RISK-BASED APPROACH FOR RISK RATING
CUSTOMERS AND SUSPICIOUS REPORTS

Saboor Siddiqui
Advanced ACAMS-FCI March, 2019, Amman Cohort

Date of Submission: 5th August, 2019
Table of Contents

Executive Summary..........................................................................................................................................................................................2
Background ..................................................................................................................................................................................................................4
Solution – Building Your Customer Risk Matrix ..................................................................................................................................................................4
Case Study - Risk Rating the Financial Institutions’ Customers .........................................................................................................................6
Scoring Based on RBA ......................................................................................................................................................................................14
Conclusion and Recommendations .......................................................................................................................................................................19
Sources Referenced ..................................................................................................................................................................................................21
Executive Summary

The Financial Action Task Force (FATF) recommends that countries identify, understand, and assess the money laundering and terrorism financing risks for the country. An appointed authority or mechanism should coordinate risk assessment and apply resources to mitigate the risks effectively. However, it is often an ongoing challenge for the senior management at financial institutions to derive a methodology to risk rate/score its customers and the suspicious reports/cases pertaining to them based on various relevant parameters.

In this white paper, I wish to address this very concern, based on my personal experience at both ends of the table: i.e., being at the side of a reporting entity as well as working with the FIU as and STR/SAR analyst.

For any good compliance regime, it is vital to categorize the subjects of the suspicious reports, and such reports themselves, based on their inherent risks. Such classification not only enhances the risk management statistics, but also lets an institution device take a systematic approach of tackling risks of different magnitudes with commensurate mitigating and escalating processes. In addition to that, it might also prove to be helpful in deciding which level of resources (in terms of experience and capabilities) handle which types of reports and cases.

This white paper expounds the factors that should be integral in determining the risk scores of individual clients, corporate clients (juridical persons) according to their different attributes, and also the risk score of the reports, which a financial institution puts together citing suspicious activities or transactions. Based on the use of such a methodology, the institution can decide accordingly which reports merit an escalation to FIU or law enforcement. Also, based on the same, the institution can assign priorities to their STRs and SARs.

By the end of reading this white paper, the reader will be able to gather his/her thoughts around devising a methodology on similar grounds while choosing the risk factors regarding what is relevant to their own segment customers and suspicious reports.

This document sets out a risk-based approach and methodology to risk rate a financial institution’s customers and also the suspicious transaction report (STR) analysis by improving on existing policies and procedures and defining enhanced procedures for analysis based on the report’s risk classification and priority. We aim to guide risk assessors through the analysis process, ultimately enabling the FCC compliance to perform its core function; i.e., to investigate and escalate intelligence to the review board/management or to the FIU of the jurisdiction.
Research and Development

— Extensive research has been carried out in relation to procedures, which most of the financial institutions follow to classify risks pertaining to the subjects of suspicious reports.

— This includes detailed interviews with key stakeholders and reviews of over 50 documents, including relevant guidelines from FATF, Wolfsberg Principles, and the best practices followed by some of the best financial institutions across the world by virtue of their own experiences, in order to broadly benchmark the risk-based approach.

Based on the research, it is noted that when financial institutions and the different assessors therein use their own arbitrary methodologies to gage the risks, it may lead to the many key risks and issues that are critical to achieving a fully efficient target state of operations for any AML/CFT compliance team. Among them, it is of paramount importance that analysts/assessors tend to follow their own techniques and workflow when handling cases. This can be attributed to the absence of well-articulated and prescribed risk indicators.
Background

Taking a Risk-based Approach
In 2007, the Financial Action Task Force (FATF) introduced guidance called “Risk-Based Approach to Combating Money laundering and Terrorist Financing.”

As a whole, this document outlines the purpose of taking a risk-based approach to AML/CTF compliance while providing insights and guidance on how a financial institution or services can effectively implement a risk-based approach with high-level principles and procedures. Since this document has been diffused among the financial sector, taking a risk-based approach has developed into a standard and crucial piece for building effective AML programs.

