RBA Compliance

Pocket Handbook

CSMB | A Risk Management & Banking Consultancy

RBA Compliance Pocket Handbook

Ana Maria de Alba, AMLCA and CPAML, has created the RBA Compliance Pocket Handbook to serve as a reference guide for risk and compliance officers. The objective of this guide is to highlight the key aspects related to the AML/CFT risk assessment process and a myriad of due diligence processes observed under regulatory requirements, from Customer Due Diligence (KYC) to the USA Bank Secrecy Act, and the international standard for the prevention of money laundering and terrorism financing. For that purpose, we have divided the handbook in three sections as follows:

Chapter 1
The Risk-Based Approach (RBA) to AML/CFT Compliance

Chapter 2
Assessing Risk – The RBA in Practice

Chapter 3
Mitigating Risks – After the Risk Assessment

We will assist you in designing solutions to ensure that your organization is up to date with everything concerning the implementation of a risk based compliance program, including high levels of due diligence, and most importantly, to protect your organization's reputation.

Chapter 1

The Risk-Based Approach (RBA) to AML/CFT Compliance

CSMB | A Risk Management & Banking Consultancy

Table of Contents

The Risk-Based Approach (RBA) to AML/CFT Compliance

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 has created a three part Compliance Handbook 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.

Compliance Handbook 1 is dedicated to understanding the Risk Based Approach (RBA) and provides guidance to meet your regulators' expectations as well as your institution's international correspondents' expectations.

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:

Country	AML Laws[1]	CFT Laws[2]
Colombia	Law 599 of 2000 of the Penal Code	Article 340 of the Penal Code
Mexico	Law 115 and Bis 400 of the Penal Code	Article 139 and 139 Bis of the Penal Code
Brazil	Law 9.613 of March 1998	Law 7170, Art. 20 of Dec 14, 983
Argentina	Law 25.245 of 2000 and 26.683 of 2011 of the Penal Code	Law 26.734 of 2011 of the Penal Code
Spain	Law 10/2010, of April 2010, on AML/CFT[3]	Law 10/2010, of April 2010, on AML/CFT

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

1. http://gafilat.org.iplan-unix-03.toservers.com/content/biblioteca/
2. http://gafilat.org.iplan-unix-03.toservers.com/content/biblioteca/
3. http://www.sepblac.es/espanol/legislacion/prevbcap/pdf/ley10_2010.pdf

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 recent 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.[4]

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

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."[5]

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' 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"[6], 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.

5. 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

6. 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 (e.g. 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 or 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 Compliance Officer, 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
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

The Benefits and Challenges of the RBA to AML/CFT Compliance[7]

The Potential benefits include:

- Better Management of risk and cost-benefits
- Focus on real and identified threats
- 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
- Greater need for more expert staff capable of making sound judgments
- Regulatory response to potential diversity of practice

7. 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

Money Laundering and Terrorist Financing Risks Defined

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

1. Risk factors

Customer characteristics (individual, corporate, foreign, domestic, Politically Exposed Person (PEP), etc.); transaction types (high volume – high frequency, cash, international wire transfers, etc.); jurisdictions of concern (OFAC listed countries, UN listed countries, non-cooperative countries, etc.)

2. High risk

Clients, products & services, and geographies that include 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, 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 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.

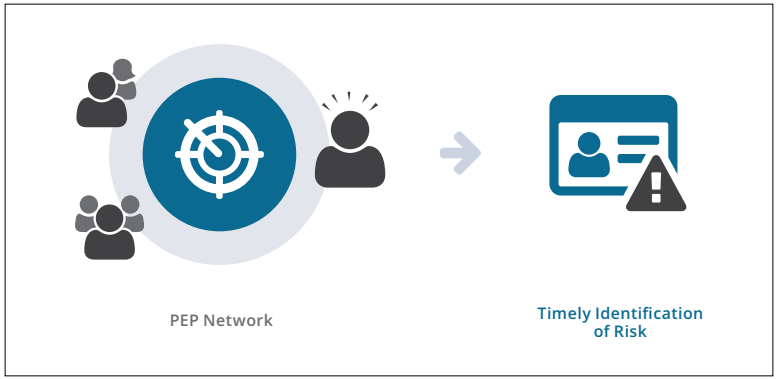
However, the definition varies among jurisdictions, and regardless of how the term is defined, a PEP has been globally identified as a customer risk factor or risk variable.

Per FATF-GAFI Recommendation N°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 Compliance Officer 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, and
5. 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)?

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
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 KYC or CDD procedures** as a core feature of the organization's risk management and control procedures
2. **Have Board approved documented risk management and control procedures**
3. **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.)

4. **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, trust account, cash management account, investment account, etc.)
    c. Type of services used (international wire transfers, cashier's checks, letters of credit, cash collateral loans, bulk cash deposits, ACH transactions, correspondent banking services, international private banking 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 generate or be remitted)
5. **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)

6. **Maintain effective and automated on-going transaction monitoring** of high risk accounts, correspondent banking, international private banking, and PEP accounts
7. **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)
8. **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 regulator's and foreign correspondents' expectations.

