Bank Secrecy Act Audit

| ABC Bank **Internal Audit Review: Bank Secrecy Act and Anti-Money Laundering Audit** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Procedure** | | **Wkpr #** | | **Comments** | **Exceptions Noted** | |
| Compliance Program - CP | | | | | | |
|  | Does the bank have a written BSA/AML/OFAC compliance policy? If so, obtain and review the policy. | |  |  | |  |
|  | Does the written BSA/anti-money laundering compliance program provide for the following:   1. A system of internal controls to ensure ongoing compliance? 2. Independent testing for compliance to be conducted by either bank personnel or an outside party? 3. Designation of a qualified individual(s) responsible for coordinating and monitoring day-to-day compliance? 4. Training for appropriate personnel? 5. Procedures for personnel to follow if they identify suspicious activity related to money laundering? 6. Compliance with a federal banking agency’s request or information and documentation concerning any account or its BSA compliance in a timely fashion? | |  |  | |  |
|  | Does the institution’s anti-money laundering policy address:   1. The various types of money laundering; 2. Compliance with BSA and related anti-money laundering laws and regulations; 3. a “Customer Identification Program” program; and 4. identify high-risk activities, businesses, and foreign countries (those commonly associated with money laundering)? | |  |  | |  |
|  | Was the compliance program approved by the board of directors and approval noted in the minutes? | |  |  | |  |
|  | Determine if anti-money laundering policies, procedures, and programs cover all areas of the bank, which may include the following:   1. Retail operations and monetary instrument sales. 2. Loan department. 3. Funds transfer function. 4. Safe deposit box rental. 5. Correspondent banking. 6. Sale of non-deposit investment products. | |  |  | |  |
| ***Customer Identification Program - CIP*** | | | | | | |
|  | Evaluate the bank’s CIP to ensure that it addresses the regulatory requirements. Determine whether the bank performed a risk analysis, taking into consideration the types of accounts offered, methods of account opening, and the bank’s size, location, and customer base. Determine also if it designed an appropriate program. The program should be in writing and included within the bank’s BSA program. The program should include, at a minimum, the following:   1. Procedures for obtaining the required identifying information (including name, address, TIN, and date of birth for individuals) and risk-based identity verification procedures (including procedures that address situations where verification cannot be performed). 2. Procedures for complying with recordkeeping requirements. 3. Procedures for checking new accounts against prescribed government lists, if applicable. 4. Procedures for providing adequate customer notice. 5. Procedures covering reliance on another financial institution or another third party, if applicable. 6. Procedures for determining whether/when a SAR should be filed. 7. Adequate internal controls, training, and procedures to ensure that the financial institution monitors and independently tests its compliance with the regulation. | |  |  | |  |
|  | Determine whether the bank’s policy for opening new accounts for existing customers appears reasonable. | |  |  | |  |
|  | Unless reviewed during the BSA program examination, review minutes and verify that the board approved the CIP, either separately or as part of the BSA program. | |  |  | |  |
|  | Evaluate the bank’s systems and controls to check all new accounts against prescribed government lists for suspected terrorists or terrorist organizations on a timely basis in the event such lists are issued. | |  |  | |  |
|  | Based on a risk assessment, prior examination reports, and a review of the bank’s audit findings, select a sample of new accounts to review for compliance with the bank’s CIP. The sample should include a cross-section of accounts (e.g., consumers and businesses, loans and deposits, credit card relationships and Internet accounts). The sample should also include the following:  Accounts   1. Opened with an application for a TIN or opened with incomplete verification procedures, 2. Opened using documentary methods and accounts opened using non-documentary methods, 3. Identified as high-risk by the bank or the regulator (High-risk accounts may include for example, foreign private banking and trust accounts, accounts of senior foreign political officials, offshore accounts, and out-of-area and non-face-to-face accounts). 4. Opened by existing high-risk customers, 5. Opened with exceptions, and 6. Opened by a third party (e.g., indirect loans). | |  |  | |  |
|  | From the above sample of accounts, determine whether the bank:   1. Opened the account in accordance with CIP requirements. 2. Formed a reasonable belief as to the customer’s true identity, including high-risk customers, or had already done so on an existing customer. 3. Obtained from each customer, prior to opening the account, the identity information required by the CIP. 4. Verified, within a reasonable time of account opening, enough of the customer’s identity information to form a reasonable belief as to the customer’s true identity. 5. Resolved situations appropriately where customer identity could not be reasonably established. 6. Maintained a record of the identity information required by the CIP and a record of the method used to verify identity and verification results (including results of discrepancies). 7. Compared the customer’s name against the list of known or suspected terrorists or terrorist organizations, if applicable. 8. Filed SARs, as appropriate. | |  |  | |  |
|  | Evaluate the level of exceptions to determine whether the bank is effectively implementing its CIP (making or approving exceptions cannot be allowed by policy, however, isolated, non-systemic errors [such as an insignificant number of data entry errors] may be deemed as not compromising the program’s effectiveness).   * Obtain a written description of the bank’s rationale for exempting existing customers from its CIP | |  |  | |  |
|  | Based on a risk assessment, prior examination reports, and a review of the bank’s audit, select a sample of relationships with third parties upon whom the bank relies or uses to perform its CIP (or portions of the CIP), if applicable. If the bank is using the “reliance provision:”   1. Determine whether the third party is a federally regulated financial institution subject to the BSA/AML program requirements of 31 U.S.C. 5318(h). 2. Review the contract between the parties, annual certifications, and other information, such as the third party’s CIP. 3. Determine whether reliance is reasonable. The contract and certification will provide a standard means for a bank to demonstrate that it has satisfied the “reliance provision,” unless the examiner has reason to believe that the bank’s reliance is not reasonable (e.g., the third party has been subject to an enforcement action for AML or BSA deficiencies or violations). 4. If the bank is using an agent or service provider to perform elements of its CIP, determine whether its oversight over such a third party is adequate as follows: 5. The bank has established appropriate internal controls and review procedures to ensure that its CIP is being implemented for third-party agent or service-provider relationships (e.g., car dealerships). | |  |  | |  |
|  | Review the adequacy of the bank’s customer notice and timing of the delivery of the notice (31 CFR 1020.220(a)-(c) | |  |  | |  |
|  | Evaluate the bank’s CIP or record retention policy and ensure that it corresponds to the regulatory requirements to maintain certain records (description of documents relied on, of methods used to verify identity, and of the resolution of discrepancies) for five years and other records (identity information) for five years after the account closes. | |  |  | |  |
| Training - TR | | | | | | |
| 1. | Review training procedures:   1. Is the BSA training adequate? The following are items that should be covered in such training:  * Reporting of large currency transactions * Exemptions from large currency transaction reporting * Identifying and reporting of suspicious activity or alleged criminal conduct * Record retention requirements * Sale/purchase of monetary instruments * Review of internal policies/procedures * Examples of money laundering cases and the methods in which activities can be detected/resolved/reported * Overview of the different forms that money laundering can take (deposit accounts, wire transfer loans, etc.) * Wire (fund) transfer activity * CIP procedures  1. Is the frequency of the training adequate? Document which personnel receive regular training and dates of last training received, etc. | |  |  | |  |
| Customer Exemptions – CE | | |  |  | |  |
|  | Determine if the bank has Phase I or Phase II exemptions. If so, verify that the bank maintains a centralized list of customers who are exempt from the large currency transaction reporting requirements, and determine if the list includes:   1. The name, street address, business, taxpayer identification number (TIN), and account number of the customer. 2. A brief description of the customer’s business. | |  |  | |  |
|  | Determine if the bank has revoked any exemptions since the previous examination. If so, determine the reason for the revocation(s) and whether the bank completed FinCEN Form 105 (formerly Form TD F 90-22.53). | |  |  | |  |
