What Auditors Should Know and Ask About BSA/AML Software Before a Successful Audit Can Be Conducted

Nancy E. Lake, CAMS
Atlantic Community Bankers Bank

Opinions posted here are that of the author and are not approved or shared by Atlantic Community Bankers Bank.
**Introduction**

When it comes to auditing BSA/AML programs, one of the first questions the average auditor will ask is: “Do you have a manual or an automated process?” The usual assumption is that since an automated system is supposed to be more effective than a manual system, that it actually is more effective. An automated process is supposed to be much better than a manual process because an automated system has the ability to analyze large amounts of transactions and produce “red flags” or alerts to identify potentially suspicious activity that may not be detected in a manual process. However, auditors need to understand that this assumption can actually be totally false. If BSA/AML software is implemented incorrectly and/or ineffectively, then monitoring and reporting can be inaccurate.

The Federal Financial Institutions Examination Council BSA/AML Examination Manual states, “Suspicious activity reporting forms the cornerstone of the BSA reporting system.” With that in mind, it is important to understand that an inaccurate and/or ineffective monitoring and reporting system could result in the complete failure of a BSA/AML program and open the financial institution to potential fines and enforcement actions.

Before beginning an audit and relying on the reports and alerts generated by the software, the auditor must ensure that the BSA/AML software has been correctly and effectively implemented and utilized. If the IT audit included the BSA/AML monitoring system, the BSA auditor can review the IT audit findings and comment on them. If the IT audit did not address the BSA/AML monitoring system, it is important that the BSA auditor understands how the software was implemented and is currently utilized. However, it is not the responsibility of the auditor to test the system but to ensure the testing was conducted and was reasonable.

While serving as a BSA Officer in several financial institutions, I have implemented and used various types of software systems. Although I am not an Information Technology expert, I observed shortcomings in some audits with regard to the automated software systems. I realize with the large variety of monitoring software on the market today, an auditor can be overwhelmed trying to understand all of them.

As such, the objective of this white paper is to assist auditors by enabling them to understand what is “behind the curtain” of an automated program and providing insight into three key areas:

1. Types of Software
2. Implementation of the Software
3. Usage of the Software

This is not intended to be an exhaustive discussion of all of the aspects that should
be addressed in the audit of an automated system, since a BSA audit is not a software audit. However, it will provide a solid introduction of critical elements that all auditors should understand thoroughly and explore with the financial institution before proceeding with the rest of a BSA/AML audit.

**TYPES OF SOFTWARE**

The rush to develop transaction monitoring systems began soon after the passage of the USA PATRIOT Act on October 26, 2001. The plethora of systems available today advertise various bells and whistles that distinguish them from one another. Some are more user friendly, provide more detailed and colorful reports, and some have different functionality. Some generate alerts that combine fraud and AML, while others separate the fraud alerts from the AML alerts. Some use fancy terms to explain how their systems operate while others claim to be “Risk-based” which is great advertising, since everything in the BSA world is based on risk. However, all systems have to employ one or more basic principles of detecting suspicious activity. One key to conducting a successful audit is to obtain a clear understanding of the detection principles of the automated system that generate the reports on which the audit is based. Although there are a multitude of BSA/AML software vendors, they all base their systems on one or more of the following principles.

**Risk-Based**

A system that detects suspicious activity cannot be only “risk-based.” Any vendor that claims to have a risk-based system must still employ some method of detecting suspicious activity, such as rules, behavior, “intelligence” or a combination of these. So when a vendor indicates a system is risk-based, it means that the system can incorporate various factors that help create risk models to identify customers that could potentially pose a low, medium or high risk of fraud or money laundering. These factors can include things such as NAICS codes, zip codes (indicating a High Intensity Drug Trafficking Area or High Intensity Financial Crime Area), volume, frequency, high risk entity types such as money services business, remote deposit customers, ATM customers, politically exposed persons, ACHs or wires to or from certain higher risk countries, correspondent banks, etc.