TABLE 1
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
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

	USA Patriot Act	FATF–GAFI	Wolfsberg Group (WG)	United Nations Convention Against Corruption (UNCAC)	Third EU Directive
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

	USA Patriot Act	FATF–GAFI
Heads of State	Not specified	Heads of State
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
Political Parties	Major foreign political party	Important political parties
Judiciary	Current or former Senior Official in the Judicial branches of a foreign country	Judicial Officials
Military	A current or former Senior Official in the Military	Military Officials
Diplomatic Representatives	Not specified	Not specified
Central Bank Boards	Not specified	Not specified

Wolfsberg Group (WG)	United Nations Convention Against Corruption (UNCAC)	Third EU Directive
Heads of State	Not specified	Heads of State
Heads of Government	Not specified	Heads of Government
Heads of Government and Ministers, and Members of Parliament or National Legislatures	Not specified	Ministers and Deputy or Assistant Ministers; Members of Parliament
Major political parties	Not specified	Not specified
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
Heads of other high-ranking officers holding senior positions in the Armed Forces	Not specified	High-ranking officers in the Armed Forces
Senior members of the Diplomatic Corps such as Ambassadors and Chargés d'affaires	Not specified	Ambassadors and Chargés d'affaires
Members of Boards of Central Banks	Not specified	Members of Courts of Auditors or of the boards of Central Banks

	USA Patriot Act	FATF–GAFI	Wolfsberg Group (WG)	United Nations Convention Against Corruption (UNCAC)	Third EU Directive
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
Members of Ruling Royal Families	Not specified	Not specified	Members of Ruling Royal Families with government responsibilities	Not specified	
Heads of Supranational Bodies	Not specified	Not specified	Heads of Supranational Bodies such as the UN, IMF, and the World Bank		
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

TABLE 2
PEP Definition / Requirement by Jurisdiction (continued)

	Argentina	Brazil	Chile	Colombia	Costa Rica	Ecuador	Dominican Republic	Mexico	Peru	Panama	Venezuela	Spain	Other EU Jurisdictions
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 a PEP	✔	✔	✔		✔	✔		✔	✔			✔	✔
Politically Exposed	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		
Publicly Exposed				✔		✔				✔		✔	✔
Family Members	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Close Associates		✔	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔
Heads of State	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔

	Argentina	Brazil	Chile	Colombia	Costa Rica	Ecuador
Heads of Government	✓	✓	✓	✓	✓	✓
Ministers and Members of Parliament	✓	✓	✓	✓	✓	✓
Political Parties	✓	✓	✓	✓	✓	✓
Judiciary	✓	✓	✓	✓	✓	✓
Military	✓	✓	✓	✓	✓	✓
Diplomatic Representatives	✓		✓		✓	✓
Central Bank Boards	✓		✓		✓	
State-owned Enterprises	✓	✓	✓	✓	✓	✓
Members of Ruling Royal Families						
Heads of Supranational Bodies						
Exclusions	✓	✓		✓		

Dominican Republic	Mexico	Peru	Panama	Venezuela	Spain	Other EU Jurisdictions
✓	✓	✓	✓		✓	✓
✓	✓	✓			✓	✓
✓	✓		✓	✓		✓
✓	✓	✓	✓	✓	✓	✓
✓	✓	✓	✓	✓	✓	✓
	✓	✓		✓	✓	✓
	✓	✓			✓	✓
✓	✓	✓	✓		✓	✓
					✓	✓
			✓			

Chapter 2

Assessing Risk – The RBA in Practice

CSMB | A Risk Management & Banking Consultancy

Table of Contents

Assessing Risk – The RBA in Practice

Welcome to Chapter 2 of the RBA Compliance Handbook, the Risk Assessment road map of our three part "Risk-Based Approach to AML/CFT Compliance" series. Chapter 1 of the Handbook 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 Handbook is dedicated to putting the RBA 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 Compliance Officer, 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 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 transactions, distribution channels, jurisdictions, etc.); 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. Investigations conducted
        ii. SARs filed
        iii. 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, analytical staff, 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 for Organization's personnel, management, and directors
        iii. Funding for automated 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 volume and number of transactions, electronic banking, and other "risks from innovation"
    b. Specialized and trained personnel to manage high risk accounts, PEPs, correspondent banking, investment banking, NGOs
    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 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 Compliance Officer together with senior management must perform a risk assessment to identify and measure the occurrence and impact of threats.

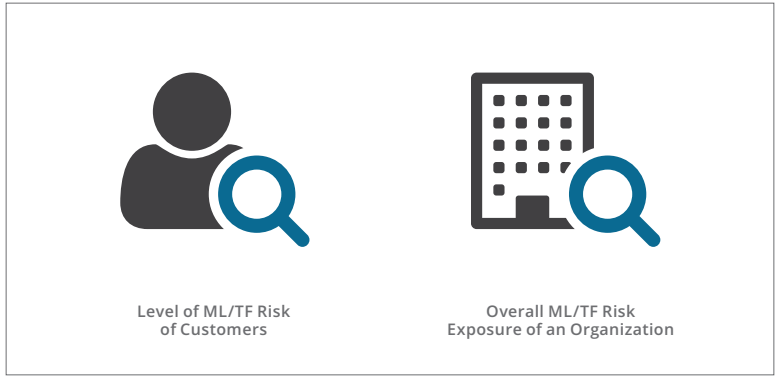
To achieve a sound level of understanding of the ML/TF risk exposure of the organization the Compliance Officer, with support from senior management, will perform a risk assessment to identify:

- **The level of ML/TF risk of a particular customer** or category of customers; and
- **The overall ML/TF risk exposure of an 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 Compliance Officer will need to identify the organization's material risks.