|  | Obtain a copy of the BSA exemption list and review the following:  Phase I   1. Determine if FinCEN Form 105 (formerly Treasury Form TD F 90-22.53) “Designation of Exempt Person” has been filed with the Internal Revenue Service for each "exempt person" (as required, note that some Phase I exemptions do not require DOEP) as defined in 31 CFR 1020.315 within 30 days of the first reportable transaction that was exempted. 2. Determine if documentation on file supports Phase I exemptions. 3. Assess whether required annual reviews are performed to determine if a customer remains eligible for exempt designation.     Phase II   1. Determine if Treasury Form TD F 90-22.53 has been filed with the IRS for each "exempt person" identified by bank management. 2. Determine if documentation on file supports Phase II exemptions. 3. Assess whether required annual reviews are performed to determine if a customer remains eligible for exempt designation. | |  |  | |  |
| Currency Transaction Report (CTR) Review – CTR | | |  |  | |  |
| 1. | Does the institution have an adequate system (training and procedures, perhaps an automated system as well) for detecting single or multiple transactions in one business day that exceed $10,000?   1. Are procedures in place for reviewing multiple transactions per customer that would aggregate to more than $10,000 in a day? This review should include monitoring of transactions completed at branches, drive-in facilities, ATMs, main lobby, and so forth. 2. Does the responsible party perform the following:  * Determine whether Transaction amounts are consistent with the type and nature of business or occupation of customer. * File a Suspicious Activity Report for any currency transaction that appeared suspicious. | |  |  | |  |
| 2. | Review new account opening procedures.   1. Determine that procedures are in place to monitor new accounts that are opened with a cash deposit greater than $10,000. 2. Verify that Form 4789 is filed for all such deposits. | |  |  | |  |
| 3. | Based on a sample of all currency transactions during a period of time, did the institution file a CTR for each transaction(s) by non-exempt customers in one business day that exceeded $10,000 (e.g., for a selected period of review, compare the EDP report of transactions greater than $10,000 to completed copies of Form 4789). | |  |  | |  |
| 4. | Verify the following for a sample of CTRs:   1. CTRs are properly completed in accordance with IRS instructions? 2. CTRs are filed within 15 calendar days after the date of the transaction (25 days if magnetically filed)? | |  |  | |  |
| Purchases and Sales of Monetary Instruments – MI | | |  |  | |  |
| 1. | Determine whether the institution retains the following information for all cash sales of monetary instruments involving $3,000 - $10,000 in currency in one business day:   1. Purchasers who have deposit accounts with the institution:  * The name of the purchaser. * The date of purchase. * The types of instruments purchased. * The serial numbers of each of the instruments purchased. * Dollar amount(s) of each of the instrument(s). * Method of verification of identity (either at time of purchase or when deposit account opened).  1. Purchaser does not have a deposit account with the institution:  * The name and address of the purchaser. * The Social Security or Alien Identification Number. * The date of birth of the purchaser. * The date of purchase. * The types of instruments purchased. * The serial numbers of each of the instruments purchased. * Dollar amount(s) of each of the instrument(s). * The document used to verify the purchaser’s name and address. * Specific identifying information (e.g., state driver’s license number).   Notes:   * Multiple purchases during one business day totaling $3,000 or more should be so noted if an employee, director, or officer of the bank has knowledge of these purchases. * Contemporaneous purchases of the same or different types of instruments totaling $3,000 or more shall be treated as one purchase. | |  |  | |  |
| 2. | Based on a review for a sample of records of the sales of monetary instruments for a period of time (i.e., large currency transaction report):   1. Is the information retained adequate to determine the amount of currency received in each sale? 2. Is the required information recorded for each transaction involving $3,000–$10,000 in currency (see step 1 above)? 3. Was a SAR filed for any suspicious transactions? | |  |  | |  |
| Suspicious Activity Report – SAR | | |  |  | |  |
|  | Determine if the compliance program provides an adequate suspicious activity identification and reporting process, and includes the following:   1. An individual responsible for preparing and filing SARs. 2. A process for ensuring that SARs are filed within timeframes established by regulation along with factual and sufficiently detailed content to describe the suspicious activity. 3. A process for ensuring that transaction amounts are consistent with the type and nature of the business or occupation of the customer. 4. A process for reviewing "exempt person" accounts for unusual or suspicious activity. 5. A process for establishing expected activity levels (for example, historical transaction pattern or input from client or bank officer) including who has the authority to change profiles. 6. A process for reconciling activity levels of higher-risk accounts against expected activity to ensure that activity levels are reasonable. 7. A system for reviewing exception reports and what parameters are used to filter exceptions. 8. A process for requesting timely and adequate explanations of activity generated by monitoring reports. 9. A system for ensuring exception reports are responded to in a timely manner and are utilized and maintained by appropriate parties to assist in detecting patterns of unusual activity. 10. A system (automated or manual) to detect structured transactions (both cash in and cash out) that are under the $10,000 threshold. 11. Procedures for documentation of decision not to file a SAR. 12. Procedures for providing notice of SARs filed to the Board of Directors. | |  |  | |  |
|  | Determine that bank management and supervisors are aware of the situations for which a SAR is required to be filed:   1. A SAR should be filed for any known or suspected crime involving $5,000 or more in bank funds and when the bank has a basis of identifying the suspect (e.g., customers who deliberately structure a transaction to avoid a CTR filing). 2. A SAR should be filed for any known or suspected crime involving $25,000 in bank funds even if the bank cannot identify a possible or specific suspect. 3. A SAR should be filed for any individual transaction or combination of transactions totaling $5,000 if: (1) the bank suspects that the funds were derived from illegal activity or the transaction was performed to hide or disguise illegal funds, or (2) the transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining all the facts. 4. A SAR should be filed for any known or suspected crime involving a bank director or employee regardless of dollar amount. | |  |  | |  |
|  | Determine if management is aware of the “safe harbor” rules that prohibit them from revealing any knowledge that a SAR has been filed. | |  |  | |  |
|  | Are personnel prohibited from assisting or permitting customers to structure accounts or transactions to avoid the reporting requirements? | |  |  | |  |
|  | Select a sample of SARs that were filed and determine the following:   1. Was the SAR filed within 30 calendar days after determining a SAR was required (or within 60 days if needed to attempt to identify a suspect)? 2. Does the institution retain a copy of the SAR and any supporting documentation for five years? 3. Did the institution keep the filing of the SAR confidential? | |  |  | |  |
|  | If available, obtain copies of the following internally generated reports. Review the following reports for suspicious activity.   1. Suspected Kiting Reports — These reports identify excessive activity in accounts and should be reviewed for cash activity. (The account profile of an account used for money laundering can be similar to that of an account used for check kiting, i.e., high volume of activity, matching deposits and withdrawals, low average balances in relation to activity.) 2. Demand Deposit Activity Reports — These reports cover all customer and employee accounts. They generally show daily balances and accumulate deposits and withdrawals over a 30-day period. Careful review will show accounts that have changed, either in average balance or in numbers of transactions. 3. Large Transaction or Cash-In and Cash-Out Reports — Most institutions prepare reports of deposits and withdrawals, either in cash or by check that exceed a certain amount that is less than the over $10,000 reporting requirement. Such reports can help identify customers who may be structuring transactions to avoid CTR reporting or who have unusual or suspicious activity in their accounts. 4. Incoming and Outgoing Wire Transfer Logs — These logs can identify transfers of funds out of the country or to remote banks, transfers funded by cashier’s checks and/or money orders in amounts under the CTR filing threshold (over $10,000) and other suspicious patterns for non-customers as well as accountholders. Additionally, review incoming and outgoing facsimile logs for payment instructions related to funds transfers. 5. Loans Listed by Collateral — Review for “significant” loans collateralized by cash (certificates of deposit, bank accounts). Review situations in which collateral was received by funds transfer and the collateral, such as certificates of deposits, is from offshore institutions. Inquire as to the purpose and terms of loans secured largely with cash and whether payments on such loans are often received in cash, if at all. Look for loans from which the proceeds are immediately used to purchase CDs. | |  |  | |  |
