Continuous Process Improvement is Key to Effective Risk Assessments

Is Your Organization’s Risk Assessment Process Dynamic or Stagnant?

ABOUT EXIGER

Exiger is a global regulatory and financial crime, risk and compliance company. Exiger arms financial institutions, multinational corporations and governmental agencies with the practical advice and technology solutions they need to prevent compliance breaches, respond to risk, remediate major issues and monitor ongoing business activities. Exiger works with clients worldwide to assist them in effectively managing their critical challenges while developing and implementing the policies, procedures and programs needed to create a sustainable compliance environment. A global authority on regulatory compliance, the company also oversees some of the world’s most complex court-appointed and voluntary monitorships in the private and public sectors, including the monitorship of HSBC. Exiger has four principal business units being: Exiger Advisory; Exiger Analytics, including DDlQ, the groundbreaking cognitive computing and intelligent search platform; Exiger Diligence and Exiger Insight 3PM. Exiger operates through offices in New York City, Silver Spring (DC Metro), Miami, Toronto, Vancouver, London, Hong Kong, and Singapore.
An effective risk assessment process is dynamic and continuous. It needs to be adjusted periodically to account for changes to an organization’s structure, product offerings, customer base and geographical footprint, as well as changes in regulatory expectations and industry benchmarks. The FFIEC BSA/AML (Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering) Examination Manual (Risk Assessment) clearly articulates the need for continuous process improvement for risk assessments:

“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.”

The complexion and timing of this sort of periodic review and adjustment depends on circumstances and industry. Generally, organizations review their risk assessment methodology and business processes just prior to conducting a periodic risk assessment. This review period allows the organization to reflect the current state of its business operations, regulatory landscape and risk appetite within the structure of the risk assessment. A number of factors should be considered when updating a risk assessment framework. Examples include changes to the customer base, new products or services offered, geographic anomalies, and mergers or acquisitions. It is critical that these factors, as well as any other lessons learned since the previous risk assessment framework review, are incorporated into the upcoming risk assessment to ensure all relevant information is included.

Business Scenario for Illustrative Purposes

Background

The following is a comparison of two organizations: Organization Y and Organization X. Both have established AML and Sanctions risk assessment methodologies, business processes and annual risk assessment cadences. While this scenario takes place within the financial services industry, the risk assessment issues described are relevant and important to all industry sectors. Organization X and Y have similar business compositions, including similar customer types and geographies, products and services offered and transactions executed. Organization X and Y are both US-based retail brokerage banks offering wealth management services to their mainly domestic, individual customer bases. They have approximately 100 branch offices located throughout the US, and the
vast majority of the transactions executed on behalf of their customers are domestic in nature.

Both Organizations X and Y have undergone the following changes to their business models in the year preceding the update period of the risk assessment framework methodology:

- They have gone through an acquisition of “Private Bank Z,” which is a financial services firm that provides tailored services to ultra-high net worth individuals, family offices, and personal investment companies.
- As a result of this acquisition, their overall customer base has expanded primarily from individuals to personal investment corporations and family offices.
- The geographical nature of their customer base has also changed, as a number of the clients of Private Bank Z are located in international jurisdictions, with business dealings and additional homes located in the US.
- Their product and service offerings have expanded, most notably to include electronic banking and remote deposit capture services, which were not previously available to the retail customer base.

The notable difference between these two organizations is that Organization Y uses the same, stagnant risk assessment framework to conduct each annual risk assessment, while Organization X reviews its risk assessment methodology and business processes two months prior to beginning its annual risk assessment.

**Organization Y Performs its AML/Sanctions Risk Assessments Without Conducting a Periodic Review**

Prior to performing the annual AML and Sanctions Risk Assessments, Organization Y does not perform a sufficient periodic review to ensure that the changes to its business from the acquisition of Private Bank Z are incorporated into the risk assessment framework. As a result, several negative impacts to the risk assessment occurred:

- The risk assessment framework failed to consider the additional customer types of personal investment companies and family offices gained through the acquisition. Personal investment companies are inherently high-risk customer types compared to individual investors due to their complex entity structure and the involvement of beneficial ownership layers. This leads to the customer type inherent risk factor being skewed to a lower risk than the current customer breakdown should warrant for Organization Y’s business.

“Organization Y was the same, stagnant risk assessment framework, while Organization X reviews its risk assessment methodology and business processes two months prior to beginning its annual risk assessment.”
Organization Y does not currently have a formal geography risk rating methodology. Therefore, it does not have a systematic method of risk-rating the additional countries to which its clients are now connected. Previously, the vast majority of its clients were located in the U.S., with a small number of clients in Canada, so a global geography risk rating matrix was not required. However, because of the acquisition, there are now bank clients connected to sensitive countries like Venezuela, Mexico, and Argentina. These new bank clients have not been included in the firm’s formal risk-rating nor in the inherent geographies risk calculation.

The risk assessment framework assessed the product and service portfolio of Organization Y prior to the acquisition, which did not account for two higher-risk products that were added to the Organization’s offerings: electronic banking and remote deposit capture. The current risk methodology remains skewed to lower risk products, which results in a lower inherent risk than warranted. In addition, the risk assessment is not assessing the strength of the control environment surrounding these new products and services to determine if the level of controls is sufficient for these high-risk products and services.