The Compliance Officer will measure these risks using the following set of risk categories:

1. Jurisdiction or geographic risk
2. Customer risk
3. Product/services risk



To establish the amount of customer risk, the Compliance Officer 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 four-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 and document the process

Steps One and Two of the process will require the gathering of historical data, whereas the third step will require a combination of historical facts as well as "sound" and "well-trained" judgments.

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:

- What will be the likelihood of adverse political situation in a country where our organization has a significant amount of operations?; or
- How will the impact of that situation affect our compliance objectives?

The Compliance Officer 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
1. Applying the "sound" judgment of senior management.

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.

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.

As described earlier, there are at least three categories of ML/TF risks: (1) jurisdiction/geographic risk, (2) customer risk, and (3) product/services risk.

Following the four-step process of the risk assessment, to determine the organization's overall level of ML/TF risk exposure, the Compliance Officer, together with senior management, will need to:

1. **Identify** all the risk factors in each risk category (i.e. risk factor of a loan or credit facility = customer directs proceeds to an unrelated third party; customer risk factor = accounts opened via non-face-to-face methods have greater difficulty in establish true identification of customer; geographic risk factor = country listed in OFAC or is a non-cooperative jurisdiction, etc.)
2. **Quantify** the amount of risk within each risk category to establish the probability of occurrence (i.e. 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 a large percentage of trade financing products will result in a greater probability of transacting with OFAC sanctioned countries, etc.); and

3. **Qualify** the risks by measuring mitigating factors, taking into account both the probability of occurrence and impact of 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 Compliance Officer 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
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. Typically, risks are rated as "high", "medium", or "low".

In this last step, the Compliance Officer 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 Compliance Officer 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
- Volume and size of the transactions
- Types of products and services offered
- Types of customers serviced

Best practices for risk assessments

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

Jurisdiction/geographic risk

Geographic risk is one of three 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 Compliance Officer 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.

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

1. Obtaining reliable data from the core banking system to quantify the total volume of operations conducted in each jurisdiction compared to the total volume 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 Compliance Officer 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 volume 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 Compliance Officer will:

1. Identify all customer categories and sub-categories (individual, corporate, foreign, high risk, PEPs, etc.)
2. Quantify the total number of accounts in each category; and
3. Quantify the volume and number of transactions within each category

Additionally, the Compliance Officer 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 Compliance Officer will take into account various variables in both customer categories, and establish a risk rating methodology that includes:

1. The type of account or 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 will be 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 or shortage of resources to perform appropriate customer due diligence or enhanced due diligence procedures may increase 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.

To assess the organization's overall ML/TF risk exposure, the Compliance Officer 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. Private Investment Companies (PIC)
   e. Trusts
   f. Mobile technology devices (phones, tablets, etc.)
   g. Other merchandise or products that can be rapidly disposed of or traded
3. Services involving precious metal trading and delivery

The Compliance Officer 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 Compliance Officer will quantify their risk, as follows:

1. Obtaining reliable data from the organization's core data system to quantify the total number and volume 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 Compliance officer will:

1. Quantify the total number and volume 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 is dedicated to wire transfers

2. Quantify the number and volume of inbound and outbound wire transfers per each category of customer that use the service as well as per jurisdiction
3. 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)
4. Measure the quantity of risk to determine the probability of occurrence, and the impact (based on "well trained" and "sound judgment" of senior management) to determine 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 Compliance Officer, together with senior management, will need to perform a risk assessment for each of the risk categories, as detailed below:

A. To conduct a Geographic Risk Assessment the Compliance Officer 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. **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.)

   c. **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:

   Inherent risk
   (–) Risk mitigating factors
   (=) Residual risk

B. To conduct a Customer Risk Assessment, the Compliance Officer 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. **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.)

c. **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 each 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:

Inherent risk
(–) Risk mitigating factors
(=) Residual risk

C. To conduct a Products and Services Risk Assessment, the Compliance Officer 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. high risk jurisdictions = 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 (i.e. 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 of occurrence:** this is a best "estimate" based on the sound knowledge of the Compliance Officer 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)

   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 filter the names of countries 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. Apply the following risk measuring formula to the risk matrix:

A. Probability of risk factors
(x) Impact of the occurrence
(=) Inherent risk exposure

B. Inherent risk exposure
(+) Risk mitigating factors
(=) Residual risk

C. Add all residual risk results and divide into total number of risk factors to yield the Residual Risk Factor of the Product

FORMULA A

FORMULA B

With Chapter 2 of the "Risk-Based Approach to AML/CFT Compliance" Handbook we are confident that we have delivered easy to follow, practical tools for you to 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.

We are committed to closing the cycle with Chapter 3, where we will deliver sample risk matrixes for each of the risk categories as well as for the consolidated risk assessment, and practical guidance to creating an adequate internal control framework to fit your organization's risk exposure.

