Best Financial Regulatory and Supervisory Practices on AML / CFT 2014

ASBA
ASSOCIATION OF SUPERVISORS OF BANKS OF THE AMERICAS

FOMIN
Multilateral Investment Fund
Member of the IDB Group

Best Financial Regulatory and Supervisory Practices on AML / CFT 2014

ASSOCIATION OF SUPERVISORS
OF BANKS OF THE AMERICAS

Best Financial Regulatory and Supervisory Practices on AML / CFT

This research report was funded by the MIF of the IDB Group and edited by ASBA in 2014.

Executing entity:
Association of Supervisors of Banks of the Americas (ASBA)

Financed by:
Multilateral Investment Fund (MIF)

Project
Strengthening Banking Supervision for Improved Access to Financial Services in the Americas

Technical Cooperation:
ATN/ME-11612-RG

To request a printed copy, contact:
asba@asbasupervision.org

C. Picacho Ajusco # 238, Oficina 601
Col. Jardines en la Montaña, C.P. 14210, México, D.F.
Tel. (52-55) 5662-0085, Fax (52-55) 2615-5603

Contents

I. INTRODUCTION

The purpose of this paper is to provide a practical guide for banking supervisors in the Americas, which can be applied in the supervisory process of *financial institutions*[*1] when assessing Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regimes.

As it is well known, financial institutions are in highly exposed to being used as instruments to commit crimes of Money Laundering (ML) and Terrorism Financing (TF).

The range of services offered by financial institutions, their use of new technologies and the dynamic nature of the financial sector are factors that make them attractive for money laundering. In addition, the methods used for money laundering are increasingly complex and difficult to detect.

As a result, financial institutions are exposed to an elevated risk of being used to commit these crimes, which in many cases materialize.

In order to prevent these crimes, several rules and international standards have been established and most countries have replicated these in their domestic regulation. However, there is still a lot of ground to cover, and the effective implementation of the standards represents the greatest challenge currently faced by supervised entities, and financial institutions in particular.

In this regard, supervisors must play a key role, directing their efforts to support financial institutions in achieving the highest possible level of compliance with international standards, the adoption of best practices, and the continuous improvement of domestic regulation.

1 The expressions and/or words in italics followed by an "*" are defined in the Glossary at the end of the document.

For the supervisor to fulfill this role, external preconditions must be present in the jurisdiction, without which supervisors would not be able to adequately perform their monitoring and oversight responsibilities. The preconditions include an appropriate legal framework, high-level political commitment, and risk-based AML/CFT policies. Given these preconditions, the supervisor must be provided with a legal structure in accordance to his role. Supervisors must be provided with the necessary powers and resources (human and physical) to perform their role efficiently.

This document will review the aforementioned topics. The paper will describe the minimum preconditions that each jurisdiction must have in place and the basic regulatory framework for an AML/CFT supervisor, as well as detail a risk-based supervisory process, describing the stages and the activities that must be performed in each stage.

I.1 ASSESSMENT

When designing this document, it was considered necessary to undertake a regional assessment with regards to AML/CFT practices. For this purpose, a survey was designed covering the factors considered relevant for an effective regulation and supervision of AML/CFT.

The survey provided an understanding of the AML/CFT legal framework in each country, the competent Supervisory Authorities, the requirements imposed on financial intermediation institutions to prevent them from being used to commit these offences, as well as the characteristics of the AML/CFT supervisory processes currently in place.

The survey results can be considered positive. In general, countries established their compliance with AML/CFT requirements, in particular in regard to the Financial Action Task Force (FATF) Recommendations.

However, weaknesses were detected in some sensitive areas, clearly showing the need for continued efforts and progress in this area. Among the weaknesses detected, four aspects are considered a priority.

First, it is necessary for countries to advance in the implementation of risk-based policies and

procedures. Even though this is a fairly new requirement (given that the new FATF Recommendations were approved in February 2012), its effective implementation will allow countries to identify and use resources appropriately, as well as conduct a more efficient and simple supervision of institutions.

Second, deficiencies still exist in the implementation of customer due diligence processes by institutions. Countries have adapted their requirements, but institutions still show weaknesses in this matter. It is not considered necessary to change the requirements in this regard, but to improve the control over their compliance. Thus, institutions should be forced to apply policies and procedures more efficiently, without taking on unnecessary risks.

