AML COMPLIANCE
CONFERENCE 2022

GSMB RiskRator®

BSA/AML & SANCTIONS PROGRAM RISK ASSESSMENT MANUAL

With the need to understand and apply, in a simplified fashion, an effective risk based approach to anti money laundering and counter terrorism financing (AML/CFT), CSMB and RiskRator® have created a BSA/AML & Sanctions Program Risk Assessment Manual in three chapters dedicated to the "Risk-Based Approach to AML/CFT Compliance" that can be used both as the road map to building a robust AML/CFT Program and a test to ensure that your organization has considered all the critical processes that lead to a strong and effective program.

Following the steps documented in each of the three chapters, you will:

- Understand the basis and purpose of performing a risk assessment;
- Be prepared to perform a risk assessment;
- Understand the process to allocate resources for the exercise and beyond;
- Be knowledgeable to identify, quantify, and qualify your institution's risks; and
- Have the tools to develop a system of internal controls that fits your organization and meet your regulators' and foreign correspondents' expectations.

CHAPTER 1 is dedicated to understanding the Risk Based Approach (RBA) and provides guidance to meet the expectations of the new AML Act 2020, your regulators' expectations, and for non-US entities, your organization's international correspondents' expectations.

CHAPTER 2 is dedicated to putting the RBA and the risk assessment in motion. For this process, CSMB has compiled easy to follow steps to guide you in developing and implementing a risk-based compliance program, understanding and preparing for an AML/CFT risk assessment (similar to the RiskRator® risk assessment methodology), and identifying and measuring ML/TF risks.

CHAPTER 3 of the Manual puts the risk assessment processes into context and provide guidance to develop and implement risk-mitigating controls.

1 http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr013.html#340
2 http://www.diputados.gob.mx/servicios/datorele/cmprtvs/iniciativas/Inic/241/2.htm
https://www.cnbv.gob.mx/Normatividad/Ley%20Federal%20para%20la%20Prevenci%C3%B3n%20e%20Identificaci%C3%B3n%20de%20Operaciones%20con%20Recursos%20de%20Procedencia%20Il%C3%ADcita.pdf
3 https://www.imolin.org/doc/amlid/Brazil_Law%209613%20de%201998_ML%20and%20COAF.pdf
4 http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/62977/texact.htm
https://observatoriolegislativocele.com/en/anti-terrorism-law-amending-law-26-734/
5 https://www.sepblac.es/wp-content/uploads/2018/03/royal_decree_304_2014.pdf
6 https://www.superbancos.gob.pa/superbancos/documentos/prevencion_op_il/regimen_antilavado/leyes/Ley_23_2015.pdf
7 https://www.cima.ky/upimages/lawsregulations/1580219233Anti-MoneyLaunderingRegulations2020Revision_1580219233_1599478036.pdf
https://www.cima.ky/upimages/lawsregulations/TerrorismLaw2018Revision_1524077980_1599485207.PDF
8 https://www.govinfo.gov/content/pkg/USCODE-2009-title18/html/USCODE-2009-title18.htm
https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg3207.pdf
https://www.govinfo.gov/content/pkg/BILLS-116hr6395enr/pdf/BILLS-116hr6395enr.pdf
https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter113B&edition=prelim

The Risk-Based Approach to AML/CFT Compliance

Following the issuance of the FATF-GAFI 40 Recommendations, which is the international standard to AML/CFT compliance, worldwide effort has been made to create laws and regulations to combat Money Laundering and Terrorism Financing. Countries around the globe have joined in this fight against criminal activity, enacting organic laws that, although they are diverse and vary in language, all have the same fundamental objectives. The table below describes some examples of the legal framework:

Country	AML Laws	CFT Laws
Colombia	Law 599 of 2000 of the Penal Code[1]	Article 340 of the Penal Code[1]
Mexico	• Law 115 and Bis 400 of the Penal Code[2] • Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita[2]	Article 139 and 139 Bis of the Penal Code[2]
Brazil	Law 9.613 of March 1998 [3]	Law 7170, Art. 20 of Dec 14, 983[3]
Argentina	Law 25.246 of 2000 and 26.683 of 2011 of the Penal Code[4]	Law 26.734 of 2011 of the Penal Code[4]
Spain	Law 10/2010, of April 2010, on AML/CFT [5]	Law 10/2010, of April 2010, on AML/CFT[5]
Panamá	Law 23 of 04/2015 on AML/CFT[6]	Law 23 of 04/2015 on AML/CFT[6]
Grand Cayman Islands	AML Regulations Supplement No. 3 published with Legislation Gazette No. 4 of 9th January 2020. [7]	Terrorism Law 14 of 2003 consolidated with Law 10 of 2008 (part), Law 10 of 2011, Law 19 of 2012, Law 35 of 2016 and Law 48 of 2017.[7]
USA	• Title 18 of the US Penal Code[8] • Public Law 99-570, Subtitle H – Money Laundering Control Act of 1986[8] • AML Act 2020[8]	Anti-Terrorism Act - 18 USC Ch. 113B: TERRORISM[8]

Generally, the AML/CFT laws described above were enacted by each of these countries to:

- Criminalize the act of money laundering and terrorism financing,
- Require specific action by regulated entities; and
- Issue sanctions for noncompliance

These laws all have very similar requirements:
- Customer Identification
- Record Retention and maintenance
- Reporting Requirements

The FATF-GAFI has also made recommendations concerning a "Risk-Based Approach" to combating money laundering and terrorist financing, and as such, for best practices in the process of implementation of AML/CFT laws and regulations. In fact, a guidance report issued by FATF on October 2014, clearly indicates that the "risk-based approach" (RBA) is central to the effective implementation of the revised FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which were adopted in 2012[9] and subsequently amended several times (last amendment as of the date of this manual was October 2021).

Furthermore, the U.S. enacted the Anti-Money Laundering Act of 2020, which became effective on January 1, 2021, and the central focus of this new law, which aims to modernize the existing regulatory framework of the U.S. is also the risk-based approach. In fact, one of the objectives of the Act is to strengthen and codify into law the risk-based approach to the prevention of money laundering and terrorist financing (AML/CFT). Hence, requiring regulated entities to prevent money laundering and terrorist financing through compliance programs reasonably designed under a risk-based approach.

By adopting a risk-based approach (RBA), authorities as well as regulated entities are able to ensure that "measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified" [10]

9 Guidance For Risk Based Approach – Banking Sector: http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

10 FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures, June 2007: http://www.fatf-gafi.org/media/fatf/documents/reports/high%20level%20principles%20and%20procedures.pdf

What do Regulators Expect from a "Risk-Based" Approach to AML/CFT Compliance?

Supervisors/regulators look for AML/CFT compliance programs that have been designed and implemented from a "risk-based" approach that allows for best utilization of available resources, directed toward priorities, and where grater risks receive utmost consideration and scrutiny. They will not want to see a compliance program based on a "tick box" approach that is focused on meeting regulatory obligations. Similarly, correspondents look for the same level of standards in their clients' (respondents') compliance programs. For that reason, many financial institutions expect that their clients, both regulated entities and other significantly large ones, maintain a risk-based compliance program.

There are generally three key considerations that supervisors/regulators will make to determine the adequacy of an organization's AML/CFT internal control structure. These include:

1. The organization is meeting minimum regulatory requirements;
2. The organization has identified its money laundering and terrorist financing risks and allocates adequate resources to the task; and
3. Senior management is properly accountable for AML/CFT controls

Within the context of "risk based", the Basel Committee on Banking Supervision addresses "sound ML/TF risk management"[11] , and specifically highlights the need for an organization to analyze its existing ML/TF risks for the design and effective implementation of policies and procedures that are commensurate with the identified risks. It addresses the need for proper governance as well as the need to allocate explicit responsibility to the Board of Directors to ensure that risks are managed effectively.

11 BIS Sound Management of Risks Related to ML/TF: http://www.bis.org/publ/bcbs275.pdf

All supranational bodies agree on the "three lines of defense". The Basel Committee in particular makes emphasis on this approach, noting the following:

1. **First line of defense** – these are the business units (i.e. front office, customer-facing activity); in charge of **identifying, assessing and controlling** the risks of their business.
   They should know and carry out the policies and procedures and be **allotted sufficient resources to do this effectively.**
2. **Second line of defense** - this is the **chief officer in charge of AML/CFT**, the compliance function but also human resources and **technology.**
3. **Third line of defense** – This is allocated to the internal audit function, responsible for confirming that the compliance program is adequate and/or identifying gaps requiring improvement.

