

Beat 9 common BSA/AML weaknesses

Find them now--before
examiners do

Is something missing
from your bank's Bank Secrecy Act/anti-money-laundering program?

By Maleka Ali, CAMS, risk
management consultant and manager, consulting and education department,
Banker's Toolbox, Inc.

Over the last several months, there have been headlines
warning of increased scrutiny by examiners on BSA/AML and dire consequences for
banks unprepared for their exams. Many financial institutions, both big and
small, are being hit with enforcement actions and severe penalties.

Over the last few years, regulators and examiners had been
concentrating their efforts on problems stemming from the recent financial
crisis. But now the trend has turned back to money laundering and the Bank
Secrecy Act. So be warned that even if your last exam went well or was even a
non-event, don't have the same expectations for the upcoming BSA/AML exams.

Remember to evaluate and review your program for any
weaknesses on a periodic basis.

"This is the way the customer has always behaved" is not a solid justification for not filing

—Maleka Ali, Banker's Toolbox

What should you be looking for? What can you do to shore up your BSA/AML program to ensure you don't fall under the regulator's lash? Let's address nine of the most common weaknesses.

An observation:

The first four shortcomings concern lack of structure or organization. Many institutions have been criticized for not having an effective suspicious activity monitoring program, for instance. It must be risk-based, but in order to be effective it must also include four basic components:

- Identification or alert of unusual activity.

- Management of alerts.

- Suspicious Activity Report decision making.

- SAR completion and filing.

The absence of any of these four components could make the effectiveness and structure of your program fall apart and fail. Look closely at your existing program and ensure that your policies and desktop procedures clearly document all four processes.

Weakness #1: Inadequate identification or alerting of unusual activity.

A good program uses a combination of methods in order to effectively identify suspicious activity. This includes employee identification, law enforcement inquiries, or other referrals and transaction and surveillance monitoring system output. (See the FFIEC BSA/AML exam manual for more detail.)

The decision of which method or methods to use is risk-based, but don't just rely on system reports or alerts. If frontline employees are not reporting any activity, an examiner may take that as a sign that staff training is inadequate. (See #9-Training.)

Weakness #2: Not managing alerts effectively.

Focus on the processes used for investigation and evaluation. Procedures must include a clearly defined path for escalating an issue from point of initial detection to completion of the investigation. The bank must assign adequate and well-trained staff to the identification, evaluation, and reporting of suspicious activity.

If the bank has significant concentration of a higher-risk product, service, or entity, you may need to employ additional staff to comprehensively monitor suspicious activity.

Weakness #3: Not documenting SAR decision making process.

Findings from research and analysis should be forwarded to the final decision maker. This process should be clearly described in your policy and procedures, in addition to defining whether it is an individual or a committee who makes the final decision.

The final decision to file or not file must be thoroughly documented, with the inclusion of a solid justification for that decision.

"This is the way the customer has always behaved" is NOT a solid justification for not filing.

Instead, document the reason why the activity is not suspicious for that customer.

A key point: Examiners are instructed not to criticize individual no-SAR decisions, unless the failure was significant or accompanied by evidence of bad faith. Instead, they are asked to concentrate on whether the institution has an effective SAR decision making process.

Weakness #4: Late, inaccurate, incomplete SARs.

Policies and procedures must be in place to ensure that SARs are not only filed in a timely manner, but are complete and accurate, including a narrative that provides sufficient description of the activity along with the reason why it is suspicious.

SAR rules require that a SAR be filed no later than 30 days from the date you determined activity to be suspicious and SAR-reportable.

The institution's AML system or initial discovery of the activity may flag the transaction; however, this should not be considered "initial detection." The countdown does not begin until an appropriate review has been conducted and the "SAR decision maker" has determined it to be SAR reportable. The review should still be completed within a reasonable period of time to assist law enforcement, but what constitutes "reasonable" will vary. The key factor is that the bank has established adequate written procedures and that those procedures are being followed.

If the activity is ongoing, FinCEN's guidelines suggest that banks should report continuing suspicious activity by filing a report at least every 90 days. A clarification was provided by FinCEN in this year's SAR Activity Review-Trends Tips & Issues (Issue 21- Section 4) in regards to the deadline for the filing of ongoing SARs. The clarification reads: "Financial institutions may file SARs for continuing activity after a 90 day review with the actual filing deadline being 120 days after the date of the previously related SAR filing."

Weakness #5: Risk assessments lack supporting documentation.

Examiners need more facts, justifications, and documentation in the risk assessment. They may not disagree with your overall conclusions

But, in order to properly examine that you have a sufficient BSA program, they have to understand the risks at your institution. Without any supporting documentation, they will not know how you came to your conclusions.

