Evolution of an AML Risk Assessment

Does Your Organization Modify Its Risk Assessment Framework to Address Current Regulations & Industry Trends?
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 DDIQ, 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 must be dynamic—not stagnant. It should be evaluated and adjusted on an ongoing basis to account for regulatory changes and industry trends. This document contains a hypothetical example for a mid-sized bank that has been developing and enhancing its financial crimes compliance (FCC) risk assessment for many years. While this scenario is fictional, it serves to illustrate the risk assessment trends that have occurred within the financial services industry during the past 15 years—these trends are relevant and important to corporations in all industries.

**Business Scenario for Illustrative Purposes**

**Background Information**

Bank X is a mid-sized commercial bank headquartered in the United States. It is primarily engaged in corporate lending and financing, but also has a fairly substantial retail operation, which includes a small wealth management division for affluent and high net worth customers. While the activity of its customer base is primarily domestic, the Bank does have representative offices in Mexico and Canada to support corporate lending in those jurisdictions.

**The Year 2002**

Based on emerging regulatory requirements and industry trends, Bank X develops a risk assessment document covering its inherent anti-money laundering (AML) risks and control framework. This risk assessment is purely a qualitative and subjective analysis, based on the personal judgment of Bank X’s compliance officer. Inherent risk is covered only at the highest organizational level, and there is no documented methodology or framework which includes supporting rationale for how risk ratings are calculated for customers, products and services, transactions or geographies. Controls are also qualitatively assessed, rather than quantitatively, and the compliance officer does not document the methodology used to assess the effectiveness of the Bank’s mitigating controls.

**The Year 2005**

Based on industry trends and increased regulatory expectations, Bank X develops a quantitative AML risk assessment scorecard. This is an Excel spreadsheet that shows relative weightings and scores for the primary inherent risk and control effectiveness categories. But there is no underlying methodology document to indicate how the weightings were assigned, and there is limited documentary evidence to support how the scores were calculated. The scorecard has a residual risk matrix, but again, the Bank has no supporting documentation for the scoring methodology used.
The AML risk assessment has been expanded to include questions related to sanctions risks and controls, but there is no independent sanctions risk rating methodology. The risk assessment exercise is conducted entirely by the compliance department using information gathered from the business and operations, and there is no governance framework documenting formal roles and responsibilities for the collection of information or the assessment of risk.

From 2007 Through 2013

Bank X develops an increasingly sophisticated FCC risk assessment based on industry trends and persistent regulatory pressure. The Bank creates separate written methodologies and risk assessment scorecards for AML, Sanctions and anti-bribery and corruption (ABC).

A formal governance structure is developed, articulating clear roles and responsibilities, timelines, deliverables and approval requirements. However, the Bank is still having difficulty monitoring these roles and responsibilities—and, as the compliance team grows—ensuring that only the correct individuals have the ability to alter or modify risk outcomes.

The enterprise-wide view is further stratified into assessment units consisting of primary operating units and geographies, so that both risk exposure and control weaknesses can be more easily identified and remedied.

From 2014 Through 2016

In spite of these many improvements, Bank X faces increased pressure from both regulators and internal audit to maintain clear audit trails, supporting documentation, and change records for the entire lifecycle of all FCC risk assessments. Bank X is repeatedly criticized for its inability to identify how, when or why process elements (including weightings, scores and questions) were introduced or modified. The bank is also criticized for its inability to identify how assessment responses were created or changed and the corresponding approval/governance process that was used to address these changes.

“Bank X develops a quantitative AML risk assessment scorecard... no supporting documentation for the scoring methodology used.”
2017 - 2018: Risk & Reputation Implications

Regulators formally criticize Bank X for having a deficient FCC risk assessment process. The areas of deficiency include a lack of:

- Clear accountability for changes to risk assessment business processes and methodologies;
- Granularity in the underlying data utilized to assess the quantitative inherent risk for AML, Sanctions, and ABC;
- Formal governance structure and reporting process for the remediation of control deficiencies identified through the risk assessment processes;
- Inclusion of certain risk assessment elements as recommended in the Federal Financial Institutions Examination Council (FFIEC) BSA/AML Manual;
- A consistent and transparent risk assessment methodology for all Bank X legal entities aligned with each risk category and control element;
- An audit trail for assessment responses, approvals, modifications and aggregate results.

“Regulators formally criticize Bank X for having a deficient FCC risk assessment process.”

Risk Assessment Evolution Timeline

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Subjective Analysis</td>
<td>Quantitative Excel Spreadsheet/Scorecard</td>
<td>Written Methodologies &amp; Scorecards:</td>
<td>Increased Pressure:</td>
<td>Formally Criticized by Regulators</td>
</tr>
<tr>
<td>Highest Organizational Level Only</td>
<td>Primary Categories No:</td>
<td>- AML</td>
<td>- Audit Trails</td>
<td></td>
</tr>
<tr>
<td>Qualitative Controls</td>
<td>No:</td>
<td>- Sanctions</td>
<td>- Supporting Documentation</td>
<td></td>
</tr>
<tr>
<td>No:</td>
<td></td>
<td>- ABC</td>
<td>- Life Cycle Change Records for All FCC Risk Assessments</td>
<td></td>
</tr>
<tr>
<td>Documentation</td>
<td>Underlying Methodology</td>
<td>Formal Governance/ Role Clarity Issues</td>
<td>Repeated Criticism:</td>
<td>Accountability</td>
</tr>
<tr>
<td>Supporting Rationale</td>
<td>Supporting Documentation</td>
<td>Enterprise-Wide View</td>
<td>- Process Elements</td>
<td>Formal Governance</td>
</tr>
<tr>
<td>(conducted by Compliance Department)</td>
<td>Governance Framework</td>
<td>Manual Process/ Version Control Problems</td>
<td>- Approval/ Governance</td>
<td>RA Methodology by Legal Entity Trail</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Audit Trail</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Begin to Leverage AI &amp; Technology</td>
</tr>
</tbody>
</table>
An effective risk assessment framework must be dynamic. It should align well with current regulations and industry trends. As shown through the high-level evolution of the AML risk assessment that is outlined in this document, the risk assessment process has become—and will continue to be—more complex over time. Organizations that:

1. Establish and periodically update a governance process that aligns with their business model, regulation and industry trends
2. Maintain clear audit trails
3. Provide supporting documentation
4. Include change records for the entire lifecycle of all FCC risk assessments
5. Leverage AI and technology tools

are better positioned to minimize both regulatory and reputational risk.

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.

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  
ppizzichetta@exiger.com