Chapter 3

Mitigating Risks – After the Risk Assessment

CSMB | A Risk Management & Banking Consultancy

Table of Contents

Mitigating Risks – After the Risk Assessment

In Chapters 1 and 2 of the Risk Based Approach to AML/CFT Compliance Handbook, 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 of an organization.

In Chapter 3 of the Handbook, we put those processes into context and illustrate a simple risk assessment matrix for each of the risk categories, as well as provide guidance to develop and implement risk-mitigating controls.

The AML/CFT risk matrix

Included in this handbook are risk matrixes for each of the three categories of risk (geographic, customer, products/services), inclusive of a consolidated risk matrix with the overall risk assessment of a hypothetical organization.

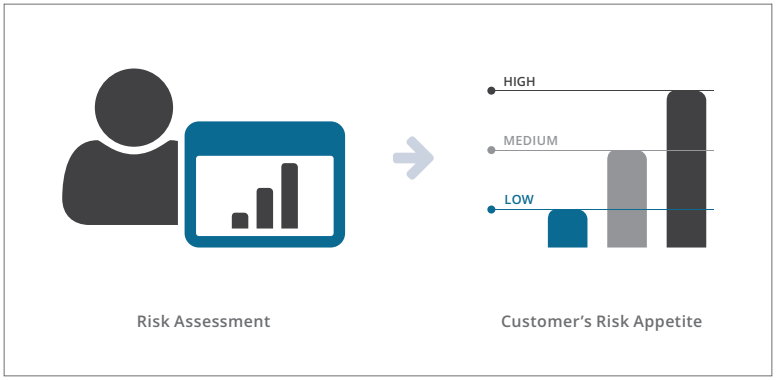
These matrixes have been designed to illustrate a practical method to understanding the risk rating methodology. You should consult with Chapter 2 of this Handbook when reviewing each risk matrix.

Risk mitigating controls

Internal controls to mitigate risks are developed 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.

Considering that the laws and regulations, as well as international standards have established the need for 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 escalation 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 Compliance Officer 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, 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

AML/CFT Training

1. **Tailor the Training Material**
2. **Tailor the Method of Presentation**
3. **Create or Deliver Content Material**
4. **Maintain a Frequency of Training**
   Related to the Risk Level
5. **Test for Knowledge**
   Commensurate with the Detail of Training

- 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
- 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 Compliance Officer 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 Compliance Officer will:

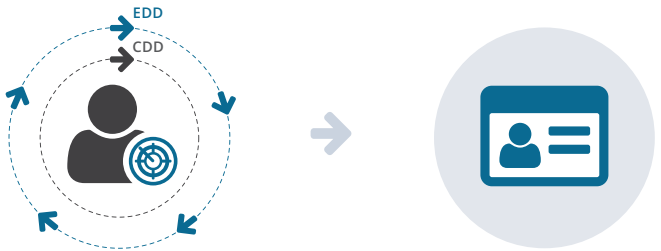
1. Tailor the training material to the appropriate staff responsibility (i.e. customer contact, operations, trading desk)
2. Tailor the method of presentation (i.e. in person, online, workshop, etc.) according to:
   a. Audience (i.e. general staff, middle management, senior management, members of the Board of Directors, and trading desk personnel, etc.)
   b. Content material / Curriculum (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 tellers 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 Compliance Officer will develop and implement internal control procedures that allow for:



Customer Due Diligence » Know Your Customer

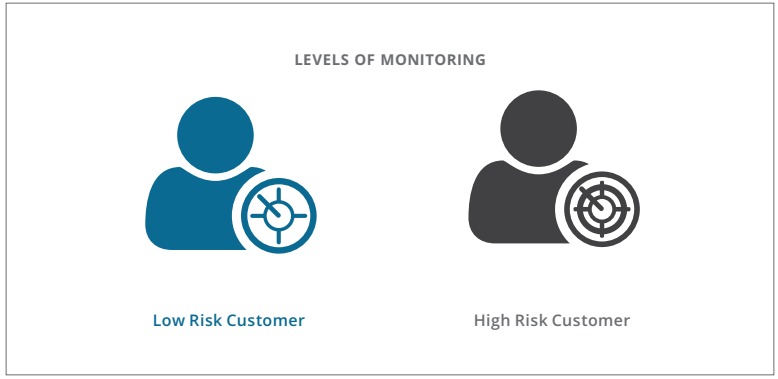
1. A standard level of due diligence, to be applied to all customers (i.e. request copy of government issued identification and register personal identifiers, including occupation and/or economic activity)
2. Timely and accurate identification of customers, including risk based measures to identify the identity of beneficial owners:
   a. At account inception and no later than 10 business days after account opening (i.e. account may not be operational until evidence of identityhas 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 15 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 remit authenticated copy 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' 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 Compliance Officer 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. Compliance Officer 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. Compliance Officer 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 action taken
4. Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel

The internal control framework designed and implemented by the Compliance Officer 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 Compliance Officer 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-part "Risk Based Approach to AML/CFT Compliance" Handbook. In this last Chapter of the Handbook, we closed the cycle by providing you with practical guidance to developing a sound internal control framework around the particular and unique risks of your organization; and we shared risk matrix models that unlock the answers to a sound risk management process.

