, as applicable:

- Locations of the bank's facilities, including foreign branches
- Locations of the bank's customers
- Geographic locations of transactions processed through the bank, such as:
  - Wire transfer originations
  - Wire transfer destinations

Higher-Risk Geographic Locations

The exam manual provides banks and examiners with a detailed listing of both international and domestic higher-risk geographies. Both are identified below. It should be noted that the Web site references may change from time to time and the current exam manual should be referenced to assure the use of the most current site or resource.

For some banks, there will be little risk related to international geographies and, depending on the location of the bank and its customers, possibly little or no risk for domestic geographies. The risk assessment will need to identify the existence of any risks associated with both the international and domestic higher-risk locations.

International Higher-Risk Geographic Locations

The following are the higher-risk international geographies, as identified in the exam manual. We will examine each of the lists in greater detail later.

- Countries subject to OFAC sanctions, including state sponsors of terrorism.
- Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State.
- Jurisdictions determined to be "of primary money laundering concern" by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the USA PATRIOT Act.
- Jurisdictions or countries monitored for deficiencies in their regimes to combat money laundering and terrorist financing by international entities such as the Financial Action Task Force (FATF).
- Major money laundering countries and jurisdictions identified in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR), in particular, countries which are identified as jurisdictions of primary concern.
- Offshore financial centers (OFC).

- Other countries identified by the bank as higher-risk because of its prior experiences or other factors (e.g., legal considerations, or allegations of official corruption).

Domestic Higher-Risk Geographic Locations

- High Intensity Drug Trafficking Areas (HIDTA).
- High Intensity Financial Crime Areas (HIFCA).

Geography Assessment Objective

The objective of the geography portion of the risk assessment process is to identify those bank locations, customer locations, and transaction locations that are affected by regulator and bank-identified higher-risk geographies. Whether assessing the risk of bank locations, customer locations, or transaction locations, the same international and domestic geographic resources will be used.

Bank Locations

The first step in performing a geography risk assessment is to determine whether any of the bank's locations are located in or near higher-risk geographies. For domestic banks, this process becomes rather simple. The bank need only consult the domestic higher-risk geography resources provided earlier. A good starting point for the domestic geography analysis is to access the bank's Community Reinvestment Act (CRA) assessment area delineation (or map). This map identifies the bank's lending market area, which usually conforms to its general market area. While the CRA assessment delineation/map is required to identify those census tracts that comprise the bank's CRA assessment area, it often also identifies those towns, cities, and counties that make up the same area. The higher-risk domestic geographies typically identify such areas using cities and counties. Having this information will assist in the domestic higher-risk analysis.

HIDTA Analysis

Using the HIDTA Web site above, the bank can access the current listing of those parts of the country that have been identified as High Intensity Drug Trafficking Areas. A current map of those areas follows.

As taken directly from the HIDTA Web site, the program overview for HIDTA is described as follows:

The Anti-Drug Abuse Act of 1988 and the ONDCP Reauthorization Act of 1998 authorized the Director of The Office of National Drug Control Policy (ONDCP) to designate areas within the United States, which exhibit serious drug trafficking problems and harmfully impact other areas of the country as High Intensity Drug Trafficking Areas (HIDTA). The HIDTA Program provides additional federal resources to those areas to help eliminate or reduce drug trafficking and its harmful consequences. Law enforcement organizations within HIDTAs assess drug trafficking problems and design specific initiatives to reduce or eliminate the production, manufacture, transportation, distribution, and chronic use of illegal drugs and money laundering.

When designating a new HIDTA, the Director of ONDCP consults with the Attorney General, Secretary of the Treasury, heads of national drug control agencies and the appropriate governors, and considers the following statutory criteria:

- The extent to which the area is a center of illegal drug production, manufacturing, importation, or distribution;

- The extent to which state and local law enforcement agencies have committed resources to respond to the drug trafficking problem in the area, thereby indicating a determination to respond aggressively to the problem;
- The extent to which drug-related activities in the area are having a harmful impact in other areas of the country; and
- The extent to which a significant increase in the allocation of federal resources is necessary to respond adequately to drug-related activities in the area.

The HIDTA Program helps improve the effectiveness and efficiency of drug control efforts by facilitating cooperation between drug control organizations through resource and information sharing, collocating and implementing joint initiatives. HIDTA funds help federal, state and local law enforcement organizations invest in infrastructure and joint initiatives to confront drug- trafficking organizations. Funds are also used for demand reduction and drug treatment initiatives. The key priorities of the Program are:

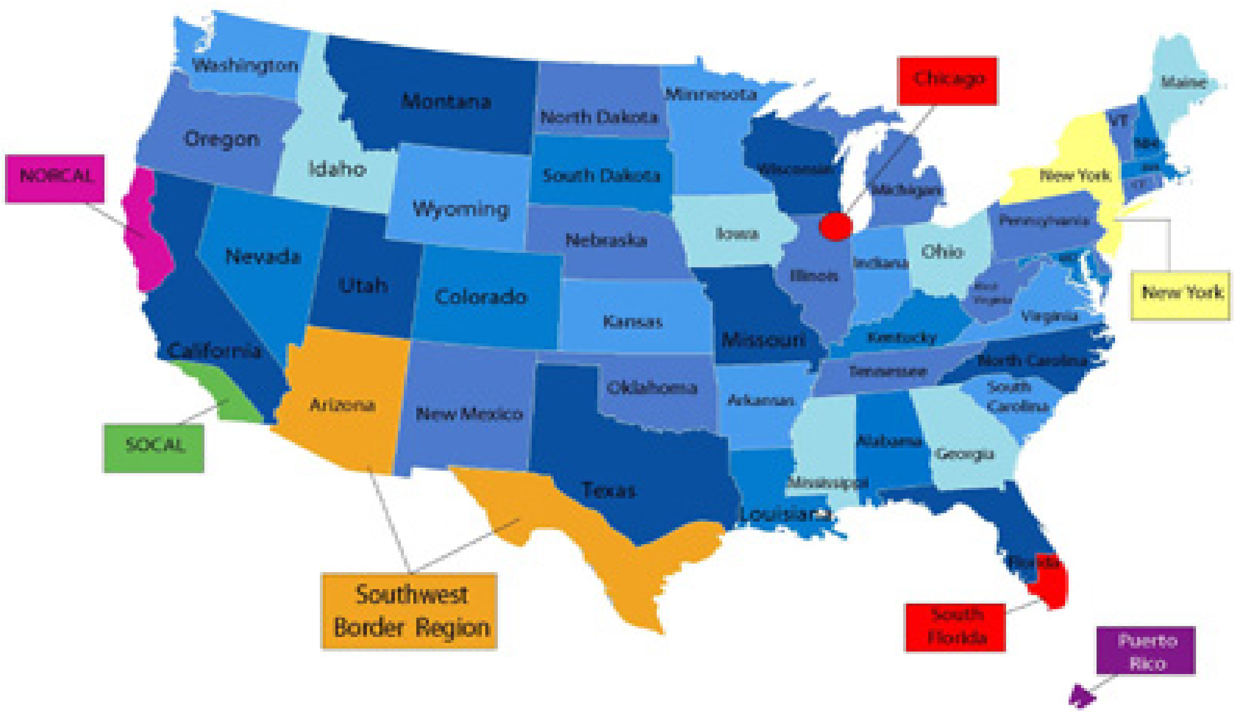
- Assess regional drug threats;
- Design strategies to focus efforts that combat drug trafficking threats;
- Develop and fund initiatives to implement strategies;
- Facilitate coordination between federal, state and local efforts to improve the effectiveness and efficiency of drug control efforts to reduce or eliminate the harmful impact of drug trafficking.

The analysis should involve the collection of all of the bank's physical domestic locations and compare them to those areas identified as HIDTAs. For example, a bank located in Indiana should consult the HIDTA Web site to determine if any of its bank locations are located in or near the Chicago identified HIDTA. Specifically, the Chicago HIDTA includes the counties of Cook, Grundy, Kendall, and Will. Banks with locations in surrounding counties will need to assess the overall impact of the HIDTA on its operations and customers served.

The appendix to this manual offers more information regarding the national situation.

HIFCA Analysis

Using the HIFCA Web site above, the bank can access the current listing of those parts of the country that have been identified as High Intensity Financial Crime Areas. A current map of those areas appears next.



There are fewer HIFCAs throughout the country than HIDTAs. Similar to the HIDTAs, specific counties within broader geographic regions are considered as HIFCAs. Specifically, they include counties in each of the following areas:

- ***California Northern District.*** Monterey, Humboldt, Mendocino, Lake, Sonoma, Napa, Marlin, Contra Costa, San Francisco, San Mateo, Alameda, Santa Cruz, San Benito, Monterey, and Del Norte;
- ***California Southern District.*** Los Angeles, Orange, Riverside, San Bernardino, San Louis Obispo, Santa Barbara, and Ventura;
- ***Southwest Border.*** All counties in Arizona, and counties bordering and adjacent to those bordering Texas and the Mexico boundary;
- ***Chicago.*** Cook, McHenry, Dupage, Lake, Will, and Kane;
- ***New York.*** All counties in New York and New Jersey;
- ***Puerto Rico.*** All of Puerto Rica and the U.S. Virgin Isles; and
- ***South Florida.*** Broward, Miami-Dade, Indian River, Martin, Monroe, Okeechobee, Palm Beach, and St Lucie.

Similar to the HIDTA analysis, the analysis of the HIFCA impact should involve the collection of all of the bank's physical locations and compare them to those areas identified as HIFCAs. Using the Indiana bank example, the bank will need to determine if any of its locations are located in or around the counties of Cook, McHenry, Dupage, Lake, Will, or Kane. It should be noted that there is some overlap of HIFCAs and HIDTAs, but they are not identical from region to region.

International Higher-Risk Areas

The following identifies each of the international higher-risk geographies found within the exam manual, along with a brief description of each.

In addition to determining whether the bank has any physical presence internationally, it is recommended that the reviewer compile a listing of foreign countries for the following:

- Customer locations
- Noncustomer originators or beneficiaries of funds transfers

This list of countries should then be alphabetized to aid in the review of each of the international higher-risk resources. The resources do not appear in identical formats, but most list the countries in alphabetical order.

