CSBS
SINCE 1902
CONFERENCE OF STATE BANK SUPERVISORS

BSA/AML Self-Assessment Tool

Overview and Instructions

February 2018

1129 20th Street, N.W. • Ninth Floor • Washington, DC • 20036
www.csbs.org • 202-296-2840 • FAX 202-296-1928

Introduction and Overview

The Bank Secrecy Act and related federal and state law requirements (“BSA/AML”) are a crucial component of money services businesses (“MSB” or “MSBs”) operations. As a first line of defense for financial crimes, MSBs play an important role in minimizing fraud, money laundering, terrorist financing, and other financial crimes. BSA/AML compliance has become increasingly complex, leading state regulators to develop an optional BSA/AML Self-Assessment Tool (“Tool”) to provide risk transparency at all levels of an institution.

The Bank Secrecy Act and its promulgating regulations require MSBs to identify risks, assess the risks, and create a compliance program based on the risk assessment. The MSB Self-Assessment Tool is designed to support communication of the results of this risk assessment process. If an institution uses the Tool, compliance staff, management, and the board of directors will be able to view all identified risks and corresponding risk assessments in one document.

Importantly:

- The MSB BSA/AML Self-Assessment Tool is **not a requirement** – MSBs should not feel obligated to performing the Self-Assessment.
- The MSB BSA/AML Self-Assessment Tool is **not a substitute for a risk assessment** – institutions that choose to use this Self-Assessment Tool should use it in addition to the FinCEN BSA/AML Examination Manual for Money Services Businesses[1] and corresponding laws and regulations, not as a replacement.

While the opportunity for MSBs to serve as a conduit for illicit financing exists regardless of circumstances, there are two bright line risk thresholds that universally require substantial controls: international transactions and cash transactions. MSBs providing international transactions and/or cash transactions must engage in enhanced risk mitigation efforts to address the heightened risk associated with these business lines.

Additionally, while policies and procedures should be developed to address institution-specific business lines, there is no scenario in which an MSB can avoid transaction monitoring. Transaction monitoring is a control that must be used to ensure compliance. The veracity of a transaction monitoring program will depend on the institution, but the program must nonetheless account for product, customer, and geographic risk.

[1] *Available at* https://www.fincen.gov/sites/default/files/shared/MSB_Exam_Manual.pdf.

BSA/AML risk continuously changes. Accordingly, the BSA/AML Self-Assessment Tool is designed to be flexible. Institutions are free to adjust the formulas, rating values, and other variables to more appropriately reflect risks and the assessments thereof. The following instructions explain how the Tool was designed for use, but institutions should not hesitate to customize the Tool.

Instructions

1. **Identify Risks**

Pre-Populated Risks

The MSB Self-Assessment Tool identifies risk in five categories:

- Products & Services, e.g. business models
- Customers
- Geography
- Operations
- Agents

These categories are pre-populated with common risk areas, but should be customized to the risks facing each institution.

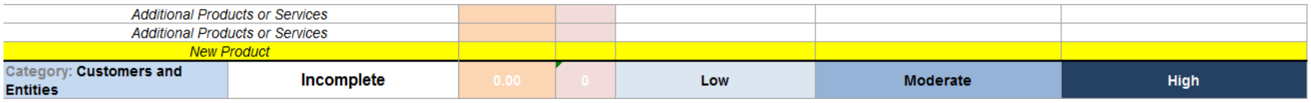
Additional Risks

The pre-populated risk areas do not include all possible risks. MSBs should add risks identified during the identification process. Each category has five additional rows for MSBs to insert identified risks that were not pre-populated.