Over time, this guidance has evolved and will continue to change and be updated.

According to FATF guidance, published on October 2014, “RBA to AML/CFT means that countries, competent authorities and financial institutions are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.”

In the FATF recommendations, it has been clearly highlighted that there is no universally agreed upon and accepted methodology to prescribe the nature and extent of a risk-based approach, leaving the financial institution to decide on the methodology they want to use based on the analysis of the risk and the risk management framework. This provides a financial institution with a degree of autonomy to customise their approach to suit their offering, yet at the same time forces a certain level of understanding to be reached before compliance can be achieved.

It is important to understand the difference between taking a risk-based approach for conducting a risk-based assessment and implementing mitigation strategies, such as assessing and updating the ML/TF risk posed by a customer. One assessment helps to inform the other, yet these should be treated as mutually exclusive processes.

Solution – Building Your Customer Risk Matrix

Why Implement a Risk-based Approach?
The risk-based approach is a method to prioritize supervision activities adopted by regulatory agencies in several countries and meant to foster an efficient relationship between the use of available human resources and financial intelligence received by the respective reporting entity.

The framework is recommended as a way to increase the effectiveness of the analysis of information provided by reporting entities through the application of risk matrices.
Building Your Customer Risk Matrix
Before we start building your customer risk matrix, first we must understand the terms more broadly and the necessary steps required for establishing a customer risk matrix.

Put simply, a customer risk matrix is a tool for placing your customer into different risk buckets. These are generally listed as low, medium, and high risk, with the scope for additional variations within these risk buckets.

The initial risk score given to a customer via your customer risk matrix can depend on many factors, such as: the results of initial customer due diligence, PEPs, and sanctions screening and demographics. Additionally, you should assess the customer interaction risk: this is a function of the product, how you are delivering it, and the customer risk.

So How Does an Institution Establish Its Customer Risk Matrix?

![Risk Matrix Steps]

A Customer Risk Assessment procedure follows these four steps:

**Identify**
- the customer’s risks based on their customer profile (such as country of residence, demographics, the source of funds, watchlist checks)
- Customer Interaction Risks = Customer Risk x Product Risk

**Assess** the likelihood and severity of these risks

**Understand** your business’ relationship with these risks

**Mitigate** the risks with policy and procedures outlined in your AML program

In order to define the customer risk, the financial institution should first know their customer. With this information, a designated service is then able to categorise the customer’s risk based on the vulnerability to money laundering and terrorist financing, and perform EDD if necessary. (The AML/CTF risk a PEP customer poses should be higher, because these individuals have more exposure to predicate offences, such as corruption.)

Considering the factors outlined when you conduct an AML/CTF risk assessment, financial institutions should understand that the risk-based approach is a quantitative methodology that will not eliminate the risk; however, it will enable the understanding of risks with the aim of mitigating the impact, which requires identification of risk factors, classification, and scoring.
**KYC & KYB Checks**

As explained in the previous blog post on Know Your Customer, these checks should be performed initially and updated on regular intervals depending on the risk that customer represents. If there are any material changes to the customer, it is best practice to update your customer risk profile.

**PEP and Sanction Watchlist Checks**

Performing a PEP (politically exposed persons) and sanctions check is often bundled up with KYC procedures.

The results from querying these global databases inform whether the individual or company with whom you are beginning a business relationship with requires additional risk mitigation strategies.

If an individual or company appears on one of these global watchlists, then the AML/CTF Rules proposes they are automatically a high-risk customer and should be treated as such in accordance with your AML operation manual.

**Enhanced Due Diligence**

Some suggestions on Enhanced Due Diligence procedures can be found in the previous post Know Your Customer.

