ACAMS TODAY™

Evaluating AML compliance programs in MSBs

The number and types of financial products and services are rapidly expanding. Various organizations have developed applications for investing, sending money or paying bills. In addition, many businesses transfer money around the world or offer check-cashing services. These unique products have improved financial accessibility to underbanked populations and changed the traditional money services business (MSB) landscape.

Businesses that offer these types of products and services need to take steps to mitigate money laundering and terrorist financing risk. One of the most critical of these steps is to evaluate the effectiveness of their anti-money laundering (AML) compliance programs. By following leading practices, MSBs can conduct business safely and in compliance with regulatory requirements.

ACAMS

Reprinted with permission from the
ACAMS Today December 2022-February 2023, Vol. 22 No. 1,
an ACAMS publication. © 2023
www.ACAMS.org | www.ACAMSToday.org

Crowe

MSBs and regulations

MSBs are required to register with the Financial Crimes Enforcement Network (FinCEN) and adhere to Bank Secrecy Act (BSA) requirements (31 CFR 1022.380 [a]-[f]).[1] According to FinCEN's definition, MSBs encompass a vast array of nonbank financial institutions, including, but not limited to, check cashers, providers of prepaid access and money transmitters.[2] This definition also includes small businesses such as liquor stores that offer MSBs services and virtual platforms with no physical presence. In addition, per FinCEN's final rule in 2011 (CFR 1010.100 [ff]), any foreign business operating in the U.S. with defined MSB services is required to adhere to MSB regulations.[3]

According to FinCEN's interim final rule (31 CFR 103.125), MSBs are required to implement an AML compliance program with adequate and appropriate policies, procedures and processes to mitigate money laundering and terrorist financing risk.[4] FinCEN's MSB exam manual outlines four pillars[5] all MSBs should maintain for an effective and robust compliance program. The four pillars are the basic foundation of an MSB AML compliance program, and the designated officer should uphold the pillars through internal and independent review processes. The pillars encompass:

1. Policies, procedures and internal controls to support ongoing compliance
2. A designated individual responsible for ongoing compliance
3. Training
4. Independent review of the program

The customer due diligence final rule issued by FinCEN in May 2016 is not applicable to MSBs.[6] However, its requirements should be considered when designing or enhancing an MSB AML program as it might be required by banking partners or by FinCEN in the future.

Per the Basel Committee's "Sound Management of Risks Related to Money Laundering and Financing of Terrorism," issued in February 2016 and amended in July 2020, AML functions must maintain three lines of defense to mitigate money laundering and financial crime.[7] The first line of defense is the line of business; the second is the internal AML compliance function; and the third is independent internal audit. The second and third lines of defense are especially important to maintaining a strong and effective AML compliance program.

Given the nature of the increasingly connected, global and expanding financial industry, MSBs should understand the importance and value of AML compliance programs. Such programs provide strong enterprise AML risk assessment that supports the identification, creation and management of mitigating controls and processes, which are assessed periodically through second-line compliance testing and third-line internal audits.

The importance of a risk assessment

A strong enterprise risk assessment is a critical component of an effective AML compliance program. All MSBs are responsible for creating a risk assessment that incorporates product, service, customer and geography risk. Because of the variety of products and services MSBs offer, the diversity of their targeted customer bases and their global reach, no two MSB risk assessments will look the same. All businesses offering services under the MSB definition should evaluate the extent and nature of their AML risks to properly assess their risk exposure and develop and implement controls to mitigate the identified risks.

For compliance officers to properly identify and evaluate risks, they must first assess the inherent risk of the following categories:

- Products and services, such as check cashing, payment processing and prepaid cards
- Customer base, including consumer and entity types, industry types and volume of transactions
- Geography, such as where products and services are offered and the incidence of business in high-risk countries

After all inherent risks are identified, MSBs must evaluate the effectiveness of the controls that are in place to mitigate each stated risk. The residual risk score incorporates the control effectiveness assessment relative to the inherent risk the control was implemented to mitigate. The risks and controls should be documented, and any gaps in the mitigating controls

A strong enterprise risk assessment is a critical component of an effective AML compliance program

should be identified and remediated to decrease overall residual risk. This risk assessment is a vital tool that can help an MSB identify risk gaps and build or evaluate its current AML compliance program.