Countries Subject to Office of Foreign Assets Control (OFAC) Sanctions. These may be found on OFAC's Web site at http://www.treas.gov/ofac. Institutions with adequate OFAC policies and procedures should have an initial idea of whether there are any OFAC issues. All areas of the bank where records are required to document OFAC compliance should be consulted in this assessment. This equates to checking customers and persons conducting transactions at or through the bank, such as checking the names of:

- Account owners at account opening, including a periodic check of the customer database against the current listing
- Noncustomer originators or beneficiaries of funds transfers
- Noncustomer purchasers and payees of monetary instruments
- Noncustomer payees on checks drawn on the bank and presented for payment in person
- Sellers of property in related loan transactions

In most banks, there are automated systems and/or procedures in place to assure that the current OFAC list is checked before opening an account or conducting a transaction. The assessment process addressing OFAC geography risks should involve a review of any prior "hits" on the OFAC list. The reviewer should obtain a listing of all positive "hits" to assess the level of risk.

Countries Identified as Supporting International Terrorism. This listing is determined by the Secretary of State. The listing appears in the Department of State's annual report "Country Report on Terrorism," which may be found on their Web site for its Counterterrorism Office at http://www.state.gov/s/ct/.

Primary Money Laundering Concerns. These include jurisdictions determined to be "of primary money laundering concern" by the Secretary of Treasury and jurisdictions subject to special measures pursuant to Section 311 of the PATRIOT Act. The special measure final rulings may be found on FinCEN's Web site at http://www.fincen.gov. This listing can be found under the "Statutes and Regulations – USA Patriot Act" page on the Web site. The list can be viewed alphabetically or in chronological order.

Non-Cooperative Jurisdictions/Countries. This resource identifies those jurisdictions/ countries identified as non-cooperative by the Financial Action Task Force (FATF) on Money Laundering. Their Web site is http://www.fatf-gafi.org.

Major Money Laundering Countries and Jurisdictions. These are identified in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR), which may be found on the U.S Department of State's Web site at www.state.gov/p/inl/rls/nrcrpt on the Bureau of International Narcotics and Law Enforcement Affairs page.

Offshore Financial Centers (OFCs). Those identified by the U.S. Department of State. Refer to http://www.imf.org/external/ns/cs.aspx?id=55 for more information. The geographic areas appear alphabetically.

Other Countries identified by the institution as higher-risk because of their prior experiences, transaction history, or other factors.

Other Higher-Risk Areas

In addition to consulting the national and International higher-risk geography resources above, the bank should also determine if there are any other local, regional, or International areas that may be considered as higher-risk. The most logical approach would be to inquire with local law enforcement.

Bank Customers and Transactions

Using the higher-risk geography resources noted above, the reviewer will need to compare the locations of its customers to those higher-risk areas. To effectively perform this assessment, the reviewer will need to have access to data that identifies bank customers' countries or domestic geographies.

Gathering a list of foreign customers should be fairly straightforward, since the bank should have a relative idea of those customers residing outside of the country. Identifying customers located in domestic higher-risk areas can possibly be more difficult. As noted with the HIDTAs and HIFCAs, most are listed by specific counties. Cross-referencing customer zip codes or towns with county listings may assist in this analysis. In general, the bank should have a good idea of where its customers reside.

Transactions

Analyzing the risks associated with transactions conducted at or through the bank is a little easier, especially related to funds transfers. Remember that an effective BSA/AML compliance program is risk-based; therefore, performing the analysis is also risk-based. In other words, it is not feasible to review every single funds transfer that was originated or received by the bank, but using the required BSA records of funds transfers will assist with this process. To aid in this analysis, it would be ideal to track those funds transfers that were international. Then, a simple review of the affected countries can be used to compare against the international higher-risk geographies. Similarly, an analysis should be performed to compare the list of domestic higher-risk geographies to those funds transfers processed through the bank.

The examination manual suggests examiners place additional emphasis on Automated Clearing House (ACH) transactions. If the bank is involved in significant international or other transaction types through the ACH system, this should be considered in any geographic analysis of transactions.

Generally, an assessment of transaction activity over the most recent 12 months will be sufficient to identify any geography risks. This period should provide the reviewer with a representative sample of typical transactions.

Other records that should be considered in the geography risk assessment are the sales of monetary instruments for currency. Other than a review of the addresses of those non-deposit customer purchasers, the focus in this analysis should revolve around the location of where the monetary instruments are purchased. Since the bank will have already identified its domestic geography risks associated with bank facilities, this process should involve assessing the level of monetary instruments purchased in these higher risk locations.

Future Tracking

Performing the initial geography risk assessment will likely take longer the first time. Although not specifically required by the governing BSA regulations, the following are provided as suggestions to assist in future assessments:

- Identify and track foreign customers and their resident countries
- Identify and track funds transfers affecting domestic higher-risk areas, including the identification of international locations

Identified Higher-Risk Geographies

Upon the completion of the geography risk assessment portion, it is recommended that the reviewer identify and list each domestic and international higher-risk geography in the assessment work papers. As part of the review, those affected geographies should be further assessed to determine the overall risk to the bank. For example, if the bank identifies that only one international funds transfer occurred to or from a higher-risk geography during the assessment review period, the residual risk to the bank would be minimal. However, if frequent funds transfers involved one or more higher-risk areas, the risk is elevated. Another consideration in this analysis is the dollar volume of said transfers: the larger the dollar amounts, the greater the risk. Likewise, a similar analysis needs to be performed for the number of customers and level of monetary instruments sold in these geographies.

Geography Risk Levels

Using the "Quantity of Risk Matrix" (Appendix J) in the exam manual, a risk rating will need to be assigned to the bank's overall geographic risk. The risk factors related to geographic factors appear below.

Low	Moderate	High
The bank is not located in a HIDTA or HIFCA. No funds transfers or account relationships involve HIDTAs or HIFCAs.	The bank is located in an HIDTA or an HIFCA. Bank has some fund transfers or account relationships that involve HIDTAs or HIFCAs.	Bank is located in an HIDTA and an HIFCA. A large number of fund transfers or account relationships involve HIDTAs or HIFCAs.
No transactions with higher-risk geographic locations.	Minimal transactions with higher-risk geographic locations.	Significant volume of transactions with higher-risk geographic locations.

Final Rating

An overall geography risk assessment rating should be assigned to the bank. This rating level should encompass each of the above geography risk factors and apply appropriate weight to each in arriving at the overall rating. A supporting narrative statement should also accompany the overall geography risk rating.

Case Study: Consider Your Bank's Geographic Risk Assessment

Answer the following questions:

1. What is the geographic risk level for your institution?

2. Are you comfortable with the comprehensiveness and completeness of your current geographic risk analysis?

3. What geographic areas do you not have in your geographic analysis that you should have due to the location of your customer base?

4. Does anything in your answer to question 3 change your risk levels? If not, at what point will you need to consider changes to your geographic risk profile?

5. Are there any other additional items that must be considered regarding your bank's geographic risk assessment?

Section 6: Customers and Entities Risk Profile

Introduction

The next step in this process involves a risk assessment of the bank's customers and entities. Fortunately, the regulators have provided banks with a detailed listing of the various types of customers or entities that they consider as possessing a higher degree of risk.

To effectively gauge the bank's overall customer risk, knowledge of each customer's profile is required. For business customers, this will require knowledge of the type of business in which they are engaged, as well as other factors. In general, consumer retail customers typically pose little risk to banks.

Higher-Risk Customer Types

The exam manual provides guidance on higher-risk customer types:

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

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

Impact to the Bank

Identifying those specific customers that pose risk to the bank is essential before effectively assessing the overall customer base risk. This requires the bank to develop and implement a risk-based CDD program, which defines various customer risk levels and assigns risk ratings to its customers. A later portion of the school's manual will address the principals relating to developing and implementing a customer due diligence (CDD) program.

Identified Higher-Risk Customers and Entities

Once the customer base has been risk rated, the BSA/AML customer risk assessment portion can be finalized. The following should be considered as part of this process and reflected within the risk assessment document.

Description of Customer Base

To assist in assigning an overall customer risk rating for the bank, it is suggested that queries be run to list those customers that fall within the various customer types. Whether the bank identifies and tracks customers by type or its instituted risk rating level, the results will allow for a broad overview of the higher risk types. For example, using the regulator-defined higher-risk customer type guidance, an identification of the number of each type should be summarized. In addition, a separate analysis of each customer type group should be performed to conclude the potential impact to the bank's BSA/AML compliance program. The following table may assist in summarizing this information.

High-Risk Category	Number of Customers	Percent to total Customers	Comments
List each type of higher-risk customer group on a separate line	Total the number of customers within each group	Divide the number of customers within each group by the total number of customers	Include any potential factors that affect each particular group. For example, discussion of the level of transactions by number or dollar amount, etc.

Links to Other Risk Factors

As the customer risk levels are evaluated, it is important to note that the reviewer must also consider the impact of the other risk factors to the bank's customer base. For example, as higher-risk customers are reviewed, consideration should be made regarding the use of the bank's higher-risk products/services and the locations of these customers. If an otherwise lower risk customer that engages in a higher-risk business also primarily uses the bank's higher-risk products and operates in a higher-risk geography, the resulting risk for the customer should be elevated.

Customers and Entities Risk Levels

Using the "Quantity of Risk Matrix" (Appendix J) in the exam manual, a risk rating will need to be assigned to the bank's overall customers and entities risk. The risk factors related to customer factors are as follows:

Low	Moderate	High
Identified a few higher-risk customers or businesses	Identified a moderate number of higher-risk customer and businesses.	Identified a large number of higher-risk customer and businesses.
Stable, known customer base	Customer base increasing due to branching, merger, or acquisition.	A large and growing customer base in a wide and diverse geographic area.

Finally, an overall customer risk assessment rating should be assigned to the bank. This rating level should encompass each of the above customer risk factors and apply appropriate weight to each in arriving at the overall rating. A supporting narrative statement should also accompany the overall customer risk rating.

Case Study: Consider Your Bank's Customer / Entity Risk Assessment

Answer the following questions:

1. What is the customer / entity risk level for your institution?

2. Are you comfortable with the comprehensiveness and completeness of your current customer / entity risk analysis?

3. What customers / entities do you not have in your customer / entity analysis that you should have included in the analysis of your customer / entity base?