If a MSB identifies more than five risks that were not pre-populated, take the following steps to add a row and update formulas:

i) Add a row to the corresponding category

ii) To quickly fill in the template's formatting, select pre-populated cells and drag the fill handle down the new cells



Additional Products or Services						
Additional Products or Services						
New Product						
Category: **Customers and Entities**	**Incomplete**	0.00	0	**Low**	**Moderate**	**High**

iii) Update the Count and Sum ranges to reflect the expanded range for the corresponding Category Inherent Risk, Select Risk Level, and Rating Cells. This can be done by clicking into the cell, which will reveal the formula. For example, if the Products and Services Category expands to include Row 13, update as follows:

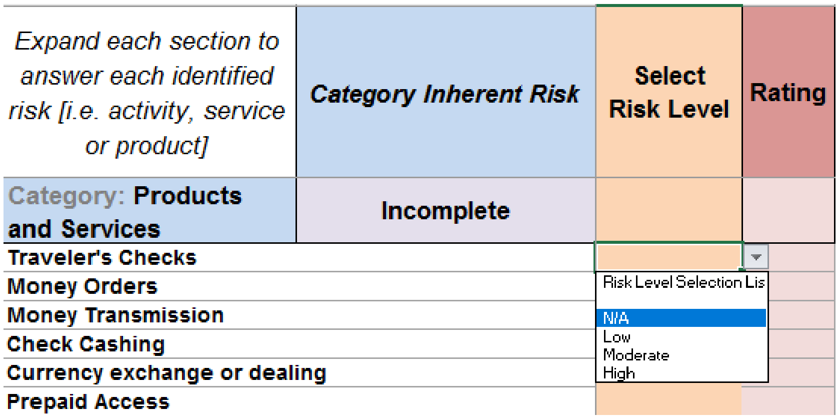
a. Cell B3: =IF(COUNTA(C4:C13)<1,"Incomplete",IF(C2<1.67,"Low",IF(C2<2.34,"Moderate",IF(C2>2.33,"High"))))

b. Cell C3: =IFERROR((D3/(COUNT(D4:D13))),0)

c. Cell D3: =SUM(D4:D13)

Eliminating Inapplicable Risks

MSBs are unlikely to engage in all risk areas identified in the template. Accordingly, inapplicable risks can be omitted from the Self-Assessment by simply selecting the blank designation or "N/A" in the "Select Risk Level" pull down menu. If a Risk Level is not selected, the risk will not count towards the inherent risk level. It is not recommended that a risk's row be deleted because the risk may emerge in the future.

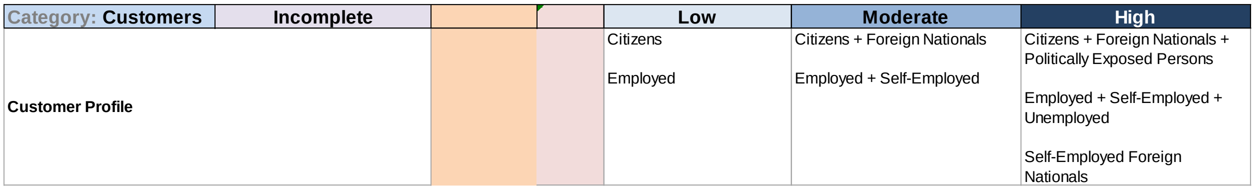


Expand each section to answer each identified risk [i.e. activity, service or product]	***Category Inherent Risk***	**Select Risk Level**	**Rating**
Category: **Products and Services**	**Incomplete**		
Traveler's Checks			
Money Orders			
Money Transmission			
Check Cashing			
Currency exchange or dealing			
Prepaid Access			

2. Defining Risk Level Criteria

Depending on the size and scope of the MSB, risk level will differ for each category. Accordingly, the tool leaves blank the corresponding cells for each identified risk. Institutions can use these blank cells to identify differing risk levels for the business model, size, and complexity.

In this example, the Customer Profile is considered low risk if customers are employed and citizens, moderate if customers include self-employed or foreign nationals, and high if customers include politically exposed persons, unemployed persons, and combined moderate risks of foreign nationals and self-employed.



Category: **Customers**	**Incomplete**			**Low**	**Moderate**	**High**
Customer Profile				Citizens Employed	Citizens + Foreign Nationals Employed + Self-Employed	Citizens + Foreign Nationals + Politically Exposed Persons Employed + Self-Employed + Unemployed Self-Employed Foreign Nationals

The New or Existing column should be used to help gauge risk definitions. If a product or service, customer, geography, operation, or agent network is new to the MSB, the risk is likely elevated compared to a practice that the MSB has experience implementing and monitoring.

