BSA/AML Risk Assessment — Overview

Objective. *Assess the BSA/AML risk profile of the bank and evaluate the adequacy of the bank's BSA/AML risk assessment process.*

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 assists 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.[17]

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

[17] Refer to "Examiner Development of a BSA/AML Risk Assessment," page 24, for guidance.

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 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.

Products and 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 — prepaid access (e.g., prepaid and payroll cards), funds transfers (domestic and international), payable upon proper identification (PUPID) transactions, third-party payment processors, remittance activity, automated clearinghouse (ACH) transactions, and automated teller machines (ATM).
- Electronic banking.
- Private banking (domestic and international).
- Trust and asset management services.
- Monetary instruments.[18]
- 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.

Customers and Entities

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)).[19]

[18] Monetary instruments in this context include official bank checks, cashier's checks, money orders, and traveler's checks. Refer to the expanded overview section, "Purchase and Sale of Monetary Instruments," page 240, for further discussion on risk factors and risk mitigation regarding monetary instruments.

- Nonresident alien (NRA)[20] 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))[21] 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).

Geographic Locations

Identifying geographic locations that may pose a higher risk is essential to a bank's BSA/AML compliance program. U.S. banks should understand and evaluate the specific risks associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not necessarily determine a customer's or transaction's risk level, either positively or negatively.

Higher-risk geographic locations can be either international or domestic. International higher-risk geographic locations generally include:

- Countries subject to OFAC sanctions, including state sponsors of terrorism.[22]
- Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State.[23]
- 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.[24]

[19] Refer to core overview, "Private Banking Due Diligence Program (Non-U.S. Persons)," page 125, and expanded overview, "Politically Exposed Persons," pages 290, for additional guidance.

[20] NRA accounts may be identified by obtaining a list of financial institution customers who filed W-8s.

[21] For explanations of PICs and IBCs and additional guidance, refer to expanded overview, "Business Entities (Domestic and Foreign)," page 314.

[22] A list of such countries, jurisdictions, and governments is available on the OFAC Web site.

[23] A list of the countries supporting international terrorism appears in the U.S. Department of State's annual *Country Reports on Terrorism*. This report is available on the U.S. Department of State Web site.

[24] Notices of proposed rulemaking and final rules accompanying the determination "of primary money laundering concern," and imposition of a special measure (or measures) pursuant to section 311 of the USA PATRIOT Act are available on the FinCEN Web site.

- 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 that are identified as jurisdictions of primary concern.[25]
- Offshore financial centers (OFC).[26]
- 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).[27]
- Domestic higher-risk geographic locations may include, but are not limited to, banking offices doing business within, or having customers located within, a U.S. government-designated higher-risk geographic location. Domestic higher-risk geographic locations include:
  - High Intensity Drug Trafficking Areas (HIDTA).[28]
  - High Intensity Financial Crime Areas (HIFCA).[29]

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

[25] The INCSR, including the lists of high-risk money laundering countries and jurisdictions, may be accessed on the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs Web site.

[26] OFCs offer a variety of financial products and services. For additional information, including assessments of OFCs, refer to the International Monetary Fund's OFC page.

[27] The Basel Anti-Money Laundering (AML) Index is an additional resource that may be useful in assisting banks to evaluate geographic locations. The Basel AML Index is a composite index that evaluates indicators from various publicly available sources such as the FATF, World Bank, Transparency International and World Economic Forum.

[28] The Anti-Drug Abuse Act of 1988 and The Office of National Drug Control Policy (ONDCP) Reauthorization Act of 1998 authorized the Director of ONDCP to designate areas within the United States that exhibit serious drug trafficking problems and harmfully impact other areas of the country as HIDTAs. The HIDTA Program provides additional federal resources to those areas to help eliminate or reduce drug trafficking and its harmful consequences. A listing of these areas can be found at the White House's Office of National Drug Control Policy Web site.

[29] HIFCAs were first announced in the 1999 National Money Laundering Strategy and were conceived in the Money Laundering and Financial Crimes Strategy Act of 1998 as a means of concentrating law enforcement efforts at the federal, state, and local levels in high intensity money laundering zones. A listing of these areas can be found at the FinCEN Web site.

vary by bank. The detailed analysis is important because within any type of product or category of customer there are 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.

As illustrated above, the bank's CIP and CDD information take on important roles in this process. Refer to the core overview sections, "Customer Identification Program" and "Customer Due Diligence," found on pages 47 and 56, respectively, for additional guidance.

Developing the Bank's BSA/AML Compliance Program Based Upon Its Risk Assessment

Management should structure the bank's BSA/AML compliance program to adequately address its risk profile, as identified by the risk assessment. Management should understand the bank's BSA/AML risk exposure and develop the appropriate policies, procedures, and processes to monitor and control BSA/AML risks. For example, the bank's monitoring systems to identify, research, and report suspicious activity should be risk-based, with particular emphasis on higher-risk products, services, customers, entities, and geographic locations as identified by the bank's BSA/AML risk assessment.