Of course with the focus on risk assessments and the expectation to tailor a BSA/AML program to a risk assessment, the capability to identify risk factors in a software system is essential. Depending on the software system, the risk factors may be set by the system itself and tweaked as needed by the user, or the risk factors may be determined completely by settings controlled by the user. As an auditor, understanding what generates the initial risk scoring and how those scores can be adjusted by the user is critical to determining if the risk scoring is appropriate based on the risk assessment of the financial institution. It will also enable the auditor to more effectively evaluate the customer due diligence, enhanced due diligence and monitoring processes.

---

**Rule-Based**

Rule-based systems are ones that identify suspicious activity by comparing transactional data to specific scenarios that mimic suspicious activity. These scenarios can be created using a multitude of factors such as transaction type (wire, ACH, ATM, etc.), frequency, volume, individual vs. entity, SS vs. EIN, percentages, inflow and outflow. The more factors that are included increase the specificity of the rules and increase the number of rules. For example, one rule could be: ACH activity: Within 30 days, a customer conducted transactions more than four times the same amount of money, which amount to larger than $5,000. Each of the underlined items could be changed and a new, but similar rule could be created. This rule could be run using other variables such as a Tax ID number, individual or business. If you create a rule with these categories and also add percentages of incoming and/or outgoing transactions, you can see how infinite the number of rules could be.

The disadvantage of rule-based systems is that they tend to generate numerous false positives, but most systems allow you to flag false positives so they do not continue to reappear. On the other hand, there are several advantages to a rule-based system. Typically these systems are not as expensive as other systems and are easier for the user to understand and explain to an auditor or examiner.

It is important to understand that most systems employ rules to some degree. As an auditor, you should know the rules being used and how the parameters of those rules are determined. Typically, software vendors provide an established set of assumptions that can be used for the initial set-up and up to the first year of usage. Then, as the users become more familiar with the system, assumptions should be re-evaluated to ensure they are appropriately tailored to the bank’s operations, needs and risk profile. It also needs to be noted that banks should keep documentation of the initial assumptions and any changes made to those assumptions. Examiners will want to see the changes made and the reasons for those changes.

**Behavior-Based**

There are some systems that track the “normal” behavior for an individual customer and generate alerts when a customer conducts a transaction outside of his/her own individual “normal” range. Other systems take all of the customer activity of a financial institution and determine the average transactions or “norms” for the entire customer base. Then, standard deviations or differences from the “normal” activity are calculated. These standard deviations are then factored into monitoring systems and trigger alerts when certain deviations are reached by a customer or group of customers.

It needs to be noted that standard deviations are only beneficial if the customer data used for comparison is comprised of similar customer characteristics or factors. For example, a community bank that is made up of customers from the local community would have a customer base of similar customer types. However, if that community bank also has money service businesses that are international money transmitters, it is more difficult to establish a “norm” because the activities are dissimilar in nature and risk. The activity of the money transmitter would
skew the norm and not give a clear picture of the normal activity for the primary customers. In such a scenario, the norms would have to be calculated separately, one for the local customers and one for the money transmitters. Only then could the monitoring system trigger effective results.

Some behavior based systems compare activity to an account holder’s profile and past behavior and assigns each transaction a “probability score” that represents the likelihood it’s legitimate.³

Other systems use “Peer Group Analysis” for various customer types and/or certain behaviors such as elder abuse. Transactions for older customers (such as over age 70) are compared and deviations from the norm generate alerts. These alerts would be investigated for potential elder abuse.

As an auditor, you should have a clear understanding of the triggers for the various alerts within the system. If a user indicates that a behavior-based system using standard deviations is being utilized, you should request the reports indicating the standard deviations that drive the alerts. If peer analysis is used, you should determine the peer groups being targeted.