During the upcoming regulatory examination of Organization Y, the regulators focus primarily on (1) the FCC controls in place for the newly acquired Private Bank Z, and (2) whether Organization Y has fully accounted for the FCC risks of acquiring this business. The regulators criticize Organization Y for not performing a periodic review of the risk assessment framework, and for not including the additional characteristics of Private Bank Z into its risk assessment. Furthermore, the regulators conduct their own independent risk assessment, which shows that the residual risk of the business is “moderate to high,” compared to Organization Y’s residual risk rating of “moderate to low.” As a result, the regulators issue an MRA (Matter Requiring Attention) to Organization Y. This MRA includes a mandate to update their risk assessment framework, and to re-perform the FCC risk assessment prior to the end of the calendar year.

Organization X Conducts a Periodic Review Prior to Conducting its AML/Sanctions Risk Assessment

Prior to performing the annual AML and Sanctions Risk Assessments, Organization X performs a formal, front-to-back review of the risk assessment framework to ensure all changes as a
Continuous Process Improvement is Key to Effective Risk Assessments

As a result of its acquisition of Private Bank Z are evaluated as part of the upcoming risk assessments. After reviewing the risk assessment and including the required updates to the framework, the results are as follows:

- During the periodic review of the risk assessment framework, the FCC risk assessment team performed a mapping exercise of all Organization X’s additional customer types to ensure they were properly captured within the framework. The additional customer types of personal investment companies and family offices were added to the framework. Since these customer types typically present an inherently higher risk compared to individuals or corporations, these additional customer types increased the customer risk from “low” to “moderate” within the risk assessment results. Remote deposit capture and electronic banking were also newly included as part of the products and services inherent risk assessment, and were determined to be “moderate” and “high” risk products and services, respectively. As a large number of former Private Bank Z clients engaged in electronic banking services, the overall products and services inherent risk for Organization X was increased from “moderate” to “high.”

- As a result of the additional geographies associated with Organization X’s new customers from the Private Bank Z acquisition, Organization X completed a formal global country risk rating analysis to evaluate the level of risk associated with each country. The risk assessment led to a proper evaluation of the inherent customer geography risk because it incorporated the risk levels that were calculated during the country risk rating process. Using the updated country risk rating methodology in the risk assessment resulted in an increase of the geographies inherent risk from “low” to “moderate.”

- While performing the control assessment for the current risk assessment process, Organization X determined that it should strengthen its overall control framework to compensate for the additional customer types, geographies, and products acquired as a result of the Private Bank Z acquisition. One of the main takeaways from the control assessment was that Organization X required additional FCC staffing in order to avoid control breaches, backlogs, and other compliance-related issues going forward. As a result, the organization created a formal project plan to (1) remediate the identified deficiencies, and (2) perform an analysis to determine the

“One of the main takeaways from the control assessment was that Organization X required additional FCC staffing in order to avoid control breaches, backlogs, and other compliance-related issues going forward.”
appropriate staffing levels for the FCC department.

■ After the completion of the FCC risk assessment, the regulators and internal audit reviewed the enhanced risk assessment framework as well as the results of the annual risk assessments, focusing on the elements that were added to Organization X’s business through the acquisition of Private Bank Z. The FCC lauded the organization for enhancing the risk assessment framework to include all of the additional customer types, geographies, and products and services.

Both the regulators and internal audit agreed with the increased residual risk results of “moderate to high,” as it fell in line with their expectations for the expanded business of Organization X. The regulators acknowledged the control deficiencies identified during the control assessment, but since formal action plans were in place to address the deficiencies and perform a staffing analysis, the FCC refrained from issuing formal criticism at the close of the examination.

How Risk 360 Can Help

Exiger Risk 360 is a web-based, content agnostic assessment platform that enables centralized administration of enterprise-wide and targeted risk assessments. This technology tool is flexible, user-friendly, and it offers transparent methodologies that provide clear audit trail documentation. When the Risk 360 platform is used in conjunction with risk assessment subject matter experts, corporations optimize their risk assessment business model and processes in a way that enhances resource efficiency while minimizing the regulatory and reputational risk to their organization.

A dynamic risk assessment is a key component of an effective risk management program. An organization that proactively focuses on continuous improvement of its risk assessment framework—prior to conducting periodic reviews—can improve risk management capabilities, minimize rework, avoid incremental costs and penalties, and help to uphold a positive reputation for their organization among regulators, clients, and the business community.

Risk 360 is part of Exiger, a global regulatory and financial crime, risk and compliance company. Exiger arms financial institutions, multinational corporations and governmental agencies with the practical advice and technology solutions they need to prevent compliance breaches, respond to risk, remediate major issues and monitor ongoing business activities. Exiger works with clients worldwide to assist them in effectively managing their critical challenges while developing and implementing the policies, procedures and programs needed to create a sustainable compliance environment.
For more information, contact:

John W. Melican  
Managing Director, Americas  
Regional Chair | Head of  
Financial Crime Practice  
jmelican@exiger.com

Chris Andre  
Managing Director, Americas |  
Deputy Head of Financial  
Crime Compliance  
candre@exiger.com

Patrick Pizzichetta  
Financial Crime Compliance  
Advisory | Managing Consultant  
pizzichetta@exiger.com

www.exiger.com