Bank Secrecy Act Auditing for Community Banks: A Risk-Based Approach

Susan Cannon, CAMS-Audit, CRCM

ACAMS® | Advancing Financial Crime Professionals Worldwide

Table of Contents

Executive Summary

Federally-insured depository institutions in the U.S. are required by regulation[i] to implement written Bank Secrecy Act/anti-money laundering (BSA/AML) compliance programs. These programs must be approved by the board of directors and at a minimum, are required to:

- Provide for a system of internal controls to assure ongoing compliance;
- Provide for independent testing of BSA/AML compliance;
- Designate an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and
- Provide training for appropriate personnel

These required program components are typically referred to as the "four pillars" of a BSA/AML compliance program.

This white paper will discuss some specific strategies for achieving compliance with the independent testing pillar for smaller banks, often referred to as "community banks," commensurate with their BSA/AML risk profiles. Specifically, I will discuss customizing the independent testing approach and accompanying audit program so that it is appropriately risk-based. Additionally, strategies for selecting risk-based transaction testing samples will be discussed. It is important to note that appropriate scoping, planning, audit programs and sampling techniques are but a few of the overall considerations in successful BSA/AML auditing. Other resources should be consulted with respect to auditor independence, managing the audit, documenting work, formulating conclusions, issuing final reports and tracking and validating clearance of exceptions.

Suggestions outlined in this paper are based on my own experiences and methodologies in conducting BSA/AML audits for community banks over the past 15 years, along with additional insights and tips I have learned from interviewing colleagues and regulators.

One Size Does Not Fit All

Defining a Community Bank

Prudential regulatory agencies in the U.S. use asset size to determine examination strategy. For example, the Office of the Comptroller of the Currency (OCC) defines community banks as banks with less than $1 billion in total assets. A national bank or federally chartered thift's asset size determines whether an institution will be examined using the Community Bank Supervision Process or the Large Bank Supervision Process.[ii] The Federal Deposit Insurance Corporation's (FDIC) *Community Banking Study*[iii] acknowledges that the standard method for defining community banks is based on asset size; however, this benchmark on a stand-along basis can be arbitrary. The study states that while banks with $1 billion or more in total assets

are typically defined as large banks, that fixed dollar limit does not take into account inflation, economic growth and the size of the banking industry itself. Therefore, a bank crossing the $1 billion total assets threshold may still exhibit the characteristics of a community bank such as a continued focus on providing traditional banking services to a smaller more localized market.

Quarterly, the FDIC publishes aggregate data for all FDIC-insured institutions.[iv] According to the *Ratios by Asset Size* data, published for March 31, 2014, roughly 90 percent of the total number of FDIC-insured depository institutions have total assets under $1 billion.

Asset Size Group	Number of Institutions Reporting	Percentage of Total Number of Institutions Reporting
Assets > $10 Billion	107	1.59%
Assets $1 Billion - $10 Billion	565	8.40%
Assets $100 Million - $1 Billion	4,053	60.22%
Assets < $100 Million	2,005	29.79%
All Insured Institutions	**6,730**	**100.00%**

Regardless of a bank's asset size, as part of its core assessment procedures, the OCC's Community Bank and Large Bank supervisory frameworks refer examiners to the Core Examination Overview Procedures section of the Federal Financial Institutions Examination Council (FFIEC) *BSA/AML Examination Manual*.[v] Both frameworks call for completion of appropriate expanded procedures in the FFIEC *BSA/AML Examination* manual when specialized activities or specific products warranting additional review are present. Similarly, the FDIC and the Board of Governors of the Federal Reserve System utilize the core and, when appropriate, expanded procedures of the FFIEC *BSA/AML Examination Manual* as part of the supervisory process for banks of all sizes.

Although all banks in the U.S. are examined using the same set of BSA/AML examination procedures, the scope, depth and frequency of independent testing increases with the size and complexity of the bank. At one end of the spectrum, community banks usually have BSA/AML audits once every 12 to 18 months compared to more rigorous continuous BSA/AML audit processes implemented by large audit teams in place at the nation's largest banks.

It is not feasible and would be cost prohibitive for a typical small community bank to apply the same independent testing strategies and techniques designed for a large, complex bank. To attempt to do so would not be a risk-based approach. The independent testing function must be adjusted to an appropriate scale.