For example, if you say you have low geographic risk, explain where your institution and your customers are located. Is it a high-intensity drug trafficking area or a high financial crime area? Do you have significant international activity? And is it within high-risk jurisdictions? If you have identified any significant risks, what types of mitigations has your institution set in place?

Update your risk assessment on a periodic basis. Periodic may mean more frequent updates than annually if your institution has major events such as mergers or acquisitions.

Weakness #6: Monitoring program has not been updated recently or independently validated.

After updating the risk assessment, management should review the suspicious activity monitoring procedures and programs established, along with filtering criteria and thresholds to ascertain they are still effective for the risk at your institution. Ensure you are keeping up with new current technology trends and emerging threats.

In addition, the monitoring system's programming methodology and effectiveness should be independently validated to ensure that they are detecting potentially suspicious activity.

Conduct a periodic data validation of the data importing into your systems to ensure you have the data you need to monitor suspicious activity and add this transaction testing to your independent audit.

Weakness #7: Customer Due Diligence (CDD) process not effective.

Having a strong and capable customer due diligence process is more than just collecting customer identification program information with verification upon proper ID. The purpose of CDD is to enable the bank to predict with relative certainty the type and volume of activity the customer will be conducting.

An institution is obligated to collect sufficient customer information in order to implement an effective suspicious activity monitoring system. This information should also provide the institution with the ability to differentiate between lower-risk and higher-risk customers at account opening.

When opening a business account, identify the business type. If it is determined the firm is a higher-risk entity (i.e., nongovernment organization, professional service provider, or nonbanking financial institution), ask for additional enhanced due diligence information. When opening a consumer account, identify the resident status, if they are a politically exposed person, or if they will be using their account for business purposes or conducting any international activity.

Remember, customer due diligence is the cornerstone of an effective suspicious activity program. If you don't really know or understand your customer, how will you determine if their activity is unusual or suspicious?

Weakness #8: Improper identification and Enhanced Due Diligence of high-risk accounts.

It is critical to identify your high-risk accounts.

Although any type of account may be susceptible to money laundering or terrorist financing, some customers may pose more specific risks by the nature of their business, occupation, or transaction activity.

The Exam Council's manual provides guidance on this: It advises that during the risk-assessment process, it is important that banks exercise judgment and not treat all members of a specific category of customer as posing the same level of risk. In assessing customer risk, banks should consider other variables, such as services sought, transaction activity, and geographic locations.

Keeping this in mind, it is recommended that accounts be risk-rated initially at account opening and then on a periodic basis to take into consideration the actual activity being conducted.

Once you have determined that a customer poses a higher risk, the bank should conduct further enhanced due diligence. Remember, the goal of having a list of high risk customers is not simply to identify them.

They are rated high risk because they pose a higher risk for fraud or money laundering. Therefore, you have an obligation to review them more closely and frequently to ensure they are not conducting suspicious activity or putting your institution at risk.

The detail and scope of review will vary depending on the level of risk at your institution or the type of customer. A high-risk consumer may require collecting information on the source of wealth or funds involved.

And the bank may need to review the customer's account for unusual activity, whereas an MSB may require a site visit and increased scrutiny to ensure that their activity is not unusual.

Weakness #9: Training isn't effective.

Often, when a weakness in a BSA program is identified, it is tied back to training. Training is crucial as it is one of the original 4 pillars to an effective program.

Hot buttons include:

- New employees. BSA training/policies and procedures should be provided to new employees as part of employee orientation prior to hitting the trenches.

- Wide coverage. BSA/AML training is critical to all business lines including branch staff, loan department, trust department, back-shop operations, etc.

- Specific training. Training should be tailored to the employee's specific duties.

- Comprehensive training. Training should include not only BSA and how to identify suspicious activity, but also include the bank's internal policies, procedures, and systems. It should also cover how to escalate any suspicious activity to the appropriate department.

- Train the experts too. BSA officers should receive periodic training that is relevant and incorporates current developments, emerging risks/trends, and changes to the BSA and related regulations.

- Train directors and trustees. The Board of Directors needs BSA training to understand the importance of BSA/AML regulatory requirements, ramifications of noncompliance, and risks posed to the bank.

- Train for your tools. Staffs utilizing BSA/AML monitoring systems need to be provided with comprehensive and ongoing training to maintain their expertise.

- Document training regime and training accomplished. Banks should document and maintain training and testing

materials, dates of training and attendance records, and should be made available for examiner review.

[This article was posted on October 4, 2012, on the website of ABA Banking Journal, www.ababj.com, and is copyright 2012 by the American Bankers Association.]