To adopt a risk-based approach to money laundering and terrorist financing prevention, the Chief Risk and Compliance Officer (hereinafter "CRCO), together with senior management, must perform the following four steps:

1. **Identify** and **categorize** (i.e. low, medium, high) ML/TF risks
2. Conduct a risk assessment to **quantify** and **qualify** ML/TF risks[12]
3. Apply **sound and well-trained judgment** to determine residual risk (i.e. agree on and establish risk rating methodology to measure impact of event occurrence and effectiveness of risk mitigating factors)
4. Implement **reasonable controls** to manage and mitigate identified risks

12 In the USA, the AMLA 2020 also requires that the risk assessment processes of the covered institution should include a consideration of priorities established by the Secretary of the Treasury under section 5318.

The Benefits and Challenges of the RBA to AML/CFT Compliance

- **The Potential benefits include:**
  - Better Management of risk and cost-benefits
  - Focus on real and identified threats (including National Priorities)
  - Flexibility to adapt to risks that change over time
- **The potential challenges include:**
  - Identifying appropriate information to conduct a sound risk analysis
  - Addressing short term transitional costs
  - Data integrity and adequate segmentation for risk analysis
  - Greater need for more expert staff capable of making sound judgments
  - Regulatory response to potential diversity of practice

Money Laundering and Terrorist Financing Risks Defined

Considering that all financial activity involves an element of risk, risk is referred to in anumber of ways:

1. Risk factors - Customer characteristics (individual, corporate, foreign, domestic, Politically Exposed Person (PEP), etc.); Products and Services, including transaction types (high volume – high frequency, cash, international wire transfers, etc.); jurisdictions of concern (OFAC listed countries, UN listed countries, non-cooperative countries, etc.); channels of distribution (face-to-face, remote access, etc.)

2. High Risk – clients, products, services, channels of distribution, and geographies that are perceived to have greater exposure to being misused or have a history of wrongdoing, includin PEPs (Politically Exposed Persons); correspondent banking relationships; private banking relationships; foreign customers; international wire transfers; high volume transactions; non-cooperative jurisdictions; jurisdictions identified in OFAC; etc. In each case, enhanced due diligence (EDD) must be applied to mitigate the risk (refer to FATF Recommendation 10, 12,and 13)

3. **Low Risk** – clients, products, services, channels of distribution, and geographies such as public companies subject to regulatory disclosure requirements; government administrations or enterprises; financial institutions that are subject to AML/CFT requirements consistent with FATF Recommendations and supervised for compliance (i.e. domestic banks); low volume domestic consumer accounts; a pension or long term investment accounts; certain insurance policies (i.e. without surrender clause or not suitable as collateral); savings accounts; well-known stable customer base; jurisdictions under adequate supervision and strong compliance with international standards. In each case, limited Customer Due Diligence (CDD) measures may be applied (refer to FATF Recommendation 10 – Reduced CDD measures)

4. **Risk from Innovation** –new or developing technologies that favor anonymity, such as Internet related banking or global payment networks (refer to FATF Recommendation 15)

5. **Risk Assessment Mechanism** – the procedures adopted to determine the degree of risk (i.e. high or low), how that risk is managed, and the determinations made to rate that risk.

Understanding ML and TF "threats" is key. Threats are **unusual or suspicious transactional or customer behavior,** which are more likely to occur when there are unidentified risks and/or weak internal controls. Therefore, timely identification of risk factors and related risk events, and effective internal controls are essential to understanding and mitigating ML and TF threats.

For example, let's consider a **PEP (Politically Exposed Person)**, who is generally a person who has been entrusted with a prominent public function, or an individual who is closely related to such a person. By virtue of their position and the influence that they may hold, a PEP generally presents a higher risk for potential involvement in bribery and/or corruption. The terms PEP, Politically Exposed Person and Senior Foreign Political Figure are used interchangeably. Globally, the term PEP has been

recognized, defined, and adopted by the Wolfsberg Group, the FATF-GAFI, the USA PATRIOT Act, the United Nations Convention Against Corruption (UNCAC), and the Third EU Directive, to name a few. However, the definition varies among jurisdictions, and regardless of how the term is defined, a PEP has been globally identified as a customer risk factor or risk variable.

Per FATF-GAFI Recommendation No. 12 and due to its inherent risk factor, an organization should:

1. Perform enhanced due diligence procedures on customers identified as PEP, and
2. Have appropriate risk management systems to determine whether a customer is in fact a PEP or not.

Therefore, for timely identification of risk factors and establishing an effective internal control system, the CRCO should consider applying global standards of identification and control, and:

1. Observe the domestic or national definition of a PEP according to local regulatory requirements, which may augment or replace global standards,
2. Determine if the customer has been identified by a foreign government as a PEP,
3. Classify the customer as a PEP,
4. Apply greater scrutiny when monitoring the relationship,
5. Update and review the account relationship on a more frequent basis (i.e. annually), and
6. Establish clear policies and procedures for de-classifying the relationship when the customer's PEP status is no longer applicable

Refer to **Tables 1 and 2** for details on global standards of PEP definition as well as some jurisdictional definitions with broader scope.

What do Correspondent Banks Expect from their Respondents?

Correspondent banking services have been identified and targeted by supervisors/regulators as potentially high-risk services. As such, entities that offer correspondent banking services are required to perform enhanced due diligence (EDD) based on the risk posed by their respondents (clients). Also, correspondent banks work diligently at maintaining a set of standards to reduce regulatory criticism, prevent fines, and ultimately comply with applicable AML/CFT regulations.

So, what does a correspondent bank expect from its respondents (clients)?

Here are the top three expectations:

1. Effective **internal controls based on a risk-based approach,** specifically sound CDD and EDD procedures, which are a critical element in the effective management of ML/TF risk (i.e. providing evidence of an entity wide AML/CFT & Sanctions Programs Risk Assessment, Customer Risk Rating methodology, etc.)
2. Assurance that AML/CFT program is **Board approved** and **independently tested,** at least annually, for adequacy and effectiveness
3. Adequate Board oversight and involvement in AML/CFT Compliance matters

For a respondent organization (that is: the financial institution's "client") to meet these top three expectations, it must:

1. Have a documented **AML/CFT and Sanctions Program Risk Assessment process and methodology,** demonstrating the organization's rationale to define its risk profile and adopted policy for assessment frequency as well as validation of the effectiveness of internal controls.
2. Execute an **AML/CFT and Sanctions Program Risk Assessment,** periodically (at least annually or more frequently to capture changing circumstances), demonstrating the organization's understanding of the risks to which it is exposed and defining its **"AML/CFT & Sanctions Programs Risk Profile."**

3. Demonstrate that it's AML/CFT Compliance Program has been designed to meet the identified threats and that it is commensurate to its defined risk profile.
4. Have **KYC or CDD procedures** as a core feature of the organization's risk management and control procedures
5. Have **Board approved** documented risk management and control procedures
6. **Conduct periodic independent testing** of risk management and control procedures (at least once per year or more frequently as circumstances may require it –i.e. entering or new markets through acquisitions, exiting markets or client base, etc.)
7. Have implemented customer risk rating methodology to identify high risk clients:
    - **a.** Type of customer (Individual, corporation, NGO, PEP, foreigner, cash intensive business, correspondent bank, etc.)
    - **b.** Type of products used (demand deposit accounts, money market accounts, credit card account, savings account, time deposits, loans and letters of credit, investment account, etc.)
    - **c.** Type of services used (international wire transfers, cashier's checks, letters of credit, cash collateral loans, bulk cash deposits, RDC services, ACH transactions, correspondent banking services, international private banking services, trust and fiduciary services, etc.)
    - **d.** Volume and number of transactions expected:
        - **i.** Establish the average transaction amount per customer and per product at the organization to determine what amount will be considered a greater risk
        - **ii.** Establish the average number of transactions per customer and per product at the organization to determine what will be considered a greater risk
        - **iii.** Establish the average frequency of transactions per customer and per product at the organization to determine what will be considered a greater risk

e. Geographic exposure (i.e. country and city of residency, country of incorporation, jurisdictions from which and where to funds will come and go – "origination" and "destination")

8. Have a documented risk-based customer identification program (CIP) that includes procedures for:
   - **a.** EDD for higher risk customers. Indicate all steps for enhanced due diligence, including:
     - **i.** On site reviews of internal controls for financial institutions
     - **ii.** On site visit to place of business or residence of all high-risk customers
     - **iii.** Background investigations of key personnel or beneficial owners
     - **iv.** Type of identification required
   - **b.** CDD procedures for lower risk. Indicate identification type, information, and verification procedures required.
   - **c.** Graduated customer acceptance policy (i.e. senior management approval for high-risk customers, correspondent banking relationships, private banking relationships, or PEP accounts)
9. Maintain effective and automated on-going transaction monitoring of high-risk accounts, correspondent banking, international private banking, and PEP accounts
10. Conduct periodic reviews of high-risk accounts, correspondent banking, international private banking relationships, and PEPs (the review must include customer visit, transaction analysis, and documentation update and verification at least once per year)
11. Demonstrate that technical validations have been executed on all automated models that perform compliance related functions, to ensure that these systems are functioning per their designed objective
12. Conduct AML/CFT functional training with adequate scope, frequency, and audience, including evaluation for awareness

We trust that this introduction to the "Risk-Based Approach to AML/CFT Compliance" has spiked your interest and served as an easy-to-follow tool to validate if the path of your existing internal control system is designed to efficiently manage and control your respondents' relationships, and if it meets your regulators' and foreign correspondents' expectations.