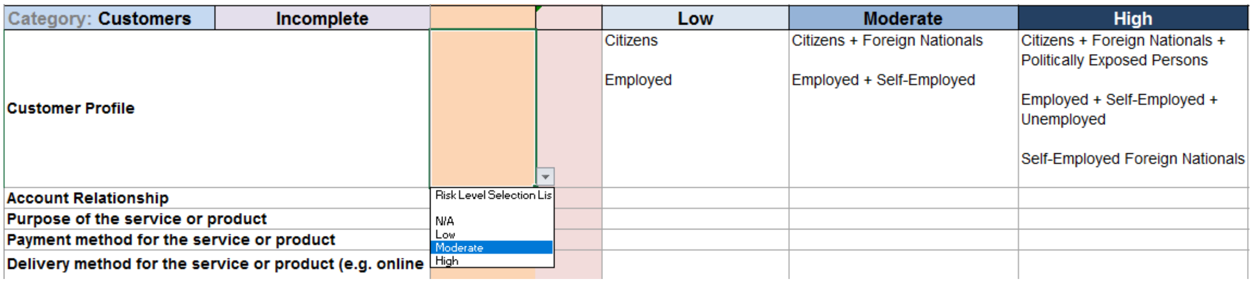
Accordingly, if a risk is new, the institution is urged to consider how risk is elevated in the corresponding risk definitions.

When defining risk levels, CSBS encourages institutions to review:

i) Scope and Complexity of Risk Coverage
ii) Methodology
iii) Governance and Follow-Up
iv) Ongoing Updates for Risk

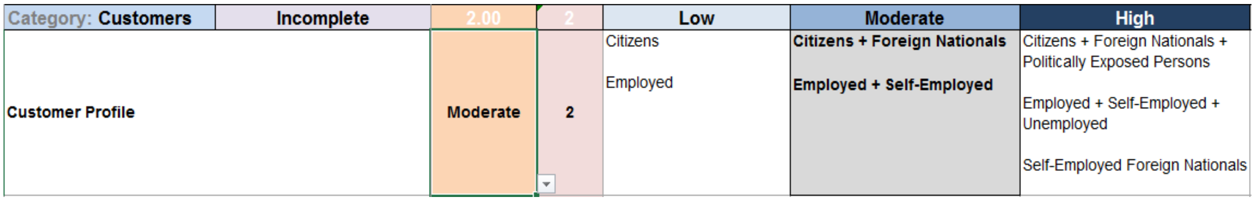
3. Selecting Risk Level for Risk Criteria

After defining the levels of risk, the institution should choose the Risk Level most appropriate for the institution's current operations. The Risk Level represents the vulnerability of each risk area to money laundering or terrorist financing. To do this, click on the drop down under "Select Risk Level for Risk Criteria" and choose from Low, Moderate, and High.



Category: Customers	Incomplete			Low	Moderate	High
Customer Profile				Citizens Employed	Citizens + Foreign Nationals Employed + Self-Employed	Citizens + Foreign Nationals + Politically Exposed Persons Employed + Self-Employed + Unemployed Self-Employed Foreign Nationals
Account Relationship						
Purpose of the service or product						
Payment method for the service or product						
Delivery method for the service or product (e.g. online						

Once selected, the corresponding Risk Level will automatically highlight.



Category: Customers	Incomplete	2.00	2	Low	Moderate	High
Customer Profile		Moderate	2	Citizens Employed	**Citizens + Foreign Nationals** **Employed + Self-Employed**	Citizens + Foreign Nationals + Politically Exposed Persons Employed + Self-Employed + Unemployed Self-Employed Foreign Nationals