**Case Study - Risk Rating the Financial Institutions’ Customers**

Based on the aforementioned, the following is an illustrative Risk Assessment Framework of customers by a bank in UAE. While reading this illustrative guidance, one must take into account the geopolitical factors pertaining to UAE and also its demographical facts—especially the fact that the UAE is a diverse society with 85% of its population expatriates from more than 120 countries who reside, do business, or are employed in the UAE.

The segmentation of risk can be broken down into **Country Risk** and **Customer Risk Assessment & Profiling** of the customer itself.

**Country Risk**

Country Risk is pertinent to the country in which the customer (individual or client) originates, hails from, resides, operates in, or is affiliated. The Country Risk Model is a conceptual framework that ranks countries (other than the sanctioned countries) across four variables, listed below.

<table>
<thead>
<tr>
<th>Variables Considered:</th>
<th>Risk Addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Corruption Perception Index (CPI)</td>
<td>Source of corrupt money</td>
</tr>
</tbody>
</table>
a) **Corruption Perception Index**

Based on expert opinion from around the world, the Corruption Perception Index measures the perceived levels of public sector corruption worldwide.

b) **International Narcotics Control Strategy Report released by U.S. Department of State (INCSR)**

This report offers a comprehensive assessment of the efforts of foreign governments to reduce illicit narcotics production, trafficking, and use in keeping with their international obligations under UN treaties, while also presenting information on governments’ efforts to counter money laundering and terrorist financing generated from narcotics trafficking.

c) **Country-wide Sanctions Programs**

The country-wide sanctions programs ratings used in the Risk Map were a combination of any of the below sanctions regimes:

- The Office of Foreign Assets Control of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security.

- The European Union’s sanctions are restrictive measures against third countries, individuals, or entities with objectives in accordance with the principles of the Common Foreign and Security Policy.

- The United Nations Security Council can take action to maintain or restore international peace and security under of the United Nations Charter. Sanctions measures encompass a broad range of enforcement options that do not involve the use of armed forces.

d) **Cost of violence containment**

Global Peace Index ranks the nations of the world according to their level of peacefulness. The index is composed of 23 qualitative and quantitative indicators from highly respected sources. The index gauges global peace using three broad themes: the level of safety and security in society, the extent of domestic and international conflict, and the degree of militarization.
Each country is assessed based on the above variables, which provide us with a risk score on a scale from lowest (4) to highest (15). A higher score means the country is at a higher risk for money laundering and terrorist financing offences.

Customer Risk Assessment & Profiling

Customer Risk Assessment (CRA) is a key component of the KYC/CDD process and a mandatory regulatory requirement. The objective of the CRA is to embed a consistent, well-defined, and risk-based method for assessing and classifying customers that may pose an “increased” level of risk to XYZ BANK, and identifying PEP and those customers with which XYZ BANK does not wish to establish a banking relationship due to their “unacceptable” level of risk.

CRA must be applied to all XYZ BANK customers with a liability product. For the overall risk assessment and risk classification of a relationship, XYZ BANK customers are classified into the following risk categories:

a) Pre-defined Neutral  
b) Assessed Neutral Risk  
c) Increased Risk  
d) Politically Exposed Person (PEP)  
e) Unacceptable Risk

All XYZ BANK private customers are, by default, increased risk and should be subject to Enhanced Due Diligence.

CRA should be performed on the overall customer relationship, and profiling needs to be done by completing fresh KYC forms (as applicable) in the following instances:

- New to bank relationships  
- Additional account opening request for existing customers  
- Existing resident customer becomes a non-resident  
- Existing sanctioned nationality customer changes passport  
- Existing legal entity customer changes its ownership, name, or business activities  
- Existing increased risk customer is upgraded  
- Customer changes mailing address (if new address is non-UAE)  
- Or any other changes to a customer profile that make overall risk classification as increased, PEP, or unacceptable risk

a) Assessed Neutral

Customers classified as “Assessed Neutral” do not require Customer Acceptance Advisory sign-off; however, a KYC form must be filled.
b) Pre-defined Neutral

Customer Risk Assessment is not required for customers that do not opt for/maintain a liability account (e.g., credit card-only relationships). These customers will be classified as Pre-defined Neutral.