4. Does anything in your answer to question 3 change your risk levels? If not, at what point will you need to consider changes to your customer / entity risk profile?

5. Are there any other additional items that must be considered regarding your bank's customer / entity risk assessment?

Section 7: Products and Services Risk Profile

Introduction

To complete the overall risk assessment, an assessment of the bank's products and services must be performed. Again, the regulators have provided banks with a detailed listing of the various types of products and services that they consider as possessing a higher degree of risk.

The assessment of products and services is less subjective than that of customers or entities. In general, the degree of risk should not vary within a product line. However, specific products within a general product group (i.e., checking accounts) will vary in their level of risk. In addition, the intended user of a product or service can have an effect on the inherent risk of a particular product or service.

Higher-Risk Products and Services

Similar to customers, product characteristics will vary from one another. These variations result in varying risk levels. A product that offers significant customer anonymity will inherently possess a greater amount of risk than one that requires the customer to be present at the bank to conduct a transaction.

Account opening methods will also impact risk. Internet banking has become more mainstream in recent years, and as more banks allow new customers to open accounts without visiting a branch facility, the associated risk for those customers will increase.

The exam manual includes the following relating to the inherent types of higher risk products or services:

Certain products and services offered by banks may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Some of these products and services are listed below, but the list is not all inclusive:

- Electronic funds payment services - electronic cash (e.g., prepaid and payroll cards), funds transfers (domestic and international), payable upon proper identification (PUPID) transactions, third-party payment processors, remittance activity, automated clearing house (ACH) transactions, and automated teller machines (ATM).
- Electronic banking.
- Private banking (domestic and international).
- Trust and asset management services.
- Monetary instruments.
- Foreign correspondent accounts (e.g., bulk shipments of currency, pouch activity, payable through accounts (PTA), and U.S. dollar drafts).
- Trade finance.
- Services provided to third-party payment processors or senders.
- Foreign exchange.

- Special use or concentration accounts.
- Lending activities, particularly loans secured by cash collateral and marketable securities.
- Nondeposit account services (e.g., nondeposit investment products and insurance).

The expanded sections of the manual provide guidance and discussion on specific products and services detailed above.

Impact to the Bank

Identifying the level of risk associated with a bank's products or services is essential to completing a thorough BSA/AML risk assessment. Many banks might not offer all of the products or services mentioned above. However, it is likely that at least three are a staple in every banking organization. These would include funds transfers, monetary instruments, and extensions of credit secured by cash collateral or deposit accounts. Whether a bank offers a few, some, or all of the higher-risk products or services, each type offered requires an assessment to determine the level of risk to the bank.

The approach to determining the risk level should consider a number of factors, which range from who will use the product or service to how it can be accessed. The following briefly discusses a suggested assessment approach for products and services.

Identify Product or Service Parameters

First, the bank must identify the parameters related to each product or service. In essence, this means identifying their characteristics. Some common elements might include:

- Access method(s)
- Range of use
- Portability
- Speed of transaction(s)
- Currency involvement

Access Method(s)

The method by which a person or entity can access a particular product or service has a significant impact on the risk level. Accessing products or services directly from the bank at a branch facility carries less risk than access by other means. Allowing access via the Internet or through a bank agent or authorized representative will increase the inherent risk. Additionally, offering the ability to become a new customer to the bank via the Internet restricts the bank from following otherwise good internal controls.

For example, relying on identity verification obtained electronically or through the mail reduces the bank's ability to make a positive verification of the customer's identity. The ID provided may be legitimate but might not match the actual person requesting the account. There is no replacement for a visual observation of the new customer, along with verifying the photo provided from the identification provided at account opening.

Other related factors associated with access methods include how a person or entity can obtain services, such as monetary instruments or executing funds transfers. Requiring a customer or individual to be present at the institution to obtain a particular service offers the opportunity to again verify his/her true identity. However, Internet banking is a unique and attractive service to many customers. The ability to conduct transactions in the comfort of their own home, office, or while traveling allows customers to more easily meet personal financial obligations.

There are many variations within Internet banking services. When assessing the risks associated with these services, the bank must identify the varying levels of transaction ability, as well as the tools or reports available to the bank to monitor customer activity. A bank Internet service that only permits account inquiry with no transaction ability, or only inter-bank transactions to or from the same customer's accounts, carries less risk than a service that permits bill payment. An increase in the level of transaction types offered will require an increased ability to monitor for suspicious activity, the review of which is part of the overall risk assessment process.

One positive aspect of Internet banking is the current inability to conduct transactions involving currency. However, special monitoring should be conducted on customers who conduct deposit transactions via an automated teller machine (ATM) or through the mail, and then uses the Internet service to initiate debit transactions. This concept holds true for any type of account or service.

Range of Use

This concept relates to the customer's ability to conduct transactions outside of the bank's market area and/or U.S. borders. One common service that permits such transactions is a funds transfer. International funds transfers, in particular, offer the ability to immediately send funds abroad. As noted in the geography risk assessment section, there are a number of domestic and international higher-risk locations that can elevate BSA/AML concerns, including the locations involved in ACH transactions.

The lack of or limited number of international funds transfers does not eliminate a bank's funds transfer service risk. There are numerous domestic higher-risk geographies located throughout the country. Banks need to be cognizant of these locations and the level of funds transfers that are sent to or from these areas.

When assessing the funds transfer risk, banks must have the ability to readily identify the origination or destination city name and compare this information to the higher-risk geographies. The ability to generate such data electronically will assist in this process, so maintaining an electronic file on funds transfers, which includes such information, will reduce review time. The general rule of thumb when considering range of use is the further away a transaction can take place, the more likely risk will increase.

Portability

The regulators have noted that the use of stored value cards is rapidly increasing. The risks associated with these services carry a higher degree of risk. Imagine the success rate of transporting a substantial sum of currency across U.S. borders as compared to sending or carrying a stored value card or cards with comparable amounts. It is much easier to transport a stored value card than a suitcase full of cash. Concerns related to portability begin with who can obtain these services, and in what methods.

Generally, a person must be present at the bank to purchase a stored value card. However, the ability for noncustomers to purchase such services will pose greater risk to the bank. For banks that offer these services to noncustomers, it will be imperative to identify this risk, and then to enhance identity verification procedures based on that risk, since there is no customer relationship to rely upon. Simply increasing fee levels to obtain these services for noncustomers might not be a large enough deterrent to money launderers. To them, it might just be seen as a small cost of doing business.

Speed of Transactions

There is no argument that funds transfers present the best opportunity to conduct a large financial transaction in a rapid manner. Currently, it is the quickest method to send funds across town or beyond U.S. borders. When assessing a bank's products or services, the speed of transactions must be considered.

Currency Involvement

Currently, there are three primary means by which a person or entity can deposit currency into a bank account to purchase services. They include visiting a branch, an ATM, or sending funds through the mail. Transactions conducted at a branch location offers staff the opportunity to make visual confirmation of the person's identity, as well as record certain transaction information. ATM transactions somewhat limit these opportunities and usually only permit deposits or withdrawals to or from an account. Bank-by-mail services inherently increase risk, especially if deposits are routinely made with currency.

One key service that is affected by the use of currency is the purchase of monetary instruments. Purchasing monetary instruments is a common method used by money launderers to place, layer, and integrate illicit funds. Even though banks are faced with the requirement to collect and record certain transaction information involving such purchases involving currency in the amounts of $3,000 to $10,000, inclusive, individuals attempting to launder money are well aware of the rules and often find ways to circumvent these records. It is common for such individuals to conduct numerous purchases involving currency under the $3,000 threshold. Banks offering the purchase of monetary instruments, especially to noncustomers, will need to adequately identify the risk, and then to institute appropriate internal controls to monitor frequent and/or unusual purchases.

Identify Users

Once the various parameters associated with products or services have been assessed, the next step involves an assessment on the types of customers that obtain these and how the bank identifies the individuals. Many of the risks associated with the user of products or services were discussed above and revolve around whether the person is a customer of the bank.

Obviously, to obtain an account, an individual will become a customer. Therefore, the bank's CIP and CDD procedures will assist in verifying the customer's identity and fulfill due diligence expectations. Use of certain products or services, however, might be made available to noncustomers. It is under these circumstances that the bank will need to assess its risk. As products or services are assessed, a number of factors should be considered as related to user identity:

- Dollar limitations
- Ability to reload stored value cards
- Verifying identity
- Purpose of use or purchase

Identify Method(s) to Open or Obtain

The last aspect of assessing products or services relates to how they may be opened or obtained. Special consideration in the risk analysis needs to be made on those products or services that may be opened or obtained outside of the bank's physical locations; in essence, the greater the distance, the greater the risk.

A related issue involves those customers who reside or operate businesses outside of the bank's market area. While this concept is covered in the customer risk assessment section, there is some overlap to the product or services risk assessment. For example, does the bank offer a particular product that targets individuals or businesses that are outside of the bank's market area, such as foreign correspondent financial institution accounts?

Identified Higher-Risk Products and Services

Once the product or services risk analysis is complete, the reviewer must then compile a listing of those designated by the bank as higher-risk. The table below can assist the reviewer in identifying these products or services.

Description of Products and Services

To assist the reader in making his/her own assessment, it is advisable to briefly identify the various types of products or services offered by the bank, including those that are higher-risk. The following table can be used to list those designated as higher-risk, using the suggestions made within the exam manual.

When identifying all of the bank's products or services, it is not necessary to specifically list each product or service name, but a general description of the various categories should be discussed. In addition, the risk assessment summary should discuss the options available to obtain products or services.

Higher-Risk Category	Number of Customers Using Higher-Risk Product/Service	Overall Significance of the Product/Service to the Bank	Comments
List each type of higher-risk product or service on a separate line	Total the number of customers within each group using these services	Rate the significance of this product or service to the bank's offerings. Consider number of accounts, number of transactions, and transaction dollar levels in the analysis. Rate each using "Highly significant," "Significant," "Moderate," and "Nominal"	Include any potential factors that affect each particular product or service. For example, discussion of the level of open accounts by number as compared to lower risk products or services of similar type.

Links to Other Risk Factors

As noted throughout this section, the risk assessment process should consider any links of products and services to other risk factors.