GLOBAL DEFINITION OF POLITICALLY OR PUBLICLY EXPOSED PERSON (PEP)

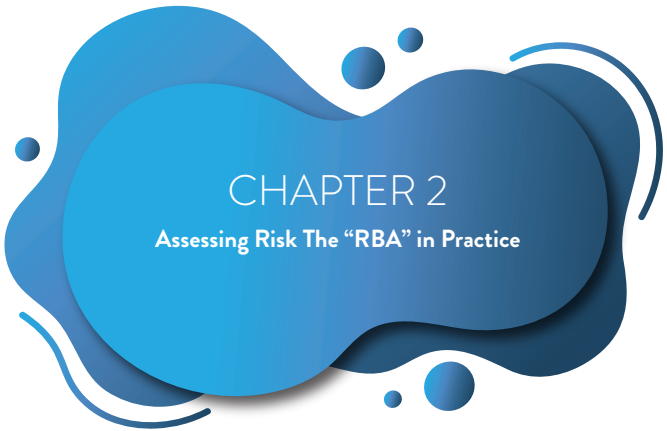
	USA Patriot Act	FATF-GAFI	Wolfsberg Group (WG)	United Nations Convention Against Corruption (UNCAC)	Third EU Directive
Basic Definition	A current or former Senior Foreign Political Figure or a legal organization formed by or for the benefit of a Senior Foreign Political Figure entrusted with a public function, who has substantial authority over policy, operations, or the use of government owned resources in a foreign country, whether or not they are or were elected officials, an immediate family member of a Senior Foreign Political Figure, or any individual publicly known (or actually known by the relevant financial institution) to be a close personal or professional associate of the Senior Foreign Political Figure	Individuals who are or have been entrusted with prominent public function in a foreign country, their family members and their close Associates	A "natural" person, foreign or domestic, that holds a public function in a senior, prominent, or important position with substantial authority over policy, operations, or the use or allocation of government-owned resources and/or the ability to direct the awards of government tenders or contracts; their close family members, or publicly close associates	Individuals who are, or have been, entrusted with prominent public functions and their family members and associates	Natural persons who are, or have been, entrusted with prominent public functions and immediate family members, or persons known to be close associates of such persons. NOTE: ***The Fifth Directive***, *which was issued in May 2018, requires Member States to publish a list indicating the specific functions which, in accordance with national laws, regulations and administrative provisions, qualify as prominent public functions.*
Natural Person or Legal Organization	Senior Foreign Political Figure or a legal organization formed by or for the benefit of a Senior Foreign Political Figure	Individuals	Natural Person	Natural Person	Natural Person
PEP may be foreign or domestic	Foreign Only	Foreign Only	Foreign and Domestic (not explicit)	Foreign and Domestic (not explicit)	PEPs residing in other countries
Specific time period to de-classify PEP	Not specified	Not specified	Not Specified	Not Specified	One year, on a risk-based approach
Politically or Publicly Exposed	Politically	Politically	Politically	Publicly	Publicly
Family Members	An immediate family member of a Senior Foreign Political Figure such as: (a) A spouse, (b) Parents, (c) Siblings, (d) Children, and (e) Spouse's parents or siblings	Not Specified	Close family member, such as a spouse, children, parents, and siblings of the PEP	Not Specified	Immediate family members shall include: (a) the spouse; (b) any partner considered by national law as equivalent to the spouse; (c) the children and their spouses or partners; (d) the parents
Close Associates	Any individual publicly known (or actually known by the relevant financial institution) to be a close personal or professional associate of the Senior Foreign Political Figure	Not Specified	A close associate, such as widely and publicly close business colleagues and/or personal advisors, in particular financial advisors or persons acting in a financial fiduciary capacity	Persons or companies clearly related to individuals entrusted with prominent public functions	Close associates shall include: (a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations with a PEP; (b) any natural person who has sole beneficial ownership of a legal organization or legal arrangement, which is known to have been set up for the benefit a PEP
Heads of State	Not Specified	Heads of State	Heads of State	Not Specified	Heads of State
Heads of Government	Not Specified	Heads of Government	Heads of Government	Not Specified	Heads of Government
Ministers and members of Parliament	Includes a Senior Official of a major foreign political party Not Specified	Includes Senior Politicians and Senior Government Officials	Heads of Government and Ministers, and Members of Parliament or National Legislatures	Not Specified	Ministers and deputy or assistant ministers; members of parliament

Political parties	Major foreign political party	Important political parties	Major political parties	Not Specified	Not Specified
Judiciary	Current or former senior official in the Judicial branches of a foreign country	Judicial Officials	Senior Judicial Officials	Not Specified	Members of supreme courts, of constitutional courts, or of other high- level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances
Military	A current or former senior official in the Military	Military Officials	Heads of other high-ranking officers holding senior positions in the armed forces	Not Specified	High-ranking officers in the armed forces
State-owned enterprises	No, but it refers to senior executives of a foreign government-owned commercial enterprise who has substantial authority over policy, operations, or the use of government-owned resources	Senior executives of state-owned corporations	No, but it refers to all holders of public functions in a senior, prominent, or important position with substantial authority over policy, operations, or the use or allocation of government-owned resources and/or the ability to direct the awards of government tenders or contracts,	Not Specified	Members of the administrative, management, or supervisory bodies of state-owned enterprises
Diplomatic representatives	Not Specified	Not Specified	Senior members of the Diplomatic Corps such as Ambassadors and Chargés d'affaires	Not Specified	Ambassadors and Chargés d'affaires
Central Bank Boards	Not Specified	Not Specified	Members of Boards of Central Banks	Not Specified	Members of courts of auditors or of the boards of central banks
Members of ruling Royal Families	Not Specified	Not Specified	Members of ruling Royal Families with government responsibilities	Not Specified	Not Specified
Heads of Supranational Bodies	Not Specified	Not Specified	Heads of Supranational Bodies such as the UN, IMF, and the World Bank	Not Specified	Directors, deputy directors and members of the board or equivalent function of an international organisation
Exclusions	No explicit exclusion, but explicitly refers to refers to senior foreign political figures, senior officers or officials and major foreign political parties	Middle ranking or more junior individuals	Middle ranking or more junior individuals	No explicit exclusion	Middle ranking or more junior individuals

PEP DEFINITION / REQUIREMENT BY JURISDICTION

(Continued)

	Argentina	Brazil	Chile	Colombia	Costa Rica	Dominican Republic	Ecuador	Mexico	Peru	Panama	United States	Spain	Other Jurisdictions in the UE
Includes Domestic / National PEP	√	√	√	√	√	√	√	√	√	√		√	√
Includes Foreign PEP	√	√	√	√	√	√	√	√	√	√	√	√	√
PEP must be a Natural Person	√	√	√	√	√	√	√	√	√	√	√	√	√
Legal Organization may be a PEP			√	√	√			√	√		√		
Specific time period to de-classify PEP	√	√	√		√		√	√	√	√		√	√
Politically Exposed	√	√	√	√	√	√	√	√	√	√	√	√	√
Publicly Exposed				√			√						
Family Members	√	√		√	√	√	√	√	√	√	√	√	√
Close Associates		√	√	√	√	√		√	√	√	√	√	√
Heads of State	√	√	√	√	√	√	√	√	√	√	√	√	√
Heads of Government	√	√	√	√	√	√	√	√	√	√	√	√	√
Ministers and members of Parliament	√	√	√	√	√	√	√	√	√	√	√	√	√
Political parties	√	√	√	√	√	√	√	√		√	√		√
Judiciary	√	√	√	√	√	√	√	√	√	√	√	√	√
Military	√	√	√	√	√	√	√	√	√	√	√	√	√
State-owned enterprises	√	√	√	√	√	√	√	√	√	√			
Diplomatic representatives	√		√		√		√	√	√	√	√	√	√
Central Bank Boards	√		√		√			√	√	√	√	√	√
Members of ruling Royal Families											√	√	√
Heads of Supranational Bodies											√	√	√
Exclusions	√	√		√						√	√	√	√



Welcome to **Chapter 2** of the RBA and AML/CFT & Sanctions Programs Risk Assessment Manual, the Risk Assessment road map of our three part "Risk-Based Approach to AML/CFT Compliance" series. Chapter 1 of the Manual provided simple and easy to follow information to understanding the risk-based approach to AML/CFT, as well as key points to meeting both your regulators' and your international correspondents' expectations.

