4/17/2013 Today’s Lesson – Learning from the Mistakes of Others

MATTERS REQUIRING ATTENTION

Kenneth Simmons

The views expressed in this paper are solely those of the author and neither reflect the opinions of the Office of the Comptroller of the Currency nor the U.S. Department of the Treasury.
## Contents

Introduction ................................................................................................................................. 3

Explanation of Analysis .................................................................................................................. 4

Summary of Institutions .............................................................................................................. 4

Summary of MRAs ....................................................................................................................... 5

MRAs by Subject ............................................................................................................................ 8

Risk Assessment ........................................................................................................................... 8

  Program Styled MRAs ............................................................................................................... 9

BSA Officer .................................................................................................................................. 11

  Program Styled MRAs .............................................................................................................. 12

Training ....................................................................................................................................... 15

  Program Styled MRAs .............................................................................................................. 15

Audit ........................................................................................................................................... 17

Internal Controls ......................................................................................................................... 24

Suspicous Activity ....................................................................................................................... 30

  Program styled MRAs ............................................................................................................. 33

Conclusions from Program Styled MRAs .................................................................................... 38

References .................................................................................................................................. 41
Introduction

There are a myriad of compliance related regulations that financial institutions must comply with. In most cases, the accompanying regulations provide specific expectations for compliance. Disclose this here; provide a notice there; submit your report annually; and keep away from unfair and deceptive practices. Compliance regulations typically include one-size-fits most expectations. Over the years, we have experienced changes to various regulations, such as Truth-in-Lending and RESPA. These adjustments are relatively slow to progress. Financial institutions have the opportunity to grasp expected changes and understand how to comply, often before the regulatory changes occur and make the necessary adjustments to internal controls to comply with the changes.

The Bank Secrecy Act is the most challenging compliance requirement facing financial institutions of any decade. Banks are required to comply with transaction monitoring and reporting requirements. FinCEN and other supervisory agencies have written line item instructions to comply with these requirements. More menacing though, are the requirements to identify, monitor, and report suspicious activity as this can be a very subjective process. This challenge directly relates to RISK. The volume of risk is broad and the level of risk is bank specific.

Compliance professionals have opportunities to discuss regulatory challenges through local roundtable groups, and various conferences about the country. External audit firms, supervisory agencies, and consultants have the opportunity to gain experience from the various financial institutions. However, these organizations must comply with professional ethics and confidentiality agreements. While most regulatory discussions are specific and clearly communicated, BSA discussions are visionary and vague. Short of an intimate relationship with a bank, it is impossible for another BSA professional to comprehend the challenges of another.

Eleanor Roosevelt once stated that we should “learn from the mistakes of others. You can’t live long enough to make them all yourself”. ii

This discussion summary provides an opportunity for financial institutions and BSA professionals to learn from the mistakes of others. The discussion summary compiles BSA examination results of 137 financial institutions issued reports including “Matters Requiring Attention” dating from September 2009 through March 2013. This summary, utilizing the proprietary information of the OCC, is the first of its kind. While industry specific information of the financial institutions identity has been redacted, the findings and conclusions are drawn directly from their examination reports. Here is our opportunity to learn from the mistakes of others.
Explanation of Analysis

The OCC employs approximately 1657 examiners. There were 799 full scope BSA examinations of community banks with assets under $10 billion completed between September 2009 and March 2013. Examiners across the continental United States assisted in the completion of this activity.

One hundred thirty seven (137) financial institutions have reports with outstanding BSA related, “Matters Requiring Attention ("MRA"). In some cases, multiple MRAs were issued to the same institution. A combined two hundred two (202) active MRAs exist. This map represents the locality (by state) of these institutions.
Summary of Institutions

The MRAs were found to be somewhat evenly distributed among institutions of varying size. Table 1 below recognizes that the largest institutions were subject to the highest number of MRAs. Surprisingly, MRAs issued to banks with assets under $500 million are evenly distributed among all banks regardless of size. While financial institutions with assets between $500mm and $1B had the fewest outstanding MRAs.

### Distribution of MRAs by size of Institution

<table>
<thead>
<tr>
<th>Banks by asset size</th>
<th>Number of MRAs</th>
<th>Percentage of MRAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1B to $10 Billion</td>
<td>65</td>
<td>32.51%</td>
</tr>
<tr>
<td>$500mm to $999mm</td>
<td>16</td>
<td>7.88%</td>
</tr>
<tr>
<td>$250mm to $499mm</td>
<td>36</td>
<td>17.73%</td>
</tr>
<tr>
<td>$100mm to $249mm</td>
<td>41</td>
<td>20.20%</td>
</tr>
<tr>
<td>Less than $100mm</td>
<td>44</td>
<td>21.67%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>202</strong></td>
<td><strong>99.99%</strong></td>
</tr>
</tbody>
</table>

*Table 1*

This investigation provides an in-depth analysis of these outstanding MRAs and draws conclusions regarding:

- Type and significance of supervisory concerns
- Root causes of deficiencies; and
- Practices designed to help improve your BSA program.

This summary discusses supervisory expectations and industry audit standards for BSA.

### Summary of MRAs

The MRAs were categorized to represent the four Pillars of BSA (Audit, Internal Controls, Training, and BSA Officer). A granular analysis and comparison of the specific MRAs within each category is further discussed below. Please note that the total of combined MRAs is 273, the difference from table 1 is explained below.
Internal controls are the bank’s policies, procedures, and processes designed to limit and control risk and to achieve compliance with the BSA. The level of sophistication of internal controls should be commensurate with the size, structure, risks, and complexity of the bank. Complex risks require complex controls. 83.88% of the outstanding MRAs address internal control deficiencies. These 203 MRAs categorize internal controls as the most difficult area for financial institutions to manage regarding BSA/AML.

Independent testing (audit) should be conducted by internal or external auditors, consultants, or other qualified independent parties. There were (32) thirty-two examinations citing significant audit deficiencies resulting in an MRA. Audit MRAs represent only 13.22 percent of the outstanding MRAs. A larger volume of Audit MRAs was expected considering the vast number of MRAs in other categories. It will become apparent why as you read through this analysis.

The BSA Officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance. The BSA officer is also charged with managing all aspects of the BSA/AML compliance program and with managing the bank’s adherence to the BSA and its implementing regulations. Twenty four (24) MRAs representing 9.50 percent of the outstanding MRAs cite BSA Officer weaknesses. As mentioned in the audit section above, there was some assumption that MRAs addressing BSA Officer weaknesses would be more voluminous considering the quantity of overall MRAs.

Training personnel to manage BSA risk is a never-ending task. Banks must ensure that appropriate personnel are trained in all applicable aspects of the BSA. Training should include regulatory requirements and the bank’s internal BSA/AML policies, procedures, and processes. At a minimum, the bank’s training program must provide training for all personnel whose duties require knowledge of the BSA. The training...
should be tailored to the person’s specific responsibilities. Training represents the smallest portion of the outstanding MRAs. Thirteen (13) training MRAs represent only 5.37 percent of all Pillar weaknesses.

Understanding how MRAs are categorized and the subject matter of MRAs provides a second aspect to understanding how management struggles to comply with BSA. Both subject matter and MRA content are broad. Table 3 below demonstrates how MRA subject matter is defined by examination staff. The four pillars are addressed and include Audit, Internal Controls, BSA Officer, and Training. In addition, fifteen percent of the MRAs address the risk assessment process. While the Pillars are specifically defined as the embodiment of BSA, a well devised risk assessment provides insight to each of the Pillars.

Examination of Table 3 provides further granularity to internal controls. Internal control MRAs address three (3) key components of the BSA program: CDD/EDD and High risk customers; transaction monitoring; and suspicious activity monitoring and reporting.