Products and Services Risk Levels

Using the "Quantity of Risk Matrix" (Appendix J) in the exam manual, a risk rating will need to be assigned to the bank's overall products and services risk. The risk factors related to these factors appear below.

Low	Moderate	High
No foreign correspondent financial institution accounts. The bank does not engage in pouch activities, offer special use accounts, offer payable through accounts (PTAs), or provide U.S. dollar draft services.	The bank has a few foreign correspondent financial institution accounts, but typically with financial institutions with adequate AML policies and procedures from low-risk countries, and minimal pouch activities, special-use accounts, PTAs, or U.S. dollar draft services.	The bank maintains a large number of foreign correspondent financial institution accounts with inadequate AML policies and procedures, particularly located in higher-risk jurisdictions, or offers substantial pouch activities, special-use accounts, PTAs, or U.S. dollar draft services.

Low	Moderate	High
No electronic banking (e-banking) or the Web site is informational / non-transactional.	The bank is beginning e-banking and offers limited products and services.	The bank offers a wide array of e-banking products and services (i.e., account transfers, e-bill payment or accounts opened via the Internet for retail customers; or funds transfers, electronic cash management, third-party payment processing, and ACH origination for corporate customers).
A limited number of funds transfers for customers, noncustomers, limited third-party transactions, and no foreign funds transfers.	A moderate number of funds transfers. A few international funds transfers from personal or business accounts with typically low-risk countries.	A large number of noncustomer funds transactions and payable upon proper identification (PUPID) activity. Frequent funds from personal or business accounts to or from higher-risk jurisdictions, and financial secrecy havens or jurisdictions.
The bank offers limited or no private banking services or trust and asset management products or services.	The bank offers limited domestic private banking services or trust and asset management products or services over which the bank has investment discretion. Strategic plan may be to increase trust business.	The bank offers significant domestic and international private banking services or trust and asset management products or services. Private banking or trust and asset management services are growing. Products offered include investment management services, and trust accounts are predominantly non-discretionary versus where the bank has full investment discretion.
Few international accounts or very low volume of currency activity in the accounts.	Moderate level of international accounts with unexplained currency activity.	Large number of international accounts with unexplained currency activity.

In addition, the following two factors do not appear in the exam manual matrix, but are worthy of consideration.

Low	Moderate	High
The bank has policies and procedures to limit sales of monetary instruments to only bank customers.	The bank will occasionally sell monetary instruments to non-deposit customers or routinely sell to non-deposit customers, and has implemented appropriate controls to sufficiently verify the purchaser's identity.	The bank routinely sells monetary instruments to non-deposit customers without extensive controls to verify the purchaser's identity.
The bank offers no or limited non-deposit products with appropriate controls to verify the account owner's identity and monitor account activity.	The bank offers non-deposit products with appropriate controls to verify the account owner's identity and monitor account activity.	The bank offers a wide variety of non-deposit products without appropriate procedures to verify the account owner's identity or monitor account activity.

Finally, an overall products and services risk assessment rating should be assigned to the bank. This rating level should encompass each of the above risk factors and apply appropriate weight to each in arriving at the overall rating. A supporting narrative statement should also accompany the overall products and services risk rating.

Consider Your Bank: Products / Services Risk Assessment

1. Consider your products, and place them in one of the following categories:

   Low Risk

   Moderate Risk

   High Risk

2. Consider your low risk product group. State all methods for a customer to move funds in and out of this account group.

3. Do the methods change your opinion of the risk level for this group of products?

4. Consider your moderate risk product group. State all methods for a customer to move funds in and out of this account group.

5. Do the methods change your opinion of the risk level for this group of products?

6. Consider your high risk product group. State all methods for a customer to move funds in and out of this account group.

7. Do the methods change your opinion of the risk level for this group of products?

Section 8: Other Risk Factors

Introduction

While this section appears last in the listing of BSA exam manual suggested risk assessment factors, it might be the logical first step in the process. The FFIEC's risk matrices contain few risk factors associated with the topics below, but the areas discussed provide a base for the reviewer to proceed with the risk assessment. The items discussed below focus more on the bank's overall profile, such as asset size, market base, staffing, and BSA systems, among others.

Bank Profile

This portion of the assessment should focus on the bank's general profile as of a certain date. While many factors could be considered, the following are the minimum suggestions:

- ***Asset Size.*** This can be obtained either internally from the bank's Chief Financial Officer (CFO) or from the bank's most recently filed quarterly Call Report. In general, asset size is not indicative of a bank's BSA/AML risks but can be somewhat related; in theory, the larger a bank's assets, the greater the inherent risk. This conclusion is drawn from the likelihood that larger banks offer a broader variety of products or services and generally have a greater number of customers, of which some might be considered as higher-risk.
- ***Number of Employees.*** This factor relates to the need to provide training and oversight to the bank's employees regarding the bank's BSA/AML compliance program. Banks with a large number of employees will face greater risks to assure compliance with the BSA/AML regulations.
- ***Staffing Turnover.*** Related to the item above, the level of staffing turnover can affect the bank's BSA/AML compliance, especially when the turnover is high for "key" BSA/AML staff, such as the BSA/AML compliance officer, BSA/AML support staff, tellers, and the auditor. This factor is included in Appendix J of the exam manual.
- ***BSA/AML Staffing Resources.*** Another consideration in the bank's overall BSA/AML profile should be the human resources dedicated to the compliance program. This part of the assessment should identify all of those key personnel involved in the day-to-day management of the bank's BSA/AML compliance program. As applicable, attention should be focused on the amount and level of training afforded to these individuals, as well as whether any retain BSA/AML-related and/or compliance-related industry certifications.
- ***BSA/AML Information Technology Resources.*** Computers and software programs have advanced banks' ability to identify and monitor suspicious activity. The evolution of CIP has also brought to bankers valuable technological resources to assist in verifying the identity of customers. While not all-inclusive, the following computer resources might be useful to a bank:
  - Suspicious activity monitoring reports (special report queries that identify transaction activity that could be suspicious)
  - Customer verification programs (systems that provide for positive, negative, or logical verification of a person's identity)
  - Data aggregation reports (reports that aggregate predefined currency transactions, such as aggregate daily cash activity by taxpayer ID number over a set amount)

- CTR generation programs (programs that prompt staff and guide them through the completion of a CTR form)
- OFAC checks (programs that allow for instantaneous checks of new and/or existing customers against the OFAC listing)

This portion of the risk assessment should focus on those technology resources available to the bank, which assists with the management of the BSA/AML compliance program. Such information may prove especially useful for banks that are approaching a need for these resources, as evidenced by the facts presented within the risk assessment.

Other Factors Risk Levels

Using the "Quantity of Risk Matrix" (Appendix J) in the exam manual, a risk rating will need to be assigned to the bank's overall operational risk. The risk factors related to these factors appear below.

Low	Moderate	High
Low turnover of key personnel or frontline personnel (i.e., customer service representatives, tellers, or other branch personnel).	Low turnover of key personnel, but frontline personnel in branches may have changed.	High turnover, especially in key personnel positions.
On the basis of the filed reports, there are few or no large currency or structured transactions.	On the basis of the filed reports, there is a moderate volume of large currency or structured transactions.	On the basis of the filed reports, there is a significant volume of large currency or structured transactions.

In addition, the following risk factors do not appear in the exam manual but are suggested as part of the bank's overall BSA/AML risk assessment, as it relates to general operations, resources, reporting, and recordkeeping.

Low	Moderate	High
Based on the most recent internal BSA review and/or external BSA examination, the bank's policies and procedures evidence compliance with the regulation's recordkeeping requirements with no or few deficiencies.	Based on the most recent internal BSA review and/or external BSA examination, the bank's policies and procedures evidence deficiencies with the regulation's recordkeeping requirements.	Based on the most recent internal BSA review and/or external BSA examination, numerous recordkeeping deficiencies were noted.

Low	Moderate	High
The bank has adopted excellent policies and procedures to identify, report, and monitor suspicious activity.	The bank has implemented adequate policies and procedures to identify, report, and monitor suspicious activity; however, recent internal BSA reviews and/or external BSA examinations have identified instances where suspicious activity was not identified or reported.	The bank has failed to implement adequate procedures to identify, report and monitor suspicious activity.
Few funds transfers are performed and limited to only bank customers.	A moderate number of funds transfers are performed for bank customers and/or few to moderate funds transfers are performed for noncustomers.	A significant number of funds transfers are performed.
Sales of monetary instruments for currency are made usually involving only deposit customers.	A moderate number of monetary instruments are sold for currency to deposit customers and/or to noncustomers.	A significant volume of monetary instruments are sold for currency to noncustomers.
Few loans are originated which are secured by cash collateral.	A moderate number of loans are originated which are secured by cash collateral.	A significant number of loans are originated which are secured by cash collateral.

Finally, an overall bank profile risk assessment rating should be assigned to the bank. This rating level should encompass the above risk factors. A supporting narrative statement should also accompany the overall bank profile risk rating.

Consider Your Bank: Other Risk Assessment Issues

Consider the issues discussed above, and comment on your bank's position on these issues:

- Asset Size
- Number of Employees
- Staffing Turnover
- BSA/AML Staffing Resources
- BSA/AML Information Technology Resources

Section 9: Summarizing the Risk Assessment

Introduction

Throughout this manual, we have indicated that each risk factor (i.e., geographies, customers, etc.) will need to be summarized. It is at this point in the process that the reviewer will need to pull together each of the risk factor summaries and organize them into an overall risk profile. This overall summary document will serve two key purposes. First, it ties each separate risk factor together. Second, it will serve as the primary source document for board, senior management, and examiner review.

Tying it All Together

Numerous references have been made to consider how the various risk factors interrelate throughout this process. As a refresher, a higher-risk customer type that uses higher-risk products or services may pose a higher degree of overall risk than the same customer that simply maintains a typical operating account with little to no cash activity that is used to receive general revenues and pay expenses.

Before finalizing the overall risk assessment summary, it is important to compare the results within each risk factor category to the other risk factors. Once completed, the final summary document can be drafted.

Summary Format

There is no right or wrong way to summarize the risk profile. The reviewer must decide on whether he/she looks at the glass "half full" or "half empty." The underlying objective is to paint a truthful picture of the bank's current BSA/AML risks.