It is critical that all staff and units involved in customer relationship establishment and maintenance for individual, as well as legal entity customers, fully understand the customer risk assessment process and strictly adhere to the prescribed guidelines.

c) Increased Risk Relationships

Customers classified as Increased Risk and/or Politically Exposed Person(s) must have designated business head approval as well as the required approval from Client Acceptance Advisory - Group Compliance, without which the account opening should be declined by the processing department.

The following customer categories present a high money laundering and terrorist financing risk; hence are identified as “increased risk.” An Enhanced Due Diligence (EDD) in accordance with the guidelines provided should be undertaken prior to establishing any banking relationship for such customers.

The business is responsible for ensuring that EDD is conducted in respect to the following relationships, and that documentary evidence of the completed EDD process is maintained in the respective customer’s file.

**High-risk Individuals Such As:**

- Private Customers (XYZ BANK Private)
- Non-UAE Resident Individuals
- UAE residents and nationals of the following sanctioned jurisdictions:
  - Iran
  - Cuba
  - Ukraine
  - North Korea
  - Sudan
  - Syria

Or, as advised by group compliance from time to time.

- UAE residents who are nationals of the following increased risk jurisdictions (as identified in the risk map):
  - Myanmar (Burma)
  - Russia
  - Somalia
- Iraq
- Afghanistan
- Yemen
- Saint Kitts and Nevis
- Nigeria

Or, as advised by group compliance from time to time.

- Owner/Partner of a Non-UAE government-owned, defense-related entity involved in manufacturing/trading of armaments/weapons or supply of parts/chemicals for defense
- Self-employed individuals whose business activity falls under any of the following high-risk categories
- General Trading (by way of “Company Name,” “Trade License type,” or “Business Activity”)
  - Diamond, jewelers, and precious stones dealers
  - Bullion/commodity traders
  - Real estate brokers
  - Used automobile and spare parts dealers

**High-risk Legal Entities Such As:**

- Free-trade zone entities, including offshore registered entities
- Trusts
- Under-formation companies
- Non-banking Financial Institutions (NBFI), including finance companies, insurance companies, and brokerages
- Investment companies
- Crowd funding/peer-to-peer lending
- Payment Service Providers (PSP)/Online payment services
- Exchange houses and money service businesses
- General trading companies (by way of “Company Name,” “Trade License type,” or “Business Activity”)
- Shipping lines
- Bullion/commodity traders
- Diamond, jewelers, and precious stones dealers
- Real estate brokers
- Used automobile and spare parts dealers
- Auction houses, art, or antique dealer
- Cash-intensive businesses (including but not limited to those availing cash pickup services
- Social and charitable organizations
• Non-UAE government entity, involved in manufacturing or trading of armaments/weapons
• Non-UAE government defense-related entities; i.e., suppliers of parts/chemicals for defense equipment
• Legal entities having one or more owner/partner/UBO national(s) of a sanctioned or increased risk jurisdiction
• Offshore legal entities by way of incorporation and/or operation

d) Politically Exposed Persons (PEPs)

Political figures, especially those from countries widely exposed to bribery, corruption, and financial irregularity, and/or that do not have acceptable anti-money laundering regulations, present a risk of being associated with corrupt practices.