Third, the survey identified difficulties in the regulation, assessment, and control of new technologies that support the provision of financial services. Given the increasing significance of this topic, which is reflected in its widespread use (current and future), we believe that this issue should be treated as a priority.

Finally, weaknesses were found in the current legal frameworks for countering the financing of terrorism. Some countries have not adequately criminalized the financing of terrorism; therefore, these countries have not imposed adequate controls over funds designated for such purposes.

II. PRECONDITIONS

The effectiveness of the supervisory process does not only depend on the process itself (its structure and activities) or the supervisor conducting the process, but also on certain preconditions which are outside the control of the supervisor.

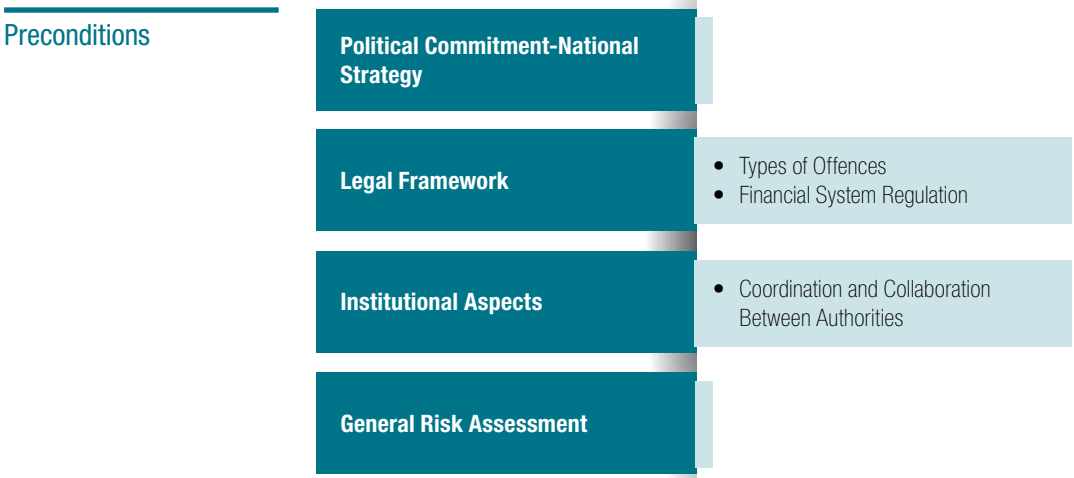
However, the supervisor must make efforts to build these preconditions. To this end, it is recommended that support and advice be provided to the authorities that have the necessary powers to generate these preconditions, collaborating among the various institutions to achieve this goal.

II.1. POLITICAL COMMITMENT (NATIONAL STRATEGY)

Political commitment at a country level is required in the fight against ML/TF crimes. This implies that the country's highest authorities must be involved, that these issues are prioritized, and that resources are assigned to the competent authorities according to the needs that may arise.

This commitment must be incorporated into the national strategy, which covers a series of planned actions directed towards preventing ML/TF crimes, including:

- **Strengthening the Legal Framework.** The legal framework must be commensurate to the challenges faced by the country. Laws and regulations must be drafted in accordance with international standards and recommendations (in particular the FATF Recommendations). However, these must also take into consideration the country's specific charac-



teristics, as well as the challenges and risks to which it is exposed, considering the regional context. This requires constant updating, mainly in what refers to regulatory standards.

- **Authorities.** Considering that ML/TF offences have a multidisciplinary incidence, countries must have an institutional infrastructure that involves authorities in all the relevant areas for the prevention of ML/TF crimes. It is necessary to have specialized authorities in criminal matters, crime investigation, and financial investigation, among others.
- **Coordination between authorities.** Competent authorities must collaborate among themselves without superimposing their roles and acting in a coordinated manner. The national strategy must include the existence of an authority responsible for coordination.
- **Risk-based approach.** A risk-based approach will direct efforts and resources towards the most vulnerable and threatened sectors in ML/TF matters. This requires conducting an effective risk assessment, as described in section II.
- **Training.** The strategy must include an ongoing, comprehensive training plan at the national level for members of the ML/FT prevention system, who should receive training internationally, as well as have a team of specialized instructors at the national level.
- **Strengthening control sub-systems.** Ongoing assistance and support must be provided to AML/CFT *control sub-systems**. In addition, their performance must be monitored to ensure their effectiveness.