Second-line compliance

All MSBs must have an AML compliance function to create, implement and manage policies, procedures and processes to mitigate money laundering risk and adhere to regulations for compliance and suspicious activity reporting. MSBs also should have a program in place to test and monitor for ongoing compliance in the following areas:

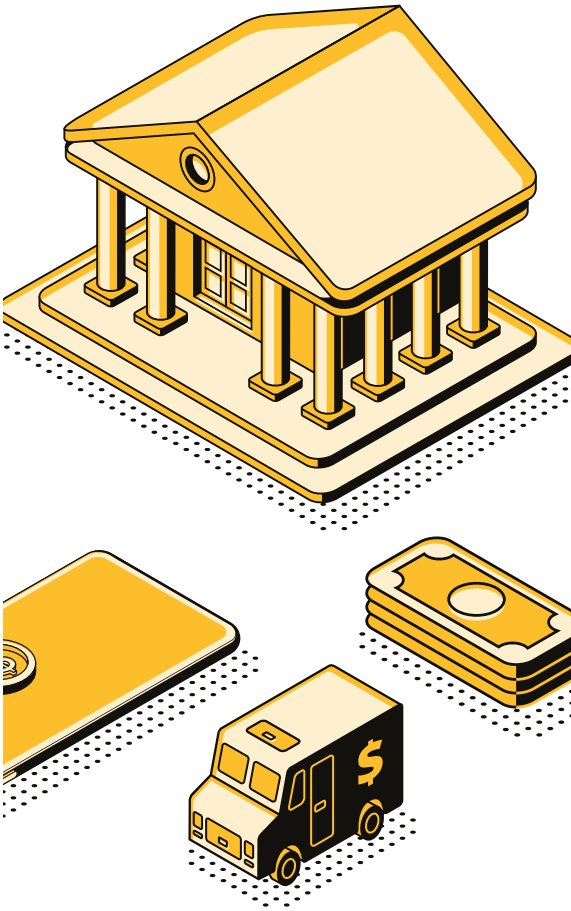
- Customer onboarding
- Enhanced due diligence for higher-risk customers
- Transaction monitoring
- Regulatory reporting through currency transactions and suspicious activity reports
- Agent due diligence and oversight

How MSBs implement, test and monitor their compliance function varies greatly based on size and complexity. Smaller MSBs might not need to address global regulations because they only operate in one jurisdiction, while larger MSBs must consider how they can use technology to simplify and strengthen their control environment.

Smaller MSBs, such as financial technology (fintech) companies offering money transfer services to a small customer base, should ensure they have designated a specific person to implement and manage the compliance function. The MSB also should appoint an individual that can oversee all functions of the compliance program, conduct all compliance duties and partner with senior management to ensure efficient communication. The designated compliance individual is especially critical to smaller MSBs because he or she has limited resources to manage the compliance function. A compliance officer at a small MSB must be knowledgeable and experienced in AML laws, regulations and risks. In addition, working in partnership with business-line leaders is paramount. MSB growth plans must be aligned with the scalability of the compliance program.

Medium-sized MSBs should maintain adequate staffing, establish oversight over the compliance function and implement technology to ensure AML effectiveness. As an MSB scales its operations, a designated compliance officer must assess whether adequate staffing is in place to conduct compliance duties. The compliance officer should oversee compliance functions, and this person will likely be unable to conduct all day-to-day duties as the business grows. Well-trained individuals should be in place to support the compliance officer and identify high-risk customers at onboarding and monitor and investigate suspicious activity. In addition, this team needs access to the right technology to support onboarding and monitoring processes. Medium-sized MSBs should have the resources to implement a transaction monitoring system, and the system should be manageable so that the compliance team can fine-tune it without specialized system experts.

Large MSBs with a global reach should have a fully staffed compliance department that reflects the volume of products and services offered, the customer base and the geographies served. Larger MSBs might have an entire department for compliance and might also need a dedicated second-line compliance testing function to monitor quality across the AML program. The compliance testing function at a large MSB independently tests and monitors the control environment, including customer onboarding, alert review and suspicious activity investigation functions, among others. With more support and resources available, larger MSBs can rely on technology to achieve efficiency and accuracy. Automated models might aid with transaction monitoring, sanctions screening and suspicious activity alerting. Technology is critical to larger MSBs, which should have the resources for systems to run effectively and make changes as needed.