|  | Obtain copies of the bank statement for the institution’s major correspondent bank for a period of at least two months, together with reconcilement sheets and general ledger sheets covering the same period. Review large transactions reflected on either the institution’s or the correspondent’s records to determine their nature, as indicated by copies of credit or debit advices, or general ledger tickets. Look at the following items for suspicious activities:   1. Advice of credit from a correspondent bank that cash has been transmitted to the correspondent for credit to the account of the customer initiating the cash shipment on the books of the institution under examination. 2. Cashier checks, money orders, or similar instruments drawn on other institutions in amounts under $10,000, more than one of which have been deposited into the same deposit account, or into accounts controlled by the same person, at the institution under examination, and possibly transferred elsewhere in bulk amounts. Traces of such transactions may be found in correspondent account statements, customer account records, or in telex records. Note whether the instruments under $10,000 are sequentially numbered. | |  |  | |  |
| Electronic Banking - EB | | |  |  | |  |
| 1. | Based on a review of procedures used to conduct due diligence on customers opening accounts (loan or deposit) through electronic means, does the institution obtain proper verification of customer identity and source of funds used to open deposit accounts? | |  |  | |  |
| 2. | Has management established and followed procedures to review transaction activity through electronic banking products for possible money laundering and suspicious activity? | |  |  | |  |
| Wire Transfer Recordkeeping - WT | | |  |  | |  |
| **Originating Bank:** | | |  |  | |  |
| 1. | Determine that the bank maintains records on all wire transfers in amounts of $3,000 or more accepted from an originator who is an established customer. Verify that the records include:   1. Originator’s name, address, and account number. 2. Amount of payment order. 3. Execution date of payment order. 4. Payment instructions received from originator with payment order. 5. Identity of the beneficiary’s bank. 6. As many of the following as are received with the payment order:  * The beneficiary’s name, address, and account number, and any other specific identifier of the beneficiary. | |  |  | |  |
| 2. | If the originator ***does not*** have an established relationship with the institution, does institution also retain the following information:   1. The name and address of the person placing the payment order; 2. Their TIN (if none, alien identification or passport number and country of issuance, or a notation of no such record); and 3. A record of the method of payment? 4. If the institution knows that the person placing the payment order is not the originator, does it retain the originator’s TIN (if none, alien identification number or passport number and country of issuance, if known, or a notation of no such record)? 5. If the payment order is made in person, does the institution verify the identity of the person placing the order and retain a record of the type of ID reviewed and the ID number? | |  |  | |  |
| **Intermediary Bank:** | | |  |  | |  |
| 1. | For funds transfers of $3,000 or more, does the institution retain the original, a microfilm, other copy, or electronic record of the payment order? | |  |  | |  |
| 2. | For transmittals of funds of $3,000 or more, does the institution include in the transmittal order to the next receiving financial institution the following, if received from the sender):   1. The name and, if the payment is ordered from an account, the account number of the transmitter? 2. The address of the transmitter (except non-expanded Fedwire)? 3. The amount of the transmittal order? 4. The execution date of the transmittal order? 5. The identity of the recipient’s financial institution? 6. As many of the following items as are received with the transmittal order (1 item if non-expanded Fedwire format):  * Name and address of the recipient; * Account number of the recipient; * Any other specific identifier of the recipient.  1. Either the name and address or numerical identifier of the transmitter’s institution? | |  |  | |  |
| **Beneficiary Bank:** | | |  |  | |  |
| 1. | For each payment order of $3,000 or more that an institution accepts as a beneficiary bank, does the institution retain either the original or a microfilm, other copy, or electronic record of the payment order? | |  |  | |  |
| 2. | If the beneficiary ***does not*** have an established relationship with the institution, does institution also retain the following information:   1. If the proceeds are delivered in person:  * The name and address of the person receiving the proceeds; * That person’s TIN (if none, alien identification number or passport number and country of issuance, or a notation of no such record)?  1. If the proceeds are not delivered in person:  * A copy of the check or other instrument used for payment, or the information contained on it, as well as the name and address of the person to which it was sent? | |  |  | |  |
| 3. | If the institution knows that the person placing the payment order is not the originator, does it retain the beneficiary’s TIN (if none, alien identification number or passport number and country of issuance, if known, or a notation of no such record)? | |  |  | |  |
| **Information Retrievability:** | | |  |  | |  |
| 1. | Are the retained records retrievable by the name of originator (for originated transfers) and name of beneficiary (for received transfers), and, if they are established customers, by account number? | |  |  | |  |
| **Internal Controls:** | | |  |  | |  |
| 1. | Is there adequate separation of duties or compensating controls to ensure proper authorization for sending and receipt of transfers, correct posting to accounts, and an audit trail of activities? | |  |  | |  |
| 2. | Does the institution accept cash for funds transfers and, if so, does the institution require identification, maintain documentation, and file CTRs, if applicable? | |  |  | |  |
| 3. | Does the institution send or receive fund transfers to/from financial institutions in other countries, especially countries with strict privacy and secrecy laws, and, if so, are amounts, frequency, and countries of origin/destination consistent with the nature of the business or occupation of the customer? | |  |  | |  |
| 4. | Does the institution have procedures to monitor for accounts with frequent cash deposits and subsequent wire transfers of funds to a larger institution or out of the country? | |  |  | |  |
| Record Retention - RR | | |  |  | |  |
| 1. | Does the institution maintain the records required by the Secretary of the Treasury under the Bank Secrecy Act for five years (either the original or a microfilm or other copy or reproduction)? | |  |  | |  |
| Domestic Correspondent Banking Activities - DCB | | |  |  | |  |
| 1. | Review the policies, procedures, and processes, and any bank service agreements related to domestic correspondent banking relationships. Evaluate the adequacy of the policies, procedures, and processes given the bank's domestic correspondent accounts and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank has identified any domestic correspondent banking activities as high risk. | |  |  | |  |
| 3. | Determine whether the bank's system for monitoring domestic correspondent accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 4. | On the basis of the bank's review of respondent accounts with unusual or high-risk activity, its risk assessment, and prior examination and audit reports, select a sample of respondent accounts. From the sample selected, perform the following audit procedures:  Review bank statements for domestic correspondent accounts.  Review large or unusual transactions to determine their nature. As necessary, obtain and review copies of credit or debit advices, general ledger tickets, and other supporting documentation.  Note any currency shipments or deposits made on behalf of a respondent bank's customer. Based on this information, determine whether:   * Currency shipments are adequately documented. * The respondent bank has performed due diligence on customers that conduct large currency transactions. * Currency Transaction Reports (CTRs) are properly filed and activity is commensurate with expected activity. | |  |  | |  |
| 5. | Review the bank statements for domestic correspondent account records, or telex records of accounts controlled by the same person for large deposits of cashier's checks, money orders, or similar instruments drawn on other banks in amounts under $10,000. These funds may possibly be transferred elsewhere in bulk amounts. Note whether the instruments under $10,000 are sequentially numbered. | |  |  | |  |
|  |  | |  |  | |  |
| ***Office of Foreign Assets (OFAC) Restrictions – OF*** | | |  |  | |  |
| 1. | Does the institution have policies and procedures in place for complying with OFAC laws and regulations?   1. Does the U.S. bank maintain a current listing of prohibited countries, entities, and individuals? 2. Are new accounts compared to OFAC listings prior to opening? 3. Are established accounts and wire transfers regularly compared to current OFAC listings? | |  |  | |  |
| USA Patriot Act – PA | | |  |  | |  |
| 1. | For each correspondent account maintained in the US for a foreign bank, has the institution obtained certification from the foreign bank that:   1. Identifies the owners of each correspondent foreign bank whose shares are not publicly traded, and 2. Identifies the name and street address of a person who resides in the US and is authorized, and has agreed to be an agent to accept service of legal process for records regarding each correspondent account. 3. Does the institution obtain a recertification of the above at least once every three years? | |  |  | |  |
| **Foreign Correspondent Banking:** | | |  |  | |  |
