

# **Southeast Bankers Outreach Forum**

## **High Priority Risks: *BSA/AML Compliance***

**Date:** September 15, 2015

---

**Presented by:** Rick MacNamara

*The opinions expressed are those of the presenter and are not those of the Federal Reserve Bank of Atlanta, the Federal Reserve System, or its Board of Governors.*



**FEDERAL  
RESERVE  
BANK  
of ATLANTA**

# Board/Mgt Oversight – BSA Manual

---

- The BSA/AML compliance program must be written, approved by the board of directors, and noted in the board minutes.
- A bank must have a BSA/AML compliance program commensurate with its respective BSA/AML risk profile.
- Management should structure the bank's BSA/AML compliance program to adequately address its risk profile, as identified by the risk assessment. Management should understand the bank's BSA/AML risk exposure and develop the appropriate policies, procedures, and processes to monitor and control BSA/AML risks.
- The bank's board of directors must designate a qualified individual to serve as the BSA compliance officer.

# Board/Mgt Oversight – BSA Manual

---

- The board of directors, acting through senior management, is ultimately responsible for ensuring that the bank maintains an effective BSA/AML internal control structure.
- The board of directors and management should create a culture of compliance to ensure staff adherence to the bank's BSA/AML policies, procedures, and processes.
- The board of directors and senior management should be informed of changes and new developments in the BSA, its implementing regulations and directives, and the federal banking agencies' regulations. While the board of directors may not require the same degree of training as banking operations personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the bank.

# Oversight Enforcement Provisions

---

- **Establish a Board BSA Director's Committee**
- **Retain an independent third party to conduct comprehensive review of BSA effectiveness**
- **Plan to develop, recruit & hire qualified staff**
- **Submit a enterprise-wide BSA/AML program**

# Risk Assessments – BSA Manual

---

- The first step of the risk assessment process is to identify the specific products, services, customers, entities, and geographic locations unique to the bank. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered when the bank prepares its risk assessment.
- The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess BSA/AML risk. This step involves evaluating data pertaining to the bank's activities (e.g., number of: domestic and international funds transfers; private banking customers; foreign correspondent accounts; PTAs; and domestic and international geographic locations of the bank's business area and customer transactions) in relation to Customer Identification Program (CIP) and customer due diligence (CDD) information.

# **Risk Assessment Provisions**

---

- **Identifies BSA risk profile**
  - Products, services, customers, entities, transactions, geographies & new risks
  - Quantifies risk based on detailed analysis of all data pertinent to risk categories (purpose, actual & anticipated activity, nature of business/occupation, location, products and services)
- **Develops risk mitigation strategies**
- **Consistent w/ BSA/AML Exam Manual**
- **Updated annually**

# CIP – BSA Manual

---

- The Customer Information Program (CIP) is intended to enable the bank to form a reasonable belief that it knows the true identity of each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer.
- Banks should conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider:
  - The types of accounts offered by the bank.
  - The bank's methods of opening accounts.
  - The types of identifying information available.
  - The bank's size, location, and customer base, including types of products and services used by customers in different geographic locations.
- The CIP must contain account-opening procedures detailing the identifying information that must be obtained from each customer.

# CDD – BSA Manual

- ***The cornerstone of a strong BSA/AML compliance program is the implementation of comprehensive Customer Due Diligence (CDD) policies, procedures, and processes for all customers.***
- ***The objective of CDD should be to enable the bank to predict with relative certainty the types of transactions in which a customer is likely to engage. These processes assist the bank in determining when transactions are potentially suspicious.***
- ***Under this approach, the bank should obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations. This information should allow the bank to determine the customer's risk profile at account opening.***
- ***CDD processes should include periodic risk-based monitoring of the customer relationship to determine whether there are substantive changes to the original CDD information.***



# EDD – BSA Manual

---

- Enhanced due diligence (EDD) for higher-risk customers is especially critical in understanding their anticipated transactions.
- Higher-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank.
- The bank may determine that a customer poses a higher risk because of the customer's business activity, ownership structure, anticipated or actual volume and types of transactions, including those transactions involving higher-risk jurisdictions.
- As due diligence is an ongoing process, a bank should take measures to ensure account profiles are current and monitoring should be risk-based. Banks should consider whether risk profiles should be adjusted or suspicious activity reported when the activity is inconsistent with the profile.