Program styled MRAs are issued when multiple weaknesses are found across the four Pillars. In these cases, a single MRA report is issued, but addresses all of the weaknesses in a consolidated manner. Examination staff and management work diligently to provide continuity in examination practices. As reflected in table 1, there are 137 banks and 202 MRAs. This obviously reflects some institutions were issued multiple (individual) MRAs. Thirty six of these were also program styled MRAs. A review of these 36 reports and analysis of the subject matter revealed an additional 105 subjects were addressed through the Program styled MRAs. Had individual MRAs been issued, they would have brought the number of MRAs to 273. This is an area which could be seen as a dual edge sword for management. One examination may find value in issuing a program styled MRA to address several deficiencies; while another would issue multiple individual MRAs. Program styled MRAs may be more difficult to resolve completely, since all of the weaknesses would require remediation before the MRA would be removed. On the other hand, five individual MRAs (for example) may appear more serious considering the sheer number of issuances.
The views expressed in this paper are solely those of the author and neither reflect the opinions of the Office of the Comptroller of the Currency nor the U.S. Department of the Treasury.

### Details of individual MRAs

<table>
<thead>
<tr>
<th>MRA's</th>
<th>Size of institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>%</td>
</tr>
<tr>
<td>32</td>
<td>11.76</td>
</tr>
<tr>
<td>69</td>
<td>25.37</td>
</tr>
<tr>
<td>34</td>
<td>12.5</td>
</tr>
<tr>
<td>67</td>
<td>24.63</td>
</tr>
<tr>
<td>35</td>
<td>12.87</td>
</tr>
<tr>
<td>23</td>
<td>4.02</td>
</tr>
<tr>
<td>13</td>
<td>4.78</td>
</tr>
<tr>
<td>273</td>
<td></td>
</tr>
<tr>
<td>137</td>
<td></td>
</tr>
</tbody>
</table>

Table 3  * defined as Internal Controls for report purposes

### MRAs by Subject

#### Risk Assessment

The risk assessment is the starting point of all BSA/AML activity including the design of an effective program, auditing of the program, and examination. The risk assessment process recognizes the positive and negative aspects of a BSA/AML program. It dictates the institution's overall BSA/AML compliance program, including the content of the institution's policies and procedures, the necessary qualifications and experience of the institution's BSA officer, the comprehensiveness of training and internal controls, the scope of the independent test, and the requirements set forth by the institution's customer identification program. Supervisory agencies use the banks risk assessment to scope an examination.

While the FFIEC guidance indicates internal controls are the cornerstone of an effective BSA program; results of examinations without significant BSA deficiencies indicate the risk assessment may be the “new” cornerstone. A well-devised risk assessment clearly defines risk and the areas of risk needing mitigation. This analysis recognized 35 existing MRAs address risk assessment deficiencies. These represent 12.87% of all MRAs.
Program Styled MRAs

Program style MRAs address risk assessment weaknesses for fourteen (14) banks. Table 4 identifies these reports and describes the other areas addressed by the MRA. Inadequate CDD/EDD processes and inadequate SAR monitoring were found in at least 50 percent of these risk assessment MRAs. This high exception rate is expected considering risk would be difficult to monitor without recognition of the risk in the first place.

Risk assessment MRAs are distributed somewhat equally across financial institutions of all sizes; with the highest number/per capita (10) relate to banks with assets greater than $1 billion. The risk assessments for the largest banks typically failed to adequately describe the risk profile of the bank including both inherent and quantitative risks. The following describes the examination comments from one of these large banks. The verbiage is commensurate throughout each of the 10 existing MRAs.

“The FFIEC BSA/AML/OFAC examination manual outlines the development of a BSA risk assessment as a two-step process. The first step is to identify and quantify the specific products, services, customers, entities, and geographic locations unique to the bank (identification of specific risk categories). The second step entails a detailed analysis of data identified during the first step, including customer due diligence and customer identification program information, to more accurately assess where the risks are present in identified categories. The second step provides management a better understanding of the bank’s risk profile in order to tailor policies, procedures, and controls to mitigate the risks identified.

Your risk assessment consists only of step one of the two-step process. The risk assessment does not include an evaluation or analysis of data obtained during the identification of specific risk categories. In addition, management does not analyze customer due diligence information or conduct a comparison of actual or anticipated activity; or review the types of products/services used by the customer.
Management’s completion of step one and lack of step two, severely compromises the ability to identify sources of BSA/AML risk and develop adequate policies, procedures, and controls to mitigate those risks.

Additionally, management does not use risk assessment findings to develop and implement suspicious activity monitoring. A review of the bank’s monitoring processes found no link to the risk assessment. Your suspicious activity monitoring is not risk-based and does not reflect risk categories identified. BSA Officer confirmed that risk assessment results are not used to tailor the suspicious activity monitoring process. This is a fundamental flaw in suspicious activity monitoring and therefore in the bank’s overall BSA/AML compliance program.”

Risk Assessment MRAs among the smaller institutions also address insufficient detail and lack of quantitative results. The primary difference between a large bank and small bank risk assessment is defined in the complexity of the Bank. The following excerpt taken directly from a recent ROE of an institution with assets under $100 million states the following.

“The 2012 BSA audit identified that the bank’s Bank Secrecy Act/Anti-Money Laundering (BSA/AML) and Office of Foreign Assets Control (OFAC) risk assessments need improvement. The risk assessment does not appropriately identify and measure specific BSA and OFAC risks for the bank’s products, services, customers, and geographies and does not contain sufficient detail regarding the individual risk and mitigating factors. A well-developed risk assessment will assist in identifying the bank’s risk profile and enable management to better identify and mitigate gaps in the bank’s controls.”

Risk Management, including the BSA risk assessment process, is based on complexity. The complexity of the financial institution dictates the complexity of the risk assessment process.

According to a recent article published by the ABA Banking Journal, BSA Risk Assessment errors were rated 5 out of 9 most common errors by the ABA. The recent article titled Beat 9 Common BSA/AML Weaknesses (October 4, 2012) eloquently describes the problem with many risk assessments, stating simply “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? In addition, is it within high-risk jurisdictions? If
you have identified any significant risks, what types of mitigations has your institution set in place?”

The entire article may be found at http://www.ababj.com/briefing/beat-the-9-common-bsa-aml-weaknesses-3342.html

The writer provides the following take-a-ways based on this analysis. Effective risk management is based on complexity while some of these recommendations may be relevant to your organization be sure to consider how these enhancements affect your program.

1. Risk assessment processes evaluate the quantity of risk and the quality of risk management. Include supporting documentation and analysis detailing the quantity of risk. The quality of risk management should be documented to describe the controls established to offset the risks. Update your risk assessment on a periodic basis. Periodic may mean more frequent than annually if your institution has major events such as mergers or acquisitions.

2. A significant portion of the risk assessment process and understanding risk is a mathematical equation. The assessment should clearly define the level of inherent risks. In most cases, these are defined as “Low”, “Moderate”, or “High”. The assessment should identify control weakness and control strengths. These, often described as “Strong”, “Satisfactory”, or “Weak”. Strengths mitigate inherent risk. Weaknesses typically do not mitigate risk. The final part of the equation is overall risk. This is the mathematical portion. Moderate/High inherent risk (plus) weak controls should not equate to lower overall risk level. At best, the inherent risk and overall risk should be equal.

3. Forecast new “known” risks. Financial Institutions plan acquisitions, new products/services, and branch changes. Forecast additional risks within your risk assessment. Identify the need for human capital, system modification, and enhanced monitoring expectations based on anticipated risk changes.

BSA Officer

Comptroller of the Currency Thomas J. Curry presented a written statement and testified on March 7, 2013 before the U.S. Senate Committee on Banking, Housing & Urban Affairs concerning supervision of national banks and thrifts (collectively, “Banks”). During this testimony, Comptroller Curry provided a list of nine corporate governance compliance requirements. The first requirement is the need for “A designated BSA Officer with sufficient knowledge, funding, authority, independence, compensation, and supporting staff to perform his or her assigned responsibilities and maintain effective compliance with the BSA and its implementing regulations.”

The views expressed in this paper are solely those of the author and neither reflect the opinions of the Office of the Comptroller of the Currency nor the U.S. Department of the Treasury.
To support this statement, this analysis determined 23 outstanding MRAs cited corporate governance deficiencies. Eleven of these were issued as individual MRAs; while the remaining twelve were addressed through program styled MRAs. Specifically, these MRAs reference the knowledge and expertise of the BSA Officer is not commensurate with the size and complexity of the Bank. In common terms, the BSA Officer was equipped to drive the “Van”; but expected to fly the “Plane”.