A positive approach might be elected to highlight those areas that pose little risk to the bank. While this approach might leave management feeling that all is under control, overlooking any higher-risk issues will likely have an adverse impact in the future.

A negative approach, on the other hand, focuses on too much doom and gloom, which could leave management with an overwhelming feeling of impossibility.

A hybrid approach, however, makes use of both the positive and negative approaches. The summary document should attempt to inform management and the board of those higher-risk areas that warrant attention. At the same time, the summary also needs to highlight those risk factors or controls that support the effectiveness of the bank's program. While we specifically made an attempt to exclude existing controls consideration during the risk assessment process, it is at this time that these controls need to be celebrated. However, management must be careful not to "spin" the message to a level that misleads the audience. The facts must be represented. In other words, the summary risk assessment, as well as the risk assessment analysis, needs to be approached in an honest and forthright manner.

Summary Overview

One possible suggestion, using the hybrid approach, would be to cover the following topics within the summary document in the order listed. Each one will then be briefly discussed.

- Introduction
- Bank Profile
- Geographies
- Customers and Entities
- Products and Services
- OFAC
- Other Risk Factors
- Conclusion

Introduction. The introduction section should be brief. It should describe the overall objectives of the BSA/AML risk assessment process. This section should note the "as of" date for the risk assessment, as well as indicate the anticipated recurring frequency for future assessments. Finally, this section might reference those individuals responsible for preparing and monitoring the risk assessment process.

Bank Profile. This section should attempt to paint a picture for the reader of the bank's general strategic objectives. It should also provide the reader with a quantitative measure of the bank's size, primary market area, and market niches. Additionally, this section should focus on the bank's BSA/AML staffing, physical resources, and information technology resources. These factors, in particular, should be presented in a manner to either support the effectiveness of the bank's BSA/AML compliance program or to alert management of the need to strengthen such resources. An overall risk rating should then be provided for the bank's profile.

Geographies. This section should summarize whether any of the bank's physical locations or customers are present in designated higher-risk areas. Significant presence in such geographical locations, or lack thereof, should be represented here. In addition, special mention of the level of transactions flowing through the bank originated from or delivered to higher-risk geographies should be made. If any, specific mention of the affected higher-risk geographical locations should be given. Rather than itemize all areas, the summary document should attempt to provide a global view of its higher-risk geographies and describe the controls in place to help mitigate those risks. These mitigating controls should be noted throughout the summary document for each risk factor. An overall risk rating should then be provided for the bank's geography risk.

Customers and Entities. This section should be used to generally describe the bank's customer base. In addition, the summary shall mention those higher-risk customer type groups that impact the bank's program. An overall risk rating should then be provided for the bank's customer risk.

Products and Services. This section should briefly describe the bank's products and services. Special attention should be made towards those products or services that are considered as higher-risk. An overall risk rating should then be provided for the bank's product and services risk.

OFAC. The OFAC summary should detail the bank's adherence to OFAC sanctions and regulations. Any potential OFAC risks should be mentioned, as well as the controls in place to mitigate those risks. An overall risk rating should then be provided for the bank's OFAC risk.

Other Risk Factors. This section should focus on specific reporting and recordkeeping requirements, and how the bank has complied with those requirements. The most logical source document for this information will be the bank's independent BSA/AML review results (i.e., audit report). While not related to specific higher-risk factors, regulatory technical compliance provides the reader with an idea of potential risks for non-compliance. Additionally, this section should highlight other quantitative information, such as:

- The number of CTR filings in the assessment review period
- The number of SAR filings in the assessment review period
- The level of currency purchases of monetary instruments
- The level of funds transfer activity, including data on both domestic and international transfers
- Changes to the bank's CIP and/or CDD programs
- The number of subpoenas received by the bank, including those with a BSA "impact," if any. Banks may also wish to include the number of garnishments, IRS actions, etc.

For each of the above factors, a brief statement should be made to attempt to explain any material variances from prior review periods. For example, if the bank filed an average of 100 CTRs each month in the current year, but had only filed an average of 25 CTRs per month in the previous year, then an attempt needs to be made to explain this significant increase. There are a number of possible reasons, one of which could be the existence of a new business customer that may be eligible for exempt status once the account has been opened for 12 months. Once exempted, the CTR filings, assuming no other changes, will drop back off. Similar analysis should be performed for the remaining factors. An overall risk rating should then be provided for the bank's operational risk.

Conclusion. Finally, the conclusion should simply provide the reader with an overall BSA/AML risk rating, which considers each of the above risk factors.

Informing Others

The summary document should then be shared with the board of directors, or committee thereof, along with senior management. Ideally, the risk assessment frequencies should be scheduled as precursors to the annual modifications of policies and procedures. This chronological order allows for informing the board of specific risks, as well as offering possible solutions to mitigate those risks.

Sharing the risk profile should not end with the board and senior management. To effectuate change, each division or department head within the bank needs to be aware of the BSA/AML risks. These individuals, in concert with the BSA/AML compliance officer, can then take the appropriate measures to strengthen the bank's policies and procedures.

Section 10: Future Risk Assessment Events

Introduction

While the BSA/AML risk assessment is a demanding process, the completion of the risk profile is not a one-time event. Additional actions are necessary to assure future compliance with the BSA/AML regulations. In brief, and as discussed below, they include:

- Assessing the impact on existing BSA/AML policies and procedures
- Modifying staff training efforts
- Future BSA/AML risk assessment updates
- Monitoring the bank's BSA/AML risk profile

Impact on BSA/AML Policies and Procedures

Probably the most important part of the entire risk assessment process is the confirmation that the bank's BSA/AML policies and procedures are commensurate with the identified risks. Simply stopping once the risk assessment is complete, with no further action, results in wasted energy and efforts.

Upon completion of the risk assessment analysis, management should be charged by the bank's board of directors to assure that its policies and procedures address the bank's risks. While a bank's policies and procedures may be considered comprehensive, new light to previously unknown or recently elevated risks may have an impact on how the bank combats money laundering and terrorist financing. The necessary changes will largely vary due to the underlying circumstances, and efforts will need to be focused on the higher-risk issues. While not all-inclusive, the following actions might be necessary, as a result of the risk assessment:

- Enhancing the bank's CDD program
- Strengthening internal controls
- Expanding CIP identity and/or identity verification procedures
- Modifying or adding tools to assist with identifying suspicious activity

Those areas of the bank that are affected by the results of the BSA/AML risk assessment will require further evaluation to make the necessary modifications to policies and procedures to assure future compliance. Management personnel responsible for the affected areas will need to be apprised of the identified risks and consulted on the most judicious manner to mitigate the risks.

Staff Training

Once policies and procedures have been modified, bank training materials will require updating to assure that staff is aware of the new procedures. Simply relying on outside training resources may not be sufficient. As with any form of training, tailoring the training material to address the bank's specific procedures is often a more effective approach. Such customization informs staff of the exact procedures expected by management, as well as demonstrates to the examiners that management is committed to comply with the BSA/AML regulations through staff development.

Depending on the risk of the issues at hand, annual or other periodic training material may be adjusted to reflect the bank's procedural changes or immediate staff training sessions may be necessary. The depth and the targeted audience will vary depending on the impact to the affected job functions. Efforts will need to be made to tailor staff training that makes use of the most effective means.

Updating Frequencies

Once the initial risk assessment process is complete, the process of ongoing risk assessment begins. An effective BSA/AML compliance program is risk-based and should continue to evolve. Such modifications to the BSA/AML risk assessment is no exception. The regulators will expect a bank to periodically update its risk assessment. More importantly, ongoing modifications to the bank's BSA/AML compliance program may be warranted, resulting from changes in risk levels.

As noted in the exam manual, the regulators state that a bank shall generally reassess its BSA/AML risks every 12 to 18 months, as circumstances warrant.

Triggering Risk Assessment Events

More frequent risk assessments shall be performed for higher-risk institutions. Additionally, certain events will affect the established frequencies. The following is a brief listing of events that should prompt a bank to reassess some or all of its BSA/AML risks immediately.

Mergers or Acquisitions. The merger of banks or the acquisition of another bank has a significant impact on the organizational structure of the surviving institution. While there are many concerns resulting from such an event, BSA/AML should not be ignored. Such an event will require an evaluation of both institutions' BSA/AML risk profiles. In addition, a new BSA/AML risk assessment will need to be completed for the resulting entity. All significant risk factors will need to be assessed individually and a determination made overall.

Branch Expansion. This event will likely prompt a new risk assessment for the geography portion of the process, since it may involve unchartered geographies. Additionally, consideration of the potential customer base within the new area should be made as well.

New Products or Services. The introduction of new products or services will impact the bank's BSA/AML risk profile. Special consideration will need to be made to determine how the proposed products or services impact the bank's BSA/AML risks. Are the new products or services considered as higher-risk within the industry? How does the bank plan to mitigate any elevated risks?

Key Personnel Changes. Significant changes to the bank's BSA/AML management staff will likely have an impact on the bank's BSA/AML risk profile. Although immediate response may not be necessary, the significance of the changes should be considered to determine if the risk assessment requires updating.

Ongoing Risk Assessment Monitoring

Finally, ongoing monitoring of the bank's risks should be conducted in between risk assessments. This concept is no different than simply managing the bank's BSA/AML compliance program on a day-to-day basis. As situations arise, the impact to the bank's

BSA/AML risks should be considered. A determination will need to be made on whether an immediate partial or complete risk assessment is necessary.

Conclusions

Performing a thorough and comprehensive BSA/AML risk assessment has become a necessary part of a bank's management of its BSA/AML compliance program. Not only is it expected by examiners, it is a logical process to assure that a bank's BSA/AML program remains compliant.

Since the regulatory environment is continually evolving, BSA/AML compliance officers will need to stay apprised of all recent regulatory changes and industry advancements. A compliant BSA/AML program today will need to evolve to maintain its status.

Section 11: OFAC Risk Assessment

OFAC Risks

Unlike the previously covered risk assessment factors, identifying customers or transactions impacting OFAC-identified individuals or countries is straightforward.

The assessment of risk depends upon many variables, making each bank unique. Regardless of bank size, location, or structure, all banks, including small neighborhood or rural banks, have a level of OFAC risk. Assessing this risk fairly is necessary to assure the identification of all OFAC risks. This process of risk assessment will assist the board, management, and the OFAC compliance officer in the design of an effective program that will meet the needs of the organization's OFAC compliance, with the minimum impact possible on normal bank operations.