| 1. | Does the institution refrain from establishing, maintaining, administering, or managing correspondent accounts in the United States for foreign “shell” banks? | |  |  | |  |
| 2. | Has the institution obtained the certification from the foreign bank that its foreign correspondent accounts are not being used by that foreign bank to provide indirect banking services to a foreign shell bank?   * Does the institution obtain a recertification of the above at least once every three years? | |  |  | |  |
| **International Transportation of Currency:** | | |  |  | |  |
| 1. | Determine whether the bank has (or has caused to be) physically transported, mailed, or shipped currency or other monetary instruments in excess of $10,000, at one time, out of the United States, or whether the bank has received currency or other monetary instruments in excess of $10,000, at one time, that has been physically transported, mailed, or shipped into the United States. | |  |  | |  |
| 2. | If applicable, review the bank's policies, procedures, and processes for filing a Report of International Transportation of Currency or Monetary Instruments (CMIR) (FinCEN Form 105) for each shipment of currency or other monetary instruments in excess of $10,000 out of or into the United States (except for shipments sent through the postal service, common carrier, or to which another exception from CMIR reporting applies). | |  |  | |  |
| 3. | On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of transactions conducted after the previous examination to determine whether the bank has appropriately completed, submitted, and retained copies of the CMIR forms. | |  |  | |  |
| **Certification:** | | |  |  | |  |
| 1. | If at any time the financial institution knows, suspected, or had reason to suspect, that any information contained in a certification or recertification provided by a foreign bank, was no longer correct, did the institution request that the foreign bank verify or correct such information, or take other appropriate measures to ascertain the accuracy of the information or to obtain correct information, as appropriate?   * If the financial institution has taken the above steps to verify or obtain corrected information from a foreign correspondent bank, if the institution has not obtained verification of the information or the corrected information within 90 calendar days after the date of undertaking the verification, did the institution close all correspondent accounts with the foreign bank within a commercially reasonable time, and prohibit the foreign bank from establishing any new positions or execute any transactions through the account, other than transactions necessary to close the account? | |  |  | |  |
| 2. | For any correspondent account that was in existence on October 28, 2002, did the institution obtain a certification (or recertification) from the foreign bank on or before December 26, 2002?   * If not, did the institution then close all correspondent accounts with such foreign bank within a commercially reasonable time, and prohibit the foreign bank from establishing any new positions or execute any transactions through the account, other than transactions necessary to close the account. | |  |  | |  |
| 3. | For any correspondent account established after October 28, 2002, did the institution obtain a certification (or recertification), or other documentation of the information required by the certification (or recertification) within 30 calendar days after the date the account was established, and every three years thereafter?   * If not, did the institution close all correspondent accounts with the foreign bank within a commercially reasonable time, and prohibit the foreign bank from establishing any new positions or execute any transactions through the account, other than transactions necessary to close the account? | |  |  | |  |
| **Recordkeeping:** | | |  |  | |  |
| 1. | Does the institution retain the original of any document provided by a foreign bank, and the original or a copy of any other document(s) relied for compliance with this rule, for at least 5 years after the date that the institution no longer maintains any correspondent account for the foreign bank? | |  |  | |  |
| **Summons/Subpoena of Foreign Bank Records:** | | |  |  | |  |
| 1. | Upon receipt of a written request from a Federal law enforcement officer for the foreign correspondent bank owner and agent for service of process information, did the institution provide the information to the requesting officer not later than 7 days after receipt of the request? | |  |  | |  |
| 2. | Did the institution terminate any correspondent relationship with a foreign bank within 10 business days after receipt of written notice from the Secretary or the Attorney General that the foreign bank has failed:   * To comply with a summons or subpoena issued under; or * To initiate proceedings in a United States court contesting such summons or subpoena? | |  |  | |  |
| **Correspondent Accounts and Private Banking Accounts:** | | |  |  | |  |
| 1. | Does the institution have appropriate, specific and, where necessary, enhanced due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering through private banking accounts or correspondent accounts? | |  |  | |  |
| 2. | If the institution maintains correspondent accounts or private banking accounts for foreign banks under the specified circumstances, does it have the required additional due diligence for money laundering that it follows? | |  |  | |  |
| 3. | If the institution offers private banking accounts, does it, at a minimum, identify the nominal and beneficial owners of the account and the account’s source of funds and report suspicious transactions, and conduct enhanced scrutiny of any account requested or maintained by a “senior foreign political figure, or any immediate family member or close associate” to detect transactions that may involve proceeds of foreign corruption? | |  |  | |  |
| **Information Sharing with Law Enforcement:** | | |  |  | |  |
| 1. | Has the financial institutions designated one person to be the point of contact at the institution regarding information requests and provided any other contact information requested by FinCEN?   * If any of the contact information has changed, did the financial institution promptly notify FinCEN of the changes? | |  |  | |  |
| 2. | For any requests received from FinCEN for information under the rule, did the institution “expeditiously” (or within the time period required in the request) search their records to determine whether it maintains or has maintained any account for, or has engaged in any transaction with, each individual, entity, or organization named in FinCEN’s request? | |  |  | |  |
| 3. | In response to the request, unless otherwise provided in the request itself, did the institution search its records for:   * Any current account maintained for a named suspect; * Any account maintained for a named suspect during the preceding twelve months; and * Any transaction conducted by or on behalf of a named suspect, or any transmittal of funds conducted in which a named suspect was either the transmitter or the recipient, during the preceding *six months* that is contained in the wire transfer log, the log of purchase/sales of monetary instruments, and any other transaction records that can be searched electronically? | |  |  | |  |
| 4. | If, as a result of the searches, the financial institution did find an account or transaction with any of the individuals or entities, did the institution report the following information to FinCEN, within the time frame specified in the request:   * The name of the individual, entity, or organization; * The number of each account, or in the case of a transaction, the date and type of each transaction; and * Any Social Security #, taxpayer identification #, passport #, date of birth, address, or other similar identifying information provided by the individual, entity, or organization when each account was opened or each transaction was conducted? | |  |  | |  |
| 5. | Did the institutions use the information provided by FinCEN only for the purpose of:   * Reporting to FinCEN as required by the rule; * Determining whether to establish or maintain an account, or to engage in a transaction; or * Assisting the financial institution in complying with any requirement of the rule. | |  |  | |  |
| **Information Sharing Among Financial Institutions:** | | |  |  | |  |
| 1. | Before engaging in the sharing of information with other financial institutions or associations, did the institution file the required notice with FinCEN (or a certification with FinCEN under the interim rules)?   * Does the institution submit a new certification each year? | |  |  | |  |
| 2. | Does the institution only share information under the rule regarding individuals, entities, organizations, and countries for purposes of detecting, identifying, or reporting activities that the financial institution or association suspects may involve possible money laundering or terrorist activities? | |  |  | |  |
| 3. | Before sharing information under the rule, does the institution take reasonable steps to verify that the other financial institution or association has also submitted the required notice to FinCEN | |  |  | |  |
| 4. | With respect to any information received as a result of sharing information under the rule, did the institution use the information for no other purpose other than:   * Identifying and, where appropriate, reporting on money laundering or terrorist activities; * Determining whether to establish or maintain an account, or to engage in a transaction; or * Assisting the financial institution in complying with any requirement of the BSA rules? | |  |  | |  |
| 5. | Does the institution maintain adequate procedures to protect the security and confidentiality of the information? | |  |  | |  |