# CIP/CDD/EDD – Provisions

---

- **RF assessment of customer base**
  - Collects, analyzes and retains customer information
  - Resolution of insufficient or inaccurate information
- **Methodology for assigning timely risk rating**
  - Purpose of account & expected volume
  - Type of customer, product and markets/geography
  - Support and validation of risk ratings
- **Ongoing monitoring for a/c requiring EDD**
- **EDD for customers with heightened risk**
  - Verify/confirm identity & customer activities
  - Understand expected transactions

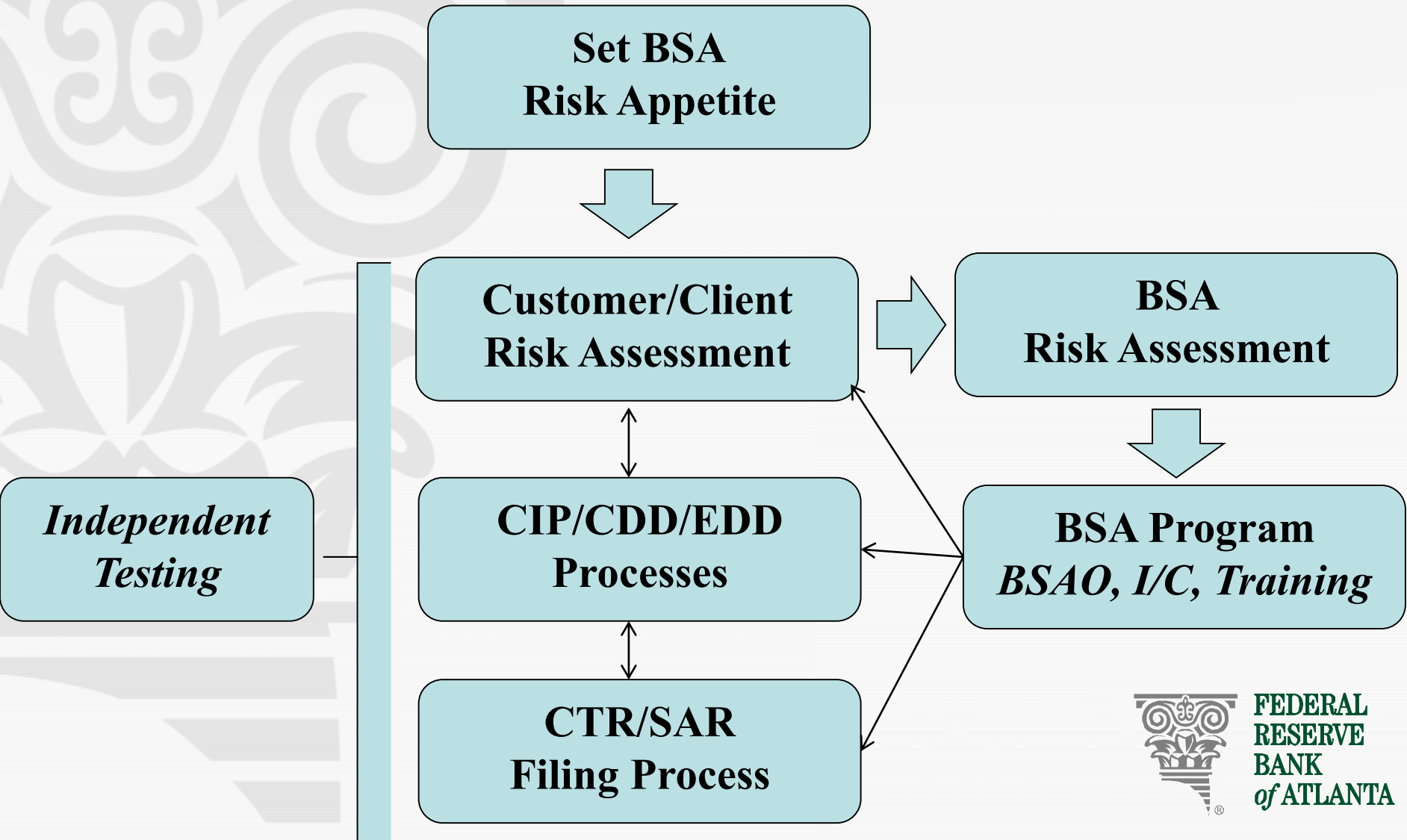
# Point of Emphasis

**FINCEN PROPOSES FIFTH BSA PILLAR**

**FinCEN's New Proposed Beneficial Ownership Policies and Regulations**

**KYC – CDD Solutions: The 5th Pillar of Core AML?**

# BSA/AML Drivers



# SAR Monitoring – BSA Monitoring

---

- Proper monitoring and reporting processes are essential to ensuring that the bank has an adequate and effective BSA compliance program. The sophistication of monitoring systems should be dictated by the bank's risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities, and geographies.
- The bank should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities, taking into account the bank's overall risk profile and the volume of transactions.
- Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.

