

**Audit of Bank Secrecy Act  
As of January 2009**

Audit Objectives and Program

**OBJECTIVES:**

- A. To test the bank's compliance with the requirements of the Bank Secrecy Act and Anti-Money Laundering Program and that bank policies and procedures are being followed.
- B. Assess the adequacy of the BSA/AML compliance program.
- C. Assess the bank's compliance with the statutory and regulatory requirements for the Customer Identification Program (CIP).
- D. To determine that internal controls are adequate.
- E. To determine that the data being produced by the monitoring systems is accurate and meets the requirements of the act.

Audit Program	Done By & Date	W/P Ref
<b>A. Preliminary Review</b>		
1. Review the prior internal audit reports and regulatory exams to develop an understanding of audit areas that were issues in past reviews. <ul style="list-style-type: none"> <li>a. Review management's responses related to corrective action to previously noted violations, deficiencies, and weaknesses, whether noted by internal audit, external, or regulatory exams.</li> <li>b. Determine whether corrective action has been implemented.</li> </ul>		
<b>B. Policy Review</b>		
2. Review the bank's written BSA/AML compliance program to ensure it contains the following: <ul style="list-style-type: none"> <li>a. A system of internal controls to ensure ongoing compliance for the following:               <ul style="list-style-type: none"> <li>i. CTR</li> <li>ii. Customer Exemptions</li> <li>iii. Monetary Instrument logs</li> <li>iv. Wire transfers</li> <li>v. SARS</li> <li>vi. Money laundering deterrent systems</li> <li>vii. CIP</li> <li>viii. OFAC Compliance</li> <li>ix. Annual training</li> <li>x. BSA Audit procedures</li> <li>xi. Record retention guidelines</li> <li>xii. Board reporting</li> <li>xiii. Account opening policies</li> </ul> </li> </ul>		

<ul style="list-style-type: none"> <li>b. Independent testing of BSA compliance</li> <li>c. A specifically designated person responsible for managing BSA compliance.</li> <li>d. Training for appropriate personnel.</li> <li>e. Ensure a Customer Identification Program is included as part of the BSA/AML compliance program.</li> <li>f. Verify that they were approved by the board of directors and documented in the minutes.</li> </ul>		
<p>3. Review the bank's BSA/AML, CIP, and OFAC risk assessments for reasonableness with the bank's profile for products, services, customers, and geographic locations. Ensure these were approved by the board.</p>		
<p>4. Verify the annual appointment of a BSA officer by the board of directors (12 CFR 326.8(c)).</p>		
<p><b>C. Reporting Requirements</b></p>		
<p>5. Currency Transaction Report (CTR) Review</p> <ul style="list-style-type: none"> <li>a. Review the procedures and forms covering CTRs (FINCEN Form 104)</li> <li>b. Review a sample of the bank's forms 104 and daily transaction records. Verify that the bank completed a CTR for every currency transaction (deposit, w/drawal, or exchange of cash) or more than \$10,000 by nonexempt customers. <ul style="list-style-type: none"> <li>i. Review system generated CTRs and teller tapes for evidence of transactions and multiple transactions that require form 104 to be filed.</li> <li>ii. Consider reviewing a sample of teller cash-ins and cash-outs for possible reportable transactions.</li> </ul> </li> <li>c. Determine that procedures are in place to detect multiple transactions in one day totaling greater than \$10,000, if an automated report is not already used (review teller tapes, journal logs, or cash in/out tickets if necessary).</li> <li>d. For all cash transactions greater than \$10,000, make sure Form 104 is filed with the IRS within 15 days of the transaction</li> <li>e. Obtain any correspondence related to incorrect or incomplete CTRs that the bank has received from the IRS since the previous audit and determine that the bank has taken appropriate corrective action (i.e., refiled). <ul style="list-style-type: none"> <li>i. Bank personnel should maintain a copy of the IRS notification, the original CTR, and the corrected CTR.</li> </ul> </li> <li>f. Review CTRs for proper completion. <ul style="list-style-type: none"> <li>i. Determine that the identity of the customer has been verified.</li> <li>ii. Determine that the revised FINCEN Form 104 is being used by the bank.</li> <li>iii. Ensure that the BSA Officer has appropriately signed the CTRs.</li> </ul> </li> </ul>		