| 6. | If, as a result of information sharing under the rule, the institution suspected that someone is or may be involved in terrorist activity, was the information reported on a SAR and/or otherwise as required? | |  |  | |  |
| Customer Due Diligence – CD | | |  |  | |  |
| 1. | Determine whether the CDD policies, procedures, and processes are commensurate with the organization's risk profile. Determine whether the organization has processes in place for obtaining information at account opening, in addition to ensuring current customer information is maintained. | |  |  | |  |
| 2. | Determine whether policies, procedures, and processes allow for changes to a customer's risk rating or profile. Determine who is responsible for reviewing or approving such changes. | |  |  | |  |
| 3. | Review the enhanced due diligence procedures and processes the organization uses to identify customers that may pose higher risk for money laundering or terrorist financing. | |  |  | |  |
| 4. | Determine whether the organization provides guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient information or inaccurate information is obtained. | |  |  | |  |
| 5. | On the basis of a risk assessment, prior examination reports, and a review of the organization's audit findings, sample CDD information for high risk customers. Determine whether the organization collects appropriate information and effectively incorporates this information into the suspicious activity monitoring process. This sample can be performed when testing the organization's compliance with its policies, procedures, and processes as well as when reviewing transactions or accounts for possible suspicious activity. | |  |  | |  |
| Special Measures - SM | | |  |  | |  |
| 1. | Determine the extent of the Bank’s international banking activities and the foreign jurisdictions in which the bank conducts transactions and activities, with particular emphasis on foreign correspondent banking and payable through accounts. As applicable, determine whether the bank has established policies, procedures, and processes to respond to specific special measures imposed by FinCEN that are applicable to its operations. Determine whether the bank has taken action in response to final special measures. | |  |  | |  |
| 2. | Determine all final measures issued by FinCEN under Section 311 that are applicable to the bank (from FinCEN website). For any of the first four types of special measures, determine whether the bank obtained, recorded, or reported the information required by each particular special measure. For the fifth measure (prohibition), determine whether the bank complied with the prohibitions or restrictions required with all actions required by the special measures. | |  |  | |  |
| U.S. Dollar Drafts - DD | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to U.S. dollar drafts. Evaluate the adequacy of the policies, procedures, and processes given the bank's U.S. dollar draft activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. Determine whether the policies address the following:   * Criteria for allowing a foreign financial institution or entity to issue the U.S. bank's dollar drafts. * Identification of unusual transactions (e.g., structuring transactions or the purchase of multiple sequentially numbered U.S. dollar drafts to the same payee). * Criteria for ceasing U.S. dollar draft issuance through a foreign financial institution or entity. | |  |  | |  |
| 2. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors high-risk U.S. dollar draft accounts. | |  |  | |  |
| 3. | Determine whether the bank's system for monitoring U.S. dollar draft accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 4. | Obtain a list of foreign bank correspondent accounts in which U.S. dollar drafts are offered. Review the volume, by number and dollar amount, of monthly transactions for each account. Determine whether management has appropriately assessed risk. | |  |  | |  |
| 5. | On the basis of the bank's risk assessment of its U.S. dollar draft activities, as well as prior examination and audit reports, select a sample of foreign correspondent bank accounts in which U.S. dollar drafts are processed. In the sample selected, include accounts with a high volume of U.S. dollar draft activity. From the sample selected, perform the following examination procedures:   * Review transactions for sequentially numbered U.S. dollar drafts to the same payee or from the same remitter. Research any unusual or suspicious U.S. dollar draft transactions. * Review the bank's contracts and agreements with foreign correspondent banks. Determine whether contracts address procedures for processing and clearing U.S. dollar drafts. * Verify that the bank has obtained and reviewed information about the foreign financial institution's home country AML regulatory requirements (e.g., customer identification and suspicious activity reporting). | |  |  | |  |
| Payable Through Accounts - PTA | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to PTAs. Evaluate the adequacy of the policies, procedures, and processes given the bank's PTA activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. Determine whether:  Criteria for opening PTA relationships with a foreign financial institution are adequate.  Appropriate information has been obtained and validated from the foreign financial institution concerning the identity of any persons having authority to direct transactions through the PTA.  Information and enhanced due diligence have been obtained from the foreign financial institution concerning the source and beneficial ownership of funds of persons who have authority to direct transactions through the PTA.  Sub-accounts are not opened before the bank has reviewed and approved the customer information.  Master or sub-accounts can be closed if the information provided to the bank has been materially inaccurate or incomplete.  The bank can identify all signers on each sub-account. | |  |  | |  |
| 2. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors PTA accounts. | |  |  | |  |
| 3. | Determine whether the bank's system for monitoring PTA accounts for suspicious activities, and reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 4. | To assess the volume of risk and determine whether adequate resources are allocated to the oversight and monitoring activity, obtain a list of foreign correspondent bank accounts in which PTAs are offered and request MIS reports that show:  The number of sub-accounts within each PTA.  The volume and dollar amount of monthly transactions for each sub-account. | |  |  | |  |
| 5. | Verify that the bank has obtained and reviewed information concerning the foreign financial institution's home country AML regulatory requirements (e.g., customer identification requirements and suspicious activity reporting) and considered these requirements when reviewing PTAs. Determine whether the bank has ensured that sub‑account agreements comply with any AML statutory and regulatory requirements existing in the foreign financial institution's home country. | |  |  | |  |
| 6. | On the basis of the bank's risk assessment of its PTA activities, as well as prior examination and audit reports, select a sample of PTAs. From the sample, review the contracts or agreements with the foreign financial institution. Determine whether the contracts or agreements:  Clearly outline the contractual responsibilities of both the U.S. bank and the foreign financial institution.  Define PTA and sub-account opening procedures and require an independent review and approval process when opening the account.  Require the foreign financial institution to comply with its local AML requirements.  Restrict sub-accounts from being opened by casas de cambio, finance companies, funds remitters, or other non-bank financial institutions.  Prohibit multi-tier sub-accountholders.  Provide for proper controls over currency deposits and withdrawals by sub-accountholders and ensure that Currency Transaction Reports (CTRs) have been appropriately filed.  Provide for dollar limits on each sub-accountholder's transactions that are consistent with expected account activity.  Contain documentation requirements that are consistent with those used for opening domestic accounts at the bank.  Provide the bank with the ability to review information concerning the identity of sub-accountholders.  Require the foreign financial institution to monitor sub-account activities for unusual or suspicious activity and report findings to the bank.  Allow the bank, as permitted by local laws, to audit the foreign financial institution's PTA operations and to access PTA documents. | |  |  | |  |
| 7. | Review PTA master-account bank statements. Determine the time period based upon the size and complexity of the bank. The statements chosen should include frequent transactions and those of large dollar amounts. Verify the statements to the general ledger and bank reconcilements. Note any currency shipments or deposits made at the bank on behalf of an individual sub-accountholder for credit to the customer's sub-account. | |  |  | |  |
| 8. | From the sample selected, review each sub-accountholder's identifying information and related transactions. Evaluate the transactions and determine whether the transactions are consistent with expected transactions or warrant further research. | |  |  | |  |
| Pouch Activities – PA | | |  |  | |  |
| 1. | Determine whether the bank has incoming or outgoing pouch activity and whether the activity is via carrier or courier. | |  |  | |  |
| 2. | Review the policies, procedures, and processes, and any contractual agreements related to pouch activities. Evaluate the adequacy of the policies, procedures, and processes given the bank's pouch activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 3. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors pouch activities. | |  |  | |  |