Defining Risk-Based Audits and Testing

A BSA/AML compliance program should have three lines of defense.[vi]

1. The first line of defense is to appropriately identify risks and implement policies and procedures to mitigate those risks for lines of business and customer-facing personnel.
2. The BSA/AML officer oversees the second line of defense through ongoing oversight and monitoring of the program to assure compliance.
3. Internal audit serves as the third line of defense by conducting independent evaluations of the adequacy of the overall program including policies, training, internal controls and compliance oversight. Management should assure that independent testing scope, methodology and frequency of reviews are appropriate for the bank's risk profile.

The BSA/AML Compliance Program Overview section of the FFIEC *BSA/AML Examination Manual* provides a discussion of regulatory expectations with respect to the Independent Testing pillar.

> *"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."*

The guidance further outlines minimum standards for independent testing. Included in those standards are conducting "appropriate risk-based transaction testing to verify the bank's adherence to the BSA record keeping and reporting requirements (e.g., CIP, SARs, CTRs and CTR exemptions, and information sharing requests)." The Certified Anti-Money Laundering study guide[vii] published by the Association of Certified Anti-Money Laundering Specialists (ACAMS) similarly provides guidance regarding what independent testing should entail. The guidance includes the following: "Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers and geographic locations)."

Increasingly, enforcement actions and Matters Requiring Attention (MRAs) in examination reports have cited weakness in independent testing. Failing to have a risk-based audit plan that focuses on high-risk areas and insufficient transaction testing are among the most common regulatory criticisms of AML independent testing functions.[viii]

In his 2013 white paper, Kenneth Simmons provided a unique analysis compiling the results of MRAs for OCC regulated banks. [ix] The analysis covered reports with BSA-related MRAs issued from September 2009 through March 2013 issued for 137 financial institutions. Of the 32 active MRAs identified in the paper related to significant BSA/AML audit deficiencies, 25 (78 percent) involved banks with total assets less than $1 billion. Simmons states in his paper that although audit staff may not recognize deficiencies from time to time, following effective risk-based auditing limits these occurrences.

Designing Risk-Based Audits and Sampling Strategies

Planning and Scoping – Laying the Ground Work for a Risk-Based Review

Yogi Berra said "*If you don't know where you are going, you'll end up someplace else*."[x] In BSA/AML independent testing, you need to know where you are going by understanding the bank's unique risks. Doing so will enable you to map out an appropriate plan so that you end up providing relevant findings and recommendations.

Independent reviews may be performed by an employee of the bank, provided he or she is sufficiently independent of the process and possesses the requisite knowledge and skills to perform the review. Alternatively, many banks outsource independent reviews to third-party service providers. Regardless of who is performing the review, initial interviews need to be held with management to determine the bank's overall risk profile so that the audit can be appropriately scoped and budgeted in line with the bank's unique characteristics.

Typically, third-party vendors also use this information to develop a proposal of the overall scope and pricing for the engagement. The stated scope should be consistent with regulatory expectations. It should also specify what is and what is not included in the review. Specific high-risk activities such as parallel banking, pouch activities and foreign correspondent banking, to name a few, often do not apply to community banks. These and other activities covered in the FFIEC *BSA/AML Examination Manual* should be specifically discussed with management in order to appropriately budget the engagement. If management indicates in initial planning sessions that some or all of these activities are not applicable, they should specifically be excluded from the proposal scope. To hold a consultant responsible for identifying all possible unusual or abnormal risks would result in cost prohibitive fees. The consultant is not an officer or employee of the bank and therefore must take at face value the representations made by management when quoting a fee for completing the work.

If, during the engagement, the consultants learn that these areas are, in fact applicable, the discovery should be immediately discussed with senior management. Despite the best efforts of the client and the consultant to define the scope to include applicable risks, this does happen upon occasion. As a result, an addendum to the engagement letter expanding the scope to include the discovered activity may be developed and approved. If the client chooses not to expand the engagement, at the very least, the consultant's report should identify the fact that the activity excluded from the scope was discovered and recommend that appropriate independent testing be performed in that area.

