Strategic Gap Assessments

A Primer for Risk Managers

Brian W. Vitale, CAMS, BSACS, NCCO
September 2013
An effective BSA/AML compliance program controls risks associated with the bank’s products, services, customers, entities, and geographic locations; therefore, an effective risk assessment should be an ongoing process, not a one-time exercise. Management should update its risk assessment to identify changes in the bank’s risk profile, as necessary (e.g., when new products and services are introduced, existing products and services change, higher-risk customers open and close accounts, or the bank expands through mergers and acquisitions). Even in the absence of such changes, it is a sound practice for banks to periodically reassess their BSA/AML risks at least every 12 to 18 months.¹

FFIEC BSA/AML Examination Manual, 2010

**Purpose**

This white paper is not a “How To” manual for the creation and implementation of a BSA/AML Risk Assessment. Rather, the purpose of the paper is to introduce three separate, yet interconnected, gap assessment strategies to proactively assist Risk Managers in the identification of gaps, vulnerabilities and potential problems prior to a regulatory finding.

**Introduction**

Have you ever heard or spoken the saying, “It’s as easy as riding a bike”? Take a moment and reflect back to when you were a child first learning to ride on two wheels. Do you remember how you felt? Were you nervous, excited or scared?

For those of you whose memory of that triumphant day has faded, perhaps you will remember your daughter, son, niece or nephew taking that first solo voyage on their two-wheeled bicycle. After mastering the balanced, yet shaky forward motion, the handlebars wobbling frantically left to right and vice-versa, the “art” of properly braking was a lesson taught in bumps and bruises. Eventually they got the hang of it. And for the next several hours and days they did what came natural to them – the comfortable, predictable and fully controllable constant left turn.

Risk Managers are tasked with a myriad of responsibilities; responsibilities rooted in regulatory requirements promulgated by their specific state or federal regulatory agency. Further, Risk Managers routinely immerse themselves in the tactical operations side of the business. Tactics sustain enterprise objectives for the common purpose of goal attainment. From a strictly BSA/AML risk perspective, goal attainment, driven by a number of internal and external factors, results in strategic positioning of the organization for risk mitigation purposes – in essence, it is the identified risk appetite of the organization.
BSA/AML Risk Assessment Background

The BSA/AML Risk Assessment is the central focus and anchor of any BSA/AML regulatory examination. Auditors will review and measure the BSA/AML Risk Assessment to assist in their planning and scoping of the audit engagement.

Within the Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering Examination Manual (2010) under the BSA/AML Program tab is the CORE EXAMINATION OVERVIEW AND PROCEDURES FOR ASSESSING THE BSA/AML COMPLIANCE PROGRAM. Within this chapter of the FFIEC manual is a section on the BSA/AML Risk Assessment.

BSA/AML Risk Assessment

Objective: Assess the BSA/AML risk profile of the bank and evaluate the adequacy of the bank’s BSA/AML risk assessment process.

1. Review the bank’s BSA/AML risk assessment. Determine whether the bank has included all risk areas, including any new products, services, or targeted customers, entities, and geographic locations. Determine whether the bank’s process for periodically reviewing and updating its BSA/AML risk assessment is adequate.

2. If the bank has not developed a risk assessment, or if the risk assessment is inadequate, the examiner must complete a risk assessment.

3. Examiners should document and discuss the bank’s BSA/AML risk profile and any identified deficiencies in the bank’s BSA/AML risk assessment process with bank management.

Risk Assessment

Identify & Measure Risk:
- Products
- Services
- Customers
- Geographic locations

Mind the Gap
EXAMINATION PROCEDURES; BSA/AML Compliance Program

Objective: Assess the adequacy of the bank’s BSA/AML compliance program. Determine whether the bank has developed, administered, and maintained an effective program for compliance with the BSA and all of its implementing regulations.