The PEP definition applies to immediate family members and close associates of the persons mentioned above. This includes the following:

<table>
<thead>
<tr>
<th>Heads of State/Government:</th>
<th>Senior Politicians/Political Party Officials:</th>
</tr>
</thead>
<tbody>
<tr>
<td>o President</td>
<td>• Senior figure of a major ruling party or other major political party, i.e., depending on jurisdiction, can include members of parliament.</td>
</tr>
<tr>
<td>o Members of a ruling/royal family</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Senior Government, Judicial, Military Officials:</th>
<th>Senior Executives:</th>
</tr>
</thead>
<tbody>
<tr>
<td>o member of the board of a central bank</td>
<td>• senior executive, director, board member of a state/government-owned corporation</td>
</tr>
<tr>
<td>o member of a court</td>
<td></td>
</tr>
<tr>
<td>o an ambassador or charge d'affaires or other high-ranking officer in the diplomatic service</td>
<td></td>
</tr>
<tr>
<td>o senior military officials</td>
<td></td>
</tr>
</tbody>
</table>

Immediate family members include a person’s:

| o parents                                      | Close associate typically includes a person who is known to maintain a close relationship with the PEP and includes a person who is in a position to conduct substantial (domestic and international) financial transactions on his or her behalf. |
| o stepparents                                 |                   |
| o parents-in-law                              |                   |
| o siblings, including half-brothers or sisters |                   |
| o spouse (including common-law)                |                   |
| o children and their spouses and partners      |                   |
| o grandparents and grandchildren              |                   |
- For the purpose of risk assessment, PEPs are further classified as UAE PEP (Domestic) and Non-UAE PEP (Foreign and International Organisation)
- All Non-UAE PEPs equate to an “increased risk” for customer onboarding; hence are subject to Enhanced Due Diligence. Existing customers found to be Non-PEPs must also be subject to Enhanced Due Diligence
- Non-UAE PEP relationships will not be accepted without the prior approval of the business group head and client acceptance advisory

A legal entity will be classified as “PEP” if owned or managed by a non-UAE PEP.

International understanding is “once a PEP, always a PEP,” although in some jurisdictions, a PEP may cease to be so classified one year after resigning from office. However, as the proceeds of corruption may potentially continue to be laundered even after ceasing the office, XYZ BANK will continue to classify PEPs indefinitely. UAE PEP must be considered as a non-UAE PEP, if opening an account in a XYZ BANK branch domiciled outside of the UAE.

Staff and units involved in customer relationship management must be alerted to any indications that an existing individual account and/or legal entity structure has developed a PEP connection, especially after the business relationship has been established. If concerns arise, or where a PEP connection is identified, Enhanced Due Diligence should also be conducted, including group head approval and group compliance approval.

e) Unacceptable Risk Relationships

Prospects assessed “unacceptable” during CDD should be rejected and reported to Client Acceptance Advisory. CAA will add those persons/entities to the Internal Blacklist System.

- Hawaladars and customers dealing in Hawala Business (Hawala is an informal value transfer system based not on the movement of cash)
- Legal entities that are incorporated in and/or individuals who are residents of the following sanctioned jurisdictions:
  - Iran
  - Cuba
  - Ukraine
  - North Korea
  - Sudan
  - Syria

Or, as advised by group compliance from time to time

- Shell Banks & Shell Companies, i.e. without physical presence
- Legal entities, including parent/subsidiary, with one or more UBO/signatory/POA holder is resident(s) of a sanctioned jurisdiction or increased risk jurisdiction
- Legal entities, including parent/subsidiary or its UBO with business links with any sanctioned jurisdictions
- Legal entities with virtual offices/flexi desks with trading business
- Entities dealing in virtual currency/crypto currencies
- Legal entities with nominee shareholder(s) in the ownership structure where the actual UBOs are not identifiable
- Legal entities (including the parent companies) with bearer shares structure
- Legal entities incorporated/registered in one of the following increased risk jurisdictions:
  - Myanmar (Burma)
  - Russia
  - Somalia
  - Iraq
  - Afghanistan
  - Lebanon
  - Yemen
  - Saint Kitts and Nevis
  - Nigeria

Furthermore, XYZ BANK will not establish a relationship with any of the following customer types:
- Accounts with assumed names or numbers
- Individuals or entities designated by the Central Bank of the UAE, UN, EU, OFAC, & UKHMT (refer to “sanctions policy”)
- Individuals and entities known to have been involved in, but not limited to, corruption, fraud, terrorism, money laundering, or illegal activities
- Entities where the legal and beneficial ownership is not absolutely clear and evident
- Customers who failed the identification and verification process
- Purpose of account opening is deemed to be for tax evasion

Where a business relationship is rejected as a direct result of failing to meet the due diligence requirements, a business unit must not under any circumstance refer the case to another business unit for consideration.