Analysis of these MRAs reflects that banks with assets less than $100mm engaged Officers with insufficient experiences to effectively manage the BSA program. As these institutions grow larger and more complex, the inexperienced BSA Officer was found to be unable to manage the additional risks and responsibilities of the position. These conclusions demonstrate a clear struggle for banks and BSA Officers when the officers level of experience does not exceed the risk complexities. As bank assets increase to $250mm, Officer weaknesses decline and were found to manage the risks more effectively. Once again, Officers at banks of $500mm in assets were even more effective. Officers of banks with assets of $1B+ continue to struggle and abilities peak at $5B. Above $5B in assets, the risk complexities grew at a rate which far exceeds the BSA Officers’ potential.

Program Styled MRAs

Table 5 describes program styled MRAs addressing BSA Officer deficiencies and the occurrence of other weaknesses within the banks’ BSA program. Twelve (12) institutions were issued program styled MRAs. There appears to be a direct relationship between BSA Officer weaknesses and other critical areas of BSA including SAR monitoring, and CDD/EDD processes. In addition, 50 percent of these program style MRAs cited both audit and BSA Officer weaknesses. In these cases, an effective BSA audit would have recognized BSA Officer weaknesses.
The following excerpt from a recent Report of Examination of a larger institution provides specific details of the types of deficiencies noted at banks with assets greater than $1 billion:

“Your designated BSA/AML Officer currently does not demonstrate the requisite competencies to direct the BSA/AML program for an institution with the size, complexity and risk profile of your bank. Your BSA Officer does not currently possess the industry exposure, experience or expertise to understand the manner in which a BSA/AML program commensurate with your bank’s BSA/AML risk should function. Your BSA Officer’s BSA/AML experience is exclusive to your institution and its affiliates. Consequently, the BSA Officer has not been afforded the opportunity to learn from a BSA professional with the requisite level of BSA/AML expertise needed to manage the BSA risk in your bank. You have not ensured that your BSA/AML officer receives appropriate, regular, comprehensive external training or participation in industry provided seminars.

You have also not provided BSA Officer with sufficient authority and resources to direct a BSA program commensurate with your bank’s BSA/AML risk. Similarly, your bank’s minimal BSA staff reports to the BSA Director rather than reporting to your bank designated BSA Officer. Consequently, neither your reporting structure nor staffing levels serve to adequately support your banks BSA Officer’s ability to effectively direct your bank’s BSA program. Inappropriate organizational structure and insufficient resource allocation have compromised BSAO’s ability to effectively manage your bank’s BSA/AML risk. Your bank’s BSA Officer is essentially functioning in the capacity of a BSA/AML investigator while your BSA bank’s function and its activities are essentially managed by your BSA Director.”

Similar to the complexities of an effective BSA Program, the MRAs also have varying complexities. The following MRA is from a small bank with assets under $100mm. In this case, the root causes provide additional information regarding the supervisory concerns.

“The Board has appointed a BSA Officer without the benefit of providing sufficient time and resources to effectively carry out those responsibilities. The BSA Officer does not have direct access to the Board or audit committee to communicate BSA related issues personally. The training program for the BSA Officer and bank employees is not adequate.

The Board and management have not provided effective oversight of the BSA/AML program. Currently, the BSA Officer also has a number of “operational” duties, which prevent her from devoting sufficient time to the oversight of the BSA program. Further, the BSA Officer, along with bank staff, has not received sufficient BSA training during 2011 in order for them to effectively carry out their responsibilities.”

There are certain expectations for the qualifications of a BSA Officer. The Officer must:
• Have full responsibility for overseeing, developing, updating, and enforcing the AML Program.
• Have sufficient authority to oversee, develop, update, and enforce anti-money laundering policies and procedures throughout the company.
• Be competent and knowledgeable regarding how the Bank is run and its money laundering risks; how money laundering is accomplished; and the anti-money laundering legal framework.
• Ability to recognize the time and resources needed to perform duties.

All institutions, regardless of size, are expected to have an effective and qualified BSA Officer. As complexity of the bank increases, the authority and reliance in the officer should also increase.

The BSA Officer’s responsibilities include:
1. Developing policies and procedures designed to deter and detect money laundering and terrorist financing.
2. Implementing the AML Program
3. Directing and enforcing the AML Program
4. Ensuring the training of employees on the AML Program
5. Ensuring independent audits of the AML Program.

BSA Officer take-a-ways:

An effective BSA Officer must have experience dealing with AML risks commensurate with the size and complexity of the bank. Management and the Board should forecast the direction of the bank and its expected AML risks when engaging a BSA Officer. An adequate BSA Officer today may soon be inadequate without sufficient funding, authority, independence, compensation, and supporting staff to perform his or her assigned responsibilities.

The writer provides the following take-a-ways based on this analysis. Effective risk management is based on complexity while some of these recommendations may be relevant to your organization be sure to consider how these enhancements affect your program.

1. The Board should have high expectations of the BSA Officer. Management must ensure human capital and financial resources are provided to the BSA Officer in order to have an effective program.

2. The BSA Officer should take charge of their own future. No matter how experienced, AML risks are ever evolving. So should the training provided to the BSA Officer. It is impossible to fly the plane if you are not equipped to do so.
Training

Training related MRAs represent only 5.37 percent of the population. Thirteen (13) MRAs were distributed across the banks equally based on size. MRAs in this category are normally direct failures to provide adequate training on BSA issues. One may believe inadequate training is a root cause of almost all BSA Violations and in-turn there would be more training related MRAs. However this is not the case. Training is often a root cause for an MRA, but not always considered a primary control function.

A more in-depth analysis of these MRAs identified only six (6) existing individual MRAs based on training weaknesses. The remaining seven (7) were imbedded within more complex program styled MRAs. If you recall, Program styled MRAs represent situations when multiple controls are weak creating strain on the entire program.

Program Styled MRAs

Table 6 provides insight to the program styled MRAs. Four (4) of these seven MRAs sight audit deficiencies in addition to training weaknesses. Audit is responsible for evaluating training’s effectiveness. Ineffective monitoring of suspicious activity; including SAR reporting weaknesses, and less than adequate CDD/EDD processes are also indicators of the need for more effective training.

Typically, risks of smaller banks are less complex. Realistically, the training of smaller, less complex, banks need only address the general aspects of BSA and specific risks of the bank. The following MRA excerpt adequately represents many of the training programs of the smallest banks examined.

“Your BSA/AML training materials are not sufficiently detailed to determine whether your training program includes required elements outlined in the FFIEC BSA/AML Examination Manual.”

Banks that are more complex accept new and expanding risks as a regular aspect of business. Mergers/acquisition, new products, services, expanding geographic markets, international and domestic customers; these are just a few examples of risk. BSA professionals and bank staff must be trained on an ongoing basis to understand these risks. Employees must receive
position specific training addressing controls designed to identify and mitigate these risks. The following excerpt is representative of an MRA issued to a larger financial institution with assets greater than $1B.

“The BSA/AML training program is inadequate given the bank’s high-risk profile and does not provide sufficient training to personnel responsible for ensuring compliance with BSA/AML requirements. You have not ensured that your BSA Officer and staff receive regular external BSA/AML training and there is no evidence that personnel bank-wide are provided with or are accountable for completing bank and job specific training.”

In 2009, a Deputy Comptroller with the OCC provided the following guidance to the author regarding training. In an article titled, Federal Agencies Weigh In on Training, the author Meg Sczyrba CRCM CRP, discusses various training topics with agency representatives. The Deputy Comptroller provided the following information. While the article is somewhat dated, the basis and points remain valid today.