The four pillars of the BSA/AML compliance program:

- A system of internal controls to ensure ongoing compliance.
- Independent testing of BSA compliance.
- A specifically designated person or persons responsible for managing BSA compliance (BSA Compliance Officer).
- Training for appropriate personnel.4

BSA/AML Risk Assessment and Audit

Auditors assess the BSA/AML compliance function in a number of ways:

- Monitor for changes; How do you do this?
- Assess the impact of changes; How well do you know your institution to understand the impact?
- Analyze the changes to current policies, procedures and processes; How well do you know what needs to be fixed?5

The BSA/AML audit process has three main stages: planning, testing and reporting.6

1. Scoping and Planning: This initial discovery phase includes a thorough review of the BSA/AML Risk Assessment.

Scoping and Planning – Overview

Objective: Identify the bank’s BSA/AML risks, develop the examination scope, and document the plan. This process includes determining examination staffing and technical expertise, and selecting examination procedures to be completed.

“The BSA/AML examination is intended to assess the effectiveness of the bank’s BSA/AML compliance program and the bank’s compliance with the regulatory requirements pertaining to the BSA, including a review of risk management practices.”7

3. Recommendations and Reporting: Discuss and validate any control weaknesses identified.

**Risk Assessment**

**Identify & Measure Risk:**
- Products
- Services
- Customers
- Geographic locations

**Internal Controls**

**Develop Applicable:**
- Policies
- Procedures
- Systems
- Controls

**Result:**

**Risk-Based BSA Compliance Program**
- Internal Controls
- Audit
- BSA Compliance Officer
- Training

**FFIEC Appendix I: Risk Assessment Link to the BSA/AML Compliance Program**
Gap Assessment Primer

The Gap Assessment Primer is the framework by which this paper is based. The underlying objectives to sustain the BSA/AML program within the parameters and expectations of the regulations is the common thread connecting each one of us within the BSA/AML compliance community. What happens when things change? Implementation and sustainment, complements of one another, cannot stand on their own. So what binds them together? A mixture of tactics and strategy.

Congress, the legislative arm of the United States government, is charged with the formation and passage of laws. Next follow the federal agencies whose charge is the writing of regulations to provide guidance to regulated bodies. Auditors, regardless of internal, external, state or federal, are the proctors of your BSA/AML program.

It is the responsibility of an Auditor to measure and test BSA/AML internal controls to ensure the safety and soundness of risk mitigation practices align with the organization’s risk exposure and industry best-practices. One common weakness within risk assessments is the assessment does not consider all the relevant and major risk categories the organization is expected to manage on an ongoing basis. Another is control gaps.

As Risk Managers, we are tasked with balancing the “What” and “How” within the framework of our BSA/AML regulatory obligations. The burden of getting it right each and every day is of critical importance to the sustainment of the BSA/AML program. Proactive controls in the BSA/AML area of your organization often dictate the expected outcome of your regulatory reviews. Unfortunately, reactive approaches to risk mitigation place your program at an elevated risk.

A reactive approach to risk mitigation, by the very definition of a reactive approach, negates any possibility of proactive vulnerability risk assessments. As a consequence, gaps can begin to form at the periphery of your program. The soundness of your program, identified, in part, by the BSA/AML risk assessment will potentially be challenged depending on when and by whom these gaps are discovered. Would you rather defend an established strategy or an undeniable gap (risk)? Who would you rather discover the gap in the program, your compliance unit or an Auditor?
The below diagram illustrates the “What” and “How” components of the Gap Assessment Primer.

If you can’t measure it, you can’t control it. What’s worse, if unforeseen risks remain unidentified, an indisputable and non-defendable gap exists in your program. The FFIEC created the BSA/AML Examination Manual to establish industry safety and soundness practices and examination procedures and parameters. Auditor BSA/AML engagements test an organization’s “What” against the FFIEC’s “How”. How can Risk Managers identify, measure, test, control and monitor a new and/or emerging risk if they do not know the new and/or emerging risk exists? They can’t. What happens when tactical and strategic risk objectives no longer align? From a risk assessment and auditing perspective, therein lies the opportunity; an opportunity to fill the “White Space”.