In-house auditors must follow a similar process in order to effectively plan the bank's overall audit schedule and meet agreed-upon deadlines for completion. Unlike their consultant counterparts, however, they have little choice but to expand the preliminary scope to capture unforeseen activities if they are discovered. This may result in missing a deadline for completing the review and cause a domino effect impacting other internal audits on the schedule. It is important for the in-house auditors to maintain good lines of communication with

management to ensure such cases are promptly recognized so that the audit schedule may be appropriately adjusted.

Prior to beginning audit work, policies, procedures, risk assessments and other materials should be requested[xi] to facilitate planning and determine products, services, customers and geographies that may present elevated risks warranting robust testing.

Auditors should not assume that all community banks automatically have low BSA/AML risk profiles. Risks may be elevated due to the geographic location of its offices and/or customer base. The bank may have entered into lines of business or accept types of customers with elevated BSA/AML risks. There has been a recent trend of "de-risking" by avoiding or terminating relationships with customers considered to present higher BSA/AML risks.[xii] One result of this trend is that community banks are increasingly approached by higher risk customers that many larger banks are no longer willing to service. Money services business (MSB) and third-party payment processes (TPPP) are two customer types in particular that have been actively de-risked by banks. Auditors should consider whether appropriate mitigating controls commensurate with management and the board's risk appetite have been established.

One high profile case in particular illustrates what can happen when a community bank takes on the elevated risks associated with high-risk customers and services without appropriately assessing and mitigating those elevated risks. First State Bank of Delaware, a bank with total assets of $222.5 million, repeatedly established customer relationships with TPPPs to indirectly provide payment processing services for the TPPPs' clients without adequately assessing AML risks associated with those customers. Red flags indicating high levels of fraud associated with transactions processed for these customers were repeatedly ignored. The Bank also failed to conduct appropriate enhanced customer due diligence (CDD) for its MSB customers. Independent testing was not appropriately risk-based; therefore, the elevated risks associated with the Bank's non-traditional products, services and business lines were not recognized or comprehensively tested. In 2012, the Bank was assessed $15 million in civil money penalties for failing to implement an effective BSA/AML Compliance Program.[xiii] Subsequently, Delaware's Office of State Bank Commissioner terminated the Bank's charter and the FDIC terminated its insurance on depositors of the Bank.

In September 2013, the FDIC clarified its policy and supervisory approach related to providing payment processing for merchant customers, both directly and indirectly through TPPPs. [xiv] While the guidance does not prohibit or discourage banks from providing payment processing services operating in compliance with applicable law, it states that banks must recognize and properly manage the elevated risks associated with these relationships. When conducting independent testing for a bank providing merchant processing services, appropriate expanded procedures to assess the adequacy of the bank's systems to manage these risks is critical. In addition to referring to the FDIC's guidance, the expanded examination procedures in the FFIEC *BSA/AML Examination Manual* for reviewing third-party payment processors should be utilized to develop an appropriate set of steps for reviewing this activity.

During the planning process, the risk assessment should be reviewed in conjunction with other information to evaluate its reliability in building a risk-based audit plan. Such resources include:

- **Previous Examination and Audit Findings** – Review the nature of weaknesses identified in the previous audit and examination reports and consider how those areas are addressed in the risk assessment. For example, the examination report may discuss a lack of internal controls associated with an inherently high-risk product or customer type. Consider the recommendations included in the report to rectify the deficiency and management response to enact corrective action. In the preliminary review of the risk assessment, does it appear that the assessment of those areas have been appropriately expanded to recognize the inherent risks involved? Do the stated mitigating controls appear to sufficiently address the identified weaknesses? Does it appear that residual risks have been brought down to an acceptable level? It is important to assure that the audit plan factors in appropriate depth of testing in historical problem areas.

- **Board minutes** – If board minutes reveal new or contemplated lines of business not addressed in the risk assessment, discussions should be held early on to determine why. This could be an indicator that the risk assessment is an annual exercise instead of an ongoing assessment of risks associated with new activities or business lines prior to engaging in them. Board minutes may also reveal material lawsuits, losses, fraud or other adverse events that occurred during the audit period that potentially warrant the filing of a suspicious activity report (SAR). The auditor should flag any such observations for discussion to determine if SARs were filed or considered. If they were not, it may be an indicator that lines of communication for reporting unusual activity are not functioning properly.