“The best training is tailored to the specific bank and enhanced with the bank’s basic policies and procedures related to the subject matter. Off-the-shelf training may not be sufficient unless tailored to address the bank specific risks. Training should also teach employees how to identify critical issues and resolve them, reduce internal control weaknesses, and prevent violations of law. At the OCC, trainers have found that teleconferences are a good way to reach large numbers of people about a specific topic. Participants also make more use of e-learning that is coupled with a teleconference hosted by a qualified instructor. For example, the student does two days of eLearning, completes a case study, and then calls in to an instructor who discusses the material, the case study, and answers questions.

Generally, OCC examiners determine whether the bank can demonstrate the training program works. We are interested in understanding whether the training covers the essential information, is provided to the right people at the right times, and is updated and revised for new or changing requirements. It is extremely important for BSA professionals to attend formalized training and conferences. Formalized external training affords the BSA Officer an opportunity to learn about new and emerging risks, inventive methods for controlling these risks, and simply staying ahead of the curve.”

Training take-a-ways:

Training is a personal event. Training providers are more effective and participants more receptive to mixed-media training. Providing varying types of training (email, face-to-face, teleconferences, on-line, and others you may think of) creates an opportunity for employees to learn in different ways. While one employee may understand a well-written memo describing BSA/AML requirements, another may need the one-on-one interaction of a classroom.
Complexity is a key consideration in determining the type of training needed. Risk of non-compliance is another prime consideration.

The writer provides the following take-a-ways based on this analysis.

1. Provide opportunities for your employees to discuss “real-life” events, and evaluate activities of existing customers (while maintaining customer anonymity). Understanding how your own customers, products, and services inter-relate reinforces how BSA/AML relates to your bank.

2. Cross-training your BSA/AML professionals is critical to maintaining an effective program. Many programs employ analysts, investigators, and AML managers (just to name a few). The fraud division may have its’ own similar staffing. Understanding the roles, determinations, and conclusions of all team members is essential. Weekly meetings to discuss cases and understand how one employee’s work integrates into the decisions of others will increase your program’s effectiveness. Internal and external round-table discussions addressing BSA risk, case management, and effective controls count for training credits.

Audit

Audit functions serve as a safety net for identifying control weaknesses and their consequences. Management considers front line personnel and processes as the first layer of controls. Quality Control functions and compliance initiatives serve as the second control layer. Audit is the third layer. This is commonly referred to as a “Three Lines of Defense model”. The expectation is when all other controls fail, Audit should be equipped to identify and report on control weaknesses.

There are certain steps generally followed by examination staff during a BSA Examination. The first is to obtain and review the BSA risk assessment. A properly designed and completed risk assessment should identify areas of higher risk. The second step is to obtain and review the most recent BSA Audit report completed since the last examination. The bank’s risk assessment and internal audit are two key components utilized to scope the examination.

The audit report and supporting workpapers are used throughout the examination process. Areas of concern in the audit report are validated during the exam. The audit report is reviewed again when deficiencies are identified through the exam (independently). This dual process verifies the audit findings are correct and helps to determine if audit overlooked any notable control weaknesses.
The views expressed in this paper are solely those of the author and neither reflect the opinions of the Office of the Comptroller of the Currency nor the U.S. Department of the Treasury.

Table 7 provides information regarding the 32 active Audit related MRAs. Sixteen of these MRAs were issued as individual reports; while the remaining were part of program styled MRAs. Audit related MRAs comprise 11.76% of all outstanding reports. Nine (9) MRAs issued to banks with assets less than $100m focused on the lack of audit independence. Banks of this size often have difficulty engaging an experienced Auditor; or the auditor has other responsibilities outside of audit. Independence is one of the most important aspects of internal auditing. Staff responsible for banking functions should be prohibited from auditing these same functions.

<table>
<thead>
<tr>
<th>Audit Related MRAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fl &gt; $1B</td>
</tr>
<tr>
<td>#</td>
</tr>
<tr>
<td>7</td>
</tr>
</tbody>
</table>

Table 7

Program styled MRAs

Sixteen (16) program styled MRAs included audit related deficiencies. Table 8 provides details distinguishing the other subject matter addressed by the MRAs. Recognize the large quantity of SAR and CDD/EDD weaknesses cited in these MRAs. These reports reflect the expectation Audit must recognize weaknesses within the banks CDD/EDD processes and monitoring of suspicious activity.

<table>
<thead>
<tr>
<th>Other subjects included in MRA</th>
<th>Banks with Program style MRAs addressing Audit deficiencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAR</td>
<td>1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16</td>
</tr>
<tr>
<td>CDD/EDD</td>
<td></td>
</tr>
<tr>
<td>I/C</td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td></td>
</tr>
<tr>
<td>Officer</td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
</tr>
</tbody>
</table>

Table 8

The International Standards for Professional Practice of Internal Auditing (Standards) viii published by the Institute of Internal Auditors (IIA) address the independence and objectivity of Audit. The IIA provides specific standards of internal audit and further defines these standards through interpretive statements. The following paragraphs describe IIA standards and their interpretive statements.

18 | Page
1100 – Independence and Objectivity

The internal audit activity must be independent, and internal auditors must be objective in performing their work.

Interpretation:

*Independence* is the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. This can be achieved through a dual-reporting relationship. Threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels.

*Objectivity* is an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others. Threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels.

1110.A1 – The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results.

The following MRA excerpt from a $65mm bank describes these type deficiencies.

The BSA/AML audit is no longer independent and the audit scope does not cover the minimum requirements as outlined in the Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual. The testing failed to address the following required areas:

- An evaluation of the overall adequacy and effectiveness of the BSA/AML compliance program; including policies, procedures, and processes.
- A review of the bank’s risk assessment for reasonableness given the bank’s risk profile
- Appropriate risk-based transaction testing to verify the bank’s adherence to the BSA recordkeeping and reporting requirements
- An evaluation of management’s efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions
- A review of staff training for adequacy, accuracy, and completeness
• A review of the effectiveness of the suspicious activity monitoring systems 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. MIS includes reports used to identify large currency transactions, aggregate daily currency transactions, funds transfers transactions, monetary instrument sales transactions, and analytical and trend reports.

The IIA’s Standards also require risk-based audit planning and audit coverage of risk management.

2010 – Planning

The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization’s goals.

Interpretation:
The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization’s risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consideration of input from senior management and the board. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization’s business, risks, operations, programs, systems, and controls.

2120 – Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Interpretation:
Determining whether risk management processes are effective is a judgment resulting from the internal auditor’s assessment that:

• Organizational objectives support and align with the organization’s mission;
• Significant risks are identified and assessed;
• Appropriate risk responses are selected that align risks with the organization’s risk appetite; and
• Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.
The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization’s risk management processes and their effectiveness.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

The Writer provides the following MRA excerpt taken from a bank with assets over $1 billion to illustrate the importance of internal audit standards and supervisory expectations.

“The scope of the internal Bank Secrecy Act (BSA) audit does not cover all of the banks activities. The BSA policy requires BSA compliance through all departments of the bank. The auditors did not perform sufficient transaction testing of high risk banking operations, such as Remote Deposit Capture (RDC), validation testing of the banks Anti Money Laundering (AML) software parameters, or perform sufficient testing of Office Foreign Asset Control (OFAC). Independent testing of the BSA/AML program was unsatisfactory. Internal Audit’s BSA/AML review, failed to identify the significant internal control and BSA compliance program deficiencies noted during the most recent BSA examination.”

Seven(7) institutions with assets greater than $1 billion were issued audit MRAs. The complexity of the independent audit goes hand-in-hand with the size and complexity of the bank. The existing MRAs focus on adequate scoping, identification and weighting assigned to risks, and adequacy of transactional testing. While statistical sampling is often a valid audit technique, BSA audits require a risk based approach. Internal controls are designed based on risk, monitoring for suspicious activity is risk based, CIP is even risk based…. The audit process must be risk based and evaluate the effectiveness of your entire program.

In addition to the specific Audit MRAs, 16 of 36 Program styled MRAs included audit within the MRAs findings. Program styled MRAs are issued to banks with deficiencies across multiple Pillars. When a BSA Program has weaknesses within several areas (such as BSA Officer, Training, Board Reporting, internal controls, and SAR monitoring); the Bank should expect additional weaknesses within the audit area. Supervisory agencies understand weaknesses will go undetected by audit from time to time. Examination staff and audit staff may not recognize deficiencies from time to time. Following effective risk-based auditing limits these occurrences. However, weaknesses stretching across several aspects of the BSA program generally point to an ineffective audit program as well.