“Intelligent” Systems
More expensive systems use more sophisticated methodologies such as decision tree analysis or neural networks. Decision trees simply determine trends in data and develop conclusions based on a variety of variables. BSA/AML software using decision tree analysis, determines trends in the customer data which is then used to generate alerts based on fitting those trends to known fraud or money laundering profiles.⁴

“Neural networks are based on efforts to model information processing in such a way that mimics the human brain’s capacity to learn. This is also referred to as artificial intelligence.”⁵ Neural networks use algorithms that enable the system to acquire knowledge or adapt. These types of systems therefore can potentially identify a variety of money laundering or fraud scenarios that other types of systems may miss.

Even though these types of systems can potentially identify many more types of suspicious activity, they are often the most difficult to audit. Explaining exactly what triggers the alerts seen in the system can be very difficult and therefore almost impossible to prove the validity of the decisions made based on those alerts. As an auditor, you should request system reports that explain the factors that would trigger alerts in the system.

Combination Systems – Think “Rubik’s Cube”
Due to the increased regulatory fines for BSA/AML and the increased expectations of regulators to capture suspicious activity, more and more financial institutions are implementing BSA/AML software. Vendors are rising to the challenge and constantly upgrading their systems to meet the expectations and demand. Therefore, most vendors are not using just one detection principle anymore but are incorporating several types in

---
order to be more effective and marketable. You will hear terms like “multidimensional,” “cross-stream,” and “cross-channel” from vendors who utilize multiple detection principles and various data sources to risk rate customers and identify suspicious activity. For example, some systems only use the standard transactional activity from the core system while others can include such things as address changes, new PIN codes, new accounts opened, etc. Each system has its own philosophy and techniques of how monitoring is performed.

As stated previously, the BSA Officer should be able to explain the factors that would trigger alerts in the system and provide reports generated from system data to support that explanation. Requesting those items should be part of your pre-planning process for each audit.

Latest Technology
Since numerous consent orders have been issued and massive fines have been levied, financial institutions are justifiably concerned that their BSA/AML program may have holes that could cost them heavily. One area of concern is international wires. For those financial institutions engaged in international activity, wire stripping (i.e., deleting critical pieces of information from wire data that would trigger an OFAC match) is a major concern. Some software companies are developing software that would indicate whether wires were stripped or even resubmitted. Resubmitted wires are wires that were originally rejected by OFAC screening software and then resubmitted with the data pieces removed that could have caused the wire to be rejected the first time. To prevent this, some software has the capability to scan all approved wires with previously rejected wires to look for similarities and identify resubmissions.

Another type of software does not risk-rate customers on transactional activity but utilizes the World Wide Web. Customers are compared to a data base of information that includes any type of international negative media that is constantly updated from global sources such as global watch lists, regulatory authority actions, and law enforcement. The users can determine what information is important to mitigate the risks within their financial institution and can filter the results accordingly. This enables them to see beyond the limits of the activity that occurs within their own four walls and gives them a global picture of each customer allowing a more complete risk profile to be determined.

IMPLEMENTATION OF SOFTWARE

Once an auditor understands the exact nature of the system utilized by the financial institution, the next step is to determine how the software was implemented. The method by which BSA/AML software is implemented can sometimes be more important than the type of detection principles the software uses, especially when it comes to the effectiveness of the system.

The method by which BSA/AML software is implemented can sometimes be more important than the type of detection principles the software uses, especially when it comes to the effectiveness of the system.
If you have never had the “joy” of implementing software, count your blessings! Those who have know that the promised three to six-week implementation schedule offered by some software vendors is often a far cry from the actual time frame required. The implementation time frame required is based on many factors. However, from the audit perspective, the key factor is ensuring data integrity.

Data integrity is determined by data validation and an auditor should confirm this was initially performed and is an ongoing process. “Data Validation is the process of ensuring that a program operates on clean, correct and useful data. It uses routines, often called ‘validation rules’ or ‘check routines’, which check for correctness, meaningfulness, and security of data that are input to the system.”⁶ Data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle.”⁷ Since many use these terms interchangeably, “data validation” will be used throughout this paper to indicate the process of ensuring accurate information within the software system.