The primary consideration for OFAC risk assessment is the size and structure of the financial institution. For instance, a large bank with an extensive branch network would have to expect additional risk relating to wires and other funds transfers. A smaller bank may have less risk in these areas, as the bank is in a position to more tightly control bank operations.

A bank's proximity to international borders could also increase the bank's OFAC risk. The closer a bank of any size is to an international border, the higher the risk of OFAC issues. However, given the current immigration difficulties and border control issues of the United States, no bank can assume that it is at no risk from international situations.

The bank should also take its general location into account. Although no bank is immune for OFAC issues, banks need to consider:

- The stability of their market base
  - Is the community stable, with little change in the customer base, or
  - Is the community in the process of changes that would increase the bank's OFAC risk
- The presence/absence of foreign nationals
- The type of community in which the bank operates (rural/suburban/urban)

The bank's structure will also have an impact upon the bank's risks. Banks with tight central controls may have a lower risk. As the bank increases the independence of the bank's offices and officers, the decision making authority of individuals must be dispensed only to individuals willing to accept the responsibilities inherent in the process.

Finally, the bank's business models and types of business will have an impact on the bank's overall OFAC compliance. For instance, banks that focus on commercial customers may have a higher incidence of international letters of credit than other banks that are more focused on consumer transactions

Impact to the Bank

In observance of sound banking practices, banks are required to maintain a reliable OFAC program in keeping with their risk profile. Again, the OFAC risk profile will be based on customers, products and services, and geographic locations. Controls must be in place that will appropriately screen, report, and test for compliance. An employee should be designated as the person responsible for OFAC compliance and a bank's training program should be comprehensive for all personnel.

Regulators consider an OFAC risk assessment critical to a bank's CDD practices. Account opening procedures must include an OFAC check prior to or shortly after account opening, generally before the customer has use of the account. The extent of parties involved in an OFAC check, such as guarantors, beneficiaries, beneficial owners, shareholders, and principals, will depend on a bank's risk and available technology.

Financial institutions should have established policies and procedures for reviewing transactions and transaction parties, such as issuing bank, payee, endorser, or jurisdiction. Current OFAC guidance states that, if the bank has reason to suspect that a party on a check is a positive OFAC target, the bank's continuance with the transaction exposes the bank to liability.

The OFAC risk assessment process will involve using the information that the bank already possess. However, an assessment does need to be made on any operations that pose risks to opening accounts or conducting transactions affecting those persons or areas contained within the OFAC lists. The following sections discuss the process to be followed in this analysis.

Section 12: Areas of OFAC Risk Assessment

The Exposures

The OFAC compliance program should address all of the bank's possible exposures which can be present in the various operational areas of the bank. While no area should be neglected, the following are areas of bank operations that might be considered the most "at risk."

Wire Transfers

When performing a risk assessment for wire transfers, the bank should consider the following:

- Wire volume
  - How many wires does the bank generate?
  - How many wires are repetitive in nature?
- Wire authority
  - Who has the authority to approve wires, and at what levels?
  - Who has oversight of the wire transfer function?
- Wire types
  - Does the bank permit international wires?
  - Does the bank originate and receive wires directly, or through a correspondent?
- Wire rules
  - What restrictions does the bank have in place?
  - Will the bank send or receive wires for noncustomers?

Outgoing wire transfers must be reviewed before being transmitted. Incoming wire transfers must be reviewed prior to being credited or disbursed as per payment instructions. Each party to the transfer must be checked – the originator and beneficiary.

Existing Accounts / Customers

When performing a risk assessment for existing accounts or customers, the bank should consider the following:

- The amount of time between periodic reviews
  - Generally, the longer the time between the periodic reviews, the higher the bank's risk levels.
- The bank's response to and review of additions or other changes in the OFAC SDN list
  - Does the bank check the portfolio each time there is a change, or only during the periodic review?
- Does the bank review the OFAC SDN listing periodically to ensure that no new customers "slipped through" the new account screening?

New Deposit Accounts

When performing a risk assessment for new account opening, the bank should consider the following:

- The methods used to check the OFAC SDN list prior to account activation
- Systems that assist in the review process and their ability to generate documentation
- The bank's ability to assure that the bank's employees follow all bank and OFAC requirements (management and audit controls)
- The types of accounts that the bank offers
- The bank's customer types / customer profiles
- The experience of new account opening clerks
- Does the bank check the listing at the end of the day; or when the new account application is made if immediate availability to funds are granted
- Delivery systems (face to face, internet, deposit brokers, etc.)

Lending

When performing a risk assessment for lending, the bank should consider the following:

- The methods used by lending personnel to check the OFAC SDN list prior to loan approval and/or note signing
- Systems that assist in the review process and their ability to generate documentation
- The bank's ability to assure that the bank's employees follow all bank and OFAC requirements (management and audit controls)
- The types of loans that the bank offers
- The mix of consumer vs. commercial business
- The bank's customer types / customer profiles
- The bank's delivery systems (phone, face to face, internet, mortgage brokers, participations, etc.)

Operational Areas / Bookkeeping

Generally, these departments do not have high levels of risk for OFAC issues in many banks. However, if these departments have responsibilities for some of the other items that are listed in this risk assessment section, the bank's risk levels could increase in these departments. Levels would increase based in part upon the methods the bank uses to place appropriate controls in place in these various departments.

Trust / Personal Bankers

When performing a risk assessment for trust department or personal banker services, the bank should consider the following:

- The types of customers that request these services of the bank
- Any unique products that these customers may require
- The bank's ability to identify all customers that use these services
- The level of experience in these departments
- The delivery methods employed by these departments
- The ability of the bank's systems to assure that none of these customers appear on the OFAC SDN list after account opening:
  - Many banks use subsystems or "stand alone" software to manage functions such as the trust department. This can sometimes limit the bank's abilities to adequately monitor these customers and accounts.

Identifying Customer Base

Assuming the bank already has a system or procedures in place to check new customers against the OFAC list, as well as periodic checks of the existing customer database against the list, the OFAC assessment of the customer base should confirm whether any of the bank's customers have been identified as being on the OFAC list.

For banks that have implemented an ongoing and periodic check of the customer base against the current OFAC list, the reviewer will need to obtain the most recent OFAC check output report to determine if there are any "positive" hits. In other words, are any of the bank's customers identified as being on the OFAC list?

If a bank does not routinely perform a periodic check of its customer base against the OFAC list, then the reviewer should consider performing such a check.

Identifying Transactions

Determining whether the bank has conducted or accepted any transactions to or from or in OFAC designated areas or involving OFAC identified individuals may require a greater amount of research. The assessment phase will depend on the level of the bank's procedures to check the OFAC list for various types of transactions. In addition, the reviewer will need to determine the reliability of said procedures. In essence, the reviewer needs to conclude how confident he/she is that no transactions were conducted over the assessment review period which involved individuals or areas contained within the OFAC list.

Unless the bank has a process to check every individual involved within a transaction, the reviewer should select a representative sample of transactions of various types and make his/her own assessment. Depending on the types of products or services offered by the bank, the following should, at a minimum, be included in this review:

- Sales of monetary instruments records, including (as available) those individuals who purchased the instruments and the names of the payee(s)
- Wire transfer records, especially including noncustomer originators, intermediaries, and beneficiaries (a targeted focus on international wire transfer should be included in the assessment, since transactions abroad pose a greater risk)
- Other transaction types, such as individuals involved in loan transactions

The assessment should include an evaluation of the level, if any, of any instances where the bank has opened an account or conducted a transaction that involved an individual on the OFAC list. Since OFAC regulations require the reporting of such instances, these reports will need to be reviewed as part of the assessment.

Finally, the OFAC risk assessment should include an analysis of the following factors, which are further discussed below:

- The bank's OFAC compliance program
- Staffing levels to comply with OFAC sanctions
- Assigned accountability for OFAC compliance
- Training of staff on OFAC requirements
- The internal controls implemented to assure OFAC compliance

OFAC Risk Levels

Using the "Quantity of Risk Matrix–OFAC Procedures" (Appendix M) in the exam manual, a risk rating will need to be assigned to the bank's OFAC risk. A copy of Appendix M appeared earlier in this manual. It should be noted that some of the risk factors below also appear within Appendix J. Therefore, there is some overlap between the assessment factors discussed earlier and the OFAC risk assessment factors. By completing the duplicate factors previously, the reviewer should be able to quickly make an OFAC assessment for these repeated items.

In addition, the following five factors do not appear in the exam manual matrix but were released by OFAC for additional consideration when an examiner assesses a bank's OFAC risks as part of an enforcement action. These should also be included in the reviewer's analysis.

Low	Moderate	High
The board of directors, or board committee, has approved an OFAC compliance program that includes policies, procedures, controls, and information systems that are adequate, and consistent with the bank's OFAC risk profile.	The board has approved an OFAC compliance program that includes most of the appropriate policies, procedures, controls, and information systems necessary to ensure compliance, but some weaknesses are noted.	The board has not approved an OFAC compliance program, or policies, procedures, controls, and information systems are significantly deficient.
Staffing levels appear adequate to properly execute the OFAC compliance program.	Staffing levels appear generally adequate, but some deficiencies are noted.	Management has failed to provide appropriate staffing levels to handle workload.
Authority and accountability for OFAC compliance are clearly defined and enforced, including the designations of a qualified OFAC officer.	Authority and accountability are defined, but some refinements are needed. A qualified OFAC officer has been designated.	Authority and accountability for compliance have not been clearly established. No OFAC compliance officer, or an unqualified one, has been appointed. The role of the OFAC officer is unclear.

Low	Moderate	High
Training is appropriate and effective based on the bank's risk profile, covers applicable personnel, and provides necessary up-to-date information and resources to ensure compliance.	Training is conducted and management provides adequate resources given the risk profile of the organization; however, some areas are not covered within the training program.	Training is sporadic and does not cover important regulatory and risk areas.
The institution employs strong quality control methods.	The institution employs limited quality control methods.	The institution does not employ quality control methods.

Finally, an overall OFAC risk assessment rating should be assigned to the bank. This rating level should encompass each of the above risk factors and apply appropriate weight to each in arriving at the overall rating. A supporting narrative statement should also accompany the overall OFAC risk rating.