Following the steps documented in each of the Handbooks, 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 regulator's and foreign correspondent's expectations.

We are confident that all three chapters of this Handbook 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 Risk Based Approach to AML/CFT compliance in motion.

About the author

Ana Maria de Alba

AMLCA, CPAML,
Founder, President and CEO

Ana Maria de Alba is a risk management and banking consultant with over 25 years combined experience and training in the banking and consulting services industries, providing forensic investigations, litigation support, and risk management consulting services to the domestic and international financial services community. Ms. de Alba founded CSMB in 1997 and since then she has conducted and participated in numerous consulting assignments throughout the United States, Latin America, and the Caribbean. She leads all of CSMB's business practices.

As a former senior banking officer in both domestic and foreign banks including SunTrust, Banco Atlántico, International Finance Bank, and BICSA, Ms. de Alba was engaged in private banking administration and organization, analysis and control of asset/liability mixes, analysis and management of foreign exchange, organizational definition, and strategic planning. Additionally, from 1997 through 2002 Ms. de Alba served as adjunct professor for senior level courses taught at the Management and International Business Department of Florida International University (FIU) in Miami, Florida, and is currently the lead academic advisor and instructor at Florida International Bankers Association (FIBA), teaching the AMLCA and CPAML certification course in partnership with FIU.

Ms. de Alba has utilized her banking and financial expertise to assist clients in conducting risk assessments, maintaining business integrity, uncovering breaches, and developing solutions to deter further criminal activity. She has supported a significant number of banks in evaluating internal controls through the process of risks assessments, as well as in developing and documenting standard operating policies and procedures, and providing advice and consultation to clients regarding the prevention, detection, and deterrence of money laundering and terrorist financing.

As a financial investigator, her experience has been instrumental in uncovering violations to further resolution and prosecution. She has been engaged by numerous financial institutions to perform mandatory and/or targeted training and development on AML/CFT subject matter, anti-money laundering and other consumer regulatory compliance evaluations, risk assessments to comply with provisions of various regulatory mandates, forensic or "look-back" reviews of high risk account activity, forensic fraud investigations, and investigations on government corruption. Ms. de Alba is also a frequent speaker at trade conferences in the United States, Latin America, and Europe.

By 1991 Ms. de Alba's educational background included a Master's Degree (MBA) in Banking and Finance from Nova Southeastern University and a Bachelors' Degree in Business Administration with a Major in Finance from the University of Miami. She is FIBA certified in both AMLCA and CPAML, and is certified by the CFATF (an FSRB for the FATF-GAFI) as an expert in Mutual Evaluations Methodology. Ms. de Alba is fully bilingual in English and Spanish.

To contact Ana María de Alba:
201 S Biscayne Blvd., 28th Floor
1. 305. 865. 5664
amdealba@cs-mb.com
www.cs-mb.com

Risk matrix models

These risk matrix models should be reviewed in conjunction with Handbook 2

Welcome to the Risk Matrix Models Appendix to Handbook 3. The risk matrix models in this supplemental brochure have been created to provide the user with working samples to apply steps three and four of the risk assessment process discussed in Handbook 2, and supplement or close the cycle discussed in Handbook 3. The AML/CFT risk assessment is an internal control processes that is designed to 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.

Each of the following risk assessment models form part to the documented process necessary to evidence the steps taken to measure risk and rate an organization's overall ML/TF risk exposure.

OFAC risk assessment

For entities that are subject to OFAC regulations, the following table is an example of the consolidated risk assessment, with key risk factor considerations that are specific to OFAC verifications. The consolidated level of OFAC risk will be equal to the average of all the risk factors considered. Refer to table below:

OFAC Risk Assessment		
The factors below identify the overall potential OFAC risk to the Organization.		
Risk Factor	**Level of OFAC Risk**	**Description of Risk Level at the Organization**
Stability of customer base	Low	Stable, well-known customer base, in a localized environment
Number of high risk customers	Medium	A moderate number of high-risk customers as determined by the Organization's customer risk assessment
Number of overseas branches and affiliates and correspondent accounts with foreign banks	Medium	The Organization maintains three affiliates and two representative offices throughout Latin America
E-Banking services	Medium	The Organization offers a limited amount of e-banking services, which are generally for information, but include account transfers capabilities
Amount of funds transfers	Medium	The Organization conducts a moderate number of funds transfers for customers and a high number of international funds transfers, only for customers. The number of international transfers are greater than 2,000 per week
Amount of other types of international transactions (e.g. trade finance, cross border ACH, and FX)	Medium	The Organization is primarily a commercial bank offering corporate banking services and trade finance, but its customer base consists primarily of well-known large or publicly traded corporations, many of which are state-owned
History of OFAC violations	Low	No history of OFAC violations. No evidence of apparent violation or circumstances that might lead to a violation
Consolidated OFAC Risk	Medium	The Organization's OFAC risk profile is MEDIUM, as its stable customer base, limited scope of operations, and lack of historical OFAC violations relatively mitigate the inherent risk in its corporate banking services and international trade finance activities