4. Use Comments Column for Tracking and Continuity

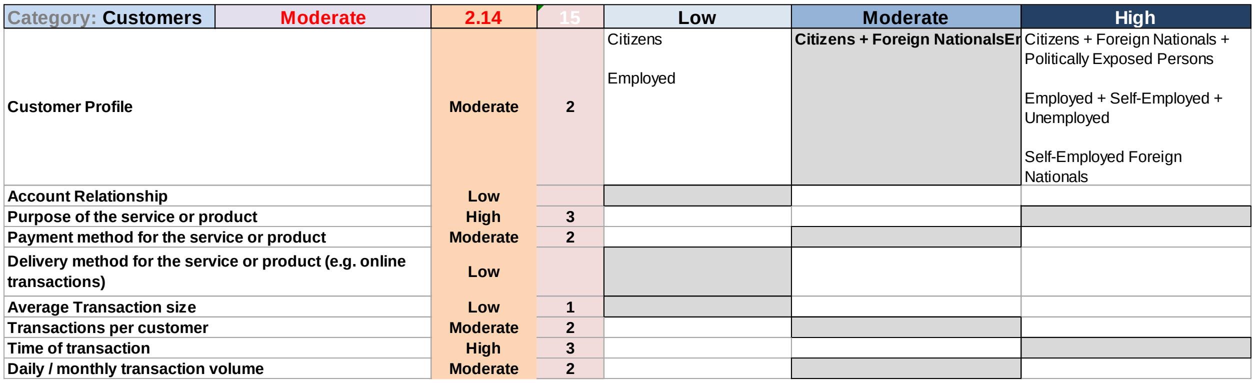
As a tool that is designed to be used on a regular basis, the comments column should be used to track reasoning and facilitate continuity. Relevant information on the risk level definitions and the reasoning for selecting a particular risk level should be tracked in the relevant Comments cell. This will improve communication between compliance professionals, management, and board members. Further, a record of the institution's reasoning is important if compliance professionals leave the institution.

It is also recommended that the comments column be used to store or reference supporting documentation.

5. How Inherent Risk is Calculated

1. Risk Levels have an assigned Rating. The default rating is as follows:
   a. Low Risk: 1
   b. Moderate Risk: 2
   c. High Risk: 3

2. After each Category (Products and Services, Customers, etc.) is completed, the Assessment Tool will calculate an average for each category.



Category: Customers	Moderate	2.14	15	Low	Moderate	High
Customer Profile		Moderate	2	Citizens Employed	Citizens + Foreign NationalsEr	Citizens + Foreign Nationals + Politically Exposed Persons Employed + Self-Employed + Unemployed Self-Employed Foreign Nationals
Account Relationship		Low		▨		
Purpose of the service or product		High	3			▨
Payment method for the service or product		Moderate	2		▨	
Delivery method for the service or product (e.g. online transactions)		Low		▨		
Average Transaction size		Low	1	▨		
Transactions per customer		Moderate	2		▨	
Time of transaction		High	3			▨
Daily / monthly transaction volume		Moderate	2		▨	

Average and Inherent Risk for Products and Services in red.

This average is calculated by determining the average Risk Level rating for all risks. Each category has its own average. The corresponding description – "Category Inherent Risk" – is based on the following assigned range:

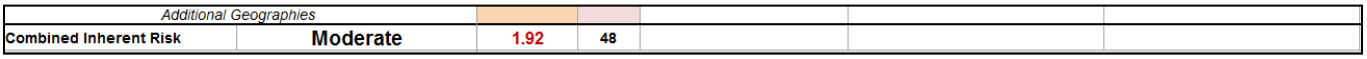
a. Low Risk: 1.66 and lower
b. Moderate Risk: 1.67 to 2.33
c. High Risk: 2.34 and higher

A category's Inherent Risk defaults to "Incomplete" if fewer than 1 Product and Agent risk area is selected, and if fewer than 3 risk levels are selected in the Customers, Geography, and Operations categories.

A "Combined Inherent Risk" figure is calculated at the end of the spreadsheet. The calculation is performed by taking a combined average of the average risk of:

- Products & Services;
- Customers;
- Geography;
- Operations; and
- Agents.

The corresponding description "Combined Inherent Risk" – is based on the same scale outlined above.