The FFIEC BSA Manual provides specific instructions regarding audit. All Banks should follow these guidelines specifically.

Independent testing (audit) should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. While the frequency of audit is not specifically defined in any statute,
a sound practice is for the bank to conduct independent testing generally every 12 to 18 months, commensurate with the BSA/AML risk profile of the bank. Banks that do not employ outside auditors or consultants or have internal audit departments may comply with this requirement by using qualified persons who are not involved in the function being tested. The person(s) 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.

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. Risk-based audit programs will vary depending on the bank’s size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology. An effective risk-based auditing program will cover all of the bank’s activities. The frequency and depth of each activity’s audit will vary according to the activity’s risk assessment. Risk-based auditing enables the board of directors and auditors to use the bank’s risk assessment to focus the audit scope on the areas of greatest concern. The testing should assist the board of directors and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

External audit firms are often engaged to conduct the annual BSA Audit. In many cases, the expectation is the external firm has more experience auditing BSA and knowledge of the regulation than bank personnel. In other cases, the bank simply does not have independent internal audit staff. There are several vital issues management should address when engaging an external firm.

1. Choosing the right audit firm can be more difficult than you may expect. The firm and audit staff should be adequately trained and experienced in conducting BSA audits. The Board should adequately vet the audit firm before engaging. In addition, the audit firm should provide resumes and ongoing training for their auditors. The firm may have decades of experience, yet this does not ensure the auditors have the same level of experience.

2. Take a few minutes and review your audit engagement letter. Understand what services the bank will be receiving. There is a wide variety of engagement letters. Does your engagement letter specify the number of auditors assigned to your bank? The areas of transactional testing that will be completed; or the volume of testing provided? Do you understand the type of sampling to be performed (random sampling, statistical sampling)?
Will your transactional testing be risk weighted? Is there any indication of the amount of time devoted to auditing your most critical high-risk areas? These are a few issues that should be addressed before engaging an audit firm.

3. There is a difference between an audit and a set of “agreed-upon procedures”. An audit engagement letter and report will state “this is an audit”. “Agreed upon procedures” often do not meet the definition of an audit. The following excerpt was taken from a recent examination where an audit was replaced with “Agreed upon procedures”. Note, the verbiage used to define the work performed. Management must ensure your program is “AUDITED”.

“We have performed the procedures which were agreed to by the Board of Directors and management of ABC Bank (the "Bank"), as set forth in our engagement letter. This engagement to apply agreed-upon procedures was performed in accordance with standards established by the American Institute of Certified Public Accountants and in accordance with the Federal Financial Institutions Examination Council's (FFIEC) Bank Secrecy Act I Anti-Money Laundering Examination Manual. The sufficiency of these procedures is solely the responsibility of the specified users of the report. Consequently, we make no representation regarding the sufficiency of the procedures either for which this report has been requested or for any other purpose. We were not engaged to, and did not perform an audit, the objective of which would be the expression of an opinion on the specified elements, accounts, or items. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.”

4. You are paying for the audit service. Be sure you are getting what you pay for. Using the following statements as examples, which of these provide the most value and least risk when engaging an audit firm?

- Audit firm ABC will review the Bank’s BSA program. We will conduct transactional testing. The audit will be concluded in two weeks”. Bank will pay a substantial fee for these services.

- Audit firm ABC will review the Bank’s BSA program. Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), High Risk Customers, Training, risk assessment, and board reporting will be included in this review. We will conduct transactional testing. We will devote 120 work hours. Bank will pay a substantial fee for these services.
• Audit firm ABC will review the Bank’s BSA program. The audit will cover the period of time since the date of the last audit. Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), High Risk Customers, Training, risk assessment, and board reporting will be included in this review. The audit will risk-weight all aspects of the program and conduct transactional testing covering the audit scope and period. Audit firm ABC will provide a senior auditor and three junior auditors to perform the audit. 240 work hours will be provided onsite and an additional 40 hours off-site. Bank will pay a substantial fee for these services.

5. Your audit reports should always distinguish between Violations and general recommendations. The report should clearly communicate findings, the auditors’ recommendations to mitigate findings, corrective action required of the bank, when corrective action is to be completed, and who is responsible for completing corrective action.

Internal Controls

The term internal controls addresses a broad range of recordkeeping, monitoring and reporting processes. These can be simple processes such as Currency Transaction Reports, processes involved in customer due diligence, monitoring high risk accounts, or even monitoring suspicious activity. A significant majority of the existing MRAs relate to internal controls. Table 9 describes internal control MRAs. One Hundred-Sixty eight (168) MRAs based on internal control weaknesses make up 71.31 Percent of all MRAs reviewed. These were placed into the following three sub-categories CDD/EDD & high risk customers (73), record-keeping and reporting (29), and Monitoring Suspicious Activity (67). One hundred five (105) of these were cited as individual MRAs; while the remaining sixty-one (61) subjects were included in Program styled MRAs issued among 18 financial institutions. Many of which address several different weaknesses including internal controls. Table 10 provides detail of the program style MRAs.

<table>
<thead>
<tr>
<th>Internal Control MRAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRA Subject</td>
</tr>
<tr>
<td>CDD/EDD</td>
</tr>
<tr>
<td>SAR Monitoring</td>
</tr>
<tr>
<td>record-keeping and reporting</td>
</tr>
<tr>
<td># MRAs</td>
</tr>
</tbody>
</table>

Table 9

Program styled MRAs
Weaknesses regarding Currency Transaction Reports, wire transfer logs and Monetary Instrument Sales are classified here as record-keeping and reporting; and accounts for the smallest percentage of the internal control MRAs. These MRAs address basic transaction monitoring errors and oversights.

Customer Due Diligence and Enhanced Due Diligence weaknesses account for 43.45 percent of the internal control MRAs. Fifty of these were issued as individual MRAs; with an additional (23) twenty-three were included in program styled MRAs.

A review of the MRAs issued to smaller institutions (under $500mm) range from not having CDD/EDD for high-risk customers to processes are simply ineffective. The following excerpts provide two examples of MRAs for banks within this range of size/complexity. The first example is from a Bank with approximately $90 million in assets. The second excerpt, recognizes more complex issues, and is taken from a Bank with assets approaching $270mm.

**Excerpt from $90mm bank:**

“Management needs to improve procedures to properly perform due diligence on new accounts, including foreign correspondent accounts. Line personnel must determine the proper risk of each bank customer, and follow effective on-going monitoring procedures to ensure potential suspicious activity is identified and reported.

- Management needs to scrub all existing customer accounts to ensure that each account is properly documented and risk rated.
- Board approved applications and forms need to be fully completed by front-line personnel.
- Proper oversight and internal controls need to be established to identify and correct any deficiencies in the process.
- The Customer Risk Assessment Profile form needs to be enhanced to include information regarding the borrowers anticipated frequency and size of transactions.
• Ongoing due diligence procedures should include a periodic review of each account to
determine unusual activity compared to initial information obtained at account opening.
• Procedures should include guidance on if and/or how often an on-site visit should be
carried out and what type of monitoring should be performed in lieu of an on-site visit.
• All affected personnel need updated training to ensure that newly implemented
procedures are understood and followed.”

Excerpt from $270mm bank:
“The bank’s CDD/EDD process needs to be improved. Branch personnel complete a
customer analysis form at account opening. However, the form does not document the high
risk activities the customer is expected to engage in such as remote deposit capture, wire
transfer and ACH origination, or request anticipated volumes and dollar value of
transactions by activity type. The bank relies solely on alerts generated by the BSA/AML
monitoring system as a way to identify high-risk accounts, in contradiction to the bank’s
CDD procedures. Each alert has a score associated with the established parameters. When
the score for the matched criteria exceed 300, the customer’s account activity is reviewed.
The bank does not manually override the system when an account has high-risk
characteristics, such as a cash intensive business. All customers are considered low risk at
account opening until their risk score elevates them to the quarterly high risk list.