<ul style="list-style-type: none"> <li>g. Review new account opening procedures <ul style="list-style-type: none"> <li>i. Determine that procedures are in place to monitor new accounts that are opened with a cash deposit greater than \$10,000. This review should include new accounts opened in person at the lobby or Internet banking transactions where the initial deposit is mailed in or dropped off.</li> <li>ii. Verify that a Form 104 is filed for all such deposits.</li> <li>iii. Determine whether the employees are knowledgeable about appropriate CTR filing procedures.</li> </ul> </li> </ul>		
<b>D. Customer Exemptions</b>		
<ul style="list-style-type: none"> <li>6. Review the CTR exemption list for compliance with either a Phase I or Phase II Exemption. <ul style="list-style-type: none"> <li>a. Phase I (31 CFR 103.22(d)(2)(i)-(v)) <ul style="list-style-type: none"> <li>i. Determine that the bank files the TD F 90-22.53 with the IRS within 30 days of the first reportable transaction that was exempted.</li> <li>ii. Assess whether ongoing and reasonable due diligence is performed, including required annual reviews to determine whether a customer remains eligible for designation as an exempt person under the regulatory requirements. Management should properly document exemption determinations.</li> </ul> </li> <li>b. Phase II (31 CFR 103.22(d)(2)(vi)-(vii)) <ul style="list-style-type: none"> <li>i. Determine that the bank files the TD F 90-22.53 with the IRS</li> <li>ii. Determine whether the bank maintains documentation to support that the “non-listed businesses” it has designated as exempt from CTR reporting do not receive more than 50 percent of gross revenue from ineligible business activities.</li> <li>iii. Assess whether ongoing and reasonable due diligence is performed, including required annual reviews to determine whether a customer remains eligible for designation as exempt from CTR reporting. <ul style="list-style-type: none"> <li>1. Determine that the customer has maintained a transaction account at the bank for at least 12 months.</li> <li>2. Check that the customer frequently engages in cash transactions over \$10,000 (at least 8 per year).</li> <li>3. Is incorporated or organized under the laws of the US, or is registered as and eligible to do business within the US.</li> </ul> </li> </ul> </li> </ul> </li> </ul>		
<ul style="list-style-type: none"> <li>7. Determine that the bank has filed a biannual renewal form by March 15 of the second year from the date of the original filing for all exempt</li> </ul>		

<p>customers.</p> <p>a. Ensure this filing includes both a notification of any change in control relative to the "exempt persons" and a certification by the bank as to its monitoring system for reporting suspicious activity.</p>		
<p>8. Determine if the bank has revoked any exemptions since the previous audit.</p> <p>a. If so, determine whether the reason for the revocation is appropriate and whether the bank completed a Form TDF 90-22.53 for revocation.</p>		
<p><b>E. Monetary Instrument Logs</b></p>		
<p>9. Review a sample of completed logs for compliance. If any were purchased with cash between \$3,000 and \$10,000, trace to the appropriate monetary instrument log. Keep in mind to look for possible structuring of transactions and aggregate customer transactions if necessary.</p> <p>a. Test the bank's log for completeness. Review internal checking account activity or GL account activity related to bank checks, cashier's checks, traveler's checks, or money orders and trace transaction activity to the original transaction to determine if cash was used.</p> <p>b. Review the system generated cash report or teller system cash reports, looking for activity related to official checks, cashier checks, traveler's checks, or money order internal accounts and trace transaction activity to the monetary instrument log. Keep in mind to look for possible structuring of transactions and aggregate customer transactions if necessary.</p> <p>c. For non-customer monetary instruments, review paid bank checks, cashier checks, traveler's checks, or money orders and trace randomly selected checks between \$3,000 and \$10,000 to the original transactions to determine if the checks were purchased with cash and appropriately logged.</p>		
<p>10. Review any large cash transaction reports for customer deposits between \$3,000 and \$10,000 and then scan the bank's monetary instrument inventory logs to determine if subsequent monetary instruments were purchased with these deposits.</p>		
<p>11. Review teller cash ins/outs for transactions between \$3,000 and \$10,000 and trace to the appropriate monetary instrument log.</p>		
<p>12. Verify that the appropriate information is obtained on the monetary instrument log.</p>		
<p><b>F. Funds Transfers</b></p>		
<p>13. Originating Bank</p> <p>a. 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.</p> <p>i. Randomly select days during the audit period and pull the</p>		