Risk Managers must be strategic with what limited resources are available to mitigate BSA/AML risks. Mitigation cannot occur when evolving gaps and vulnerabilities remain unidentified. As such, the following three strategies are offered as proactive methodologies Risk Managers may employ to assist in the identification of current and/or emerging program gaps. The Now, What, Why & How, 3-Circle and Resource Based Analysis strategies are methodologies any Risk Manager can employ to uncover gaps and/or vulnerabilities within the BSA/AML Risk Assessment.
Now, What, Why & How Strategy

The Now, What, Why & How strategy is an information gathering and analysis methodology; an interrogatory approach to gap identification. The basic tenet of this strategy is for Risk Managers to remain current on regulatory issues relevant to their specific environments. Ask questions. Risk Managers are buried in the tactical side of the business, often focused on the “What” and “How”. What about the “Now”? How much attention is given to the “Now” in your organization? Does your BSA/AML Risk Assessment fully identify the risks your organization faces “Now”?

When you are in the “know”, gaps and vulnerabilities are less likely to exist. BSA/AML Risk Assessment reviews every 12-18 months may meet the intent of the FFIEC, yet the impact can be drastic for your business. Any sound strategy to identify and assess gaps within the BSA/AML Risk Assessment must begin with an understanding of the risk landscape today. Take an Auditor’s perspective and don’t be caught by surprise. An Auditor’s job is to remain current on existing, new and amended regulations. Just as important as staying current on the regulatory front, what new risks are introduced due to organizational changes? Asking questions and evaluating the “Now” is of critical importance to understanding and addressing BSA/AML risks.

Questions every Risk Manager must ask on an ongoing basis to remain in the “K’Now” to ensure BSA/AML risks are addressed timely, accurately and with purpose are as follows:

The **Now** – What problem or opportunity does the organization face Now and what were the internal actions or external events that put the organization in this situation? What are the internal constraints (i.e., resources, past audit findings, lack of understanding) and external constraints (i.e., risk factors, lost opportunities, regulatory environment) that the organization will have to take into account as it moves forward?

Skills in identifying the Now are of critical importance in distinguishing the core problem from a symptom of the problem. Many organizations allocate a lot of resources to address the symptoms and then are surprised that the risk is not fully identified and controlled. Risk Managers must learn to dig beneath the surface to find the core problem that is responsible for causing the symptoms they are noticing. Ensure that when addressing a gap within the BSA/AML Risk Assessment, the identification and control is not targeted at the symptom, rather it is focused specifically on the core problem.

The **What** – What should the organization’s desired course or courses of action be at this point? What direction do you think it should pursue? How will you pursue it?
The **Why** – Why should the organization take this course of action? Is it going to meet the challenges we face? Allow us to create a maintainable competitive advantage? Create new opportunities in the “White Space”? Overall, does it provide the best opportunity to solve the core problem?

The **How** – How should Risk Managers go about employing current capabilities, enhancing those capabilities, or perhaps even acquiring new capabilities to best remedy this situation? What actions will Risk Managers have to take to implement this solution effectively? What internal or external resources will be required? What is the most cost-effective way to provide this solution?

The Now, What, Why & How strategy will assist the Risk Manager, and Auditor, in establishing the risk and risk trending of the organization.
3-Circle Strategy

The Now, What, Why and How strategy focused on the Now and laid the framework for the 3-Circle strategy. Not unlike the Now, What, Why and How strategy, the 3-Circle strategy continues the focus on the Now, albeit in a different way.

Consider all known and unknown factors impacting your BSA/AML Risk Assessment are in one large barrel of information. Looking inside the barrel from the top, no real sense of meaning or interconnections between factors is evident. Products, services, customers, entities and geographic implications, all known and unknown risks, are mostly unidentifiable. It is just noise. Where to Begin?

The below circles, red for ‘BSA/AML Risk Assessment’, blue for ‘Audit – Internal Controls and Measurement’ and black for influential observations or ‘Outliers’, are the visual equivalents of the aforementioned barrel of mostly unidentifiable risk factors. Empty the barrel and separate the factors into three separate barrels of information – circles of influence as shown below.
Once separated into their respective circles, the BSA/AML Risk Assessment can now be compared to audit expectations. Where the BSA/AML Risk Assessment (B) and Audit (C) circles overlap (below), this area identifies the known and mitigated risk factors. Together, both can now be measured against any ‘Outliers’, unknown and unidentified risk factors that will impact the Quality and/or Quantity of your BSA/AML Risk Assessment.