Third-line compliance testing

Third-line compliance testing engages an independent party (internal or external) to review the entirety of the AML program. This independent perspective is critical to identifying AML program enhancement opportunities and potential regulatory risks. Smaller MSBs should consider hiring an independent auditor, while larger MSBs might have an internal audit function to perform the review.

Independent auditors engaged for such reviews should have appropriate qualifications and expertise and be:

- Well-versed in regulatory requirements for MSBs
- Experienced with the independent review process
- Associated with a trusted or well-known firm, if a third party
- Up to date on industry best practices that should be incorporated into the testing plan

The internal audit process should be sound and include the following:

- An understanding of the MSB's unique business model
- A tailored scoping plan to evaluate all risks
- Sample-based testing for control areas
- An explanation of the results of any findings
- A documented action plan to remediate identified gaps or exceptions
- Follow-up on the actions taken to confirm remediation has been completed

Each MSB is unique in the products and services it offers, and therefore all MSBs cannot be tested in the same way. Whether the independent auditor is internal or from a third party, he or she must fully understand the business type and unique risks in order to adapt the testing plan to the business.

During the review, the auditor must critically challenge the entire AML program and the related products and services covered by AML requirements. First, the auditor will need to review the risk assessment to fully understand the testing program and all applicable customers, products, services and geographies that are in scope. The auditor should also assess the policies and procedures to confirm that the design of controls is appropriate and aligned with regulatory requirements and expectations as well as industry best practices. Second, the auditor should test the effectiveness of controls through a sampling approach. The independent review can determine if the documented controls are properly implemented and executed to mitigate AML risk. This review is an opportunity for the MSB to have the program thoroughly tested to identify any weaknesses in its AML compliance program and confirm the effectiveness of the controls that are in place.

One of the more critical components of the independent review process is reporting all observations to the compliance officer so the officer can develop a remediation plan. The compliance officer should communicate the noted observations to senior management and track the remediation progress. Regular, independent reviews are essential for identifying deficiencies and continually strengthening an AML program.

An effective AML compliance program is cohesive, effective, inclusive of all risks and adaptable to future changes

Takeaways

An effective AML compliance program is cohesive, effective, inclusive of all risks and adaptable to future changes. The designated compliance officer should focus on implementing and managing a controlled environment that is tailored to specific risks and that aligns with regulatory requirements. For ongoing compliance effectiveness, the program should be regularly tested. Regular testing can identify any potential deficiencies and strengthen an AML compliance program to successfully mitigate money laundering within any MSB. AT

Gary Lindsey, principal, Crowe, gary.lindsey@crowe.com

Kristina French, Crowe, kristina.french@crowe.com

Jacob Rivkin, Crowe, jacob.rivkin@crowe.com

1 "BSA Requirements for MSBs," *Financial Crimes Enforcement Network*, https://www.fincen.gov/bsa-requirements-msbs

2 "Money Services Business Definition," *Financial Crimes Enforcement Network*, https://www.fincen.gov/money-services-business-definition

3 "Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses," *Federal Register*, July 21, 2011, https://www.federalregister.gov/documents/2011/07/21/2011-18309/bank-secrecy-act-regulations-definitions-and-other-regulations-relating-to-money-services-businesses

4 "Financial Crimes Enforcement Network; Anti-Money Laundering Programs for Money Services Businesses," *Federal Register*, April 29, 2002, https://www.federalregister.gov/documents/2002/04/29/02-10453/financial-crimes-enforcement-network-anti-money-laundering-programs-for-money-services-businesses

5 "MSB Examination Materials," *Financial Crimes Enforcement Network*, https://www.fincen.gov/msb-examination-materials

6 "Information on Complying with the Customer Due Diligence (CDD) Final Rule," *Financial Crimes Enforcement Network*, https://www.fincen.gov/index.php/resources/statutes-and-regulations/cdd-final-rule#:~:text=It%20requires%20covered%20financial%20institutions,owners%20of%20companies%20opening%20accounts

7 "Sound management of risks related to money laundering and financing of terrorism: revisions to supervisory cooperation," *BIS*, July 2, 2020, https://www.bis.org/bcbs/publ/d505.htm