The goal of an auditor should be to determine whether all the critical pieces of data that would affect the monitoring processes or risk profiles of the system are correctly flowing into the system. These pieces would include things such as customer profiles, transaction codes and transaction types. The old principle still applies, “garbage in, garbage out”! Generally, an auditor is not responsible for conducting data validation of a financial institution's automated software.

However, an auditor should ensure that testing was conducted in accordance with regulatory guidance.

The first thing to determine is if the software compares transaction activity to anticipated activity and utilizes customer profile information to risk rate customers. If the system compares the transactional activity to anticipated activity, it must be determined how the anticipated activity is captured and stored in the system. If the front end is not obtaining anticipated activity or the information is obtained but not flowing into the system, this will make accurate risk rating difficult.

If the system is utilizing data from customer profiles, the auditor must investigate the steps taken to ensure the accuracy and completeness of the financial institution’s customer profiles. If no steps were taken, then there is no guarantee that the results the system generates are accurate. Before implementing software, some financial institutions perform a sampling of customer profiles while others check all customer profiles to determine accuracy and completeness. Of course time, staffing and money are key factors in determining the level of testing the financial institution can and should perform.

Secondly, understanding how transactions are identified in the software is vital to understanding data integrity. Financial institutions utilize transaction (tran) codes. Transaction codes are typically a combination of three or four alphanumeric (letters and numbers) characters used to identify every type of transaction that can occur in a financial institution. These codes are very specific and are used to delineate specific transactions such as

---


whether a deposit was for a time deposit, checking account or a savings account. There might be different codes for a transfer initiated at the teller window, a transfer via the phone or one initiated via internet banking. Each financial institution has a list of these codes. Some BSA/AML Officers will even be instrumental in assigning specific transactional codes for such things as remote deposit capture transactions to increase the effectiveness of the monitoring system’s capabilities to track suspicious activity. As an auditor, it is imperative that you confirm that all of the financial institution’s transactional codes are being utilized in the BSA/AML software.

It is important to mention that transactions hitting general ledger accounts (referred to as GL’s) are often not able to be imported into BSA/AML software. For example, if a financial institution is depositing cash into GL’s for wire transfers or monetary instrument purchases, BSA/AML software would not be able to separate out each individual transaction and tie it to a specific customer. Therefore the auditor should determine how cash purchases of wires and monetary instruments are processed and captured. Some financial institutions deposit the cash into a customer’s account first and then do a withdrawal in order to tie the transaction to a particular customer. Other financial institutions have teller systems that utilize an identification field to accomplish the same thing.

The expectation of most financial institutions and vendors is that auditors will ask about data validation and will verify whether it was completed at the front end and remains an ongoing process. Therefore, it is a prudent practice for financial institutions to implement an ongoing process for data validation. If a new product is implemented, some system or process fails to function properly, a switch is turned off, or something else occurs, data validation could be undermined. As an auditor, understanding the rationale for the frequency and method of these processes is critical.

One other critical point in data validation is understood best by this wisdom from the Bible, “But they measuring themselves by themselves, and comparing themselves among themselves, are not wise.” II Corinthians10:12 KJV. Many vendors provide data validation reports “proving” the accuracy of the data contained within their system. However, if those reports are comparing only the file sent to the software with what went into the software, the picture could be incomplete. Numerous things could have affected the file sent by the institution and/or the provider’s input into the system. The most effective data validation can only occur when core data is compared to the data in the software system.

The most effective data validation can only occur when the core data is compared to the data in the software system.

One way to compare the core data to the software data is to compare total transaction counts and dollar amounts. For example, the total dollar amount and transaction count for such things as DDA’s, COD’s, checks, wires, etc. from the core system can be compared with the automated BSA software totals. If those match, all of the core data flowed into the
BSA software. On the other hand, that comparison will not show if the data was displayed correctly in the software system. Some software vendors are satisfied with less than 100 percent data validation and recommend you only validate the system at installation and seldom thereafter. On the other hand, some financial institutions validate data to the penny every day! Their concern is if validation is not performed daily to the penny, they may miss critical transactions and not even know it. When an error is found, research must be conducted all the way back to the previous data validation date to guarantee accurate CTR and SAR filings. The longer the time frame the financial institution waits to validate data, the more research will need to be conducted when an error is found to ensure all previous reports were filed accurately!