Chapter 2 of the Manual is dedicated to putting the RBA and the risk assessment in motion. CSMB has compiled easy to follow steps to guide you in developing and implementing a risk based compliance program, understanding and preparing for an AML/CFT risk assessment, and identifying and measuring ML/TF risks.

The Backbone of an Effective AML/CFT Compliance Program

There are no universally accepted methodologies for a RBA, in fact, the specifics of an organization's risk-based process should be based on the particular operations of the organization and should be done on a group-wide basis.

To develop and achieve an effective AML/CFT "risk-based" compliance program, the CRCO, with the support from senior management, must (A) apply key processes; and (B) adopt a methodology to allocate resources, as detailed below:

A. Apply the following key processes:

1. Set the **framework** to focus on those customers and transactions (through products and services) that potentially pose the greatest risk by:
   a. Identifying the criteria to assess potential ML and TF risks (i.e. type of customers, type of product, type of service, distribution channels, and jurisdictions); and
   b. Identifying the degree of potential ML and TF risks associated with customers or categories of customers and transactions (i.e. high, medium, or low)
2. Establish reasonable **controls** to mitigate the risks (i.e. applying EDD procedures to foreign customers vs. reduced CDD measures for lower risk customers, or applying a greater degree of scrutiny to international wire transfer transactions than to checks drawn on personal or consumer accounts, etc.)
3. Allocate **adequate resources** to fund the AML/CFT Program
   a. Conduct an analytical risk assessment of historical events and possible threats using valid inputs such as:
      i. Events related to published national priorities
      ii. Investigations conducted
      iii. SARs filed
      iv. FinCEN, FATF or other public advisories
   b. Based on the assessment indicated above, identify the ML and TF threats relevant to your organization (possible unusual transactions or customer

behavior relevant to your organization)
   c. Create a budget to invest on mitigating the threats identified (need for automated technology, augment analytical staff, training, etc.)
   d. Identify and prioritize issues that require the most immediate attention:
      i. Matters identified by auditing or the regulator requiring corrective actions
      ii. Annual training and continuing education
      iii. Funding for automated models and processes
      iv. Support and staffing
4. Set **priorities** for monitoring and control:
   a. For addressing and responding to transaction alerts
   b. For addressing changes in customer profile
   c. For reviewing and analyzing high risk accounts
   d. For training and awareness
   e. For testing critical controls

B. The methodology to allocate resources must:

1. Cover the business focus, including:
   a. Automated technology to monitor high value and number of transactions, electronic banking, and other "risks from innovation" (i.e. activity to / from cryptocurrency dealers or distributors)
   b. Specialized and trained personnel to manage special class of customers, business, or activity such as high-risk accounts, PEPs, correspondent banking, investment banking, NGOs, etc.
   c. Specialized and trained personnel to monitor trade finance activity and international commerce
2. Cover the risk profile of the organization (i.e. investment on resources must be commensurate to the organization's risk appetite and risk profile)

3. Consider and measure the internal control environment to invest on or allocate resources based on:
   a. Strong internal controls with few if any deficiencies noted in audits or regulatory inspection
   b. Internal control system needs improvement
   c. Weak, needs major improvements
   d. Volatile internal controls due to mergers and acquisitions
4. Be updated on an ongoing basis

The Risk Assessment

A risk assessment of ML/TF is considered a description of fundamental background information to assist senior management and the Board to ensure that decisions about allocating responsibilities and resources in the organization are based on a practical, comprehensive and up-to-date **understanding of the risks.**

The first step in conducting an effective risk assessment is to ensure that the risks are well understood. As such, the CRCO together with senior management must perform a risk assessment to identify and measure the occurrence and impact of threats, as well as assess the quality of internal controls to mitigate said risks.

To achieve a sound level of understanding of the ML/TF risk exposure of the organization the CRCO, with support from senior management, will perform two types of risk assessments: a customer risk assessment, and an entity wide risk assessment, to identify:
1. The level of ML/TF risk of the organization's customer base; and
2. The overall ML/TF risk exposure of the organization (based on its size and the nature of its activities)

To understand the overall level of the organization's ML/TF risk exposure, the CRCO will need to identify the organization's material risks. The CRCO will measure these risks using the following set of risk categories:

1. Customer risk;
2. Product risk;
3. Service risk;
4. Channels of distribution risk; and
5. Jurisdiction or geographic risk

To establish the amount of customer risk, the CRCO will assess the risk profile of the organization's customers:

1. At **inception** of the relationship, based on a set of factors, including the anticipated or expected transactional activity of the relationship; and
2. Overtime once the customer has begun transacting through an account, through transaction monitoring and on-going reviews, based on:
   a. Alerts produced from set rules or transaction patterns
   b. Alerts from individual threshold applied to higher risk accounts
   c. Alerts produced from media sources or other intelligence sources as result of ongoing normal or enhanced due diligence measures (i.e. customer becomes a PEP or customer's jurisdiction falls under FATF watch, etc.)

Identifying, Quantifying, and Qualifying ML/TF Risks

In a risk-based approach to AML/CFT compliance, the first step is to conduct a risk assessment that will allow the organization to identify where the greatest risks are in order to direct more resources and establish proper and reasonable controls to mitigate those risks.

The risk assessment is a five-step process:

- **Step One**: Identify the risk factors,
- **Step Two:** Quantify risks identified
- **Step Three:** Qualify the risks
- **Step Four:** Rate the overall risk exposure
- **Step Five:** Document the risk assessment process, including the detailed methodology applied and the transaction flow details that support the definition of the inherent risk, as well as the mitigation controls that yield the residual risk.

Steps One and Two of the process will require the gathering of historical data, whereas Step Three will require a combination of historical facts as well as "sound" and "well-trained" judgments concerning the effectiveness of controls in place. These judgments will call for senior management's estimated perceptions or anticipation of the likely occurrence and level of impact of a particular situation. For example:

1. What will be the likelihood of adverse political situation in a country where our organization has a significant amount of operations?; or

2. How will the impact of that situation affect our compliance objectives?

The CRCO and senior management involved in the risk assessment process will answer these questions by:
1. Gathering historical data archived in the organization from similar past events;
2. Obtaining information available from credible sources[1] ; and
3. Applying the "sound" judgment of senior management.

All risk categories have an **inherent** risk level, yet the **quality** of the mitigating factors (established internal controls) as well as a combination of risk variables (political unrest vs. stable government) will mitigate or exacerbate the **residual** risk of a given category, and ultimately the risk profile of the organization.

As described earlier, there are at least five categories of ML/TF risks: (1) jurisdiction/geographic risk, (2) customer risk, (3) product risk (4) services risk; and (5) channels of distribution risk

Following the five-step process of the risk assessment, to determine the organization's overall level of ML/TF risk exposure ("risk profile"), the CRCO, together with senior management, will need to:

1. Identify all the risk events in each risk category – for example:
- 1.12 risk event of a loan or credit facility = customer directs proceeds to an unrelated third party;
- 1.13 channels risk event = accounts opened via non-face-to-face methods may pose greater difficulty in establishing the true identification of customer;
- 1.14 geographic risk event = country listed in OFAC or is a non-cooperative jurisdiction, etc.

1 "Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the Financial Action Task Force and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the IMF, the World Bank, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-governmental organizations.

