



As Seen in

International Banker

September 2019

US Regulators Reinforce the Importance of Risk Assessments

By Efren Marquez Alba, Engagement Director, Treliant

No matter the industry you may be in or your country of domicile, the framework for an effective compliance program requires a risk assessment. It is the foundational element of every compliance program. A company simply cannot mitigate its risks or design an effective compliance program if it doesn't know what its risks are. And depending on the complexity of the company and corresponding risk-management needs, a poorly designed risk assessment can have a severely negative cascading effect across the institution's risk-management infrastructure.

There are a number of guiding principles or expectations for risk assessments, both through international organizations such as the Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision (BCBS) to regional or country-issued expectations, such as the Anti-Money Laundering Directives in Europe and the Bank Secrecy Act (BSA) and related regulatory releases in the United States.

The recent "Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision" (July 22, 2019) in the US reiterates the critical importance of a sound and comprehensive risk-assessment methodology for the establishment and maintenance of a risk-based regulatory-compliance program that identifies and reports potential money laundering, terrorist financing and other illicit financial activity. Many of the related challenges are elaborated below.

Elements of risk-focused examinations

The July statement does not establish new requirements but emphasizes that examination plans and procedures will be tailored to the unique risk profile of each bank. Common practices for assessing that profile are described, including the leveraging of available information from various sources, interaction between examinations and analyses of a bank's ability to identify, measure, monitor and control risks.

One common practice is to review a bank's BSA/AML risk assessment prior to an examination. "Risk assessments and other independent testing that properly consider and test all risk areas (including products, services, customers, and the geographic locations in which the bank operates and conducts business) are used in determining the examination procedures and transaction testing that should be performed," the statement says. "The federal banking agencies generally allocate more resources to higher-risk areas, and fewer resources to lower-risk areas."

The importance of risk assessments

Although there is no statutory regulatory requirement, there is an established regulatory expectation that a well-designed and executed risk assessment should support the development of any AML or economic-sanctions compliance program. In underscoring this point, the recent joint statement by the Federal Reserve Board of Governors (the Fed), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC) and Financial Crimes Enforcement Network (FinCEN) supplements previous guidance promulgated by others—namely, the Federal Financial Institutions Examination Council (FFIEC), Financial Action Task Force (FATF), Wolfsberg Group and Basel Committee on Banking Supervision (BCBS), in addition to other international, regional and national regulatory bodies.

A bank simply cannot mitigate its risks or design an effective compliance program if it doesn't know what those risks are. As the joint statement noted, "A risk-based compliance program enables a bank to allocate compliance resources commensurate with its risk." And so, depending on the complexity of the financial institution (FI) and corresponding risk-management needs, a poorly designed risk assessment can have a severely negative cascading effect across a bank's risk-management infrastructure.

Risk assessments provide the foundation for establishing and automating controls. Key controls used to mitigate BSA/AML risks include:

- ✓ Know Your Customer:
 - Customer Identification Program
 - Customer Due Diligence
 - Customer Risk Rating Tool
 - Enhanced Due Diligence
 - Due Diligence Tools and Methods
- ✓ Suspicious Activity Reporting:
 - Transaction Monitoring
 - Case Management
 - Investigative Tools and Methods
- ✓ Currency Transaction Reporting Tools and Methods
- ✓ OFAC and other Watchlist Screening Tools and Methods
- ✓ Program Governance/Oversight:
 - Issue Management
 - Management Information
 - Model Risk Management
 - Data and Technology
- ✓ Training Delivery Methods and Role-Based Training
- ✓ Audit Coverage

Automating risk management

Many banks have been automating transaction-monitoring controls, and depending on the complexity of the organization, related decisions can include:

- manual or automated transaction monitoring;
- hosted or non-hosted implementation;
- rules-based or behavior-based detection methods;
- the designation of the automated transaction-monitoring method as a model within a bank's model risk-management inventory (subject to independent review and robust, effective challenge);
- the degree of below-the-line testing conducted for initial and ongoing threshold setting and calibration;
- the frequency of tuning and optimization cycles;
- the sophistication and configurability of the case-management system; and
- implementation of regtech (regulatory technology) solutions leveraging robotic process automation (RPA) and machine learning (ML) for data input and analysis.

Increasing regulatory focus on assessments

Meanwhile, recent regulatory enforcement actions have more frequently made specific reference to the need for “a comprehensive BSA/AML risk assessment that identifies and considers all products and services of the branch, customer types and geographic locations, as appropriate, in determining inherent and residual risks”. This has been particularly true in actions taken by the New York Federal Reserve Bank since 2017, especially with respect to branches of foreign banks.