Ongoing Risk Assessments

The bank's OFAC risk assessment may change from time to time due to internal factors such as:

- A change in the bank's delivery systems,
- A change in the bank's strategic plans which refocuses the bank on geographic or products areas that are not as familiar to bank personnel,
- Other factors, such as the addition of a branch in a new and different market area.

External factors can also require a review of the bank's OFAC risk. These factors would include:

- A change in the types of customers available to the bank
- A change in the types of businesses in the bank's service area
- A change in the type of areas served (for instance, some banks find that their market is changing, as rural areas begin to change from family farms into areas of upscale housing)

As the bank's risk factors change, management must continue to reexamine the bank's risk to assure that the bank takes all prudent and appropriate steps.

Consider Your Bank: OFAC Risk Assessment

Based on what you have heard in the last section, comment regarding your bank's OFAC Risk Assessment.

General Bank Profile		
Risk Factor	**Assessment Results**	**Comments**
Bank asset size (as of assessment date)	$	
Number of bank employees		
Employee turnover rate for frontline and "key" BSA personnel (Risk Factor)		
Describe "key" BSA personnel and assess their knowledge base/experience		
Describe the bank's system resources that support its BSA responsibilities		
Regulatory Reporting, Recordkeeping, and Policies & Procedures		
Risk Factor	**Assessment Results**	**Comments**
Identify level of large currency transactions (Significant, Moderate, or Nominal)		
Describe level of structured transactions identified through BSA/AML monitoring (Significant, Moderate, or Nominal)		
Level of compliance with BSA reporting and recordkeeping requirements (Strong, Satisfactory, or Weak)		
Adequacy of procedures to identify suspicious activity (Strong, Satisfactory, or Weak)		
Level of funds transfer activity (Significant, Moderate, or Nominal)		
Level of monetary instrument sales (Significant, Moderate, or Nominal)		
Level of cash-secured loans (Significant, Moderate, or Nominal)		
Overall Bank Profile Risk Rating		
Supporting Justification for Risk Rating		

Geography Risk Profile				
High-Risk Location	**Does the Bank have any facilities or customers, or conduct transactions, in these locations? (Yes or No)**	**If yes, describe the significance of such presence.**	**Impact to Geography Risk Profile (Significant, Moderate, or Nominal)**	**Comments**
OFAC-identified locations				
Countries supporting international terrorism				
Jurisdictions of primary money laundering concern				
Jurisdictions/Countries identified as non-cooperative				
Major money laundering countries or jurisdictions				
Offshore financial centers				
HIDTAs				
HIFCAs				
Other bank-identified high-risk geographies				
Overall Geography Risk Rating				
Supporting Justification for Risk Rating				

Note: *Italicized* items above are linked to risk factors in Appendix J of the FFIEC's *BSA/AML Examination Manual*.

Customer and Entity Risk Profile			
High-Risk Customer Type	**Number of Customers**	**Percent to Total Customers**	**Comments**
Cash-intensive businesses			
Pawn brokers			
Vehicle, vessel, aircraft, farm equipment, or mobile home dealers			
Auctioneers			
Chartering of ships, buses, or aircraft			
Gaming entities			
Trade unions			
Title companies			
Professional service providers (e.g., doctors, attorneys, accountants, real estate brokers)			
Non-governmental organizations or charities			
Non-bank financial institutions			
Senior political figures			
Foreign corporations			
Deposit brokers			
Foreign financial institutions			
Non-resident aliens			
Other types (describe)			
Customer Stability			
Growth rate of customer base (Significant, Expected, or Stable)			
Overall Customer/Entity Risk Rating			
Supporting Justification for Risk Rating			

Product and Service Risk Profile			
High-Risk Product Type	**Number of Customers Using Product or Service**	**Overall Significance of Product or Service (Significant, Moderate, or Nominal)**	**Comments**
Foreign correspondent accounts			
Electronic banking			
Funds transfers			
Private banking, or trust and asset management			
International accounts			
Monetary instruments			
Trade finance			
Loans secured by cash collateral			
Non-deposit account services			
Overall Product/Service Risk Rating			
Supporting Justification for Risk Rating			

Note: *Italicized* items above are linked to risk factors in Appendix J of the FFIEC's *BSA/AML Examination Manual*.

OFAC Risk Profile		
Risk Factor	**Rating (High, Moderate, or Low)**	**Comments**
Customer stability		
High-risk customers		
Oversees branches or foreign correspondent accounts		
Electronic banking services		
Funds transfers		
Other international transactions (e.g., trade finance, cross border ACH, etc.)		
OFAC actions against the Bank		
Adoption of OFAC policies and procedures		
OFAC staffing levels		
OFAC officer and support personnel		
Staff training on OFAC		
OFAC internal controls		
Overall OFAC Risk Rating		
Supporting Justification for Risk Rating		

Note: *Italicized* items above are linked to risk factors in Appendix M of the FFIEC's *BSA/AML Examination Manual*.

Overall BSA/AML Risk Profile		
Risk Area	**Risk Rating**	**Supporting Justification(s)**
General Bank Profile		
Geography Risk Profile		
Customer and Entity Risk Profile		
Product and Service Risk Profile		
OFAC Risk Profile		
Overall BSA/AML Risk Rating		

Risk Assessment Date	
Performed by	
Next Scheduled Risk Assessment Date / Frequency	

Section 14: Case Studies - Introduction

The Approach

In an effort to make this seminar as interactive as possible and to promote the application of the concepts presented, we have devised several individual case studies to be completed throughout the next several days.

We have elected to organize our presentation of individual topics in the order of how a bank may consider them from the inception to the evaluation of its BSA compliance program or development cycle. More specifically, we began our journey with an examination of the regulators' expectations of a bank's BSA/AML/OFAC risk assessment. The case studied will include "Performing the Risk Assessment," the "dos and don'ts" of developing the annual BSA audit scope (as part of Regulatory Update and Emerging Trends), when and when not to file a Suspicious Activity Report (SAR), and written policy and procedure development, using your bank's policy as a case in point.

To begin, we will provide you with a set of facts about a fictional bank and ask you to perform a BSA/AML/OFAC risk assessment. Then, following the annual audit discussion, you will recall back on the risk assessment results for our fictional bank and attempt to define an acceptable audit scope for the bank's next scheduled audit, which just happens to fall a few short months before your next scheduled regulatory examination. Next, we will introduce a case study focusing on a number of specific "fictional" customers and ask that you conclude as to whether a SAR should or should not be filed in each instance. We will conclude the case study work with an opportunity for you to review your own bank's BSA/AML/OFAC written program based on the concepts and information presented during this seminar.

We hope you find the case study work useful or, at the very least, find that it may prompt ideas not already considered back in your own bank.

Collaborative Effort

For most of the case study work, we encourage you to work in small groups, maybe 2-4 persons. Whether you team up with persons representing banks of similar size or complete opposites, a group approach should prompt ideas or concepts you might not consider working on your own.

Section 15: Case Studies - Performing the Risk Assessment

Your Assignment

Using the background information below and the information provided within the following worksheets, conclude as to this fictitious bank's BSA/AML risks using the guidelines discussed today. For this exercise, you will need to adopt the perspective that you have been hired to serve as the new BSA Officer. As you will soon learn, many of the aspects of your new employer's BSA program were not necessarily divulged during the interview process. Needless to say, you may have some work cut out for you in your first few months with the bank should you decide to stay.

To complicate matters even more, you learn on your first day of employment that the bank is expecting its next BSA examination by the FDIC in about six months. Furthermore, bank management also shares with you the internal auditor's assessment from his last audit nine months ago. The audit revealed a few issues, as well as the scope of the audit may not have been as thorough as you would expect for a bank of this size and complexity. The bank has been without a BSA Officer for roughly six months now, so needless to say many of the audit issues have yet to be resolved.

To accomplish this first goal of assessing the bank's BSA/AML/OFAC risks:

- Assign a risk rating of LOW, MODERATE, or HIGH to specific risk factors.
- Assign overall risk ratings to each risk area (i.e., geography, customers, products and services, etc.), and
- Assign an overall BSA/AML risk level to the bank.

As you proceed through the risk assessment process, set aside suggestions you might consider to enhance the audit function, as well as any controls that would help prevent future deficiencies from occurring.

General Bank Information

To complete the bank's risk assessment, most of the background information that you will need is found within the partially completed BSA/AML risk assessment worksheets. The following additional information is also provided for your reference and consideration:

- The bank is located in two Indiana counties and operates a headquarters and three additional branches. All have drive-up facilities and night drops for business customer use. The headquarters and one branch are in northern Indianapolis (Marion County), with additional branches in Noblesville and Brownsburg.
- The two Indianapolis facilities are in areas with significant illegal drug sales, especially variants of cocaine and meth.
- The bank has undergone an annual BSA/AML audit with some deficiencies noted.
- The bank has identified a low to moderate number of higher-risk customers, mostly from the lists provided by examining agencies. To date, all professional service providers, regardless of specific risks, are rated as high-risk. The bank assigns a default risk rating of "Low" to all new customers if it does not have any specific factors that would prompt it

to rate a new customer as High or Moderate risk at the time the new relationship is established.

- The products and services offered by the bank are typical of most community banks, such as:
  - Standard deposit products (e.g., checking, savings, CDs, etc.)
  - Consumer and commercial loans.
  - All new accounts are opened face-to-face if the customer is new to the bank. A small percentage of accounts are opened by mail if another account already exists.
  - Electronic banking services (e.g., Internet banking and bill payment, mobile banking, telephone banking, ACH, debit and ATM cards.)
  - Wire transfer services, including a low to moderate number of International wires (approximately 5 percent of total wires.)
  - The Bank has actively, for the past 12 months, attempted to promote its Internet banking services, specifically on-line bill payment services. This active effort has resulted in nearly 60 percent of the Bank's consumer deposit customers enrolling and using the service.
  - The Bank has developed a strong remote deposit capture program involving 39 clients of whom 17 are outside the Bank's primary service area. The program is being managed by the assistant head bookkeeper.
  - The Bank is also within a few months of rolling out its program to solicit and open deposit accounts via the Internet. The senior vice president of on-line banking has assured management that the Bank will be compliant with the BSA's CIP requirements as it related to accounts opened on-line. CDD issues do not seem to have been addressed
  - The Bank recently added mobile check deposit (using smart phone technology) with no consideration of any BSA related issues.
- As far as you are aware, the bank has no OFAC identified customers or persons involved in transactions conducted at or through the bank. Additionally, there have been no OFAC sanctions against the bank.