2. Quantify the amount of risk within each risk category to establish the probability of occurrence – for example:
- 2.12 a large percentage of accounts opened via non face-to-face methods in the organization will result in a greater probability of the organization not being able to establish the true identification of its customers; or
- 2.13 a large percentage of trade financing products will result in a greater probability of transacting with OFAC sanctioned countries

3. Qualify the risks by measuring mitigating factors, taking into account both the probability of occurrence and impact of the risk event, to yield a residual value upon which to determine what controls must be established to manage the risk exposure.

Step Three calls for an **evaluation** of the "effectiveness" of the organization's internal controls (mitigating factors) as well as external factors (i.e. actions of third parties.)

The CRCO will use the following information and documents to qualify the risks:
1. Internal factors such as:
   a. The results of the independent testing of the organization's AML/CFT program
   b. The report of examination issued by the organization's principal supervisor/regulator
   c. SARs filed in a given year
   d. Training results and employee performance evaluations
   e. Tenure of the staff (front line, second line, and third line of defense)
2. External factors, such as information obtained from credible sources about:
   a. Particular category of customers (i.e. PEPs)
   b. The known levels of corruption in a particular jurisdiction

Step Four of the risk assessment process is to **reach a conclusion** as to the overall risk exposure to ML/TF and rate that risk, thus defining the risk profile. Typically, risks are rated as "high", "medium", or "low", but depending on the complexity of the organization, it can also be valuable to add more layers and define risk as "high", "moderate-high", "moderate", "moderate-low", and "low".

In this step, the CRCO will:

1. Calculate the inherent and residual risk value of each category of risk and each associated risk event within each sub-category (i.e. Risk Category = Products; Sub-Category = Type of product (such as Time Deposit));
2. Consolidate the risk value (inherent and residual) of each risk event within a risk category (i.e. Products) to arrive at the final residual risk score of that particular risk category
3. Consolidate the result of each of the five risk categories to arrive at the organization's risk profile.

Step Five is where the entire risk assessment gets documented in a report of assessment with corresponding risk matrixes that graphically demonstrate the risk factors analyzed, the probability of occurrence and impact values, the description of the mitigation controls, and the description of the activity that defined the organization's inherent risk (based on actual flow of funds) and the conclusions upon consideration of existing mitigation controls. To that end, the CRCO will:

1. Document the entire process upon which the organization based its risk assessment and reached its conclusions, and
2. Present said documented assessment to the Board of Directors for approval.

As mentioned above, the level of risk associated with ML/TF is affected by internal and external factors. For example, an organization's weak compliance resources,

inadequate risk controls and insufficient senior management involvement are internal factors that may increase the level of its ML/TF risks. Whereas, action of third parties (i.e. an organization's customer or vendor), or political issues (i.e. public unrest, political instability, corruption, etc.) are external risk factors that may increase the level of an organization's ML/TF risk exposure.

The CRCO will consider the following factors when conducting the risk assessment:

- Compliance culture
- Corporate governance
- Quality and effectiveness of implemented AML/CFT policies and procedures
- Quality and effectiveness of the AML/CFT Training Program
- Diversity of operations, including geographical diversity
- Customer, product, and activity profile
- Distribution channels used
- Value and size of the transactions
- Types of products and services offered
- Types of customers served

Best Practices for Risk Assessments

Here are some best practices to conduct Steps One through Three:

- **Jurisdiction/Geographic Risk**

Geographic risk is one of the categories of ML/TF risk and a key indicator of potential money laundering and terrorist financing risks.

To assess the organization's overall jurisdiction/geographic risk, the CRCO will:

1. Collect information concerning all the countries or jurisdictions where the organization operates and where it offers its services; and

2. Obtain reliable information from the organization's core database system to reach an acceptable level of understanding concerning its "geographic" risk exposure. For example, analyzing all inbound and outbound transfers to establish the value of activity to and from high-risk jurisdictions.

Once all jurisdictions have been identified, the CRCO will quantify the risk by:

1. Obtaining reliable data from the core banking system to quantify the total value of operations conducted in each jurisdiction compared to the total value of operations of the organization; and

2. Establishing the percentage of total operations in each of the particular jurisdictions where the organization operates or offers its services.

To determine the level of geographic risk, the CRCO will take into account the following risk factors:

1. Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations ("UN") or OFAC.

2. Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.

3. Countries, or geographic areas within a country identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them.

4. Countries or specific geographic areas identified by credible sources as having significant levels of corruption, or other criminal activity.

5. Internal or domestic geographic concerns (i.e. HIFCAs and/or HIDCAs)

For example, an organization that receives, moves, or operates a significant amount of transactions by providing correspondent banking services in a jurisdiction with strong laws, regulations and other AML/CFT measures may determine that its ML/FT risk exposure based on "geographic risk" for that particular jurisdiction is lower than that of its lower value transactional operations to or from a jurisdiction that has been identified by credible sources as having significant levels of corruption or criminal activity. Therefore, the risk factors together with the quantity of the identified risk are a key component in reaching a determination of the level of risk that will be assigned to a particular jurisdiction.

Additionally, internal or domestic geographic concerns should also be addressed when identifying and quantifying risk. For instance, an organization that has a high concentration of business in a costal area known domestically to have a significant amount of criminal activity may determine to classify that area as higher risk even if the country as a whole may not be considered a high-risk jurisdiction, as is the case with Peru, Chile, or Ecuador.

- **Customer Risk**

In a risk-based process, an organization must determine which customers or category of customers pose the greatest risks in order to develop reasonable controls to mitigate those risks. To reach that determination, the organization must "risk rate" its customers, individually.

Generally, customers fall into two categories "Personal" or "Business". The two customer categories will have "sub-categories" that will need to be risk rated. For example, an organization may have the following "sub-categories" of customers within the category of "Personal" accounts:

- Domestic/local individuals
- International/foreign individuals
- High risk customers
- Politically Exposed Persons (PEP)

To assess the organization's customer risk the CRCO will:

1. Identify all customer categories and sub-categories (individual, corporate, foreign, high risk, PEPs, etc.)

2. Quantify the total number of customers in each category; and

3. Quantify the value and number of transactions within each category

Additionally, the CRCO will consider other risk variables such as:

1. Channels of distribution (accounts open via the internet or other non-face to face methods vs. accounts opened at the branch, accounts opened via deposit brokers, etc.), and

2. Stability of the customer base (growing, expanding into other categories, etc.)

To assess the **individual customer risk level,** the CRCO will take into account various variables in both customer categories, and establish a risk rating methodology that includes:

1. The type of account and services that the customer uses,
2. Customer geographic location,
3. Purpose of account,
4. The duration of the relationship and frequency of customer contact, and
5. The level of assets or transaction sizes anticipated or undertaken by the customer

Based on its own risk rating criteria, the organization will determine whether a particular customer poses a higher risk. Generally, an international or foreign personal account may pose a greater risk than a personal domestic account intended to facilitate traditional or low denominated consumer transactions. However, if the percentage of operations conducted by domestic personal accounts is far greater than the percentage of operations conducted by international accounts, the overall level of ML/TF risk exposure of the organization may be deemed low.

The organization should be mindful about risk **mitigating factors** when assessing its overall ML/TF risk exposure. For example, risk mitigating factors such as "strong and effective" customer due diligence procedures may lower the residual risk of a foreign customer account, whereas inadequate staff training, very low employee tenure, or shortage of resources to perform appropriate customer due diligence or enhanced due diligence procedures may contribute to an increase in the residual risk of a domestic/local individual account.

- **Products/Services Risk**

Another key component to assessing the overall ML/TF risk of an organization is to determine potential risk exposure from its products and services offerings. When it comes to products and services, the organization should pay close attention to risks associated with new or innovative products or services offered by non-financial institutions, which make use of the organization's services to deliver their products.

A good example of these products is "stored value" cards or "digital money" distributed or offered by non-bank financial institutions ("FinTechs").

To assess the organization's overall ML/TF risk exposure, the CRCO will identify, quantify, and qualify the following risk factors:

1. Potentially high-risk services such as:
    a. International correspondent banking services involving transactions such as commercial payments for non-customers (i.e. acting as an intermediary bank), deposit compensation via currier, or trade financing services; and
    b. International private banking services

2. Products/services that inherently provide a greater degree of anonymity or can readily cross international borders, such as
    a. Online banking,
    b. Stored value cards,
    c. International wire transfers,
    d. The use of Private Investment Companies (PIC)
    e. Mobile technology devices (phones, tablets, etc.)
    f. Other merchandise or products that can be rapidly disposed of or traded
3. Services involving cryptocurrencies and precious metal trading and delivery

The CRCO will identify all the products and services to determine if any of the above listed, which have inherently high-risk characteristics, or any other that may be perceived by the organization as having an inherently high level of risk, are part of its product/service offerings.