# SAR Monitoring – BSA Monitoring

---

- **The five key components to an effective monitoring and reporting system are:**
  - Identification or alert of unusual activity (which may include: employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output).
  - Managing alerts.
  - SAR decision making.
  - SAR completion and filing.
  - Monitoring and SAR filing on continuing activity.

# SAR Monitoring – BSA Manual

- Management should periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process. Each bank should evaluate and identify filtering criteria most appropriate for their bank. (Manual monitoring)
- Management should document and be able to explain filtering criteria, thresholds used, and how both are appropriate for the bank's risks. Management should also periodically review and test the filtering criteria and thresholds established to ensure that they are still effective. (Automated monitoring)
- The monitoring system's programming methodology and effectiveness should be independently validated to ensure that the models are detecting potentially suspicious activity. The independent validation should also verify the policies in place and that management is complying with those policies.

# **SAR Monitoring – EA Provisions**

---

- **Reasonably ensure the identification & timely, accurate & complete reporting of known or suspected criminal activity**
- **Support for management's decision to file or not to file a SAR**
- **Scope and frequency of transaction monitoring**
  - Establishment and periodic testing of thresholds
  - Including cash, intl & dom WT, ACH & ATMs
  - Periodic review of aggregate cash, MI, WT & pouch



# Independent Testing – BSA Manual

---

- The persons conducting the BSA/AML testing should report directly to the board of directors or to a designated board committee comprised primarily or completely of outside directors.
- Banks that employ outside auditors or consultants should ensure that qualified persons doing the BSA/AML testing are not involved in other BSA functions such as training or developing policies and procedures that may present a conflict or lack of independence.
- Those persons responsible for conducting an objective independent evaluation of the written BSA/AML compliance program should perform testing for specific compliance with the BSA, and evaluate pertinent management information systems (MIS). The audit should be risk based and evaluate the quality of risk management for all banking operations, departments, and subsidiaries.

# Independent Testing – BSA Manual

---

- An evaluation of the overall adequacy and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes. Typically, this evaluation includes an explicit statement about the BSA/AML compliance program's overall adequacy and effectiveness and compliance with applicable regulatory requirements.
- A review of the bank's risk assessment for reasonableness given the bank's risk profile (products, services, customers, entities, and geographic locations).
- An evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations.
- A review of staff training for adequacy, accuracy, and completeness.

# Independent Testing – BSA Manual

---

- **Appropriate risk-based transaction testing to verify the bank's adherence to the BSA recordkeeping and reporting requirements (e.g., CIP, SARs, CTRs and CTR exemptions, and information sharing requests).**
- **A review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for BSA/AML compliance.**
- **An assessment of the overall process for identifying and reporting suspicious activity, including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness of the bank's policy.**
- **An assessment of the integrity and accuracy of MIS used in the BSA/AML compliance program.**

# **Independent Testing – Provisions**

---

- **Assess Integrity and Effectiveness of BSA program**
- **BSA/AML Risk Assessment**
- **BSA Reporting and Recordkeeping Requirements**
- **Customer Identification Program**
- **Adequacy of Customer Due Diligence P&Ps**
- **Adherence to BSA/AML P&Ps**
- **Appropriate Transaction Testing w/ emphasis on HRAs**
- **Integrity and Accuracy of MIS**
- **Evaluate Resolution of Violations and Deficiencies**
- **Assessment of Process for Identifying and Reporting Suspicious Activity**

# Summary

---

- **BSA Compliance begins with the Culture of Compliance demonstrated by the board and management.**
- **Management should understand the bank's BSA/AML risk exposure.**
- **BSA/AML compliance program should be commensurate with its respective BSA/AML risk profile.**
- **Board of directors need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the bank.**

---

# Thank You

---