Documentation of high risk account reviews must be improved. The BSA Officer utilizes an
EDD/High Risk worksheet that contains a screen shot of the alerts that were generated by
the system to reach the score of 300. The worksheet contains a very brief description of due
diligence performed (e.g. “check volume reviewed”) and a Yes/No indication whether “the
customer’s activity was commensurate to the depositor’s Customer Analysis Profile.” As
previously noted, the Customer Analysis Form does not document expected transactions or
anticipated activity levels. Accordingly, there is no information available in the customer’s
profile that can be referenced to determine if an activity is within the expected scope of
products and services and volume parameters.”

There were 17 individual MRAs and an additional 6 program styled MRAs issued to institutions
with assets greater than $500mm for CDD/EDD deficiencies. The complexity of these
institutions increases the need for more complex controls. As a result, supervisory expectations
are more stringent. The first MRA (listed below) was taken from an institution with assets just
over $500mm. The second MRA is from a bank with assets greater than $3B. This particular
excerpt is from the corrective action portion of the MRA.

Excerpt from $500mm bank:
“Customer due diligence and enhanced due diligence practices do not adequately
determine expected transaction activity at account opening, require periodic reviews of
high risk accounts or maintain a robust customer risk rating system. High risk business
and consumer accounts are not reviewed on a periodic basis unless an automated alert
warrants attention. The transaction monitoring system parameters have not been validated by an independent third party. Suspicious Activity Reports (SARs) do not describe how the activity was detected nor does it explain what the customer’s typical transaction activity was prior to the suspicious activity.”

Excerpt from #3B bank:
“The Board and management must fully implement and demonstrate sustained performance of comprehensive and effective CDD and EDD processes to include, at a minimum, the following:

- Assessment of staffing levels to ensure that there is a sufficient and experienced staff to conduct and document CDD/EDD activities;
- Implementation of a process and corresponding form to collect CDD on non-business customers using a risk-based approach;
- Development of a process to collect and document customer due diligence where the information has not been previously obtained. This could be accomplished on a risk-based approach through ongoing due diligence, suspicious activity monitoring, the investigatory process and as new accounts are opened for existing customers;
- Incorporation of findings/notes from ongoing suspicious activity monitoring into the customer’s due diligence files; and
- Performance of EDD for all high risk customers to include a close review of high-risk customers and their transactions at account opening and more frequently throughout the term of their relationship with the bank. It must also include establishment of appropriate dossier/files to capture the due diligence information and analysis performed.”

In developing due diligence processes, it is important to understand the difference between the Customer Identification Program (CIP) and customer due diligence (CDD). Although both generally occur at account opening, they have distinctly different purposes. CIP is a statutory requirement to determine and verify the identity of a customer. The CIP requirements are very specific. CIP itself is not a primary factor in customer BSA/AML risk assessment, but is the starting point for CDD. CDD enables a bank to develop a reasonable understanding of a customer’s risk and anticipated activity. It is a key element of customer BSA/AML risk assessment and is relied upon in monitoring and analysis for potential suspicious activity. A sound CDD program is critical for effective risk assessment, enhanced due diligence and suspicious activity monitoring processes.

The CDD process begins with the verification of the customer’s identity through the application of the bank’s CIP and assessing the BSA/AML risks associated with that customer. Bank’s should obtain information at account opening sufficient to develop an understanding of the normal and expected activity for the customer’s occupation or business operations. Generally, CDD information includes:
• Beneficial owners
• Country of origin (if foreign customer)
• Nature of business activities / occupation
• Source of wealth and funds used to open account
• Types of products and services to be used by the customer
• Customer’s anticipated activity (e.g. types/volumes, international/domestic, purpose)
• Additional detail as appropriate depending on risk: key customer’s/suppliers, financial information, references, site visits, etc...

Customer due Diligence take-a-ways:

The basic requirements for customer due diligence may be defined by policy and procedure. Documentation requirements for specific customer types are simple to define. However, customers are not simple. Often customers will fit into multiple categories. For example: Customer “A” is a college professor by trade, but also a principle owner in his/her spouse’ accounting firm. Your employees must be savvy enough to understand risks and requirements based on a multitude of account/ customer characteristics.

The writer provides the following take-a-ways based on this analysis.

1. Develop a customer questionnaire completed either manually or within the bank’s account opening platform and establish a quality assurance process to ensure the questionnaire is being completed appropriately.

2. Tailor CDD/EDD questions to the underlying risks associated with a customer – for example, some of the information needed for a cash intensive business would be different from the information needed for a charitable organization.

3. Train frontline staff on the process for collection of due diligence information and why it is important.

Specific CDD/EDD expectations for money services businesses are outlined in the Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States issued April 26, 2005.

High risk customer take-a-ways:

The identification of high-risk customers involves consideration of CDD information to determine the inherent BSA/AML risk for the customer. This is generally accomplished either by consideration of individual risk factors or with a risk scoring process. The process may be manual or involve the use of an internally developed or vendor system. A similar risk
identification/rating process is generally applied to the existing customer base on a periodic basis considering actual activity and other risk factors.

The writer provides the following take-a-ways based on this analysis.

1. Identify key risk factors to be used to initially determine whether or not a customer is high-risk. The factors would then be scored or manually considered in determining a customer’s BSA/AML risk.

2. Document the risk rating in the customer’s CIF file or AML system (if applicable) and establish a process and controls for risk rating changes.

3. BSA/AML risk related keyword searches of customer names on the bank’s system can help identify existing customers with potentially high-risk businesses (e.g. “exchange”, “import”, “export”, “casa”, “wire”, “cash”, “gold”, etc...)

Additional scrutiny or enhanced due diligence (EDD) is generally expected for customers representing a higher level of BSA/AML risk. EDD generally involves a more detailed review of the customer and their activity. EDD generally confirms the customer risk rating and establishes a baseline of reasonable activity patterns and volumes against which the customer will be analyzed going forward. The EDD analysis might be updated on an annual basis and serves as an important part of the ongoing suspicious activity monitoring process. Some higher-risk accounts might warrant more frequent reviews/updates. Information that might be considered as part of EDD includes:

- Volumes/patterns of actual activity compared to the expected business activity.
- The nature and locations of customer suppliers and customers in relation to the nature of the customer’s business.
- Results of internet searches and vendor database searches on the customer, beneficial owners and key suppliers/customers.
- Site visits to assess the business size, location, business/product offerings, etc....

Enhanced Due Diligence take-a-ways:

While initial EDD may be prudent at time of account opening, additional scrutiny and due diligence is an ever-evolving process. The customer’s basic characteristics may place the account in a higher-risk category. Transaction activity, and the varying products and services utilized by the customer helps define the level of risk and ongoing enhanced due diligence required.

The writer provides the following take-a-ways based on this analysis.
1. Establish a profile form for completion of the EDD review. Include the scope of the review, a detailed description of the customer’s business activities, a summary of customer activity, a summary of the results of any internet searches or vendor database searches, a confirmation of the risk rating and a conclusion on the reasonableness of the customer’s activity in relation to the CDD information.

2. An EDD review is often scheduled 90 days after a high-risk account is opened. This enables the bank to compare actual activity to the expectations from the collection of CDD information.

3. Maintain a list of high-risk customers with the date of the last EDD review and the date the next EDD update is due. Track the status of timely completion of EDD reviews and report results to management and/or the Board.

Auditing enhanced due diligence take-a-ways:

The BSA/AML audit scope should include an assessment and testing of the bank’s CDD/EDD process. If the bank uses a scoring system to risk rate customers, that system should be tested and validated.

The writer provides the following take-a-way based on this analysis.

1. Periodically review customers scoring under the bank’s established high-risk cutoff score to determine if the cutoff score is set appropriately.

2. Obtain an Excel spreadsheet of customers with active deposit accounts. Search the spreadsheet for verbiage such as “Auto”, “check”, “advance”, “Payday”, “Package”, etc... to identify higher risk customers. Based on your results, determine if the level of risk assigned, enhanced due diligence performed, and identification of high risk customers is accurate for these accounts.