Consolidated risk assessment

The Consolidated AML/CFT Risk Assessment matrix is a graphic representation of the summary of each category of risk, which is intended to provide a "consolidated" risk level of the overall organization's ML/FT risks. See table below:

Consolidated AML/CFT Risk Assessment		
The Organization's Consolidated Risk Assessment reviews the products & services, customer, and geographic risk assessments, reviews the critical business factors underlying each analysis and reaches a conclusion to the overall potential money laundering risk to the Organization.		
Risk Area	**Risk Rating**	**Reasoning for Risk Rating**
Overall jurisdiction/ geographic risk	Medium	Most of the operations of the Organization are concentrated in Brazil, Argentina, Mexico and Colombia, and Panama, which combined account for 54.5% of all transactions. These countries are generally rated medium and low risk. There are a few countries rated high, but they represent a lower concentration of our operations and the Organization has strong internal controls to mitigate risks associated with doing business in those jurisdictions
Overall customer risk	Low-Medium	The Organization conducts a significant portion of its business private corporations, a few state-owned corporations and a small amount of personal accounts, mostly as a service to its corporate clients. The Corporations include Industrial, Agricultural, and Manufacturing companies, with a nominal amount of PICs and non-bank financial institutions
Cont.		The Organization also maintains a nominal amount of PEP accounts and High Risk accounts. According to the FFIEC Manual as well as the FATF-GAFI Guidance reports on RBA, from our mix of customers, the only companies that are considered high risk are the PIC which may have bearer shares and/or be incorporated in high risk jurisdictions and the non-bank financial institutions. Currently, only 4% of our customer base is within these two customer categories. The other categories pose a lower risk to the Organization
Overall product & service risk	Low-Medium	Generally, specific money laundering risk factors within Organization's products and services, represent a low to medium exposure to money laundering. This is due to strong mitigating factors, including extensive due diligence on each customer and full periodic review of all high risk services as well as strong manual and automated transaction monitoring of all transactions passing through the Organization. As such, the overall residual money laundering risk of each product is low to medium. Therefore, the overall products and services risk rating is deemed to be Low-Medium
Overall potentail money laundering risk to the organization	Low-Medium	The average of the areas of risk (products and services, customers and geographies) is Low-Medium

Geographic risk assessment

To conduct a Geographic Risk Assessment, the Compliance Officer will measure risk as follows:

1. Establish the risk level by country or geographic area considering:
   a. Each geographic area (country or local zone)
   b. Comments concerning noted deficiencies or special sanctions programs (i.e. corruption events, drug source or transit country, terrorism situation
   c. A summary of the most recent FATF-GAFI Mutual Evaluation or if there has been no report issued, any information known information about the geographic area concerning ML/TF (i.e. INCSR Report, UN sanctions, etc.)
   d. A value (i.e. 1-3) to determine the jurisdictions Risk Rating of High, Medium, or Low
2. 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. **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.)
   c. **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
3. Calculate the business conducted in each jurisdiction as a percentage of total debits and credits of the organization
4. Apply the following risk measuring formula to the risk matrix:

   Inherent risk
   (–) Risk mitigating factors
   (=) Residual risk

See the following table:

Geographic Risk Assessment

Country	AML Risk Rating*	Percentage of business conducted in Country (as of July 31, 2015)
Argentina	Insert risk rate from Sovereign Rating table (low, medium, or high)	15.50%
Brazil	Insert risk rate from Sovereign Rating table (low, medium, or high)	12.00%
Bolivia	Insert risk rate from Sovereign Rating table (low, medium, or high)	1.50%
Chile	Insert risk rate from Sovereign Rating table (low, medium, or high)	5.60%
Colombia	Insert risk rate from Sovereign Rating table (low, medium, or high)	8.50%
Costa Rica	Insert risk rate from Sovereign Rating table (low, medium, or high)	5.40%
Ecuador	Insert risk rate from Sovereign Rating table (low, medium, or high)	4.30%
El Salvador	Insert risk rate from Sovereign Rating table (low, medium, or high)	4.30%
Grand Cayman	Insert risk rate from Sovereign Rating table (low, medium, or high)	4.30%
Honduras	Insert risk rate from Sovereign Rating table (low, medium, or high)	3.20%
Ecuador	Insert risk rate from Sovereign Rating table (low, medium, or high)	3.20%

Geographic Risk Assessment		
Country	AML Risk Rating*	Percentage of business conducted in Country (as of July 31, 2015)
El Salvador	Insert risk rate from Sovereign Rating table (low, medium, or high)	2.20%
Honduras	Insert risk rate from Sovereign Rating table (low, medium, or high)	3.30%
Mexico	Insert risk rate from Sovereign Rating table (low, medium, or high)	10.20%
Panama	Insert risk rate from Sovereign Rating table (low, medium, or high)	8.30%
Peru	Insert risk rate from Sovereign Rating table (low, medium, or high)	2.20%
Paraguay	Insert risk rate from Sovereign Rating table (low, medium, or high)	2.20%
Dominican Republic	Insert risk rate from Sovereign Rating table (low, medium, or high)	1.50%
Venezuela	Insert risk rate from Sovereign Rating table (low, medium, or high)	1.30%
Uruguay	Insert risk rate from Sovereign Rating table (low, medium, or high)	1.00%