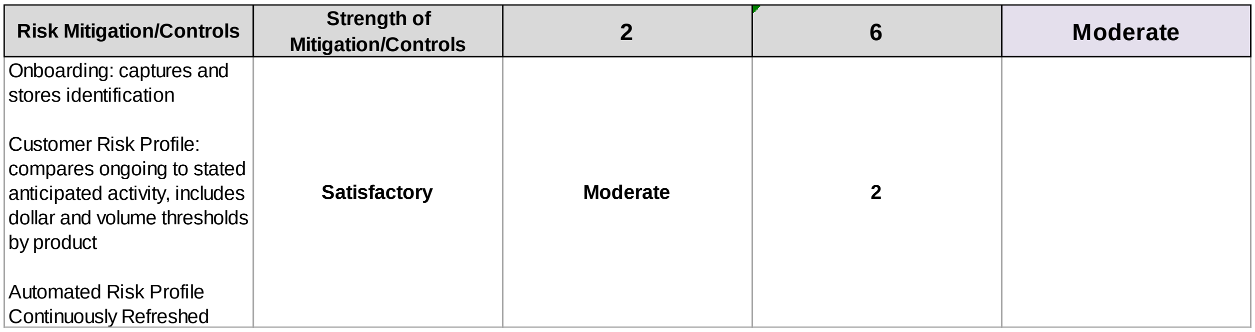


Additional Geographies						
Combined Inherent Risk	**Moderate**	**1.92**	**48**			

6. Risk Mitigation

i) To calculate the risk level after mitigating controls have been applied, input the risk mitigation action taken under Column I, "Risk Mitigation/Controls."

ii) After typing in the action taken by the institution in Column I, the user can input the strength of the mitigation/controls under Column K. The dropdown gives five options: N/A, Weak, Satisfactory, or Strong.

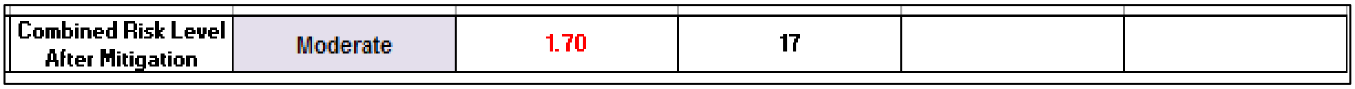


Risk Mitigation/Controls	Strength of Mitigation/Controls	2	6	Moderate
Onboarding: captures and stores identification Customer Risk Profile: compares ongoing to stated anticipated activity, includes dollar and volume thresholds by product Automated Risk Profile Continuously Refreshed	**Satisfactory**	**Moderate**	**2**	

iii) The user can also specify the "Risk Level after Mitigation," which will trigger a "Rating After Mitigation." The dropdown gives four options: N/A, Weak, Satisfactory or Strong.

iv) The choice of "Risk Level After Mitigation" triggers a numerical response in Column L, "Rating After Mitigation," and is scaled as follows:

- N/A – No fill
- Low – 1
- Moderate – 2
- High – 3



Combined Risk Level After Mitigation	Moderate	1.70	17		

When reviewing Risk Level Mitigation, CSBS encourages institutions to consider:

i) BSA/AML Compliance Officer and Staffing
ii) Internal Controls
iii) AML Training
iv) Independent Testing
v) Consumer Due Diligence and Beneficial Ownership

For more details, please see the appended Compliance Supplement.

7. Customization & Logical Override

MSBs can customize the risk areas, designations, and scoring to improve the risk analysis for their institution. There are several ways a MSB may customize this spreadsheet, including:

- Add risk definitions, e.g. "Higher Risk"
- Adjust assigned values to give higher weight to higher risks
- Adjust the scale for Inherent Risk descriptors.
- Adjust conditional formatting to color code risk selections

These changes can all be made by adjusting the formulae in the corresponding cells.

MSBs are also urged to use logic when analyzing the results. The MSB Self-Assessment Tool makes conclusions based on averages. For example, if a category has a majority of its risk designated as High Risk, but nonetheless has a Category Inherent Risk of Moderate, the MSB may want to consider more advanced controls given the number of high risks. Further, if a MSB is expanding into new areas, a series of low risk products, customers, or geographies does not mean there is not staffing and other growth risks.

Compliance Supplement

<u>AML Program "Pillars"</u>

The observations resulting from the risk assessment should inform and guide the MSB's development and implementation of its AML program. In doing so, the MSB's AML program should include measures to support the below program components, or "pillars."