<p>wire transfer logs maintained manually or by the bank's wire transfer software. Pull the wire request form and determine that all information is included.</p> <p>ii. Verify this information is kept for 5 years to comply with BSA requirements.</p> <p>b. If cash is accepted for wire transfers, determine through inquiry and observation that the bank requires proper identification, maintains documentation, and records and files a CTR if applicable.</p> <p>c. Determine if the bank maintains records relating to sending a payment order for an originator so that it can retrieve them by originator's name and by account number.</p>		
<p>14. Beneficiary Bank</p> <p>a. Verify that the bank retains copies of payment orders greater than \$3,000. If the customer is not established, review the incoming wire log and verify that it obtains the proper information.</p> <p>b. Determine if the bank maintains records relating to receiving a payment order for an originator so that it can retrieve them by originator's name and by account number.</p>		
<b>G. OFAC</b>		
<p>15. Determine that the policies and procedures related to OFAC compliance appropriately address:</p> <p>a. Maintaining and distributing a list of prohibited countries, entities, and individuals.</p> <p>b. Comparing new accounts to the OFAC listing.</p> <p>c. Comparing incoming and outgoing wire transfers to the OFAC listing.</p> <p>d. Monitoring transactions for possible prohibited activity, including transactions through non-bank financial institutions.</p> <p>e. Comparing the bank's entire database to the OFAC listing periodically.</p>		
<p>16. Review the bank's risk assessment and consider the following:</p> <p>a. The extent of, and method for, conducting OFAC searches of each relevant department/business line</p> <p>b. The extent of, and method for, conduction OFAC searches of beneficiaries, guarantors, principals, powers of attorney, and signatories.</p> <p>c. The process used to investigate potential matches.</p> <p>d. The process used to block and reject transactions.</p> <p>e. How responsibility for OFAC is assigned.</p> <p>f. Timeliness of obtaining and updating OFAC lists or filtering criteria.</p>		
<p>17. Determine whether the bank has filed an annual Report of Foreign Bank Financial Accounts declaring interest in a foreign account.</p>		
<p>18. Determine that each bank employee responsible for opening accounts or</p>		