| 4. | Determine whether the bank's system for monitoring pouch activities for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 5. | Review the list of bank customers permitted to use pouch services (incoming and outgoing). Determine whether management has assessed the risk of the customers permitted to use this service. | |  |  | |  |
| 6. | On the basis of the bank's risk assessment of its pouch activities, as well as prior examination and audit reports, and recent activity records, select a sample of daily pouches for review. Observe the pouch opening and data capture process for items contained in a sample of incoming pouches, and observe the preparation of outgoing pouches. Review the records and the pouch contents for currency, monetary instruments, bearer securities, stored value cards, gems, art, illegal substances or contraband, or other items that should not ordinarily appear in a bank's pouch. | |  |  | |  |
| 7. | If the courier, or referral agent who works for the courier, has an account with the bank, review an appropriate sample of their account activity. | |  |  | |  |
| Electronic Cash (E-Cash) – EC | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to e-cash. Evaluate the adequacy of the policies, procedures, and processes given the bank's e-cash activities and the risk they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors high-risk e-cash transactions. | |  |  | |  |
| 3. | Determine whether the bank's system for monitoring e-cash transactions for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 4. | On the basis of the bank's risk assessment of its e-cash activities, as well as prior examination and audit reports, select a sample of e-cash transactions. From the sample selected perform the following audit procedures:  Review account opening documentation, including Customer Identification Program (CIP) and transaction history.  Compare expected activity with actual activity.  Determine whether the activity is consistent with the nature of the customer's business.  Identify any unusual or suspicious activity. | |  |  | |  |
| Third Party Payment Processors – TPP | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to third-party payment processors (processors). Evaluate the adequacy of the policies, procedures, and processes given the bank's processor activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors processor relationships, particularly those that pose a high risk for money laundering. | |  |  | |  |
| 3. | Determine whether the bank's system for monitoring processor accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 4. | On the basis of the bank's risk assessment of its processor activities, as well as prior examination and audit reports, select a sample of high-risk processor accounts. From the sample selected:  Review account opening documentation and ongoing due diligence information.  Review account statements and, as necessary, specific transaction details to determine how expected transactions compare with actual activity.  Determine whether actual activity is consistent with the nature of the processor's stated activity.  Identify any unusual or suspicious activity. | |  |  | |  |
| Brokered Deposits – BD | | |  |  | |  |
| 1. | 1. Review the policies, procedures, and processes related to deposit broker relationships. Evaluate the adequacy of the policies, procedures, and processes given the bank's deposit broker activities and the risks that they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | 1. From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors deposit broker relationships, particularly those that pose a high risk for money laundering. | |  |  | |  |
| 3. | 1. Determine whether the bank's system for monitoring deposit broker relationships for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 4. | 1. On the basis of the bank's risk assessment of its brokered deposit activities, as well as prior examination and audit reports, select a sample of high-risk deposit broker accounts. When selecting a sample, examiners should consider the following:   New relationships with deposit brokers.  The method of generating funds.  Types of customers.  A deposit broker that has appeared in the bank's Suspicious Activity Reports.  Subpoenas served on the bank for a particular deposit broker.  Foreign funds providers.  Unusual activity. | |  |  | |  |
| 5. | 1. Review customer due diligence information on the deposit broker. For deposit brokers who are considered high risk, assess whether the following information is available:   Background and references.  Business and marketing methods.  Client acceptance and due diligence practices.  The method for or basis of the broker's compensation or bonus program.  The broker's source of funds.  Anticipated activity or transaction types and levels. | |  |  | |  |
| Privately Owned ATMS | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to privately owned ATM accounts. Evaluate the adequacy of the policies, procedures, and processes given the bank's privately owned ATM and ISO relationships and the risk they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors privately owned ATM accounts. | |  |  | |  |
| 3. | Determine whether the bank's system for monitoring privately owned ATM accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 4. | Determine whether the bank sponsors network membership for ISOs. If the bank is a sponsoring bank, review contractual agreements with networks and the ISOs to determine whether due diligence procedures and controls are designed to ensure that ISOs are in compliance with network rules. Determine whether the bank obtains information from the ISO regarding due diligence on its sub-ISO arrangements. | |  |  | |  |
| 5. | On the basis of the bank's risk assessment of its privately owned ATM and ISO relationships, as well as prior examination and audit reports, select a sample of privately owned ATM accounts. From the sample selected, perform the following audit procedures:  Review the bank's customer due diligence (CDD) information.  Determine whether the information adequately verifies the ISO's identity and describes its:   * background. * source of funds. * anticipated activity or transaction types and levels. * ATMs (size and location). * currency delivery arrangement, if applicable.   Review any MIS reports the bank uses to monitor ISO accounts. Determine whether the flow of funds or expected activity is consistent with the CDD information. | |  |  | |  |
| 6. | Determine whether a sponsored ISO uses third-party providers or servicers to load currency, maintain ATMs, or solicit merchant locations. If yes, review a sample of third-party service agreements for proper due diligence and control procedures. | |  |  | |  |
| Nondeposit Investment Products – NDIP | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to NDIP. Evaluate the adequacy of the policies, procedures, and processes given the bank's NDIP activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | From a review of management information systems (MIS) reports (e.g., exception reports, funds transfer reports, and activity monitoring reports) and internal risk rating factors, determine whether the bank effectively identifies and monitors NDIP, particularly those that pose a high risk for money laundering. | |  |  | |  |
| 3. | Determine how the bank includes NDIP sales activity in its enterprise-wide BSA/AML aggregation system. | |  |  | |  |
| 4. | Determine whether the bank's system for monitoring NDIP and for reporting suspicious activities is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 5. | On the basis of the bank's risk assessment of its NDIP activities, as well as prior examination and audit reports, select a sample of high risk NDIP. From the sample selected, perform the following audit procedures:  Review appropriate documentation, including CIP, to ensure that adequate due diligence has been performed and appropriate records are maintained.  Review account statements and, as necessary, specific transaction details for:   * expected transactions with actual activity. * holdings in excess of the customer's net worth. * irregular trading patterns (e.g., incoming funds transfers to purchase securities followed by delivery of securities to another custodian shortly thereafter).   Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the account. Identify any unusual or suspicious activity. | |  |  | |  |
| Insurance – IN | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to insurance sales. Evaluate the adequacy of the policies, procedures, and processes given the bank's insurance sales activities, its role in insurance sales, and the risks the insurance sales present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | Review the contracts and agreements for the bank's networking arrangements with affiliates, operating subsidiaries, or other third-party insurance providers conducting sales activities on bank premises on behalf of the bank. | |  |  | |  |
| 3. | Depending on the bank's responsibilities as set forth in the contracts and agreements, review management information systems (MIS) reports (e.g., large transaction reports, single premium payments, early policy cancellation records, premium overpayments, and assignments of claims) and internal risk rating factors. Determine whether the bank effectively identifies and monitors covered insurance product sales. | |  |  | |  |