1. BSA/AML Compliance Officer and Staffing

Ultimate responsibility for an MSB's AML compliance resides with its most senior leadership, such as the Board of Directors (Board). Owners, Boards, or representatives of senior management often appoint BSA/AML officers to oversee the MSB's day-to-day compliance. This designation is typically memorialized in Board meeting minutes, and notification of such designation to regulatory agencies may be required. Simply naming someone to this role is not enough. The BSA/AML Officer is ideally an individual who:

- Demonstrates certain minimum qualifications, which may even be prescribed by state regulations, such as expertise in BSA/AML regulations and professional experience, which may include recognized industry certifications and degrees;
- Has the capacity to coordinate, manage, and oversee day-to-day compliance with the BSA and its implementing regulations;
- Is empowered and has the appropriate level of authority, responsibility, and access to resources within the MSB;
- Understands how to implement appropriate risk mitigating controls for the company's product and service offerings, consumer base, and associated risks;
- Has the ability to influence the MSB's business teams and decisions;
- Communicates with regulators and fellow Compliance Officers and attends industry outreach events;
- Can confidently engage in discussions with examiners and auditors on the details of the MSB's AML program;
- Regularly informs the Board and senior management of AML compliance initiatives, potential issues, audit and examination report observations, and corrective actions; and
- Has an independent reporting line in the company and a direct line of communication to the Board or other executives.

For small currency exchangers, the BSA/AML Compliance Officer may also be the owner of the currency exchange business and have responsibilities for both conducting the day-to-day business and overseeing compliance. For medium sized providers of prepaid access, the BSA/AML Compliance Officer may also have other duties in addition to overseeing a compliance team focused on BSA/AML matters. For a larger money transmitter, the BSA/AML Compliance Officer may oversee a sizable team focused on BSA/AML matters. In all cases, the BSA/AML Compliance Officer should be able to dedicate the adequate time to oversee the program and should be of sufficient seniority to effect change within the organization.

2. *Internal Controls*

A system, or structure, of internal controls must be in place at each MSB. That system, based on the results of an ongoing risk assessment, creates the framework for an effective compliance program. At minimum, MSBs should develop internal control processes for:

- Policies and procedures, including periodic reviews and updates;
- Consumer identification;
- Integrating automated data processing of attempted and completed transactions;
- Monitoring to identify reportable activity;
- Tools calibrated to the specific MSB business model;
- Dual control and segregation of duties;
- Management information reporting;
- Regulatory reporting, including quality assurance and/or control processes;
- Responding to law enforcement and other information requests; and
- Recordkeeping and retention.

MSBs should keep in mind that regulators generally expect controls to be documented. It may not be enough to be able to verbally explain the control system or process without providing an accompanying procedure document against which examiners can validate. It is also worth noting, the act of creating written procedures that do not reflect actual practices will likely garner regulatory criticism.

3. *AML Training*

Documenting processes and requirements is an important step toward meeting requirements. The next logical step is to ensure all appropriate employees are trained to understand and adhere to these processes and requirements. At a minimum, the MSB should:

- Require training for newly hired employees either before they begin working or within a very short period after commencing work;
- Consider requiring AML training for all employees regardless of role or title;
- Tailor training content to job descriptions ensuring those with highest risk jobs receive more frequent and more targeted and detailed training;
- Update training content to include changes in internal policies, regulations and lessons learned from recent enforcement actions;
- Ensure that individuals who change job title or responsibilities receive appropriate training within a reasonable period after assuming the new role;
- Provide access to specialized training and certifications for compliance officers and other staff, as appropriate;
- Create Board and senior management specific training to convey the importance of a "culture of compliance" and to explain the contents of audit and examination reports that they will receive;
- Require ongoing and relevant training rather than a one-time, one-size-fits-all training;
- Test comprehension after training sessions and retrain if employees fail to grasp concepts;
- Offer targeted training when employees breach specific internal or regulatory requirements;
- Issue reminders to employees and supervisors of employees when training is coming due; and
- Retain records of all training attendance.