Consider now an exercise that requires an evaluation of influential observations of yet unidentified risk factors that are not enumerated within the BSA/AML Risk Assessment. As a Risk Manager, you cannot mitigate a risk if it remains unidentified. An evaluation of emerging and new risk factors, a change in products, services, customers, entities, geographic locations and ‘others’, should be at the forefront of your BSA/AML Risk Assessment mitigation program.

Risk Managers own the process by which risks are identified, measured, controlled and mitigated. Auditors, as previously stated, are the proctors of the BSA/AML program. Auditors are tasked with the measurement and testing of all BSA/AML risk factors impacting the organization. Are Risk Managers not tasked with performing this identical function?

The 3-Circle methodology is a focus on the Now. It provides a visual illustration of the process of gap assessment within the interrogatory of the Now, What, Why and How strategy. When the two align, the Outliers (D) can be merged into areas B and C. Consider further that the above circles are in a constant state of motion and represent a snapshot in time only. When that snapshot is taken, focus on the “White Space” (A); area of opportunity and identified gap(s).
An overview of the 3-Circle snapshot is as follows:

The “White Space” (A) represents gaps within the BSA/AML Risk Assessment. As identified within the GAP Assessment Primer: Gaps occur on the horizontal, anywhere between Strategy and Tactic. Gap assessment strategies are just that – strategies. The Now, What, Why and How strategy and the 3-Circle strategy share a purpose – to assist Risk Managers in the affirmation of the known and gap assessment and identification of the unknown risk factors impacting the BSA/AML compliance function.

BSA/AML Risk Assessment “White Space” Outliers are borne from various factors:

1. Regulations
   a. Amended
   b. New
   c. Emerging

2. Cost of Implementation
   a. What are the costs?
   b. What resources are required (FTE)?

3. Indifference
   a. If not broken, don’t fix it.
   b. Lack of understanding.

4. Unmet needs
   a. Don’t know any differently.
   b. Current system of BSA/AML risk mitigation is working, right?
Resource Based Analysis Strategy

The Resource Based Analysis methodology is rooted in competitive advantage measurement between competitors. This is not to suggest financial institution compliance departments are competing with one another. However, all regulated bodies subject to the Bank Secrecy Act operate from the standard set of expectations found within the FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (2010). Measurement of the effectiveness and operational efficiency of the BSA/AML Risk Assessment and gap assessment process is best explained by way of the Resource Based Analysis strategy. It brings it all together from the perspective of an Auditor.

The Now, What, Why and How strategy and the 3-Circle strategy, both established interrogatory methodologies, can be considered the Orthodox side of the business. Risk Managers are tasked with creation, implementation and sustainment of the BSA/AML Risk Assessment. Identified risks are measured and mitigating controls instituted per the risk appetite of the organization. Therefore, the following Orthodox rules follow any BSA/AML Risk Assessment:

1. Do it as required per the Bank Secrecy Act.
2. Do it well by ensuring all BSA/AML risks are identified and controlled.
3. Do it no better or worse than the median.

What about the Unorthodox approach? Agreed, points 1-3 are important and true competition amongst financial institution compliance departments is difficult, if not impossible, to identify. However, if these were identifiable amongst financial institution compliance departments, a comparative competitive set could be established in the Now, and not from the platform of retrospective rationality as learned vis-à-vis the numerous civil money penalties for BSA/AML deficiencies.

The Resource Based Analysis methodology is an Auditor’s ‘See One, Do One, Teach One’ competitive perspective, and can be the established comparative competitive set for your organization. If Risk Managers measure the effectiveness of gap assessment strategies to the point gaps and vulnerabilities are quickly identified and addressed within the BSA/AML Risk Assessment, the median has now been set for that specific compliance department and organization. How can this median transcend organizations to establish best-practices within and among compliance departments and Risk Managers? Through the guidance and best-practices provided by your Auditor.
Competitive gap analysis, measured in Rare, Durable, Relatively Non-Substitutable and Valuable, will affirm the interrogatory methodologies for gap assessment and fulfillment. Risk Managers can employ this knowledge and establish an internal comparative competitive set of gap assessment strategies for the purpose of sustainment of the BSA/AML Risk Assessment; sustainment with an ongoing established median of BSA/AML Risk Assessment gap and vulnerability awareness, identification and mitigation.