*Include a "Sovereign Rating" Table with decisions for assigning a risk value. Generally, use scale of 1 = low, 2 = medium, and 3 = high

Sovereign Rating			
Countries	Comments	FATF-GAFI Information	Risk
A. Enter country name	B. Insert comments concerning noted deficiencies or special sanctions programs (i.e. corruption events, drug source or transit country, terrorism situation)	C. Insert summary of last FATF-GAFI Mutual Evaluation or if there has been no report issued	D. Assign a value (1-3) to determine Risk Rating of High, Medium, or Low

Customer risk assessment

To conduct a Customer Risk Assessment, the Compliance Officer 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. **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.)
   c. **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 each 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:

   Inherent risk
   (–) Risk mitigating factors
   (=) Residual risk

See the following table:

Customer Risk Assessment

The table below illustrates the Organization's customer categories as of July 31, 2015. Also, a brief description of each customer category, including the Organization's risk assessment, are detailed in the table below.

Customer Category	Description and AML Rating Reasoning	Rating	Percent of Total Customer Base as of July 31, 2015
Corporations: Industrial	Publicly traded, privately owned, and state-owned. Most Mexican oil companies as well as other Brazilian commodity related companies (metal ore, cement, and oil)	Low	25%
Corporations: Agricultural	Agricultural and food products. All Brazilian and Colombia agricultural companies	Low	12%
Corporations: Personal investment companies	Companies that have bearer shares and are incorporated in foreign jurisdictions	High	3%
Corporations: Manufacturing & processing machinery	Mostly privately owned corporations	Low	43%

Customer Risk Assessment			
Customer Category	Description and AML Rating Reasoning	Rating	Percent of Total Customer Base as of July 31, 2015
Non-bank financial institutions: currency exchange houses, money transfer agents and broker dealers	Mostly privately owned corporations of well know beneficial owners, some publicly traded and two money transfer agents of a state-owned bank in Brazil	High	2%
Personal: Consumer	Mostly domestic customer base utilizing bank services for traditional low denominated consumer transactions	Low	13%
High Risk Customers and Politically Exposed Persons	Identified a moderate amount of high risk customers and corporations as well as a few PEPs, but from a stable and well known customer base and Organization has adequate EDD procedures that are periodically tested for effectiveness	Medium	2%
Consolidated Customer Risk Assessment		Low-Medium	100%

Consolidated product and services risk assessment

A Consolidated Products & Services risk assessment matrix is a graphic representation of the summary of an organization's Products & Services risk assessment. An assessment of the ML/TF risk per individual product or service must be conducted prior to arriving at the "consolidated" risk level. The consolidated products and services risk assessment table will feed from the risk assessment matrix of each individual product or service. See table below:

Consolidated Products & Services Risk Assessment		
This table consolidates the risk assessments of the Organization's Products/Services risks assessments found in ensuing tables. Refer to ensuing tables for further detail on rating of each product.		
Product	Product Overall Risk Rating	Reasoning for Risk Rating
Lending activity – Working capital	Low	See Table 1
Lending activity – Trade finance	Low	See Table (you will have created a table for another product and made reference to that table here)
Letters of credit	Low	See Table (you will have created a table for another product and made reference to that table here)
Checking/Current accounts	Low	See Table (you will have created a table for another product and made reference to that table here)

Consolidated Products & Services Risk Assessment		
Services	Services Overall Risk Rating	Reasoning for Risk Rating
Private banking services	Medium	See Table (you will have created a table for another product and made reference to that table here)
International wire transfer services	Medium	See Table (you will have created a table for another product and made reference to that table here)
E-Banking services	High	See Table (you will have created a table for another product and made reference to that table here)
Consolidated Products and Services Risk	Low-Medium	Generally, specific money laundering risk factors within Organization's products and services represent a low to medium exposure to money laundering. This is due to strong mitigating factors, including extensive due diligence on each customer and full periodic review of all high risk services as well as strong manual and automated transaction monitoring of all transactions passing through the Organization. As such, the overall residual money laundering risk of each product is low to medium. Therefore, the overall products and services risk rating is deemed to be Low-Medium

To conduct a Products and Services Risk Assessment, the Compliance Officer 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. high risk jurisdictions = 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 (i.e. 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 of occurrence:** this is a best "estimate" based on the sound knowledge of the Compliance Officer 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)
   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 filter the names of countries 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. Apply the following risk measuring formula to the risk matrix:

A. Probability of risk factors
(x) Impact of the occurrence
(=) Inherent risk exposure

B. Inherent risk exposure
(÷) Effectiveness of the risk mitigating factors
(=) Residual risk

C. Add all residual risk results and divide into total number of risk factors to yield Final Residual Risk Factor for the Product

See the following table:

Product & Service Risk Assessment (working capital)									
Product or Service	Product or Service Definition	Risk Factors	Probability	Impact	Exposure		Mitigating Factors	Effective-ness Risk	Residual Risk
Lending activities–Working capital	Loan disbursements related to working capital activities Working capital loans are a short-term loans to finance day-to-day operations of a business. It is normally a loan for a comparably small amount, and is not used for long-term investment purposes. Rather, it funds immediate needs, such as advancing trade	Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction	2	3	6	Medium	AML Scrutiny—including CIP, KYC, CDD and EDD—all transactions are examined with special attention, without regard to the amount involved	2	3
		Customer directs payment of proceeds to an unrelated third party	2	3	6	Medium		2	3
		Transactions directed to geographic regions that are unregulated or do not comply with the regulations for the prevention of money laundering or terrorism financing	2	4	8	Medium		2	4
		Underlying clients or countries listed on the OFAC and other lists	2	4	8	Medium	OFAC Verifications – Organization uses LexisNexis tool to ensure that underlying clients or countries are not involved in criminal activity or appear in SDN lists or other similar lists	2	4
									4
									LOW

Probability		Impact		Effectiveness of Controls		Overall Exposure & Risidual Risk	
1	Low	0	No impact	1	Bad	0 – 4	**Low**
2	Medium	1	Low	2	Average	5 – 8	**Medium**
3	High	2	Medium	3	Good	9 – 12	**High**
		3	High				

Glossary of terms and acronyms

ALD/CFT
Anti Money Laundering/
Counter Financing of Terrorism

ML/TF
Money Laundering/Terrorism Financing

FATF-GAFI
English and French acronym for "Financial Action Task Force – Le Groupe d'Action Financiére", which is the supranational intergovernmental body headquartered in Paris, France for the development and promotion of national and International policies on anti Money laundering and counter Financing of terrorism.

SAR
Suspicious Activity Report

NGO
Non-Government Organizations

HIFCA
High Intensity Financial Crime Area

HIDTA
High Intensity Drug Trafficking Area

PIC
Private Investment Company; generally paper companies with bearer shares

KYC
Know Your Customer

FinCEN
The Financial Crimes Enforcement Network (FinCEN) is the U.S. Financial Intelligence Unit, a Bureau of the U.S. Department of the Treasury. FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities. FinCEN carries out its mission by receiving and maintaining financial transactions data; analyzing and disseminating that data for law enforcement purposes; and building global cooperation with counterpart organizations in other countries and with international bodies.

OFAC
The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

Wolfsberg Group
Group of 11 international private Banks, created in the year 2000 in the city of Wolfsberg, Switzerland.Its main objective is to develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies. The Wolfsberg Anti-Money Laundering Principles for Private Banking were subsequently published in October 2000, revised in May 2002 and again most recently in June 2012. The Group published a Statement on the Financing of Terrorism in January 2002, and also released the Wolfsberg Anti-Money Laundering Principles for Correspondent Banking in November 2002 and the Wolfsberg Statement on Monitoring Screening and

Searching in September 2003. In 2004, the Wolfsberg Group focused on the development of a due diligence model for financial institutions, in cooperation with Banker's Almanac, thereby fulfilling one of the recommendations made in the Correspondent Banking Principles.

USA PATRIOT Act

The official title of the USA PATRIOT Act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001." The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and other purposes, some of which include to strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism; to subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse; to require all appropriate elements of the financial services industry to report potential money laundering; and to strengthen measures to prevent use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong.

UNCAC

The United Nations Convention against Corruption (UNCAC) is a multilateral convention negotiated by members of the United Nations. It is the first global legally binding international anti-corruption instrument.

European Union Third AML Directive

The current EU legislation, the so-called Third Anti-Money Laundering Directive (hereinafter, the 3rd AMLD), has been in force since 2005. It provides a European framework built around the international Financial Action Task Force (FATF) standards. The Directive applies to banks and the whole of the financial sector as well as to lawyers, notaries, accountants, real estate agents, casinos and company service providers. Its scope also encompasses all dealers in goods (such as dealers in precious metals and stones). Those subject to the Directive must comply with customer identification procedures, customer due diligence, reporting requirements, and training of personnel. The Directive introduces additional requirements and safeguards (such as the requirement to conduct enhanced customer due diligence) for situations of higher risk (e.g. trading with correspondent banks situated outside the EU).

CDD

Customer Due Diligence

EDD

Enhanced Due Diligence

Correspondent Bank

A financial institution that offers a current or other liability account, and related services, to another financial institution, including affiliates, used for the execution of third party payments and trade finance, as well as its own cash clearing, liquidity management and short-term borrowing or investment needs in a particular currency. A Correspondent Bank is effectively acting as its Correspondent's agent or conduit, executing and/or processing payments or other transactions for the Correspondent's customers.

Respondent

A financial institution that maintains a correspondent banking relationship with a correspondent bank to receive services such as funds transfers, International trade services, and clearing services, among others.

CIP

Customer Identification Program

About CSMB

CSMB is a risk management and banking consultancy focused in regulatory compliance, international banking, forensic financial investigations stemming from allegations of fraud or money laundering, and training and development. The leaders of organizations that operate under a strong culture of compliance are 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 objectives and with the expectations of their regulators, their clients, and their service providers.

Allow us to guide you through your risk management process; contact CSMB from anywhere in the world:

Miami	amdealba@cs-mb.com csmith@cs-mb.com
Panama & Caracas	jcaguirre@cs-mb.com rs@cs-mb.com
Mexico	telizondo@cs-mb.com

Or visit our web page for additional details:
www.cs-mb.com

NOTES

www.cs-mb.com