Suspicious Activity

Monitoring customer activity and subsequent reporting of suspicious activity is the epicenter of BSA/AML regulations. Employees are trained to identify suspicious activity, systems are designed to identify and report unusual transactions that point to suspicious activity. Regulations require banks to monitor and report predicate transactions (CTRs, wires, etc.); and to identify and report suspicious activity based on account characteristics, transactional activity, and human behavior.
Identifying unusual activity is the simplest portion of the SAR processes. *Customer A, a pharmacist, deposits $86,000 cash in increments less than $7,800 over a short period of time when his profile is to only deposit $3000 per month in corporate checks.* This is an example of cash transactions banks monitor each day. CTRs and MILs also identify transactions required to be reported. viii

In auditing, a number of BSA programs for financial institutions in the US and internationally, a top ten CPA and consulting firm with experience in auditing the technical completion of SARs advises... “The technical completion of SARs has dramatically improved over the last two to three years, due, in part from increasing awareness through guidance, public forums such as ACAMS, and much more heightened outreach from law enforcement agencies. However, the introduction of the new SAR form has thrown a wrinkle in these advancements. Many organizations are struggling with the technical completion of the form, particularly non-critical fields. The time required in completing the SAR form has significantly increased and from an auditing perspective, we are encountering issues stemming in both the technical completion of the SAR form as well as lack of resources to keep up with production.

A two tier investigation processes has been largely adopted by the vast majority of institutions (e.g. alerts vs. investigations) in which we are associated and we have seen advancement in adherence to documentation standards at both levels. This is attributable to both enabling technology to support these functions coupled with more maturity in policies, procedures, training, and decision matrixes to support these crucial processes.

The concept of a SAR investigation should be enterprise wide. Many organizations continue to struggle with aspects of conducting an enterprise wide investigation. For example, a bank has an insurance or broker/dealer affiliate and investigators may not have all the investigative tools at their disposal to support a complete investigation. A lot of themes in recent consent orders point to the inability to assess customer risk and perform investigative activities through a single enterprise view. More organizations appear to be adopting and consolidating systems to support these efforts. Case management has evolved to support dynamic workflows and processes that retain a complete audit trail and help mitigate manual tickler lists or tracking. Organizations have looked to technology to align workflows and documentation standards directly to unique processes and procedures, and these processes are generally more mature at larger organizations with the capacity to invest in these systems. The biggest area in suspicious and unusual monitoring that organizations have the greatest issue with is model risk management. These include processes to validate the systems, continually tune and optimize the system, and maintain a prescriptive and statistically valid approach to managing alerts and being in a position to efficiently and effectively report on suspicious activity.” ix

The more difficult concept of monitoring suspicious activity takes into consideration the human facet of conducting transactions, operating a business, and simply understanding how a
customer manages their finances. To represent this statement, there are 67 suspicious activity monitoring and reporting MRAs analyzed through this report. Forty-eight (48) of these are individual reports; while the remaining nineteen (19) are issued as program styled MRAs addressing an additional 43 topics. Table 11 provides insight to this subject matter.
Further analysis of these MRAs helped define root causes for the MRAs based on the complexity of the banks.

Ten MRAs were issued to banks with assets less than $100mm. Comprising 14.93 percent of the population, these banks failed to have written policy and procedures for suspicious activity reporting; or failed to establish proper controls for monitoring suspicious activity. Five (5) of these MRAs were issued as individual MRAs; while the remaining were included in program styled MRAs. The following MRA verbiage was used in one of these reports and is commensurate with the population.

“Suspicious activity identification, monitoring and reporting processes are not adequate. The bank lacks an effective program that establishes a system of internal controls and processes to ensure compliance with the requirements to file SARs, as set forth in 12 C.F.R. §163.180. This resulted in a violation to file Suspicious Activity Reports. We found 16 of the 44 accounts we sampled, had transactions that were questionable, but there was insufficient information on the customer to determine if it was appropriate to file a SAR.”

Seventeen MRAs (25.39 percent) were issued to banks with assets less than $250mm. Eleven of these were individual MRAs. While these banks had established Policy and monitoring controls, the controls established needed improvement.

“This MRA is directly associated with Article VI of the FA. The BSA Officer was required to develop an effective system to identify potential high risk customers, anticipated account activity, and a consistent and formal process for monitoring high risk accounts, both at account opening and throughout the relationship. The review cycle for cash transactions was required to be shortened from quarterly to monthly. Results of these
monitoring activities must be documented and reported to the Board on an ongoing basis.”

Banks with assets less than $500mm were issued twelve (12) MRAs. Only three of these were program styled MRAs. These account for 17.91 percent of the MRAs issued. These MRAs address the bank’s failure to file SARs, file SARs timely, and inadequate monitoring of transaction activity.

“Management transitioned from the prior software system in May 2012 and the system is effective in generating alerts regarding suspicious activity. However, the Board and management’s procedures lack a formal process to ensure timely submissions of Suspicious Activity Reports (“SARs”). As a result, our sample review of twenty SARs (filed from August 2012 to December 2012) identified three instances where management failed to file a SAR within 30 days of detecting suspicious activity, as required by 12 CFR 163.180(d)(5).

**Cause:** Management did not formalize the process for timely SAR submissions subsequent to the implementation of the bank’s new suspicious activity monitoring system. This oversight, coupled with employee turnover in the second half of 2012, resulted in management’s failure to meet the 30-day SAR filing deadline on three separate occasions based on our sample of 20 SARs.”

The largest category, those with assets greater than $500mm, had automated systems with design deficiencies. These nineteen MRAs (28.36 percent) describe transaction filtering and account threshold deficiencies. Fourteen of these were issued as individual MRAs with the remaining being program styled MRAs.

“The bank is not utilizing the suspicious activity monitoring system efficiently and to its full capability. The adequacy of current staffing is uncertain.

**Cause of Concern:** The bank recently upgraded to a new version of the XYZ BSA monitoring system. This system provides in-depth monitoring of account activity. However, some monitoring features of this software are not fully utilized. For example, system deviance thresholds are currently set to zero and generate approximately 6,000 alerts per month. This very high level of alerts places a strain on staffing and hinders effective monitoring. The Bank’s external audit firm also identified this issue in their recent independent Risk Management Assessment. While staffing was increased, personnel are not experienced with the XYZ system and BSA monitoring.”

The following table, “Maturity Cycle of SAR Monitoring”, expresses my conclusions regarding SAR related MRAs. Recognize the direct relationships between risk, the bank’s complexity, and supervisory expectations for monitoring suspicious activity.
Financial Crimes Enforcement Network (FinCEN) instructions for filing suspicious activity reports state:

A financial institution must report any transaction that requires reporting under the terms of 31 CFR Chapter X if the transaction is conducted or attempted by, at, or through the financial institution and involves or aggregates at least $5,000 ($2,000 for money services businesses, except as provided in Section 6 of this document) and the financial institution knows, suspects, or has reason to suspect that the transaction or pattern of transactions of which the transaction is a part:

- Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;


- Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of
no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, or

- Involves the use of the financial institution to facilitate criminal activity.

Suspicious Activity Monitoring and Reporting take-a-ways:

1. Policy and Procedure. One of the most important definitions regarding BSA is that of “Suspicious Activity”. Understanding the difference between unusual and suspicious activity is critical to filing valuable reports. Include examples and analogies of both unusual and suspicious activity within your written procedures. Discuss these type scenarios during training and staff discussions. Using examples, such as the following one, may help employees understand when to report activity.

   “Mary” deposits her payroll check each week. Her account balances and transactions reflect she has difficulty saving money. In an effort to save money, Mary opens a safe deposit box to use as a safe keeping (money hard-to-get to). She places $50 each week in her box. She has explained to the teller that this is her way of saving money. This is an example of unusual activity. Mary’s practices may not be the smartest financial decision, but the activity does not correlate to illegal activity.