- **Financials** – A review of the bank's most recent quarterly Call Report[xv] may reveal activities not included in the risk assessment such as foreign due-froms and brokered deposits. High non-interest income could be an indicator of TPPP, MSB or other higher risk customer relationships in need of enhanced review. Rapid growth in total assets, the number of employees or in specific asset or liability categories should be noted to assure that the overall BSA/AML compliance program kept pace with the growth. Similarly, a significant decrease in the number of employees may be an indicator that sufficient resources are no longer allocated to the BSA/AML function.

- **Website** – The Bank's website might promote products and services that are not addressed in the risk assessment. Of particular interest are products and services that have inherently higher BSA/AML risks such as correspondent banking services, international services, remote deposit capture and automated clearing house (ACH) origination services. The website might also target customers that pose inherently higher BSA/AML risk profiles such as MSBs, international customers or charitable organizations.

- **Money Laundering Risk Assessment (MLR)** – Community banks regulated by the OCC submit an annual Risk Summary Form providing metrics on the types and volumes of a bank's various products, services, customers and geographies as part of the MLR process. A review of the previous MLR may reveal inherently high-risk areas in need of review. Comparing the previous two MLR reports may help the auditor understand whether there have been significant changes indicating that the bank has increased or decreased inherently high-risk customer relationships or product offerings.

- **Preliminary Interviews and Request Letter Responses** – Management's responses to specific questions, policies, procedures, high-risk customer listings and other materials received during the planning stage may identify risk areas not addressed in the risk assessment.

The preliminary observations made with respect to the bank's risk assessment during planning also serves as a starting point for the auditor's review of the overall quality of the risk assessment. Throughout the review, observations regarding the bank's actual activities, types of products and customers, geographies associated with customers and services, procedures, and effectiveness of internal controls should be traced back to the risk assessment. Doing so will enable the auditor to make a meaningful conclusion regarding the overall accuracy and quality of the risk assessment.

Once the risk-based audit plan is established, initial assumptions may prove to be incorrect as the audit progresses. As a result, adjustments may need to be made to the plan to decrease or intensify procedures once additional information comes to light. Consistent with the guidance given to examiners in the Scoping and Planning section of the FFIEC *BSA/AML Examination Manual*, it is useful to document any changes to initial assumptions in the audit work papers to demonstrate utilization of a risk-based approach, as well as to support any need for additional resources or commitments from management.

Audit Program Development

The examination procedures in the FFIEC *BSA/AML Examination Manual* are designed for use by supervisory agencies, but they are often adapted as audit programs by auditors conducting BSA/AML independent testing.

Many auditors of community banks use the actual examination procedures as an audit program while others formulate customized programs based on the examination procedures. Customized audit programs may, for example, group similar testing areas together to improve efficiencies. For example the BSA/AML Overview section of the examination manual contains several comprehensive steps for evaluating a bank's overall BSA/AML training program. In addition, the Customer Identification Program and Office of Foreign Assets Control (OFAC) examination procedures contain additional review steps for examining training adequacy of bank staff for compliance in those respective areas. It may be more efficient to consider overall training adequacy for all of these areas in a consolidated training review than separately in conjunction with three different testing programs.

When customized audit programs are used, it is important to ensure that they encompass all applicable regulations and guidance from the examination manual along with supplemental guidance issued by prudential regulators and the Financial Crimes Enforcement Network (FinCEN). Finally, customized programs should be mapped back to the examination manual to assure coverage of required areas.

The documented scope developed in the planning stage should correlate to the selected intensity level of testing steps performed. One challenge with the expanded procedures in the FFIEC *BSA/AML Examination Manual* is that they may take us further than necessary when conducting a risk-based review, particularly for smaller, less complex community banks. By adopting a three-level approach to testing, procedures may be customized to incorporate the core and expanded procedures, or a hybrid between them to facilitate appropriate coverage based on risk. For example:

Level 1- Low Intensity: Assess the risk level and volume of the activity. If the risk is very low or volumes are negligible, a limited review and documentation of observations may be all that is needed.

Example – an institution sells gift cards as an agent for a large bank. Policies and procedures are in place to limit sales to the bank's customers. There is a $500 purchase limit and reloads are not offered. Sales logs are maintained and monitored by the BSA department and cash sales are specifically tracked and reviewed. Review of the log revealed less than $15,000 in total sales in the past year. Based on these observations, these facts would be documented and it would be appropriate to conclude that risks are relatively low and appropriately mitigated and no further review is warranted.