4. *Independent Testing*

The fourth pillar of a sound compliance program is the independent, or third party, review of the other program pillars. While the risk assessment the MSB performs should dictate the frequency with which independent testing is performed, MSBs should generally consider having annual reviews, at a minimum.

Regarding independent testing, there are several important points for MSBs to consider, including:

- Regulators will assess the competency, independence, and any potential conflicts of interest of the third party selected to perform testing;
- The reviewer, or testing team, must be truly independent, which may include an Internal Audit department;

- MSBs should carefully interview multiple qualified third-party firms – with expertise in the products and services particular to the MSB - to perform the independent review;
- MSBs should obtain and document Board selection and approval of the selected testing candidate;
- Upon completion of the review, the final testing report should be addressed directly to the Board of Directors; and
- MSBs should consider new independent parties every few years to ensure a fresh perspective.

When vetting third party firms, MSBs should verify that the scope of the independent test will include:

- Review of the risk assessment;
- Transaction testing to verify adherence to reporting and recordkeeping;
- Review of the monitoring systems;
- Testing of processes to identify unusual activity;
- Evaluation of adequacy of human and other resources;
- Determination of the adequacy of training materials and record retention;
- Assessment of management's efforts to remediate previously identified issues;
- Evaluation of the overall adequacy and effectiveness of the AML compliance program; and
- An executive summary and audit opinion.

When preparing for the independent testing process, MSBs should:

- Designate a knowledgeable spokesperson(s) to interact with the auditors;
- Provide training to staff on the audit process, interacting with auditors, and the process for providing documents and answers to auditor questions;
- Track requests and retain records of all items provided;
- Request feedback throughout the review process as issues are identified and escalate material items to senior management immediately;
- Request that the auditors cite legal requirements for any identified issues when possible; and
- Following the review, develop specific action plans to resolve identified issues, assign ownership, and track findings through to resolution, since subsequent auditors will review remedial actions.

Consumer Due Diligence and Beneficial Ownership

FinCEN issued the expectation for establishing a risk-based, consumer due diligence (CDD) procedure on May 5, 2016. The final rule became effective July 11, 2016 and requires all covered institutions to comply by May 11, 2018.

The CDD Final Rule, also referred to as "the Fifth Pillar of AML Compliance", adds a new obligation for covered institutions[2] to collect and verify personal information of the actual people (beneficial owners) who own, control, and profit from companies when accounts[3] are opened in those company names.

This Rule does not currently apply to MSBs. However, with the potential that this requirement could pertain to MSBs in the future, it is worth considering its implications when building a compliance program.

Culture of Compliance (Line of Business Involvement)

While compliance personnel of MSBs are the individuals responsible for designing and implementing all pillars of a compliance program as described above, the success of the program depends on a strong companywide, senior level commitment to a culture of compliance. If the risk assessment is the framework upon which each pillar of a compliance program is built, a strong compliance culture is the insurance for the program.

In a 2014 Advisory,[4] FinCEN explains that MSBs will successfully create cultures of compliance if:

- The leadership team is active and engaged in understanding compliance efforts;
- The desire to increase revenue does not supersede mitigating risks;
- Information is shared across various departments; and
- Adequate resources are devoted to compliance initiatives.

In short, Compliance departments do not exist without the business and vice versa. With this in mind, an MSB compliance officer should:

- Define and communicate cultural values and expectations;

[2] Some financial institutions, such as money services businesses, are not yet covered, but FinCEN has indicated it may extend CDD requirements to other financial institution types in the future.

[3] Many MSB operating models do not involve opening "accounts;" however, if certain services (e.g., business to business payments) are offered by an MSB, it is foreseeable that collection and verification of beneficial ownership could be required.

[4] See FIN-2014-A007: "Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance" (August, 2014).

- Be involved in new product discussions with the business staff prior to launch;
- Do not sacrifice necessary controls when considering ways to serve consumers of the MSB;
- Create frequent opportunities for Compliance and Business representatives to discuss successes, opportunities, challenges, and ways to support each group’s initiatives; and
- Provide safe ways for employees to report malicious or negative news.