Customers who have been rejected as a result of due diligence considerations relating to potential sanctions target, money laundering, or who have otherwise been considered as posing an unacceptable risk to the business operations of XYZ BANK, should be notified directly (with full details) to Customer Acceptance Advisory.
Scoring Based on RBA

The Customer Risk Matrix

Here is a visual example of what your risk matrix may look like:

“Risk should be understood as the combination of the likelihood of an adverse event (hazard, harm) occurring, and of the potential magnitude of the damage caused (itself combining the number of people affected, and severity of the damage for each).” World Bank RBA.

Perform due diligence based on the matrix above.

- **Ready Reckoner + CDD (Customer Due Diligence):** In the instance of low-risk scoring, the financial institution will adopt the regular KYC procedures.
- **Simplified Due Diligence:** Simplified due diligence will assist the financial institution to justify and satisfy the risk component by requesting further information.
- **Enhanced Due Diligence:** Enhanced Due Diligence in a high-risk instance should be conducted through a thorough search on the potential customer in various search engines and outlets of information to determine and better understand the customer’s risk. Requesting information from the customer via questionnaires designed for individuals and entities and even PEPs is an additional method of EDD.

Each of these mitigation controls should be well documented when you design your AML program.

In recommending the parameters and scoring for the RBA model, various factors have been taken into consideration: i.e., information from multiple sources, including FATF, the Egmont
Group, the Basel Institute, the Wolfsberg Group, and Transparency International, as well as insights gained from multiple financial institutions across the globe.

In addition, on the basis volumetric analysis on the prior years’ data with respect to the number of escalations of suspicious reports from various financial institutions, key trends were identified that have been critical in deriving the risk classifications of the RBA parameters.

The below table is an illustration of a distribution that can be adopted as a starting point to serve the model, and must be updated on a regular basis through the quality improvement process and the prevalent circumstances. The factors in the below table pertain to the subject(s) around which the financial institution may be trying to find the suspicion in order to determine its further discourse of escalation or no escalation.

<table>
<thead>
<tr>
<th>#</th>
<th>Parameter</th>
<th>Weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reason of suspicion</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>Subject of information requests from LEA</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>Public domain search/media reports on the subject</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Sector/industry risk where the subject is engaged</td>
<td>Low</td>
</tr>
<tr>
<td>5</td>
<td>Expected vs actual account activity of the subject</td>
<td>Medium</td>
</tr>
<tr>
<td>6</td>
<td>Transaction type/method</td>
<td>Low</td>
</tr>
<tr>
<td>7</td>
<td>Country of subject’s residence/business operation/nationality</td>
<td>Medium</td>
</tr>
<tr>
<td>8</td>
<td>Complexity of subject’s account ownership/activity/transactions</td>
<td>High</td>
</tr>
<tr>
<td>9</td>
<td>Previous alerts generated on the subject</td>
<td>Medium</td>
</tr>
</tbody>
</table>

The aforementioned can be further broken down to a more accurate picture of the inherent risk associated with the subject. As an example, the suspicion which may arise due to the amount of the transaction or account activity/turnover can vary based on the profile of the customer or the nature of the business. As such, the scoring matrix should be dynamic enough to correctly gage what is suspicious in the particular context of that very subject of suspicion. Similar breakdown can also be done in case of adverse media reports. Another example is if the subject of the adverse media report pertaining to terrorism should be graded higher risk than a person who had adverse media reports related to tax evasion, or by virtue of just being identified as a PEP. Therefore, there should be sub-categorisation of risks within each parameter, as well.
A holistic score based on the defined parameters and their respective magnitudes should result in a sum total, which should help an analyst determine whether or not the suspicion is worth escalating to the management or to the FIU. *Let us assume for an illustration that this sum total should be a value between 0 (denoting no risk) up to 10 (denoting the highest level of risk).*