| 4. | Depending on the bank's responsibilities as set forth in the contracts and agreements, determine whether the bank's system for monitoring covered insurance products for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 5. | On the basis of the bank's risk assessment of its insurance sales activities, as well as prior examination and audit reports, select a sample of covered insurance products. From the sample selected, perform the following examination procedures:  Review account opening documentation and ongoing due diligence information.  Review account activity. Compare anticipated transactions with actual transactions.  Determine whether activity is unusual or suspicious. | |  |  | |  |
| Concentration Accounts - CA | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to concentration accounts. Evaluate the adequacy of the policies, procedures, and processes in relation to the bank's concentration account activities and the risks they represent. | |  |  | |  |
| 2. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors concentration accounts. | |  |  | |  |
| 3. | Review the general ledger and identify any concentration accounts. After discussing concentration accounts with management and conducting any additional research needed, obtain and review a list of all concentration accounts and the bank's most recent reconcilements. | |  |  | |  |
| 4. | Determine whether the bank's system for monitoring concentration accounts for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 5. | On the basis of the bank's risk assessment of its concentration accounts, as well as prior examination and audit reports, select a sample of concentration accounts. From the sample selected, perform the following audit procedures:  Obtain account activity reports for selected concentration accounts.  Evaluate the activity and select a sample of transactions passing through different concentration accounts for further review.  Focus on high-risk activity (e.g., funds transfers or monetary instruments purchases) and transactions from high-risk jurisdictions. | |  |  | |  |
| Lending Activities - LA | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to lending activities. Evaluate the adequacy of the policies, procedures, and processes given the bank's lending activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors high-risk loan accounts. | |  |  | |  |
| 3. | Determine whether the bank's system for monitoring loan accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 4. | On the basis of the bank's risk assessment of its lending activities, as well as prior examination and audit reports, select a sample of high-risk loan accounts. From the sample selected, perform the following audit procedures:  Review account opening documentation, including CIP, to ensure that adequate due diligence has been performed and that appropriate records are maintained.  Review, as necessary, loan history.  Compare expected transactions with actual activity.  Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the loan. Identify any unusual or suspicious activity. | |  |  | |  |
| Trade Finance Activities - TFA | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to trade finance activities. Evaluate the adequacy of the policies, procedures, and processes governing trade finance-related activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | Evaluate the adequacy of the due diligence information the bank obtains for the customer's files. Determine whether the bank has processes in place for obtaining information at account opening, in addition to ensuring current customer information is maintained. | |  |  | |  |
| 3. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors the trade finance portfolio for suspicious or unusual activities, particularly those that pose a higher risk for money laundering. | |  |  | |  |
| 4. | Determine whether the bank's system for monitoring trade finance activities for suspicious activities, and for reporting of suspicious activities, is adequate, given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 5. | On the basis of the bank's risk assessment of its trade finance portfolio, as well as prior examination and audit reports, select a sample of trade finance accounts. From the sample selected, review customer due diligence documentation to determine whether the information is commensurate with the customer's risk. Identify any unusual or suspicious activities. | |  |  | |  |
| 6. | Verify whether the bank monitors the trade finance portfolio for potential OFAC violations and unusual transactional patterns and conducts and records the results of any due diligence. | |  |  | |  |
| Private Banking Activities - PB | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to private banking activities. Evaluate the adequacy of the policies, procedures, and processes given the bank's private banking activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | From a review of management information systems (MIS) reports (e.g., customer aggregation, policy exception and missing documentation, customer risk classification, unusual accounts activity, and client concentrations) and internal risk rating factors, determine whether the bank effectively identifies and monitors private banking relationships, particularly those that pose a higher risk for money laundering. | |  |  | |  |
| 3. | Determine whether the bank's system for monitoring private banking relationships for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 4. | Review the private banking compensation program. Determine whether it includes qualitative measures that are provided to employees to comply with account opening and suspicious activity monitoring and reporting requirements. | |  |  | |  |
| 5. | Review the monitoring program the bank uses to oversee the private banking relationship manager's personal financial condition and to detect any inappropriate activities. | |  |  | |  |
| 6. | On the basis of the bank's risk assessment of its private banking activities, as well as prior examination and audit reports, select a sample of private banking accounts. The sample should include the following types of accounts:  Politically exposed persons (PEPs).  Private investment companies (PICs), international business corporations, and shell companies.  Offshore entities.  Cash-intensive businesses.  Import or export companies.  Customers from or doing business in a high-risk geographic location.  Customers listed on unusual activity monitoring reports.  Customers who have large dollar transactions and frequent funds transfers. | |  |  | |  |
| 7. | From the sample selected, perform the following audit procedures:  Review account opening documentation and ongoing due diligence information.  Review account statements and, as necessary, specific transaction details.  Compare expected transactions with actual activity.  Determine whether actual activity is consistent with the nature of the customer's business.  Identify any unusual or suspicious activity. | |  |  | |  |
| Trust and Asset Management Services - TMS | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to trust and asset management services. Evaluate the adequacy of the policies, procedures, and processes given the bank's trust and asset management activities and the risks they present. Assess whether the controls are adequate to reasonably protect the bank form money laundering and terrorist financing. | |  |  | |  |
| 2. | Review the bank's procedures for gathering additional identification information, when necessary, about the settler, grantor, trustee, or other persons with authority to direct a trustee, and who thus have authority or control over the account, in order to establish a true identity of the customer. | |  |  | |  |
| 3. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors trust and asset management relationships, particularly those that pose a high risk for money laundering. | |  |  | |  |
| 4. | Determine how the bank includes trust and asset management relationships in an enterprise-wide BSA/AML aggregation system. | |  |  | |  |
| 5. | Determine whether the bank's system for monitoring trust and asset management relationships for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 6. | On the basis of the bank's risk assessment of its trust and asset management relationships, as well as prior examination and audit reports, select a sample of high-risk trust and asset management services relationships. Include relationships with grantors and co-trustees, if they have authority or control, as well as any high-risk assets such as Private Investment Companies (PICs) or asset protection trusts. From the sample selected, perform the following audit procedures:  Review account opening documentation, including the Customer Identification Program (CIP), to ensure that adequate due diligence has been performed and that appropriate records are maintained.  Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity.  Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the account.  Identify any unusual or suspicious activity. | |  |  | |  |
| Non-Resident Aliens and Foreign Individuals - NRA | | |  |  | |  |
| 1. | Review the bank's policies, procedures, and processes related to NRA and foreign individual accounts. Evaluate the adequacy of the policies, procedures, and processes given the bank's nonresident alien and foreign individual activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | From a review of management information systems (MIS) and internal risk-rating factors, determine whether the bank effectively identifies and monitors high-risk NRA and foreign individual accounts. | |  |  | |  |
| 3. | Determine whether the bank's system of monitoring NRA and foreign individual accounts for suspicious activities, and for reporting of suspicious activities, is adequate based on the complexity of the bank's NRA and foreign individual relationships, the types of products used by NRAs and foreign individuals, the home countries of NRAs, and the source of funds and wealth for NRAs and foreign individuals. | |  |  | |  |