The longer the time frame the financial institution waits to validate data, the more research will need to be conducted when an error is found to ensure all previous reports were filed accurately!

Another good reason to ensure that validation is performed regularly is that often other factors affect the input of data into the system. If a core report or process fails to function properly and incorrect data or no data is pulled into the software, it is incumbent on the financial institution and not the software vendor to detect that.

Communication between departments is critical to the effectiveness of the system. For example, if IT personnel change parameters in the core systems or changes are made to the teller platform, Internet banking platform, etc., without communicating those changes to the BSA Officer, incorrect data or none at all could flow into the software. It is good for the auditor to determine the safeguards in place to prevent these scenarios from occurring.

When data validation has been completed, another factor to consider is how data is displayed in the BSA/AML software. It is assumed by many that if all transaction codes are flowing into the software that the user has a clear picture of all account activity. This is not always correct. For example, the system may capture a transfer transactional code. However, the system may only show the transfer affecting one account such as the one it left and not the one to which it was deposited. If users can only see the activity of one account at a time, the user may miss the significance of the flow of money from one account to another.

It is also important to understand that what the core cannot identify, the software may not be able to either. For example, check cashing can present a significant problem if the core cannot accurately identify the customer receiving the cash. Various teller systems handle the capture of on us checks (your own bank checks) and foreign checks (other banks’ checks) cashing in a variety of ways. To ensure the accuracy of CTR data, the auditor should verify how this capture occurs.

Another example is ATM cash deposits. Many banks do not have the latest ATM machines that can identify cash vs. check deposits. Therefore, an auditor should determine how cash is captured when it is deposited into an ATM. Some financial institutions use a manual process to track
ATM cash even if they have implemented software. Others use the ATM data to generate reports or feeds that allow the software to capture the information (similar to what is used for wire transactions by using FED files).

If an auditor cannot verify the accuracy of the data and understand how the data is displayed within a software system, then there is no foundation on which to test transactions and confirm CTRs and SARs have been reported accurately.

SOFTWARE USAGE

Once the type of system and the effectiveness of implementation have been determined, another area to consider is how the software is being utilized. It is vital to understand that poor utilization of a software system can negate the effectiveness of even a well implemented accurate system and presents a significant risk to the financial institution.

Poor utilization of a software system can negate the effectiveness of even a well implemented accurate system and presents a significant risk to the financial institution.

Regulators and financial institutions rely on the audit process to reveal any weakness in the BSA/AML program. However, if an auditor does not explore the way in which the software is utilized, fatal weaknesses can be hidden and not identified until it is too late to prevent significant loss to the institution via regulatory fines or fraud.

With that said, all auditors know that training needs to be conducted and documented by the financial institution. It should be a standard part of all audits to review training logs and materials presented for all training sessions, especially BSA/AML. However, it is understood that attendance at a training session does not guarantee training has occurred. According to Wikipedia, “Training is the acquisition of knowledge, skills, and competencies as a result of the teaching of vocational or practical skills and knowledge that relate to specific useful competencies. Training has specific goals of improving one’s capability, capacity, and performance.” 8

(Underlining is mine.) Determining the effectiveness of training is critical to determining effective system usage.

If the user of the software system has not acquired the needed knowledge, skills and competencies to utilize the capabilities of the system, it is like a doctor giving vaccinations with an empty syringe. Competent BSA Officers should have the requisite knowledge, skills and competencies needed to utilize the system effectively. However, the BSA Officer may not be the only user of the software. Therefore, it is the job of the auditor to ensure all users have been trained to possess the knowledge, skills and competencies required to effectively use the software.