Only time will tell whether other regulatory agencies will follow suit, but other signs also point to regulators’ changing expectations. In addition to enforcement actions cited in publicly available information, numerous financial institutions operating in the US have received Matters Requiring Attention (MRA) or Matters Requiring Immediate Attention (MRIA), with specific observations and recommendations to enhance their risk-assessment methodology. These actions commonly focus on deficient methodology, inadequate methodology documentation, lack of quantitative data in identifying and measuring inherent risks, insufficient staffing and investment, and flawed timing and frequency of annual risk assessments.

Risk-assessment execution issues

In addition to increasing regulatory expectations, banks face numerous challenges in conducting AML and economic-sanctions risk assessments. When using a quantitative methodology to identify and measure inherent risks, financial institutions must address issues related to:

- insufficient data quality and completeness, constraining the accuracy and precision of the risk assessment;
- use of electronic-data warehouses, data hubs or data lakes to retrieve and appropriately allocate inherent risk data;
- appropriate selection of inherent risk factors to accurately and completely identify all inherent risks;
- dependencies on upstream risk models to identify and measure customer, geographic, transaction, channel and product/service risks across the enterprise;
- completeness in including all relevant business units with AML and economic-sanctions risk exposure;
- appropriate selection of risk weights and sufficient testing and justification for weights and thresholds;
- mapping of inherent risks to controls and assessment of the adequacy of those controls, to determine residual risks;
- consolidation of business units within an enterprise-wide risk assessment; and
- designation of enough qualified employees with the appropriate levels of business-analysis and data-modeling skills to gather, assess and document data

sources and to conduct the calibration and tuning of risk factors, weights and thresholds.

Although all of the challenges cited above are important limiting factors for a comprehensive and accurate risk assessment, one challenge rises above the others. A lack of quantitative data continues to be a severe challenge for most FIs, resulting in defaulting scoring logic when data is “Not Available” (missing data often triggers a high-risk designation, which frequently overstates the degree of risk if the risk exposure is in reality *de minimis* or low) or non-reconcilable responses due to competing data sources and insufficient maker-checker and data-reconciliation controls.

To resolve this issue, banks should consider developing a roadmap for the efficient retrieval, validation and reconciliation of the required data. The design of a curated data store with data specific to the risk assessment, with clear data-lineage and data-retrieval protocols, and allowing for efficient data-reconciliation and data-integrity checks could greatly enhance the efficiency and accuracy of annual risk-assessment processes. Additionally, the establishment of a repeatable process would allow for storage of historical risk-assessment quantitative data to assess risk directionality for each assessment cycle and allow more frequent data pulls to facilitate risk-assessment and risk-management processes that are closer to real-time and on-demand.

Risk assessment in the bigger picture

If the risk assessment is deemed to be a quantitative methodology, the financial institution should consider whether to include the methodology within its model inventory consistent with its enterprise model risk-management policy and categorize the methodology as a model or non-model quantitative method, thereby subjecting the methodology to the higher rigor of the FI's model risk-management requirements, which may include more comprehensive documentation and risk-based independent review of the risk-assessment methodology.

Banks should also link their risk assessments to their enterprise risk-management frameworks by leveraging the assessments to establish and support financial-crime compliance-program risk-appetite statements, risk-appetite thresholds, the identification of risk-appetite breaches and of appropriate risk management within established risk tolerances and risk-acceptance processes.

As FIs continue to move forward in this era of big data and data analytics, and given the relatively low number of data points associated with AML and economic-sanctions risk assessments, the future challenge for FIs is to harness the power of their vast data stores to identify and accurately measure inherent risk exposures and to allow for more precise allocation of appropriate levels of resources when designing and operating

financial-crimes compliance programs. This approach is consistent with safety and soundness principles, seeking to identify and report potentially suspicious activity and to reduce the potential flows of illicit funds through the financial institution.

Efren Alba

Efren Marquez Alba, Engagement Director at Treliant, has over 30 years of leadership experience in financial services and professional services advisory organizations. His areas of expertise include a range of Bank Secrecy Act/Anti-Money Laundering (BSA/AML), Office of Foreign Assets Control (OFAC), and Patriot Act requirements. These include regulatory program compliance, risk identification and measurement, BSA systems and technology administration, suspicious activity investigations, Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD), BSA compliance program independent assessment, quality assurance, written policies and procedures, regulatory relations, and operational efficiency and effectiveness. Efren has worked at the global, national, and regional level with commercial banks, savings and loans, broker-dealers, investment advisors, and credit card associations. He has participated as a key manager in addressing multiple regulatory enforcement actions involving correspondent bank and wire transfer transaction reviews and EDD lookbacks, restructuring of departments reporting to Financial Intelligence Units (FIUs), and BSA/AML/sanctions model risk management. He has also designed and documented various risk models including customer, country, enterprise money laundering, and terrorist financing risk.