**Parameters That Can be Incorporated Into the Case-scoring Model**

In determining the parameters and scoring for the RBA model, we have taken into consideration information from multiple sources, including FATF, the Egmont Group, the Basel Institute, the Wolfsberg Group, and Transparency International, as well as insights gained from open source.

The weighting used can be a starting point to serve the model, and must be updated on a regular basis.

<table>
<thead>
<tr>
<th>#</th>
<th>Parameter</th>
<th>Illustrative Weightage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Previous reports on the subject</td>
<td>4%</td>
</tr>
<tr>
<td>2</td>
<td>Previous RFI(s) from LEAs</td>
<td>4%</td>
</tr>
<tr>
<td>3</td>
<td>Subject of ECDD request from correspondent bank(s)</td>
<td>4%</td>
</tr>
<tr>
<td>4</td>
<td>Subject of previous freeze notice from regulator</td>
<td>4%</td>
</tr>
<tr>
<td>5</td>
<td>World-Check match/open source adverse info</td>
<td>4%</td>
</tr>
<tr>
<td>6</td>
<td>Sector risk (business/profession)</td>
<td>25%</td>
</tr>
<tr>
<td>7</td>
<td>Amount of transaction/A/c turnover</td>
<td>20%</td>
</tr>
<tr>
<td>8</td>
<td>Transaction type</td>
<td>15%</td>
</tr>
<tr>
<td>9</td>
<td>Country(nationality/residency/operation)</td>
<td>10%</td>
</tr>
<tr>
<td>10</td>
<td>Complexity</td>
<td>10%</td>
</tr>
</tbody>
</table>

Parameters can also have their own further breakdown. As an illustration, an adverse open source information, or World-Check hit on one of the subjects of the report/case draft can be further parameterized as follows:

**Parameter Breakdown – World-Check Match**

<table>
<thead>
<tr>
<th>#</th>
<th>Hit Type</th>
<th>Risk Classification</th>
<th>Illustrative Weightage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Priority</td>
<td>Score</td>
</tr>
<tr>
<td>---</td>
<td>----------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1</td>
<td>No Match</td>
<td>N/A</td>
<td>4%</td>
</tr>
<tr>
<td>2</td>
<td>Negligible Risk</td>
<td>N/A</td>
<td>4%</td>
</tr>
<tr>
<td>3</td>
<td>PEP</td>
<td>Medium</td>
<td>4%</td>
</tr>
<tr>
<td>4</td>
<td>FPEP</td>
<td>High</td>
<td>4%</td>
</tr>
<tr>
<td>5</td>
<td>Sanctions</td>
<td>High</td>
<td>4%</td>
</tr>
<tr>
<td>6</td>
<td>Bribery &amp; Corruption</td>
<td>High</td>
<td>4%</td>
</tr>
<tr>
<td>7</td>
<td>Terrorism</td>
<td>High</td>
<td>4%</td>
</tr>
<tr>
<td>8</td>
<td>Organized Crime</td>
<td>High</td>
<td>4%</td>
</tr>
<tr>
<td>9</td>
<td>Third Party Risk</td>
<td>High</td>
<td>4%</td>
</tr>
</tbody>
</table>

As a result of the use of such a methodology, there might be changes in the workflows of risk escalation on the basis of priority levels derived by virtue of risk scores of the suspicious reports and the subjects therein.

Wherein:

**Low Priority** requires minimum procedures, such as just archival.

**Medium Priority** requires a full suite of procedures, including review by analysts, checks across different available databases, drafting a summarized write-up for law enforcement (if the case merits), etc.