Internal Audit Results Summary

A more detailed internal audit report will be presented in the next case study, but to assist in the risk assessment process, we have provided you with the following summary of issues noted in the audit:

- Risk assessment:
  - Risk assessment summary not communicated to the Board during the last two calendar years.
- Written BSA compliance program:
  - Lacking specific written procedures addressing the monitoring of sales of monetary instruments for currency.
  - Remote deposit capture is not mentioned in the written BSA compliance program documents.

  - Lacking specific written procedures addressing when OFAC checks are performed for wire transfer activity.
  - CIP procedures do not address the opening of accounts by methods other than face-to-face.
- Suspicious activity monitoring:
  - Several instances of suspicious activity detected with a low percentage of actual SARs filed.
  - Numerous cash purchases of monetary instruments by non customers.
- Currency transaction reports:
  - An overall 7 percent error rate on filed CTRs, including but not limited to the following:
    i. Not marking or completing all required "boxes"
    ii. Inaccurate transaction amounts (mostly related to improper rounding)
    iii. Occasional inaccurate information regarding the participants in the transaction
- Monetary instrument sales recordkeeping:
  - Missing date of birth and address on approximately 5 percent of records for sales to non deposit customers.
- Wire transfer recordkeeping:
  - No OFAC checks on some parties, other than originator and intermediary, on incoming wire transfers.
- Information Sharing – 314(a) Requests:
  - Several 314(a) searches not completed due to BSA officer's medical leave and the "hole" where no one held the position.

General Bank Profile		
Risk Factor	**Assessment Results**	**Comments**
Bank asset size (as of assessment date)		Mid-sized community bank serving communities in two counties of one state with assets of $332 million.
Number of bank employees		72 FTEs
Employee turnover rate for frontline and "key" BSA personnel (Risk Factor)		45% turnover for tellers, 10% for front-line staff, 2% for loan officers.
Describe "key" BSA personnel and assess their knowledge base/experience		As evidenced by your new employment, the Bank now has a new BSA Officer. The position is responsible for all BSA/AML activities. The prior BSA Officer was with the Bank for 2 years. Given the Bank's size, there are no support staff positions within the BSA department.
Describe the bank's system resources that support its BSA responsibilities		Internal controls are manual with some concerns noted in internal audits and examinations. Bank relies on manual methods to identify suspicious activity based on the use of reports, such as a large cash transactions report, and detection of unusual activity by both support and front line staff. The prior BSA Officer pushed hard for automated monitoring systems with no success.

Note: *Italicized* items above are linked to risk factors in Appendix J of the FFIEC's *BSA/AML Examination Manual*.

Regulatory Reporting, Recordkeeping, and Policies & Procedures		
Risk Factor	**Assessment Results**	**Comments**
Identify level of large currency transactions (Significant, Moderate, or Nominal)		For the past 12 months, the Bank has filed approximately 600 CTRs. Most recurring CTRs filed (about 400/ year) are for the same customers. The Bank has made good use of the exemption process in past years, but the exempt list had not been updated in three years.
Describe level of structured transactions identified through BSA/AML monitoring (Significant, Moderate, or Nominal)		Despite the moderate number of CTRs filed, the Bank has filed very few SARs (2 filed last year, 4 in prior year, 9 the year before that). While the prior BSA Officer had considered numerous SARs, the President has routinely made the case not to file to avoid law suits. In the last five years, all SARs filed were on noncustomers.
Level of compliance with BSA reporting and recordkeeping requirements (Strong, Satisfactory, or Weak)		As noted in the most recent audit report, there were some issues noted when completing CTRs.
Adequacy of procedures to identify suspicious activity (Strong, Satisfactory, or Weak)		Despite the manual monitoring systems employed, the auditor has not confirmed instances of potential suspicious activity that were overlooked. Regardless, there is concern by the auditor about monitoring of monetary instruments and wires.
Level of funds transfer activity (Significant, Moderate, or Nominal)		The Bank originates and receives approximately 1,200 and 2,000 wires per year, respectively. Many are recurring for a few select customers. Very few are international.
Level of monetary instrument sales (Significant, Moderate, or Nominal)		To increase fee income, the Bank began selling cashier's checks to non deposit customers a year and a half ago. This accounts for approximately 150 per year and must be purchased with currency.
Level of cash-secured loans (Significant, Moderate, or Nominal)		The Bank makes very few, as compared to entire loan portfolio, loans secured by deposit accounts.
Overall Bank Profile Risk Rating		
Supporting Justification for Risk Rating		

Note: *Italicized* items above are linked to risk factors in Appendix J of the FFIEC's *BSA/AML Examination Manual*.

Geography Risk Profile				
High-Risk Location	**Does the Bank have any facilities or customers, or conduct transactions, in these locations? (Yes or No)**	**If yes, describe the significance of such presence.**	**Risk Rating**	**Comments**
OFAC-identified locations	No	N/A		Possibly unknown since some parties to incoming wires not checked.
Countries supporting international terrorism	No	N/A		None noted in last risk assessment.
Jurisdictions of primary money laundering concern	No	N/A		None noted in last risk assessment.
Jurisdictions/Countries identified as non cooperative	No	N/A		None noted in last risk assessment.
Major money laundering countries or jurisdictions	No	N/A		None noted in last risk assessment.
Offshore financial centers	No	N/A		None noted in last risk assessment.
HIDTAs *Low*	No	No Bank branches in an HIDTA		Metro area has significant drug activity and related crime.
HIFCAs Low	No	No Bank branches in an HIDTA		No bank branches in an HIFCA
Other bank-identified high-risk geographies	N/A			None noted in last risk assessment.
Overall Geography Risk Rating				
Supporting Justification for Risk Rating				

Note: *Italicized* items above are linked to risk factors in Appendix J of the FFIEC's *BSA/AML Examination Manual*.

Customer and Entity Risk Profile			
High-Risk Customer Type	**Number of Customers**	**Percent to Total Customers**	**Comments**
Cash-intensive businesses	95	Approx. 7% of business customers	Primarily local convenience stores, grocery, gas stations, bars and restaurants
Pawn brokers	2	N/A	None
Vehicle, vessel, aircraft, farm equipment, or mobile home dealers	21	Nominal	Mostly auto dealers who send loans to Bank.
Auctioneers	0	N/A	None
Chartering of ships, buses, or aircraft	0	N/A	None
Gaming entities	1	N/A	One
Trade unions	1	N/A	None
Title companies	5	Nominal	None
Professional service providers (e.g., doctors, attorneys, accountants, real estate brokers)	97	Approx 7% of business customers	None
Non governmental organizations or charities	33	Nominal	Mostly denominational churches.
Non bank financial institutions	15	Nominal	All convenience stores.
Senior political figures	0	N/A	None
Foreign corporations	0	N/A	None
Deposit brokers	0	N/A	None
Foreign financial institutions	0	N/A	None
Non resident aliens	612	Approx 9% of all customers	Has doubled over the last three years.
Customer Stability			
Growth rate of customer base (Significant, Expected, or Stable)			Historical rate is stable.
Overall Customer/Entity Risk Rating			
Supporting Justification for Risk Rating			

Note: *Italicized* items above are linked to risk factors in Appendix J of the FFIEC's *BSA/AML examination Manual.*

Product and Service Risk Profile			
High-Risk Product Type	**Number of Customers Using Product or Service**	**Overall Significance of Product or Service (Significant, Moderate, or Nominal)**	**Comments**
Foreign correspondent accounts	0	N/A	None
Electronic banking	4,105	Significant	Nearly 60% of consumer customers use Internet banking.
Funds transfers	1,200 outgoing, 2,000 incoming	Moderate	Mostly recurring. Nearly 5% are International.
Private banking, or trust and asset management	0	N/A	None
International accounts	0	N/A	None
Monetary instruments (for cash)	1,500	Significant	Non customer purchases with currency only. Deposit customers deposit into account first before purchase. Average amount is $2,000.
Trade finance	0	N/A	None
Loans secured by cash collateral	15	Nominal	Only if secured by one of the Bank's CODs.
Non deposit account services	0	N/A	None
Overall Product/Service Risk Rating			
Supporting Justification for Risk Rating			

Note: *Italicized* items above are linked to risk factors in Appendix J of the FFIEC's *BSA/AML Examination Manual*.

OFAC Risk Profile		
Risk Factor	**Rating (High, Moderate, or Low)**	**Comments**
Customer stability		Stable, well-known customer base
High-risk customers		Approximately 65 bank-identified higher-risk customers. None on OFAC list.
Oversees branches or foreign correspondent accounts	N/A	None
Electronic banking services		Typical e-banking services offered with minimal OFAC impact.
Funds transfers		Moderate level of funds transfers.
Other international transactions (e.g., trade finance, cross border ACH, etc.)	N/A	No current monitoring system exists.
OFAC actions against the Bank	N/A	None
Adoption of OFAC policies and procedures		OFAC procedures adopted and implemented. They assign responsibility for OFAC compliance. New accounts monitored, as well as existing accounts.
OFAC staffing levels		Wire Department staff monitors funds transfer OFAC compliance for domestic wires and outgoing International wires.
OFAC officer and support personnel		BSA Officer is ultimately responsible.
Staff training on OFAC		Last training was three years ago.
OFAC internal controls		All new accounts are checked against OFAC listing.
Overall OFAC Risk Rating		
Supporting Justification for Risk Rating		

Note: *Italicized* items above are linked to risk factors in Appendix M of the FFIEC's *BSA/AML Examination Manual*.

Overall BSA/AML Risk Profile		
Risk Area	**Risk Rating**	**Supporting Justification(s)**
General Bank Profile		
Geography Risk Profile		
Customer and Entity Risk Profile		
Product and Service Risk Profile		
OFAC Risk Profile		
Overall BSA/AML Risk Rating		

Risk Assessment Date	Two and a half years ago
Performed by	BSA Officer
Next Scheduled Risk Assessment Date / Frequency	**Annually**