Level 2 – Moderate Intensity: Certain enhanced risks exist warranting some testing. This level of testing would be a hybrid between the core and expanded examination procedures.

Example – Taking the gift card scenario above, assume overall sales of $50,000 in the past year and assume that the bank allows reloads. While overall volume and risk level still may be considered to be relatively low, the auditor observes several customers with multiple card purchases and/or reloads. Targeted review of activity for these customers (such as review of their onboarding documentation, account statements, cash activity and ascertaining the reason for the multiple purchases and/or reloads) may be appropriate in this instance.

Level 3 – High Intensity: Robust testing consistent with the full expanded examination procedures would be warranted for areas with high inherent risks and/or lack of mitigating controls.

Example – the bank administers its own gift card program or acts as an agent, but sells a high volume of gift cards to both customers and noncustomers. Limited monitoring is conducted and there is no overall analysis of sales patterns or trends. A more robust review of mitigating controls and extensive sampling would be warranted in this instance.

Developing methods for assessing the integrity and accuracy of management information systems (MIS) used in the BSA/AML compliance program must be included in the independent testing process. Because the examination procedures are designed for examiners and not auditors, specific steps for achieving this end must be customized for the audit process.

MIS used to identify and report large currency transactions should be tested rather than simply relying on the accuracy of system generated reports to make sample selections. For example, batch processing, non-posted items (caused by encoding errors) and use of internal accounts (such as for loan payments, official checks, wires or foreign currency sales) may contribute to an inaccurate portrayal of actual cash activity by customers on system generated reports. Many core processing systems aggregate daily cash at the Tax Identification Number (TIN) level; however, third parties such as a bank customer's employees cashing checks drawn on their account may falsely alert the need to file a currency transaction report (CTR) on the bank's customer. A system report may aggregate monetary instruments purchased or cashed under the bank's internal TIN, potentially masking the need to file a CTR for the individual conducting the transaction. Many of the teller platform systems mitigate these problems by prompting tellers to input conductor information into the system at a certain dollar threshold.

It is important for the auditor to understand the system(s) used for CTR reporting, how they are utilized and any potential gaps or control weaknesses. Sampling should include manually reconstructing cash activity using teller journals, customer statements and review of items processed to test the accuracy of these systems.

If large CTRs are utilized as part of a manual suspicious activity monitoring system, auditors should review the dollar threshold established for these reports. This is particularly important for banks relying only on system generated reports to manually monitor potential structuring activities. The selected setting should be evaluated to determine whether it is sufficiently low enough to recognize customers potentially structuring cash transactions below the reporting thresholds. For example, if an institution sets the daily cash report limit at $10,000 per customer, such trends would not be recognized.

The examination procedures, along with additional supervisory Model Guidance, [xvi] should be used by the auditor to devise specific testing steps to evaluate the use of automated surveillance systems. Banks adopting these systems typically consider them to be a key internal control to assure unusual and suspicious activities are appropriately detected and reported. Therefore, is it crucial from a risk-based auditing perspective to design specific testing steps that will enable the auditor to conclude whether management oversight, ongoing monitoring

and independent validation concepts addressed in the Model Guidance have been appropriately considered and applied by the bank.

The Model Guidance is not tailored specifically for BSA/AML automated surveillance systems. It is broadly designed to encompass a wide spectrum of systems used for various purposes including strategic planning, monitoring financial risks and overall risk management. Therefore, it is useful to outline the overall concepts and design audit program steps that make sense from a BSA/AML independent testing perspective. An excellent resource for devising testing steps consistent with the examination manual and Model Guidance is the Advanced AML Audit Certification white paper by Nancy Lake.[xvii]

The master audit program should be kept current on an ongoing basis to reflect emerging issues, regulatory changes and guidance, examination manual updates and lessons learned from enforcement actions.[xviii] These regular updates will help auditors identify and address emerging risks and appropriately incorporate them into testing.

Work paper quality should be sufficient in detail to demonstrate the review performed and support the conclusions and recommendations reached. A checklist approach is not conducive in this endeavor. Meaningful work paper documentation of observations, rationale for testing intensity and sample sizes, and clear documentation of testing performed is extremely important from an overall audit best practice perspective. Well documented work papers are also important to support how specific risk-based testing decisions were made.