**High Priority** requires immediate action utilizing the full suite of procedures as aforementioned. Moreover, this may also require urgent escalations to law enforcements in the form of a dedicated workflow meant for critical and urgent cases and may also be backed up by dedicated correspondences and meetings with various stakeholders.

Also, after having a comprehensive view of the draft of suspicious report, there can be one of the following scenarios in terms of escalation prospects.
Items Not Requiring Case Analysis

— This would include cases where there are no further actions required to be performed by the compliance dept.

— Due to the low-risk nature of these cases, they would be closed after review by the case assessor only.

— Such cases do not require further review by a case analyst, senior case analyst, or the MRO/head of dept.

Low-risk Cases

— This classification pertains to cases that have been deemed low risk by the RBA model during the case-scoring phase.

— Due to the low-risk nature of these cases, they would be closed after analysis by the case analyst only (after the case assessor has deemed that it merits further analysis).

— Such cases do not require further review by a senior case analyst or the MLRO/head of dept.

Medium-risk Cases

— This classification pertains to cases that have been deemed medium risk by the RBA model during the case-scoring phase.

— Due to the nature of these cases, they would be closed after analysis by the case analyst and review by the senior case analyst (after the case assessor has deemed that it merits further analysis).

— These would not be reviewed by the MLRO/head of dept.

High-risk Cases

— This classification pertains to cases that have been deemed high risk by the RBA model during the case-scoring phase.

— These cases would be analyzed by the case analyst and reviewed by the senior case analyst (after the case assessor has deemed that it merits further analysis).

— Due to the nature of these cases, they would be closed only after approval by the MLRO/head of dept.
Conclusion and Recommendations

It is vital that banks establish and maintain robust AML/CFT risk management systems and controls to manage and mitigate the financial crime risks arising from trade finance and correspondent banking relationships. It is imperative that senior management set the right tone at the top and inculcate an appropriate risk and compliance culture amongst its staff, across all levels and functions, to ensure effective implementation of a strong AML/CFT framework.

Banks are expected to periodically review their policies and processes taking into account changes in the operating environments and regulatory developments. Banks should also devote attention to raising the effectiveness of their AML/CFT controls through adequate systems, processes, staff expertise, and training.

For any jurisdiction to maintain its reputation as a clean and trusted commercial, trading, and transportation hub, banks must ensure that their AML/CFT controls remain effective and are commensurate with the size, nature, and complexity of their business.

Once implemented successfully, the RBA aims to provide a structured and documented method for the financial institutions to prioritize the redressal of Money Laundering and terrorism financing risks, and to more efficiently determine the need of further escalation. Also, it should help a compliance department in better planning the workflows as well as more effective resource planning and allocation.

Use RBA as a Tool for Senior Management

Senior management more often than not faces a challenge as to how institutions seamlessly and effectively enable RBA in its business. Not only do they need to genuinely align AML/CTF with their business objectives and strategy, they need to see AML/CTF as an ongoing and continually evolving program that should go beyond mere compliance.

Senior management should demand and support the implementation of RBA. Given the emerging and dynamic ML/TF risks, senior management that doesn’t have the RBA are left to decide blindly or turn to the common practices of their peers, which may not necessarily be right for the entity’s business. This may lead to improper allocation of resources where investments are wasted on irrelevant controls, or inadequate investments are made on controls that mitigate higher risks.

An effective RBA provides senior management with the information about the risks so they can make informed decisions about where resources should be invested. It also needs support to invest in talent or experts and implement changes in the processes of an entity to regularly generate the required data. Changes in sourcing data and data management may be aligned with current initiatives of other parts of the entity, such as marketing or credit risk management. More importantly, support is needed to drive the involvement of the executives who primarily own the risks.
With the greater emphasis on combating money laundering and terrorist financing, senior management should understand that a risk-based approach to implement an effective AML/CTF program is actually a significant way to gain competitive advantage in a fluid and uncertain market.
Sources Referenced