<p>wiring international funds has access to and uses a listing of SDNs when suspicious of any customer wiring funds or opening a new account.</p> <ul style="list-style-type: none"> <li>a. For wire transfers completed for non-customers, the originator should be verified. If beneficiary information is provided, the beneficiary information should be verified.</li> <li>b. For incoming wire transfers, the bank should verify beneficiary information if the customer is not a customer of the bank. <ul style="list-style-type: none"> <li>i. Check to ensure the wire transfer form is being initiated for checking of OFAC.</li> </ul> </li> </ul>		
<p>19. Determine that all incoming ACH files and outgoing ACH originations are scanned for matches to the most current SDN listing.</p>		
<p>20. Determine if management has performed a scan of the bank's entire customer database for SDN matches. Should be performed quarterly.</p>		
<p>21. Review a sample of potential OFAC matches and evaluate the bank's resolution and blocking/rejecting processes.</p>		
<p>22. Document procedures for ensuring that OFAC is notified within 10 days when any accounts are blocked for SDNs or blocked entities.</p>		
<p><b>H. Suspicious Activity Reports (SARs)</b></p>		
<p>23. Determine if the bank's BSA policies and procedures have adequate suspicious activity identification and reporting requirements:</p> <ul style="list-style-type: none"> <li>a. An individual responsible for preparing and filing the SARs.</li> <li>b. A process for ensuring that the SARs are filed within time frames established by regulation along with factual and sufficiently detailed content to describe the suspicious activity.</li> <li>c. A process for ensuring that transaction amounts are consistent with the type and nature of the business or occupation of the customer.</li> <li>d. A process for reviewing "exempt person" accounts for unusual or suspicious activity.</li> <li>e. A process for establishing expected activity levels for exempt customers.</li> <li>f. A process for reconciling activity levels of higher risk accounts against expected activity to ensure that activity levels are reasonable.</li> <li>g. A system for reviewing exception reports and the parameters used to filter exceptions (suspect kite reports, cash transaction reports, NSF, and overdraft reports).</li> <li>h. A process for requesting timely and adequate explanations of activity generated by monitoring reports.</li> <li>i. 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.</li> <li>j. A system (automated or manual) to detect structured transactions (both cash in and out) that are under the \$10,000 reporting</li> </ul>		

	threshold. k. Procedures for documentation of decisions not to file a SAR.		
24.	Obtain all SARs filed within the last year and verify that they were properly filled out and filed in a timely manner (30 calendar days after the date of the initial detection of facts).		
25.	Determine that bank management and supervisors are aware of the situations for which a SAR is required to be filed.		
26.	Determine if management is aware of the "safe harbor" rules that prohibit them from revealing any knowledge that a SAR has been filed.		
27.	Ask management about situations in which a SAR was contemplated and not filed. Does management have sufficient documentation to support their decision not to file? Determine whether the exclusion from filing a SAR was appropriate.		
28.	Determine that the bank has established procedures to review transaction activity through electronic banking products for money laundering and suspicious activity (e.g. activity logs, etc.)		
<b>I. Taxpayer Identification Number (TIN) Review</b>			
29.	Review a sample of interest bearing and non-interest bearing deposit accounts to determine that the bank has a record of the depositors' TINs. a. If the bank does not have a TIN on hand for each depositor, verify that it has back-up withholding procedures in place.		
<b>J. Non-Bank Financial Institution (NBFI) Review</b>			
30.	Determine if the bank has identified if it has any non-bank financial institutions (NBFIs) within its customer base, such as a qualified money service business (MSB). a. Document the bank's processes for researching its customer database and identifying these customers.		
31.	Document the bank's due diligence for monitoring these NBFIs for suspicious activity. a. Determine if the bank conducted a risk assessment of its NBFI customers to determine the level of due diligence required for each customer b. Determine if the bank's MSB customers have registered as MSBs with FINCEN and the appropriate state agencies. c. Determine if the bank followed its CIP procedures when the accounts were opened.		
32.	Risk Assessment Process a. Determine if the bank's risk assessment process addresses the types of products its NBFI customers offer. Does this address the locations and markets served by the NBFI business? b. Determine if the risk assessment addresses and analyzes the anticipated account activity and purposes of the account.		
33.	Determine if the bank has a procedure in place to monitor the registration status of MSBs (e.g. ticklers)		