| 4. | On the basis of the bank's risk assessment of its NRA and foreign individual accounts, as well as prior examination and audit reports, select a sample of high-risk NRA accounts. Include the following risk factors:  An account for resident or citizen of a high-risk jurisdiction.  Account activity is substantially currency based.  An NRA or foreign individual who uses a wide range of bank services, particularly correspondent services.  An NRA or foreign individual for whom the bank has filed a Suspicious Activity Report (SAR). | |  |  | |  |
| 5. | From the sample selected, perform the following audit procedures:  Review the customer due diligence information, including Customer Identification Program information, if applicable.  Review account statements and, as necessary, transaction details to determine whether actual account activity is consistent with expected activity. Assess whether transactions appear unusual or suspicious.  For W-8 accounts, verify that appropriate forms have been completed and updated, as necessary. Review transaction activity and identify patterns that indicate U.S. resident status or indicate other unusual and suspicious activity. | |  |  | |  |
| Politically Exposed Persons – PEP | | |  |  | |  |
| 1. | Review the risk-based policies, procedures, and processes related to PEPs. Evaluate the adequacy of the policies, procedures, and processes given the bank's PEP accounts and the risks they present. Assess whether the risk-based controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | Review the procedures for opening PEP accounts. Identify management's role in the approval and ongoing risk-based monitoring of PEP accounts. | |  |  | |  |
| 3. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors PEP relationships, particularly those that pose a high risk for money laundering. | |  |  | |  |
| 4. | Determine whether the bank's system for monitoring PEPs for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 5. | On the basis of the bank's risk assessment of its PEP relationships, as well as prior examination and audit reports, select a sample of PEP accounts. From the sample selected, perform the following audit procedures:  Determine compliance with regulatory requirements and with the bank's established policies, procedures, and processes.  Review transaction activity for accounts selected. If necessary, request and review specific transactions.  If the analysis of activity and customer due diligence information raises concerns, hold discussions with bank management. | |  |  | |  |
| Embassy and Foreign Consulate Accounts – EFC | | |  |  | |  |
| 1. | Review the policies, procedures, and processes related to embassy and foreign consulate accounts. Evaluate the adequacy of the policies, procedures, and processes given the bank's embassy and foreign consulate accounts and the risks they present (e.g., number of accounts, volume of activity, and geographic locations). Assess whether the risk-based controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | Identify senior management's role in the approval and ongoing monitoring of embassy and foreign consulate accounts. Determine whether the board is aware of embassy banking activities and whether it receives periodic reports on these activities. | |  |  | |  |
| 3. | From a review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors embassy and foreign consulate accounts, particularly those that pose a high risk for money laundering. | |  |  | |  |
| 4. | Determine whether the bank's system for monitoring embassy and foreign consulate accounts for suspicious activities, and for reporting of suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships. | |  |  | |  |
| 5. | On the basis of the bank's risk assessment of its embassy and foreign consulate accounts, as well as prior examination and audit reports, select a sample of embassy and foreign consulate accounts. From the sample selected, perform the following audit procedures:  Determine compliance with regulatory requirements and with the bank's established policies, procedures, and processes.  Review the documentation authorizing the ambassador or the foreign consulate to conduct banking in the United States.  Review transaction activity for accounts selected. If necessary, request and review specific transactions. | |  |  | |  |
| Non-bank Financial Institutions – NBFI | | | | | | |
| 1. | Determine the extent of the bank's relationships with NBFIs and review the bank's risk assessment of this activity. | |  |  | |  |
| 2. | Review the policies, procedures, and processes related to NBFI accounts. Evaluate the adequacy of the policies, procedures, and processes given the bank's NBFI activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 3. | From review of management information systems (MIS) and internal risk rating factors, determine whether the bank effectively identifies and monitors NBFI accounts. | |  |  | |  |
| 4. | Determine whether the bank's system for monitoring NBFI accounts for suspicious activities, and for reporting of suspicious activities, is adequate given the nature of the bank's customer relationships. | |  |  | |  |
| 5. | Determine whether the bank has policies, procedures, and processes in place for accounts opened or maintained for money service businesses (MSBs) to:  Confirm FinCEN registration, if required. Registration must be renewed every two years.  Confirm state licensing, if applicable.  Confirm agent status, if applicable.  Conduct a risk assessment to determine the level of risk associated with each account and whether further due diligence is required. | |  |  | |  |
| 6. | Determine whether the bank's policies, procedures, and processes to assess risks posed by MSB customers effectively identify higher-risk accounts and the amount of further due diligence necessary. | |  |  | |  |
| 7. | On a basis of the bank's risk assessment of its NBFI accounts, as well as prior examination and audit reports, select a sample of high-risk NBFI accounts. From the sample selected, perform the following audit procedures:  Review account opening documentation and ongoing due diligence.  Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity.  Determine whether actual activity is consistent with the nature of the customer's business and identify any unusual or suspicious activity. | |  |  | |  |
| Professional Service Providers – PSP | | | | | | |
| 1. | Review the policies, procedures, and processes related to professional service provider relationships. Evaluate the adequacy of the policies, procedures, and processes given the bank’s relationships with professional service providers and the risks these relationships represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing. | |  |  | |  |
| 2. | From a review of management information systems and internal risk rating factors, determine whether the bank effectively identifies and monitors professional service provider relationships. The reports obtained should include information about an entire relationship.  For example, an interest on lawyers’ trust account (IOLTA) may be in the name of the law firm instead of an individual. However, the bank’s relationship report should include the law firm’s account *and* the names and accounts of lawyers associated with the IOLTA. | |  |  | |  |
| 3. | Determine whether the bank’s system for monitoring professional service provider relationship’s suspicious activities, and for reporting of suspicious activities, is adequate given the bank’s size, complexity, location, and types of customer relationships. | |  |  | |  |
| 4. | On the basis of the bank’s risk assessment of its relationships with professional service providers, as well as prior examination and audit reports, select a sample of high-risk relationships. From the sample selected, perform the following examination procedures:   * review account opening documentation and a sample of transaction activity. * determine whether actual account activity is consistent with anticipated account activity. Look for trends in the nature, size, or scope of the transactions, paying particular attention to currency transactions. * determine whether ongoing monitoring is sufficient to identify potentially suspicious activity. | |  |  | |  |
| Non-Governmental Organizations and Charities – NGO | | | | | | |
| 1. | Review the policies, procedures, and processes related to NGOs. Evaluate the adequacy of the policies, procedures, and processes given the bank’s NGO accounts and the risks they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering ad terrorist financing. | |  |  | |  |
| 2. | From a review of management information systems and internal risk rating factors, determine whether the bank effectively identifies and monitors high-risk NGO accounts. | |  |  | |  |
| 3. | Determine whether the bank’s system for monitoring NGO accounts for suspicious activities, and for reporting of suspicious activities, is adequate given the bank’s size, complexity, location, and types of customer relationships. | |  |  | |  |
| 4. | On the basis of the bank’s risk assessment, its NGO and charity accounts, as well as prior examination and audit reports, select a sample of high-risk NGO accounts. From the sample selected, perform the following examination procedures:   * review account opening documentation and ongoing due diligence information. * review account statements and, as necessary, specific transaction details. * compare expected transactions with actual activity. * determine whether actual activity is consistent with the nature of the customer’s business. * identify any unusual or suspicious activity. | |  |  | |  |
| Closing Meeting – CM | | |  |  | |  |
| 1. | Discuss the results of the review with the appropriate personnel and document, at a minimum, those in attendance, date of discussion, and any comments expressed related to the results of the review. | |  |  | |  |