Once all the product and service offerings have been identified, the CRCO will quantify their risk, as follows:

1. Obtaining reliable data from the organization's core data system to quantify the total number and value of transactions per each product offering; and

2. Considering variables such as customer type using the products or services and jurisdictions where the products are used or offered.

For example, **the CRCO will:**

1. Quantify the total number and value of inbound and outbound wire transfers compared to the total number of all other inbound and outbound transactions of the organization to determine what percentage of its operations involves this service (wire transfers).
2. Quantify the number and value of inbound and outbound wire transfers per each category of customer that use the service as well as per jurisdiction and compare it to the rest of the number and value of other transactions to understand the percentage that this service represents within the activity of the organization.
3. Measure the quantity of risk to determine the probability of occurrence and assign an impact value (based on "well trained" and "sound judgment" of senior management) to determine the "true" inherent risk exposure.
4. Measure the sufficiency and effectiveness of mitigating factors such as established internal controls (internal factors) or strong anti-money laundering regimes from the jurisdictions where service is offered (external factors) to define the residual risk exposure.

- **Channels of Distribution Risk**

Another key component to assessing the ML/TF risk profile of an organization is to determine potential risk exposure from the channels by which it delivers its products and services and by which customers interact with the organization. When it comes to channels, the organization should pay close attention to risks associated with new or innovative methods offered. A good example of these methods is "online banking".

Some Distribution Channels inherently present a higher risk of ML/TF risks than others. Such services may be perceived by customers to have a greater level of anonymity, and some can facilitate the handling of large values of money or expedite the international transfer of funds. For instance, transactions conducted via online services may be perceived as having greater anonymity, but the organization may limit the activity that can be transacted or the value of transactions that can be executed. Conversely, commercial offices, or branches, may be perceived by customers as more transparent, yet all products and services are accessible through that channel, generally without amount limits.

To assess the organization's overall ML/TF risk exposure, the CRCO will identify, quantify, and qualify the risk of Distribution Channels, including those that inherently provide a greater degree of anonymity or can be used to execute cross border transactions such as:

a. Online / Internet Banking
b. Mobile Apps
c. Satellite branches such as kiosks or desks at commercial sites
d. Third party agents or brokers

The CRCO will identify all the distribution channels to determine if any of the above listed, which have inherently high-risk characteristics, or any other that may be perceived by the organization as having an inherently high level of risk, are part of its service delivery methods.

Once all the distribution channels have been identified, the **CRCO** will quantify their risk, as follows:

1. Obtaining reliable data from the organization's core data system to quantify the total number and value of transactions per each distribution channel; and
2. Considering variables such as customer type using the channel, type of product and value and count of transactions processed as compared to operations conducted in a face-to-face manner (say at the branch level)

For example, **the CRCO will:**

1. Quantify the total number and value of deposits executed through Mobile App as compared to the total number of all other deposits of the organization to determine what percentage of all deposits involve this channel (Mobile App).
2. Quantify the number and value of deposits per each category of customer that use the service as well as per jurisdiction and compare it to the rest of the number and value of other transactions to understand the percentage that this channel represents within the activity of the organization.
3. Measure the quantity of risk to determine the probability of occurrence and assign an impact value (based on "well trained" and "sound judgment" of senior management) to determine the "true" inherent risk exposure.
4. Measure the sufficiency and effectiveness of mitigating factors such as established internal controls (internal factors) to define the residual risk exposure.

Measuring ML/TF Risks

To arrive at a conclusion of the overall level of ML/TF risk exposure of an organization, the CRCO, together with senior management, will need to perform a risk assessment for each of the risk categories, for example:

A. To conduct a **Customer Risk Assessment,** the CRCO will measure risk as follows:

1. Create a risk matrix that includes each of the organization's customer categories and sub-categories to arrive at the overall residual risk, taking into account and establishing the following:
   a. **Inherent risk factors:** high, medium or low as determined by pre-established standards (i.e. high risk customers = foreign customers, or cash intensive businesses, etc.)
   b. **Probability of risk occurrence:** this is measured through historical data of past events as well as the nature of the organization's business and quantity of the particular risk category. For example, if the organization offers accounts to foreign entities, consider the probability of a foreign company depositing or withdrawing cash from the account.
   c. **Impact** (if the risk event were to materialize): this is a best "estimate" based on the sound knowledge of the CRCO and senior management. The impact of occurrence is typically measured from high impact to no impact (i.e. 0= no impact and 4 = high impact), and as it pertains to ML/TF the impact considerations are related to the legal, operational, and reputational risks.
   d. **Inherent risk exposure:** this is the probability of risk divided into the estimated impact of the occurrence
   e. **Risk mitigating factors:** these are the established internal controls designed by the organization to reduce the impact of the risk (i.e. internal procedures of risk rating methodology to identify high risk customers, automated systems in place to filter the names of individuals that may appear on the OFAC list, enhanced due diligence measures applied to identified PEPs, etc.)
   f. **Residual risk:** the amount of risk that the organization is actually taking, which could be high, medium, or low depending on the adequacy and effectiveness of the risk mitigating factors

2. Calculate the total of the categories and sub-categories as a percentage of the total population of the organization's customer portfolio

3. Apply the following risk measuring formula to the risk matrix:
   Probability of risk factors X Impact of the occurrence = Inherent risk exposure
   Inherent risk exposure ÷ Risk Mitigating Factors = **Residual Risk**
   Add all Residual Risk results and divide into total number of risk factors to yield the Residual Risk Factor of Customers

B. To conduct a **Products and Services Risk Assessment**, the CRCO will measure risk as follows:

1. Create a risk matrix that includes each of the product and service offerings of the organization to arrive at the overall residual risk, taking into account and establishing the following:
   a. **Inherent risk factors:** high, medium or low as determined by pre-established standards (i.e. international funds transfers = large value transactions that can rapidly cross borders to offshore financial centers, high transit or drug trafficking countries, or countries identified by FATF, etc.)

b. **Probability of risk occurrence:** this is measured through historical data of past events as well as the nature of the organization's business and quantity of the particular risk category. For example, if the organization offers letters of credit, the probability of a customer directing payment to an unrelated third party, based on the organization's existing data, will be commensurate to the percentage of the business)
c. **Impact** (if the risk event were to materialize): this is a best "estimate" based on the sound knowledge of the CRCO and senior management. The impact of occurrence is typically measured from high impact to no impact (i.e. 0= no impact and 4 = high impact), and as it pertains to ML/TF the impact considerations are related to the legal, operational, and reputational risks.
d. **Inherent risk exposure:** this is the probability of risk divided into the estimated impact of the occurrence
e. **Risk mitigating factors:** these are the established internal controls designed by the organization to reduce the impact of the risk (i.e. internal procedure to monitor funds transfers to and from high risk jurisdictions or that are large in value and / or deviate from the expected activity of a customer)
f. **Residual risk:** the amount of risk that the organization is actually taking, which could be high, medium, or low depending on the adequacy and effectiveness of the risk mitigating factors

2. Calculate the total number and value of funds transfers as a percentage of total debits and credits of the organization

3. Apply the following **risk measuring formula** to the risk matrix:
Probability of risk factors X Impact of the occurrence = Inherent risk exposure

Inherent risk exposure ÷ Risk Mitigating Factors = **Residual Risk**
Add all Residual Risk results and divide into total number of risk factors to yield the Residual Risk Factor of the Product or Service

C. To conduct a Channels of Distribution Risk Assessment, the CRCO will measure risk as follows:

1. Create a risk matrix that includes the percentage of business conducted by the organization through each of the channels by which it distributes its products and services and by which customers access their funds to arrive at the overall residual risk, taking into account and establishing the following:
a. **Inherent risk factors:** high, medium or low as determined by pre-established standards (i.e. high risk channels = Internet Banking)
b. **Probability of risk occurrence:** this is measured through historical data of past events as well as the nature of the organization's business and quantity of the particular risk category. For example, calculate the probability that the organization will process a significant number and value of transactions through this channel.
c. **Impact** (if the risk event were to materialize): this is a best "estimate" based on the sound knowledge of the CRCO and senior management. The impact of occurrence is typically measured from high impact to no impact (i.e. 0= no impact and 4 = high impact), and as it pertains to ML/TF the impact considerations are related to the legal, operational, and reputational risks.
d. **Inherent risk exposure:** this is the probability of risk divided into the estimated impact of the occurrence
e. **Risk mitigating factors:** these are the established internal controls designed by the organization to reduce the impact of the risk (i.e. the organization has implemented internal control procedures to identify high

value transactions and structured transactions, or there are robust customer due diligence and customer identification controls in place, etc.)