Whether the auditor has experience with the software being utilized and has formulated ideas concerning the strengths or weaknesses of the software, or the auditor is totally new to the software, the approach should be the same. Auditors should not reveal their level of understanding of the software and simply ask the user to explain it. Not all users

will be able to immediately articulate everything about the system that the auditor should know. However, letting the user talk first, allowing for brief moments of silence after the user is finished speaking, and finally asking specific questions about what the user describes, will reveal a great deal about the understanding of the user.

Once the training and competency of the users has been determined, it is important to determine the effectiveness of the communication among all users. Some financial institutions have multiple users and software that not only covers BSA/AML but fraud as well. If that is true, the auditor should determine how different cases and conclusions are communicated to all users. If there is a breakdown in communication, then suspicious activity reporting requirements cannot be effectively met.

Another key factor to consider is the authority level of the BSA Officer compared to the other users. Auditors know that the FFIEC BSA/AML Examination Manual states, “While the title of the individual responsible for overall BSA/AML compliance is not important, his or her level of authority and responsibility within the bank is critical. The BSA Compliance Officer may delegate BSA/AML duties to other employees, but the officer should be responsible for overall BSA/AML compliance. The Board of Directors is ultimately responsible for ensuring that the BSA Compliance Officer has sufficient authority and resources (monetary, physical, and personnel) to administer an effective BSA/AML compliance program based on the bank’s risk profile.” However, as is well known in the compliance community, financial institutions can claim their BSA Officers have sufficient authority to accomplish their job, when in actuality they do not. If the BSA Officer does not have the authority to ensure all users are held accountable for their activities in the system, there will be no guarantee that the system is being used correctly or to its fullest capability.

Finally, the auditor should determine which users control the parameters of the system such as access levels, monitoring thresholds and filing of reports. It also involves determining how cases are managed and documented within the system, and identifying what checks and balances are in place to ensure the system is being utilized as designed.

You, as the auditor, can be very beneficial to BSA Officers by identifying during the audit process if users:

1. Do not possess the needed knowledge, skills or competencies to utilize the system effectively.
2. Do not communicate cases and conclusions to one another.
3. Are not being held accountable for any reason, including the lack of sufficient authority of the BSA Officer.
4. Do not have defined roles and access levels.

**CONCLUSION**

It may seem like an overwhelming project to ensure that the BSA/AML software has been correctly and effectively implemented and utilized to its fullest.

---

However, a few basic questions can help quickly reveal the true picture behind the curtain of the software and give the auditor a solid foundation on which to conduct the audit.

1. **What system do you have in place?** Even if the auditor is extremely familiar with the software, playing “dumb” and asking the following questions will be extremely enlightening.

2. **What steps did you take to implement the system?** The depth of the answers will indicate very quickly if they have a thorough understanding of data validation or not.

3. **How and how often is data validation conducted?**
   Remember, comparing a system to itself is not the most effective data validation!

   **Remember, comparing a system to itself is not the most effective data validation!**

Core reports should be compared against software reports if effective data validation is to be performed. Once you are confident that their data is accurate and checked on a regular basis, you can move on to the next question.

4. **Does your system risk rate your customers and what triggers your alerts?** If the user cannot answer these questions, then you have a user that needs additional training.

5. **Who sets the parameters for the alerts generated?**
   - Ask to see the parameters.
   - Find out how the parameters were determined and if the risk assessment was utilized in the process.
   - Find out the controls in place to determine the parameters and make changes to them.

6. **How are cases displayed and worked in the system?** Find out if the fraud and AML cases are joined or separated.

7. **How does the case management work and what documentation is in place?** This is a good question to discover whether or not the financial institution has silos or has good communication between fraud personnel and BSA/AML personnel.

8. **How is your risk assessment reflected in your software?** Higher risks should have more focus within the system and should be tweaked as risk assessments are updated.

Once these questions are answered, the auditor will have a good understanding of the accuracy and use of the software system and can continue with the normal scope of a BSA/AML audit. Without this understanding, auditors cannot guarantee the quality of their audit and a knowledgeable BSA Officer will be surprised by what questions are not asked rather than what questions are asked!