Auditors will assess the two interrogatory strategic gap and vulnerability methodologies during the pre-audit interview and review of the BSA/AML Risk Assessment. As stated, the Now, What, Why and How and 3-Circle strategies are tools for Risk Managers to employ to avoid unknown and unidentified gaps and vulnerabilities within the BSA/AML compliance program.

Audit Process → Audit Risk Model → Competitive Advantage → Addresses the “White Space”

Scoping and Planning: This initial discovery phase includes a thorough review of the BSA/AML Risk Assessment. The approach the Auditor will take to assess and/or affirm identified BSA/AML risks of the organization will shift, in part, due to the groundwork and strategic interrogatory methodologies the Risk Manager has employed.

Policy Reviews and Testing: A gap analysis of the financial institutions BSA/AML Risk Assessment and overall risk profile. When all BSA/AML risk factors have been identified and affirmed by the Auditor, the review and testing phase of the audit engagement will follow its normal and customary course. This will allow the Risk Manager to offensively interact with the Auditor to uncover best-practices, rather than a defensive position of inadequate risk identification and control.

Recommendations and Reporting: Discuss and validate any control weaknesses identified. No Risk Manager is perfect. Findings happen.

Rare: Relatively unique to the specific organization.

Durable: Does the BSA/AML Risk Assessment align with regulatory expectations and identified risks of the organization? Have all risks been identified?

Relatively Non-Substitutable: Subjective and rooted in best-practices for risk mitigation.

Valuable: Does this approach provide the commensurate risk identification, measurement, testing, control and mitigation per organizational risk appetite and regulatory expectations?
An overview of the Competitive Gap Analysis is as follows:

The Resource Based Analysis strategy is a proactive best-practice and is the Unorthodox side of the risk assessment process. Why? The Now, What, Why and How and 3-Circle strategies introduced BSA/AML Risk Assessment gap assessment tools to assist Risk Managers to avoid surprises. These two interrogatory methodologies can be employed by any Risk Manager to establish a move-forward plan on stepping out of the daily “What” and “How” tactical operation and into the “Now” strategic gap and vulnerability assessment approach.
Conclusion

Inaction is a strategy, albeit an unwise one. Operational value-add is rooted in tactics for the attainment of strategic objectives. Risk Managers are tasked with a myriad of regulatory responsibilities. As such, Risk Managers must leverage gap and vulnerability assessment methodologies to ensure compliance with new and emerging BSA/AML risk factors. These new and emerging BSA/AML risk factors must be identified via the BSA/AML Risk Assessment in a proactive, rather than reactive, manner. Be Your Own Auditor is not a second full-time job. It is the one and only best practice this white paper is attempting to impart to the Risk Manager reader.

Strategic gap assessment testing is about staying in the “Now”. For those Risk Managers who have been stuck in the comfortable, predictable and fully controllable left turn – turn right tomorrow. See what happens. And before you know it, you may cross that line into the dark side of the compliance industry: Audit.
Resources


5 Association of Certified Anti-Money Laundering Specialist CAMS Advanced AML Audit Certification Program Materials; Module 2: POLICIES, PROCEDURES, PROCESSES, January 2013.


9 Daniel H. McQuiston, Ph.D., Professor of Strategic Marketing, University of Notre Dame; Executive Masters of Business Administration Program, Strategic Marketing, Now, What, Why and How Strategy, Fall 2013.

10 Joel E. Urbany, Ph.D., Professor of Marketing, University of Notre Dame; Executive Masters of Business Administration Program, Introduction to Marketing, 3-Circle Strategy, Fall 2012.

11 Charles E. Bamford, Ph.D., Professor of Entrepreneurship & Strategy, University of Notre Dame; Executive Masters of Business Administration Program, Strategic Thinking, Resource Based Analysis Strategy, Fall 2012.