Independent testing (audit) should review the bank's risk assessment for reasonableness. Additionally, management should consider the staffing resources and the level of training necessary to promote adherence with these policies, procedures, and processes. For those banks that assume a higher-risk BSA/AML profile, management should provide a more robust BSA/AML compliance program that specifically monitors and controls the higher risks that management and the board have accepted. Refer to Appendix I ("Risk Assessment Link to the BSA/AML Compliance Program") for a chart depicting the risk assessment's link to the BSA/AML compliance program.

Consolidated BSA/AML Compliance Risk Assessment

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. Refer to the expanded overview section, "BSA/AML Compliance Program Structures," page 155, for additional guidance.

Bank's Updating of the Risk Assessment

An effective BSA/AML compliance program controls risks associated with the bank's products, services, customers, entities, and geographic locations; therefore, an effective risk assessment should be an ongoing process, not a one-time exercise. Management should update its risk assessment to identify changes in the bank's risk profile, as necessary (e.g., when new products and services are introduced, existing products and services change, higher-risk customers' open and close accounts, or the bank expands through mergers and acquisitions). Even in the absence of such changes, it is a sound practice for banks to periodically reassess their BSA/AML risks at least every 12 to 18 months.

Examiner Development of a BSA/AML Risk Assessment

In some situations, banks may not have performed or completed an adequate BSA/AML risk assessment and examiners must complete one based on available information. When doing so, examiners do not have to use any particular format. In such instances, documented workpapers should include the bank's risk assessment, the deficiencies noted in the bank's risk assessment, and the examiner-prepared risk assessment.

Examiners should ensure that they have a general understanding of the bank's BSA/AML risks and, at a minimum, document these risks within the examination scoping process. This section provides some general guidance that examiners can use when they are required to complete a BSA/AML risk assessment. In addition, examiners may share this information with bankers to develop or improve their own BSA/AML risk assessment.

The risk assessment developed by examiners generally are not as comprehensive as one developed by a bank. However, similar to what is expected in a bank's risk assessment, examiners should obtain information on the bank's products, services, customers, entities, and geographic locations to determine the volume and trend for potentially higher-risk areas. This process can begin with an analysis of:

- Information retrieved from FinCEN Query, the BSA-reporting database.

- Prior examination or inspection reports and workpapers.
- Response to request letter items.
- Discussions with bank management and appropriate regulatory agency personnel.
- Reports of Condition and Income (Call Report) and Uniform Bank Performance Report (UBPR).

Examiners should complete this analysis by reviewing the level and trend of information pertaining to banking activities identified, for example:

- Funds transfers.
- Private banking.
- Monetary instrument sales.
- Foreign correspondent accounts and PTAs.
- Branch locations.
- Domestic and international geographic locations of the bank's business area.

This information should be evaluated relative to such factors as the bank's total asset size, customer base, entities, products, services, and geographic locations. Examiners should exercise caution if comparing information between banks and use their experience and insight when performing this analysis. Specifically, examiners should avoid comparing the number of SARs filed by a bank to those filed by another bank in the same geographic location. Examiners can and should use their knowledge of the risks associated with products, services, customers, entities, and geographic locations to help them determine the bank's BSA/AML risk profile. Examiners may refer to Appendix J ("Quantity of Risk Matrix") when completing this evaluation.

After identifying potential higher-risk operations, examiners should form a preliminary BSA/AML risk profile of the bank. The preliminary risk profile provides the examiner with the basis for the initial BSA/AML examination scope and the ability to determine the adequacy of the bank's BSA/AML compliance program. Banks may have an appetite for higher-risk activities, but these risks should be appropriately mitigated by an effective BSA/AML compliance program tailored to those specific risks.

The examiner should develop an initial examination scoping and planning document commensurate with the preliminary BSA/AML risk profile. As necessary, the examiner should identify additional examination procedures beyond the minimum procedures that must be completed during the examination. While the initial scope may change during the examination, the preliminary risk profile enables the examiner to establish a reasonable scope for the BSA/AML review.

Examiner Determination of the Bank's BSA/AML Aggregate Risk Profile

During the "Developing Conclusions and Finalizing the Examination" phase of the BSA/AML examination, the examiner should assess whether the controls of the bank's

BSA/AML compliance program are appropriate to manage and mitigate its BSA/AML risks. Through this process the examiner should determine an aggregate risk profile for the bank. This aggregate risk profile should take into consideration the risk assessment developed either by the bank or by the examiner and should factor in the adequacy of the BSA/AML compliance program. Examiners should determine whether the bank's BSA/AML compliance program is adequate to appropriately mitigate the BSA/AML risks, based on the risk assessment. The existence of BSA/AML risk within the aggregate risk profile should not be criticized as long as the bank's BSA/AML compliance program adequately identifies, measures, monitors, and controls this risk as part of a deliberate risk strategy. When the risks are not appropriately controlled, examiners must communicate to management and the board of directors the need to mitigate BSA/AML risk. Examiners should document deficiencies as directed in the core examination procedures, "Developing Conclusions and Finalizing the Examination," page 43.