<b>K. Customer Identification Program (CIP) (Section 326 of the USA Patriot Act)</b>			
34.	Verify that the bank's policies, procedures, and processes include a comprehensive program for identifying customers who open accounts after October 1, 2003. The written program must be included within the bank's BSA/AML compliance program and must include the following: <ul style="list-style-type: none"> <li>a. Identification of information required to be obtained (including name, address, TIN, date of birth (individuals), and risk-based identity verification procedures.</li> <li>b. Procedures for complying with record-keeping requirements.</li> <li>c. Procedures for checking new accounts against prescribed government lists, if applicable.</li> <li>d. Procedures for providing adequate customer notice when the bank is requesting information to verify the customer's identity.</li> <li>e. Procedures covering the bank's reliance on another financial institution in verifying a customer identity.</li> <li>f. Procedures for determining whether and when a Suspicious Activity Report (SAR) should be filed.</li> </ul>		
35.	Determine that the bank has performed a risk analysis and if it addresses the types of accounts offered, the bank's size, location, and customer base.		
36.	Determine whether the bank's policy for opening new accounts for existing customers appears reasonable.		
37.	Review board minutes and verify that the board of directors approved the CIP (31 CFR 103.121(b) (1)).		
38.	Evaluate the bank's training programs to ensure that the CIP is adequately incorporated (31 CFR 103.121 (b) (1)).		
39.	Select a sample of new accounts for review for compliance with the bank's CIP. Review to the BSA manual page 180 for compliance.		
<b>L. Information Sharing Requirements (USA Patriot Section 314)</b>			
40.	Determine if the bank has a program to comply with Section 314(a) information requests, which includes the following: <ul style="list-style-type: none"> <li>a. Designation of an employee as the contact person responsible for handling Section 314(a) information requests.</li> <li>b. Procedures to ensure that all required records are searched, with positive hits reported to FINCEN within designated time frames.</li> <li>c. Procedures to ensure that the confidentiality of the information requested is safeguarded.</li> <li>d. Maintaining appropriate records of search results.</li> </ul>		
41.	If the bank uses a third-party vendor to conduct information searches, determine that there is an agreement and procedures to ensure confidentiality.		
<b>M. Training</b>			
42.	Determine that adequate training procedures for employees are established with regard to the requirements of the BSA (12 CFR 208)		

<p>43. The BSA training program should address the following:</p> <ul style="list-style-type: none"> <li>a. Importance management places on ongoing education and training related to the BSA.</li> <li>b. Documenting the appropriateness of the scope and frequency of training.</li> <li>c. The inclusion of personnel from all functional areas of the bank.</li> <li>d. Coverage of bank policies and procedures related to the BSA.</li> <li>e. Coverage of new rules and requirements.</li> <li>f. Enhanced procedures to address previously cited violations and deficiencies.</li> <li>g. Coverage of different forms of money laundering.</li> <li>h. Identification of suspicious activity.</li> </ul>		
<b>N. Record Retention</b>		
<p>44. Determine that the bank maintains records for at least five years after the date of the report for the following:</p> <ul style="list-style-type: none"> <li>a. CTRs</li> <li>b. Each exemption</li> <li>c. Record keeping requirements for wire transfers.</li> <li>d. Each extension of credit in an amount over \$10,000 (except when secured by real property).</li> <li>e. Each advice, request, or instruction received or given to another financial institution regarding a transfer over \$10,000.</li> <li>f. Listing of customer accounts with missing TINs.</li> <li>g. Each document granting signature authority over each deposit account.</li> <li>h. Each state of each deposit showing each transaction involving the account.</li> <li>i. Each document relating to a transaction of more than \$10,000 remitted to a person outside the United States.</li> <li>j. Minimum CIP account information (name, address, date of birth, TIN) for five years from the date the account is closed or becomes dormant.</li> </ul>		
<p>45. Determine that the bank maintains other CIP information created, such as the description of government-issued identification or non-documentary methods used to verify identification, for a minimum of five years after the record is recorded.</p>		
<b>O. MIS System Testing</b>		
<p>46. Test the integrity and accuracy of MIS systems used in the BSA compliance program. Test a sample of cash in/out tickets to Large Cash Transactions report. This ensures that large cash transactions are accurately reflected on the report.</p>		