   “Tom” owns the local car wash. When Tom conducts transactions at the bank, he routinely opens his safe deposit box. On occasion, the Bank has exchanged smaller bills for larger bills before his safe deposit box visit. The car wash appears to be very busy. However, cash deposits are less than expected. This is an example of suspicious activity.

2. Provide specific requirements when investigating and reporting suspicious activity. Prompt employees to tell their story… (Who is involved, what are they doing, when is it being done, where is the activity being completed, why are they performing these actions, and how is the activity being conducted). Keep in mind, the referring employee may not know all the answers. However, your investigator should complete the story and conclude on the reasoning for Filing or not filing the SAR. Answers to these questions must be documented in writing and include supporting documentation.

3. Writing policy, and especially procedure, are a continuous effort. As new products and services are brought into your banks portfolio, P&P must be updated. Remember to upgrade your P&P when you make improvements to your manual or system derived processes. Mergers and acquisitions almost always dictate the need to revisit P&P.

The views expressed in this paper are solely those of the author and neither reflect the opinions of the Office of the Comptroller of the Currency nor the U.S. Department of the Treasury.
4. Take a lesson from the Duggar family with 19 (plus) children. The family currently owns two cars, one van, a 45-foot bus, and a fleet of five Suburbans. This listing of automobiles may have some resemblance to the systems purchased by your bank to comply with BSA through the years. Having a few children did not entice the family to buy a bus. They grew into their needs and eventually came into it. As their family became larger and more complex, their needs dictated a more complex form of transportation. Following the table (above), how does this concept apply to your bank? Your policy, procedures, and systems must grow with your family. The Duggars did not wake up one morning with 19 kids, needing a bus. They planned and forecasted their needs. They would have been in a real fix if they had eight kids and a Volkswagen beetle. What are you driving?

5. Documenting your investigation and conclusion for not file a SAR is just as important, or more important, than when you file a report. Criticism is almost always easier when something does not occur. SAR filing includes a subjective factor. Documenting why a SAR was or was not filed documents the subjectivity of the process.

6. Patience is a virtue. Especially when implementing a BSA/AML reporting software system. Systems designed to monitor transaction activity and report suspicious activity are not “plug-n-play” utilities. In many cases, these software packages require 6-months to setup and up to 2-years before being completely functional. These systems must be “tuned” to your institutions risk profile.

7. Mercedes and BMWs are costly to maintain. Regularly scheduled maintenance is required. When employing BSA/AML software, be prepared to perform regular maintenance validating system parameters. Similar to owning an expensive import, skip the system maintenance to find out just how costly things can really get.

FinCen and the Office of U.S. Immigration and Customs Enforcement (ICE) are the two primary agencies directly responsible for oversight and investigation of suspicious activity in the US. Both of these Agencies publish ongoing guidance to financial institutions.

FinCEN serves as the FIU for the United States and is one of more than 100 FIUs making up the Egmont Group, an international entity focused on information sharing and cooperation among FIUs. An FIU is a central, national agency responsible for receiving (and, as permitted, requesting), analyzing, and disseminating to the competent authorities disclosures of financial information.

FinCEN is a bureau of the U.S. Department of the Treasury. The Director of FinCEN is appointed by the Secretary of the Treasury and reports to the Treasury Under Secretary for Terrorism and Financial Intelligence. FinCEN’s mission is to safeguard the financial
system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

FinCEN carries out its mission by receiving and maintaining financial transactions data; analyzing and disseminating that data for law enforcement purposes; and building global cooperation with counterpart organizations in other countries and with international bodies.

FinCEN publishes *The SAR Activity Review – Trends, Tips & Issues* periodically as a product of close collaboration between FinCEN's regulatory, law enforcement and industry partners. It is intended to provide meaningful information about the preparation, use, and value of Suspicious Activity Reports (SARs) filed by financial institutions. *SAR Activity Review – Trends, Tips & Issues* may be accessed at http://www.fincen.gov/news_room/rp/sar_tti.html.

U.S. Immigration and Customs Enforcement (ICE) is the largest investigative arm of the Department of Homeland Security (DHS). Cornerstone, ICE’s comprehensive enforcement initiative focusing on financial and trade fraud investigations, is a key component of that mission. Cornerstone detects and closes down weaknesses within U.S. financial, trade and transportation sectors that can be exploited by criminal networks. Law enforcement entities share criminal typologies and methods with businesses and industries that manage the very systems that terrorists and criminal organizations seek to exploit. In addition to financial and money laundering investigations, Cornerstone targets commercial fraud, smuggling and trafficking, export and trade violations and intellectual property crimes. Every day ICE special agents, intelligence specialists and contract employees review and analyze Suspicious Activity Reports (SARs). The goal—to identify criminal organizations through their behavior patterns. Bank Secrecy Act (BSA) reporting requirements and effective anti-money laundering programs have caused criminal organizations to resort to acts of desperation in their attempt to earn, move and store their illicit funds. Cornerstone’s web address is http://www.ice.gov/cornerstone. The Cornerstone Report is a quarterly bulletin highlighting key issues related to ICE Home-land Security Investigations (HSI) financial, narcotics and special operations investigations. Cornerstone Reports are available at http://www.ice.gov/news/library/reports/cornerstone.

**Conclusions from Program Styled MRAs**

This analysis discussed individual MRAs and program styled MRAs. Individual MRAs typically address one area with deficiencies. Program” styled MRAs represent situations when multiple
controls are weak creating strain on the overall program. Over Seventeen percent (17.73%) of all MRAs were program styled MRAs. 78 percent of the program styled MRAs were issued to banks with less than $500mm in assets. The following outline describes the volume of these MRAs and the subject matter.

- 25% (9) MRAs affect institutions with assets less than $100mm. These cited weaknesses regarding risk rating accounts, SAR monitoring, Risk Assessments, internal control, and training. Supervisory expectations at institutions of this size and complexity include an understanding the BSA Officer is in a developmental role. Although weaknesses are identified in other areas, the BSA Officer is often not directly cited as a root cause for these deficiencies.

- 25% (9) MRAs also affect institutions with assets between $100mm and $250mm. These cited failure to file SARs, Training, BSA Officer, and Audit concerns. The expectations increase at this level of complexity. Both BSA Officer proficiency and audit expectations are more defined. These MRAs focus on the level of experience and capability of the BSA Officer. In some cases, weaknesses at this level may be a pre-determinant to replacing the BSA Officer.

- 28% (10) MRAs were issued to Financial Institutions with assets between $250mm and $500mm. Audit weaknesses are the predominant factor; with BSA Officer and internal controls deficiencies also cited. Many institutions share BSA and Compliance roles in order to cut cost and maintain efficiencies. However, at this maturity level, they soon realize managing both of these functions is too demanding on a single resource. Management also realizes the BSA Officer needs to be more experienced and devoted to BSA; hence, the internal control weaknesses. During this phase, many banks begin outsourcing their BSA audit functions. These MRAs represent the institutions failing to recognize these requirements.

- 22% (8) MRAs were issued to banks with assets greater than $500mm. Only three of these were issued to institutions with assets under $1B. These institutions have more complex issues and supervisory expectations. Monitoring system validation and filtering, Internal control processes, BSA Officer weaknesses are the predominant subject of these MRAs. Growth of these institutions is exponential in comparison to smaller banks. In some cases, management is finding out the BSA Officer’s expertise cannot keep up with the expanded risks and control needs of their institution.

Correlate the findings of this analysis to your own bank’s BSA/AML program. Whether you are the BSA Officer, Management, or General Auditor self-reflection and acknowledgement of the status of your program may keep you from getting into a “pickle”. Learn from the Mistakes of Others.
As commented previously, Eleanor Roosevelt once stated we should “learn from the mistakes of others. You can’t live long enough to make them all yourself”. 
References

2 http://www.goodreads.com/quotes/20393-learn-from-the-mistakes-of-others-you-can-t-live-long
6 Federal Agencies Weigh in on Training, ABA Bank Compliance, January/February 2009.
7 Institute of Internal Auditors, “The international Standards for Professional Practice of Internal Auditing”
8 www.stu.com Stu Rees esq.
9 Paul Osborne, Partner Crowe Horwath LLP,