Best Practice BSA/AML Risk Assessment

The cost of the annual risk assessment process, which we covered in parts 1 and 2 of this series is just one facet of the risk assessment issue. As discussed in the two previous articles, all but the smallest institutions are spending $60,000 plus annually to produce their BSA/AML risk assessments. Which leads us to ask, with that kind of spending, are we being effective? According to the OCCs "Spring 2018 Semiannual Risk Perspective" AML and cybersecurity are the two major areas of risks of concern in the financial services industry. This position is unchanged from the Fall of 2017. However, a new emphasis on BSA risk assessments and new technologies were both areas of particular focus in the Spring report. The OCC stressed the need for sufficient risk assessments, noting that there is a disconnect between the business, with regard to introduction of new products, and the risk assessment process. The report noted that material changes in the business were not reflected in the risk assessment of many institutions. This disconnect in the risk mitigation strategies and the reality of the business operations is concerning to many regulators.

Is the Risk Assessment Critical, Important, or Just Another Box to Check?

The Philadelphia Federal Reserve Bank sounded a warning in a definitive work on requirements for BSA/AML risk assessments: "Many institutions, particularly community banks, simply do not know where to begin when attempting to develop a BSA/AML risk assessment." [Is Your Institution's Risk Assessment Adequate? Philadelphia Federal Reserve Bank, *SRC Insights*] More recently, in publishing a "job aid" for BSA/AML risk assessment, the Conference of State Bank Supervisors (CSBS) recognized a significant need to a standardized BSA/AML risk assessment practice.

The New York Department of Financial Services (NYDFS) has taken a bit more, shall we say, aggressive regulatory posture by requiring directors or officers of regulated institutions, including banks and MSBs, to certify that their institution's BSA program complies with 21 specific requirements set forth in Part 504 of the DFS Superintendent's Regulations. The NYDFS rules, which are consistent with the FFIEC's BSA/AML Examination Manual, make clear that a compliant BSA/AML program must start with a comprehensive risk assessment and that the institution's transaction monitoring system settings must "be based on the Risk Assessment of the institution."

What's Required, What's Best?

Best BSA/AML risk assessment practice is simple in concept and complex in execution. There's no dispute that an adequate risk assessment must, at a minimum, (1) assign an inherent risk, (2) detail mitigating controls, and (3) determine residual risk for:

- Every place in which the institution does business (including HIDTA, HIFCA, high-risk foreign locations) without regard to whether it has a physical presence
- Every product and service (including non-traditional banking products like securities trading, insurance, etc.)
- Every customer group/profile (e.g., convenience stores, MSBs, casinos, attorneys, etc.)

It must also evaluate and document its BSA/AML training programs (and whether they comply with regulations and are responsive to the institution's specific risks) and the administration of the BSA/AML compliance program. It should also take into account the institution's specific risk experience (red flags, SARs, and CTRs) with respect to each.

The Philly Fed and examiners of all stripe make clear that the risk assessment shouldn't be a "once a year" endeavor but a "living document" that is continually updated and used to manage the institution's BSA/AML risks. And it must do all of that with little specific regulatory guidance as to what will be acceptable. Indeed, a good risk assessment is updated when the institution:

- Begins business in a new location
- Acquires or merges with another institution
- Adds a product or service
- Begins serving a new customer type

and also

- When regulations materially change (think beneficial ownership)
- When the institution's risk profile changes (e.g., material changes in SAR/CTR activity)

After the institution has performed the perfect risk assessment, there's more…and it's what may be missing from your risk assessment practice even if you're pretty good at it.

We do that and we're done, right?

Not exactly… How does your institution react to your risk assessment? Hint: the answer is not: file it until next year.

We recently talked BSA/AML with the four major bank regulators, OCC, FDIC, Federal Reserve, and NYDFS. They stated, unequivocally and as a group, that the most common BSA/AML compliance deficiency was an inadequate risk assessment. They also made crystal clear that it's not only that risk assessments are often inadequate, but that the risks identified don't result in any change in the institution's behavior. In other words, the institution may identify some money laundering risks, but it often can't point to a single change in controls, transaction monitoring, investigation/SAR practice that relates to the specific risks in the risk assessment.

The very first requirement in the NYDFS regulation (which most of us think will be a guide for future federal practice) is that the transaction monitoring systems tie directly to the institution's money laundering risks as shown in the institution's risk assessment. Making, documenting, and explaining the connection will take your risk assessment practice from adequate to impressive.

Even if we agree with you, we don't have the time or resources to create a best practice risk assessment.

With technology, you actually do…and for less money and less effort than you're spending on the "manual spreadsheet/old fashion" way…
If you set out to develop a great BSA/AML risk assessment technology (and we did) it would:

- ✓ Collect information via intuitive wizards or direct connection to your core or transaction monitoring system that makes data collection simple and consistent.
- ✓ Contain inherent risk ratings for virtually every location, product, service, and customer profile a typical institution would offer or serve.
- ✓ Provide hundreds of mitigating controls customized to the specific products, services, and customer profiles.
- ✓ Rate risk on a categorical and institutional basis using a proprietary algorithm.
- ✓ Provide real time, plain language reports that give managers and executives the information they need to make informed decisions.
- ✓ Contain detailed documentation ready to provide regulators with a granular as well as an institutional view of BSA compliance.
- ✓ Be continually updated for regulatory changes and best practices.

About the Author

Debra Geister is Manager and CEO of Section 2 Financial Intelligence Solutions. Section 2 (S2) focuses exclusively on the tracking and documentation of the "hybrid threat." She and her team are passionate about education and detection of transnational criminal organizations in our financial systems. Previously, she was Managing Director for AML Advisory Services at Matrix International Financial Services. Geister has 15 years of experience in leadership roles in banking compliance. She worked at US Bank as a VP of Risk and Compliance and spent three years at Meta Bank as Senior Vice President, leading the combined Fraud and Bank Secrecy Act (BSA) Unit.

About RegSmart

RegSmart brings the people, processes, and technology together to meet your BSA and OFAC risk management and governance needs with cloud-based technology. Supported by subject matter experts, RegSmart collects data with intuitive wizards and stores that data for regulatory compliance and change management. RegSmart delivers complete, plain language reports with actionable intelligence. Please visit us at www.beregsmart.com.

If you would like to see a demonstration of our best-in-class automated BSA, OFAC, and cybersecurity risk assessment, governance, and audit applications, please contact us at 214.919.4670, or email John Ravita at jravita@beregsmart.com or Mark Stetler at mstetler@beregsmart.com. We look forward to visiting with you.