f. **Residual risk:** the amount of risk that the organization is actually taking, which could be high, medium, or low depending on the adequacy and effectiveness of the risk mitigating factors

2. Calculate the business conducted through each distribution channel as a percentage of total debits and credits of the organization

3. Apply the following risk measuring formula to the risk matrix:
Probability of risk factors X Impact of the occurrence = Inherent risk exposure
Inherent risk exposure ÷ Risk Mitigating Factors = **Residual Risk**
Add all Residual Risk results and divide into total number of risk factors to yield the Residual Risk Factor of the Channels of Distribution

D. To conduct a **Geographic Risk Assessment**, the CRCO will measure risk as follows:

1. Create a risk matrix that includes the percentage of business conducted by the organization in each of jurisdictions (by region: local and international) to arrive at the overall residual risk, taking into account and establishing the following:
   a. **Inherent risk factors:** high, medium or low as determined by pre-established standards (i.e. high risk jurisdictions = FATF non-cooperative countries or OFAC listed countries, etc.)
   b. **Probability of risk occurrence:** this is measured through historical data of past events as well as the nature of the organization's business and quantity of the particular risk category. For example, calculate the probability that the organization will process a significant number and value of transactions to and from high risk jurisdictions (domestic and international).

c. **Impact** (if the risk event were to materialize): this is a best "estimate" based on the sound knowledge of the CRCO and senior management. The impact of occurrence is typically measured from high impact to no impact (i.e. 0= no impact and 4 = high impact), and as it pertains to ML/TF the impact considerations are related to the legal, operational, and reputational risks.
d. Inherent risk exposure: this is the probability of risk divided into the estimated impact of the occurrence
e. **Risk mitigating factors:** these are the established internal controls designed by the organization to reduce the impact of the risk (i.e. internal procedures to identify high risk countries such as automated systems in place to filter the names that may appear on the OFAC list, process of enhanced due diligence measures applied, etc.)
f. **Residual risk:** the amount of risk that the organization is actually taking, which could be high, medium, or low depending on the adequacy and effectiveness of the risk mitigating factors

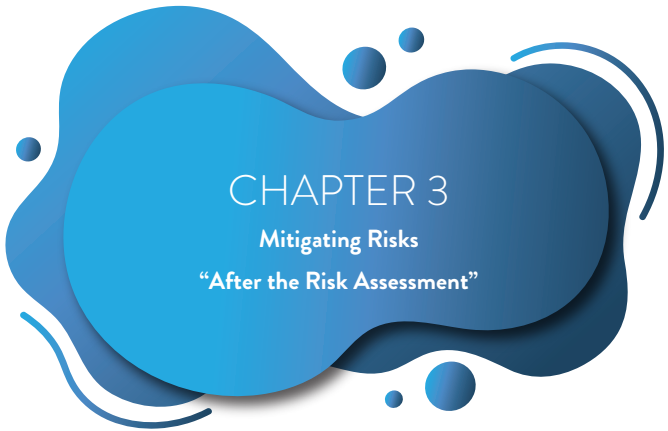
2. Calculate the business conducted in each jurisdiction as a percentage of total debits and credits of the organization

3. Apply the following risk measuring formula to the risk matrix:

Probability of risk factors X Impact of the occurrence = Inherent risk exposure
Inherent risk exposure ÷ Risk Mitigating Factors = **Residual Risk**
Add all Residual Risk results and divide into total number of risk factors to yield the Residual Risk Factor of Geographic Risk.

With Chapter 2 of the "AML/CFT & Sanctions Programs Risk Assessment Manual" we are confident that we have delivered easy to follow, practical tools for you to begin your risk assessment and set your RBA to AML/CFT Compliance in motion, giving you the necessary background knowledge to understanding the basis for a risk assessment, the methodology to create your own risk matrix, and simple formulas to calculate and measure your organization's ML/TF risks.

NOTES



In Chapters 1 and 2 of the "Risk Based Approach to AML/CFT Compliance" and AML/CFT & Sanctions Program Risk Assessment Manual, we provided guidance and practical information concerning laws and regulations, ML/TF risks, the requirements to conduct a risk assessment, and step-by-step procedures to perform a risk assessment to arrive at the overall risk exposure or "risk profile" of an organization.

In Chapter 3 of this Manual, we put those processes into context and provide guidance to develop and implement risk-mitigating controls.

Risk Mitigating Controls

Internal controls to mitigate risks are developed, updated, eliminated, or strengthened after the risk assessment has been completed and a final overall risk exposure (your organization's risk profile) has been established. The results of the risk assessment will reflect the risk appetite of the organization and will allow the members of the Board make sound judgments on their risk-taking strategies, as well as understand the resources necessary to meet their risk appetite.

Considering that laws and regulations, as well as international standards, have established the need for regulated entities to implement appropriate policies, procedures, and controls to mitigate potential ML/TF risks, the RBA focuses on the application of these policies, procedures, and controls on a graduated or escalated process.

Based on the aforementioned, to mitigate risk exposure from each of the risk categories that, based on the risk assessment have been determined to be higher risk, the CRCO will establish the following measures and controls:

1. Increased level of **training and awareness** concerning higher risk customer and transactions throughout the business lines (i.e. functional training providing: case studies highlighting ML/TF typologies, suspicious activity detection techniques, investigation techniques, etc.)
2. Increased levels of customer due diligence **(CDD)**, know your customer **(KYC)**, or enhanced due diligence **(EDD)** within business lines across the organization (i.e. escalated process at account inception and throughout the life of the account.)

3. Escalation for account opening approval, specifically for PEPs, correspondent banking and high-risk accounts.
4. Increased level of monitoring and scrutiny of higher risk transactions (i.e. rule driven alerts, methods of artificial intelligence to develop suspicious transaction patterns, lower transactional thresholds, structured transactions, complex transactions, etc.)
5. Increased levels of ongoing controls and frequency of reviews of relationships (i.e. more frequently for high risk accounts, PEP accounts, new accounts, etc.)

Training and Awareness

An organization's commitment to a sound and efficient AML/CFT control system relies on a robust "training and awareness" program. Recommendation 18 of the FATF-GAFI requires that entities provide their staff with appropriate and proportional training in AML/CFT subject matter. A risk-based approach provides flexibility regarding the frequency, delivery methods, and focus of the training.

Also, following the guidance provided by the Basel Committee, training and awareness is a key component of the "first line of defense". To that end, the Basel Committee recommends organizations to maintain:

- Adequate policies and processes for screening prospective and existing staff to ensure high ethical and professional standards.
- Implement ongoing employee training programs so that staff are adequately trained to implement AML/CFT policies and procedures.
- The timing and content of training for various sectors of staff will need to be adapted according to the organization's risk profile.

- Training needs will vary depending on staff functions and job responsibilities and length of service with the organization.
- Training curriculum and materials should be tailored to an employee's specific responsibility or function to ensure that the employee has sufficient knowledge and information to effectively implement internal AML/CFT policies and procedures.
- Specific training policies and procedures to ensure that all new employees are required to attend training as soon as possible after being hired, and refresher training should be provided to ensure that staff is reminded of their obligations and their knowledge and expertise are kept up to date.
- An adequate scope and frequency of training that is tailored to the risk factors to which employees are exposed due to their responsibilities and the level and nature of risk present in the organization.

Based on the above, and as detailed in Chapter 2, the **CRCO** will budget for and allocate adequate resources to implement the organization's compliance program. Training is a core feature of the AML/CFT compliance program and must be designed to the **staff's specific responsibilities**, particularly to all personnel whose duties require knowledge of AML/CFT matters.

To develop and implement an adequate **Risk-Based Training Program**, the CRCO will:

1. Tailor the training material to the appropriate staff responsibility (i.e. customer contact, operations, trading desk)
2. Tailor the method of presentation (i.e. in person, online, workshop, etc.) according to:
    a. Audience (i.e. general staff, middle management, senior management, members of the Board of Directors, and trading desk personnel, etc.)
    b. Content material (i.e. general concepts and induction material, function specific, etc.)

3. Create or deliver content material at the appropriate level of detail and encompass all business lines (i.e. front-line personnel, trust services, international banking, etc.)
4. Maintain a frequency of training that is directly related to the risk level of the business line involved (i.e. more frequent for staff who have customer contact than for back office personnel who do not.)
5. Test for knowledge commensurate with the detail of training (i.e. 10 – 15 question self-assessment quiz at end of online or in person training, pose case to solve based on real examples at the organization, etc.)