Risk-Based Sample Selections

A risk-based approach to independent testing calls for risk-based, not statistical or random, samples. Testing should be designed to judgmentally include potentially higher risk products, services, customers and geographies rather than employing a "needle in a haystack" approach of randomly or haphazardly selecting samples for review.

For example, in making judgmental selections for risk based customer identification procedures, CDD, enhanced due diligence (EDD), and suspicious activity monitoring, it is useful to review system-generated and manual reports and queries in concert with one another. Source data may include trial balances, new account reports, system queries that include additional customer details (e.g., occupation, type of business, risk rating, etc.), large cash reports, wire logs, cash sales of monetary instruments (MI) logs and listings of remote deposit capture (RDC) customers and ACH originators.

Pivot tables may be created from the activity reports to identify cash, wire and MI activities by customer and the results, along with other salient information (e.g., ACH origination or RDC customer, whether or not the customer is internally risk rated high) could be appended to the overall trial balance or account query. The resulting information is a good starting point for making risk-based selections of customers exhibiting potentially high risk characteristics based on a variety of factors including: activity (e.g., cash, wires, ACH origination, RDC), occupation or type of business (if such information is included in the raw data) and geographic location of

customers or transactions (particularly higher risk jurisdictions). Whether or not SARs were filed on these customers should also be considered; however, care should be exercised to assure that the confidentiality of SAR filings is not compromised in work paper documentation.

Considering the total number of locations, new customers, lines of business and report volumes should be factored into determining appropriate sample sizes. Work papers should include documented rationale for sample sizes based on these factors. For example, an appropriate representative CTR sample size for a bank filing 50 CTRs a year versus another bank filing 50 CTRs a day would be vastly different.

By utilizing a risk-based approach in selecting samples, the auditor has a higher probability of observing the bank's application of mitigating controls for higher risk products, services, customers and geographies, as well as validating their suspicious activity review process. Whatever method is employed, an auditor should strive to see the big picture in order to evaluate internal controls rather than simply focusing testing only on customers internally identified as high risk.

Conclusion

Although all banks in the U.S. are examined under the same set of BSA/AML examination procedures, a risk-based audit for a community bank is much smaller in scale than for a large complex bank. However, it is important to appropriately plan, scope and tailor a community bank's BSA/AML audit plan so that appropriate focus and emphasis is placed on areas of highest risk. A generic testing plan or checklist approach applied evenly across the board for all community bank clients is not a risk-based approach.

It is important to understand the risks prior to scheduling an audit in order to budget the appropriate number of hours needed to complete the work. Taking time to review the risk assessment in conjunction with additional information will enable the auditor to identify areas in need of enhanced review based on risk. A comprehensive audit program with scalable procedures calling for more intensive review commensurate with risk level is an important tool for the audit team to carry out a risk-based review.

Efforts should be made to maximize the quality of samples using risk-based sample selection techniques rather than relying only on internally identified high risk customer lists or management's selection of customers to be reviewed.

A risk-based review must place appropriate emphasis on manual and automated systems used to identify reportable transactions and detect suspicious activity. A good, risk-based plan will include appropriate testing of the accuracy and integrity of those systems.

A comprehensive and appropriately scoped risk-based audit will enable senior management and the board to better understand potential weaknesses in the bank's BSA/AML program

before such matters are identified in regulatory examinations. Rectifying and mitigating those weaknesses reduces the likelihood of MRAs and formal enforcement actions.

References

(hyperlinks are subject to change)

[i] Federal regulations requiring procedures for monitoring BSA Compliance codified by the prudential regulatory agencies as follows: Office of the Comptroller of the Currency - 12 CFR Part 21.21 (national banks and federally chartered thrifts); Federal Reserve Bank Board of Governors – 12 CFR Part 208.63 (state chartered banks that are a member of the Federal Reserve System); and the Federal Deposit Insurance Corporation – 12 CFR Part 326.8 (state chartered banks that are not members of the Federal Reserve System) http://www.gpo.gov/

[ii] Office of the Comptroller of the Currency Safety and Soundness Booklets (2012) for *Community Bank Supervision* http://www.occ.gov/publications/publications-by-type/comptrollers-handbook/cbs.pdf and *Large Bank Supervision* http://www.occ.gov/publications/publications-by-type/comptrollers-handbook/lbs.pdf