Customer Due Diligence & Enhanced Due Diligence

The cornerstone and core feature of a sound AML/CFT program is a strong Customer Due Diligence/Know Your Customer program. For an organization to be in a strong position to detect and deter money laundering or terrorist financing activity, it must be confident that it reasonably knows the true identity of each of its customers, as well as understand the transactions that its customers are likely to conduct.

To implement a sound and effective Risk Based CDD/EDD Program, the CRCO will develop and implement internal control procedures that allow for:

1. A standard level of due diligence, to be applied to all customers (i.e. request copy of government issued identification and register personal identifiers, including occupation and/or economic activity)
2. Timely and accurate identification of customers, including risk-based measures to identify the identity of beneficial owners:
    a. At account inception and no later than a pre-determined number of business days after account opening (i.e. account may not be operational until evidence of identity has been established)
    b. At notification of changes in the beneficial ownership of an account (i.e. new shareholders, new signatories, etc.)

    c. At time of account information update and/or renewal and no later than a pre-determined number of business days as result of periodic account review.
3. Timely and accurate verification methods of customer identification, including risk-based measures to verify the identity of beneficial owners, based on the method of account opening:
    a. **In person:** request copy of identification and other identification documents
    b. **Online and other non-face to face methods:** customer must submit copy of identification by presenting original document in person at organization or customer will use digital method used by the organization that can guarantee the authentication process (i.e. two-step factor or similar) or remit authenticated copies validated by competent authority such as consulate, embassy, or verifiable notary public
    c. **Brokered accounts:** organization must have third service provider contract with detailed customer identification procedures and perform enhanced due diligence on broker prior to accepting customers from broker
4. Perform background checks for higher risk customers to establish the true identity of the client and identify any familial ties to PEPs or other high-risk concerns
5. Performing additional due diligence procedures (enhanced due diligence), where necessary, to understand the nature of the customers' business:
    a. Develop a sound knowledge of your client's business activities,
    b. Understand who their clients are and, where possible, their reputation
    c. Verify if the jurisdictions and markets fit the business and the nature of the business transactions

6. Obtaining additional information to understand the expected nature and level of transactions:
    a. Verify the name of your client through media searches and other intelligence applications to establish connections with other similar businesses
    b. Understand your client's market to justify their level of transactions
    c. Perform peer group analysis to establish expected level of activity

7. Enhanced due diligence of identified high risk customers, correspondent banking relationships, and PEPs:
    a. Conduct background checks on high-net-worth individuals and corporations
    b. Verify the names of your clients' and beneficial owners against search engines, databases, and intelligence applications
    c. Conduct onsite visits and verify compliance with regulatory requirements
    d. Ensure that their systems of internal control are adequate and effective

Internal Control Framework

The CRCO will develop and implement an internal control framework to ensure that the highest risks receive the appropriate level of attention, including procedures for:
1. Independent testing and validation of implemented controls, at least once annually or more frequently if necessary (i.e. testing the risk assessment process, customer risk rating methodology, customer risk profiles, etc.)
2. Ensuring that adequate controls are in place before new products and services are offered:

    a. CRCO must be made aware of all strategic plans of the organization, including entering new markets, new products and services, exiting lines of business, etc.
    b. CRCO will assess the AML/TF risk of the new product or servicer prior to launching and distribution
    c. Document new controls, if any, and update AML/CFT manual accordingly
    d. Train all relevant personnel on the risks associated to new product or service as well as new internal controls
3. Maintaining the Board and senior management informed of compliance initiatives, identified compliance deficiencies and corrective actions taken.
4. Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.

The internal control framework designed and implemented by the CRCO and senior management, must allow for independently validating and testing the efficiency and sufficiency of the organization's AML/CFT Compliance Program.

It will be the responsibility of the CRCO to ensure that:
1. The parties responsible for validating the system of control are not involved in the implementation or operation of the AML/CFT Compliance Program; and
2. The independent testing is tasked to:
    a. The organization's internal audit team,
    b. Specialist consultants, or
    c. Other qualified professionals who must be well trained and certified in AML/CFT subject matter
3. The independent testing includes:
    a. Adequate and sufficient scope and methodology;
    b. Adequate and sufficient testing procedures commensurate to the organization's size and complexity of operations;

c. Risk-based testing and evaluation procedures (targeting higher-risk customers, products and services);
d. Transaction stress testing, covering all business lines and activities;
e. An evaluation of the quality of risk management for the organization's operations, departments and subsidiaries; and
f. An evaluation and opinion concerning the adequacy and sufficiency of the organization's overall AML/CFT compliance program

This concludes our three-chapter AML/CFT & Sanctions Programs Risk Assessment Manual on the "Risk Based Approach to AML/CFT Compliance". In this last Chapter of the Manual, we closed the "RBA" cycle by providing you with practical guidance to developing a sound internal control framework around the particular and unique risks of your organization.

We are confident that all three chapters of this Manual will have a permanent home in your compliance library and that you will keep them at hand for ease of reference, as well as a training tool for your staff, senior management, and members of the Board. Our goal has been to deliver practical guidance on which to set you on your way to achieving your compliance objectives from a risk-based approach. Look for us to continue supporting your organization, as partners, in the fight against money laundering and terrorism financing. Please contact us if you need additional support in setting a Risk Based Approach to AML/CFT compliance in motion, or to automate your AML/CFT & Sanctions Program Risk Assessment.

About CSMB

CSMB is a risk management and banking consultancy focused in regulatory compliance, international banking, forensic investigations stemming from allegations of fraud or money laundering, and training and development. The leaders of organizations reach out to CSMB to support their compliance objectives, as they are keenly aware that to operate under a strong culture of compliance, a competent independent source is a strong ally, they are also aware that to prevent money laundering and terrorism financing, their organizations are required to maintain adequate human and technological resources that allow them to meet their compliance obligations and the and the expectations from their regulators, their clients,, and their servicer providers. Allow us to guide you through your risk management process; contact CSMB to learn about our services and our automate risk assessment tool, RiskRator®. Follow us on LinkedIn.

About RiskRator®

The RiskRator® Risk Assessment Platform is a breakthrough automated system that follows FFIEC examination guidance as well as Basel and FATF-GAFI international standards, and ISO and COSO standardization guidelines to dynamically assess and calculate the BSA/AML/OFAC or AML/CFT risk profile at the Enterprise and individual Bank level. Built on the entire base of an institution's transaction flows, this bottom-up approach is the most comprehensive and rigorous in the industry. The RiskRator® automated process reduces time & cost to complete your institution's Risk Assessment; utilizes the entire base of transactions in-flows & out-flows as the basis for analysis; it's real-time, so it supports "as needed" updates to reflect business changes; it produces robust quantitative & qualitative analysis; and reduces errors and operational risk. RiskRator® performs over 57 million calculations per 1 million transactions, it produces a formal and uniform methodology for strong risk oversight by management, supervisory authorities, and correspondents. RiskRator® contains a powerful analytics & reporting system. Follow us on LinkedIn.

About the Author

Ana Maria H. de Alba is the Founder and CEO of CSMB International, Inc., a risk management consulting firm based in Miami since 1997. Ana Maria has 30 years of professional experience in both the financial services and consulting industries, specializing in areas such as due diligence in support of mergers and acquisitions, in risk and risk mitigation related matters, financial fraud investigations, forensic investigations of other financial crimes, independent evaluations of internal controls, and in professional and continuing education training. As a former senior banking officer, Ms. de Alba held senior management positions in both domestic and international banking entities; as a consultant she has led and participated in multiple engagements, providing her services to a wide range of business sectors that include the financial services industry in the private sector as well as government entities throughout the USA, Latin America, and the Caribbean. Additionally, Ms. de Alba is a lead instructor for FIBA, and a recognized and frequent speaker at numerous international conferences, where she has exposed on issues related to risk mitigation and internal controls. Ana Maria has a Bachelor's Degree in Business Administration with a Major in Finance from the University of Miami, a Master's Degree specialized in Banking from Nova Southeastern University, she is certified by the FATF-GAFI as an expert Country Evaluator, and holds both the AMLCA and CPAML professional certifications in anti-money laundering offered by FIBA and Florida International University (FIU). Follow Ana Maria on LinkedIn.

NOTES

AML COMPLIANCE CONFERENCE 2022

CSMB RiskRator®

www.cs-mb.com