[iii] Federal Deposit Insurance Corporation (2012) *Community Banking Study* http://www.fdic.gov/regulations/resources/cbi/study.html

[iv] Federal Deposit Insurance Corporation *Quarterly Banking Profiles – Ratios by Asset Size Group-Excel* http://www2.fdic.gov/qbp/timeseries/RatiosByAssetSizeGroup.xls

[v] Federal Financial Institutions Examination Council (2012) *Bank Secrecy Act Anti-Money Laundering Examination Manual* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm

[vi] Basel Committee on Banking Supervision (2014) *Sound management of risks related to money laundering and financing of terrorism http://www.bis.org/press/p140115.htm*

[vii] The Association of Certified Anti-Money Laundering Specialists (2012) *Study Guide for the Certification Examination Fifth Edition*

[viii] Association of Certified Money Laundering Specialists 12th Annual AML & Financial Crime Conference (2013) *Evolving the Audit Role to Safeguard Your Institution*

[ix] *Today's Lesson - Learning from the Mistakes of Others, Matters Requiring Attention*, Kenneth Simmons / Advanced AML Audit Certification White Paper published by the Association of Certified Anti-Money Laundering Specialists http://acams.org/advanced-aml-audit-certification-white-papers/

[x] http://www.goodreads.com/author/quotes/79014.Yogi_Berra?page=2

[xi] *Appendix H: Request Letter Items* in the Federal Financial Institutions Examination Council (2012) *Bank Secrecy Act Anti-Money Laundering Examination Manual* is a good starting point for creating a request letter https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_108.htm

[xii] *Comptroller Curry Addresses Senior Management's AML Compliance Responsibilities, Criticizes "De-Risking"* (2014) http://www.infobytesblog.com/comptroller-curry-addresses-senior-managements-aml-compliance-responsibilities-criticizes-de-risking/

[xiii] Joint Press Release (2012) *FDIC and FinCEN Assess Civil Money Penalty Against First Bank of Delaware* and Attachments http://www.fdic.gov/news/news/press/2012/pr12135.html

[xiv] Federal Deposit Insurance Corporation Financial Institution Letter FIL-43-2013 (2013) *FDIC Supervisory Approach to Payment Processing Relationships With Merchant Customers That Engage in Higher-Risk Activities* http://www.fdic.gov/news/news/financial/2013/fil13043.html

[xv] Federal Deposit Insurance Corporation *Bank Find* http://research.fdic.gov/bankfind/

[xvi] Federal Reserve Bank Board of Governors of the Federal Reserve System (SR Letter 11-7) http://www.federalreserve.gov/bankinforeg/srletters/sr1107.htm and the Office of the Comptroller of the Currency (OCC 2011-12) *Supervisory Guidance On Model Risk Management* (2011) http://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12.html

[xvii] *What Auditors Should Know and Ask About BSA/AML Software Before a Successful Audit Can Be Conducted,* Nancy Lake / Advanced AML Audit Certification White Paper published by the Association of Certified Anti-Money Laundering Specialists http://acams.org/advanced-aml-audit-certification-white-papers/

[xviii] The following are good resources for keeping abreast of emerging BSA/AML issues:

- Financial Crimes Enforcement Network https://public.govdelivery.com/accounts/USFINCEN/subscriber/new?
- Office of Foreign Assets Control https://public.govdelivery.com/accounts/USTREAS/subscriber/new?topic_id=USTREAS_61
- Office of the Comptroller of the Currency E-mail List Service http://www.occ.gov/tools-forms/subscribe/occ-email-list-service.html and RSS Feeds http://www.occ.gov/rss/index-rss.html
- Board of Governors of the Federal Reserve System E-mail Notifications http://www.federalreserve.gov/newsevents/subscribe.htm
- Federal Deposit Insurance Corporation E-mail Updates https://public.govdelivery.com/accounts/USFDIC/subscriber/new? and RSS Feeds https://public.govdelivery.com/topics/USFDIC_26/feed.rss
- Financial Action Task Force E-mail Updates http://www.fatf-gafi.org/pages/e-mailalert.html
- Bank for International Settlements – Basel Committee RSS Feeds http://www.bis.org/list/press_releases/index.rss