II.2. LEGAL FRAMEWORK

Countries must have an appropriate and comprehensive legal framework involving all competent areas and sectors.

This requires the establishment of general legislation and regulations related to these issues, but also specific regulation for the various sectors involved.

II.2.1. Criminalization of Offences

It is required for ML/TF offences to be criminalized, according to FATF Recommendations 3 and 5[2].

Recommendation 3 requires the criminalization of ML on the basis of the Vienna Convention and the Palermo Convention, as well as applying the crime of ML to all serious offences.

According to the interpretative note of FATF Recommendation 3, predicate offences may be described by reference to all offences; or to a threshold linked either to a category of serious offences; or to the penalty of imprisonment applicable to the predicate offense (threshold approach); or to a list of predicate offences; or a combination of these approaches.

As for the TF offence, Recommendation 5 requires its criminalization on the basis of the Terrorist Financing Convention, criminalizing not only the financing of terrorist acts but also the financing of terrorist organizations and individual terrorists.

In addition, considering the particular nature of these offences, it is recommended that countries have a specialized structure to prosecute these offences, involving judges and prosecutors specialized in these issues.

This structure must have the appropriate powers and monitoring tools that would allow for the investigation of these offences, as well as freezing and confiscating assets related to these crimes[3].

II.2.2. Regulation of the Financial System

In regard to this topic, countries must require financial institutions to have ML/TF prevention systems in place, in accordance to the risks faced by these institutions.

These requirements must take into account, as a minimum, FATF Recommendations 1 and 10 to 21. For example, minimum conditions must be set for the ML/TF prevention systems of financial institutions

2 FATF 40 Recommendations can be found at "Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems," FATF, 2013.

3 Refer to FATF Recommendations 4 and 30 regarding confiscation and provisional measures, and Responsibilities of law enforcement and investigative authorities

(policies, customer due diligence procedures, personnel policies, transactions reports, among others).

Countries should also require institutions to comply with Corporate Governance best practices, as a way of ensuring that all the areas of the institution are involved, and that the various functions are adequately assigned.

II.3. INSTITUTIONAL ASPECTS THAT COUNTRIES MUST HAVE IN PLACE

ML/TF prevention systems include the participation of various bodies[4] (specialized courts, district attorneys, Financial Intelligence Units - FIUs, commissions, banking supervisors, among others).

This requires the functions and responsibilities of the competent authorities to be clearly defined in the internal regulation of each country.

The role of the FIU must be separated from that of the banking supervisor, as its activities are complementary and under no circumstance should superimpose.

The FIU must comply with the requirements under FATF Recommendation 29. That is, act as a national center for receiving and analyzing suspicious transaction reports, and other information relevant to money laundering, predicate offences, and terrorist financing.

On the other hand, banking supervisors must have the characteristics provided by FATF Recommendations 26 and 27. They must effectively regulate and supervise financial institutions, to ensure these effectively implement the FATF Recommendations and the national AML/CFT regulation.

Countries must clearly establish that the role of the supervisor is not to investigate ML/TF offences, but to monitor and control financial institutions. The purpose of the supervisor is to verify that financial institutions have appropriate and effective risk mitigating measures in place, according to the transactions and services that they offer to the public, as well as minimizing the risk of being used for ML/TF purposes.

4 The designation of each body shall depend on each country.

II.3.1. Coordination and Collaboration Between Authorities

There must be a regulatory framework for the coordination and collaboration between competent authorities involved in AML/CFT matters, as set forth in FATF Recommendation 2 (National cooperation and coordination).

This refers to the coordination and collaboration between authorities in the same jurisdiction, without considering information sharing with other jurisdictions, whether this takes place at between FIUs, banking supervisors, or any other authorities.

It should be required for competent authorities to freely share information, but ensuring that information is used solely for the purpose for which it was obtained.

To this end, there must be an authority in charge of coordinating the exchange of information between the various bodies.

II.4. GENERAL RISK ASSESSMENT

Countries should conduct a risk assessment to evaluate the ML/TF risk to which they are exposed, covering the various activities, services, and geographic locations, among others. For this purpose, it is recommended that an inter-institutional body is put in charge of coordinating the risk assessment at the national level.

The risk assessment must allow countries to strengthen their knowledge about the risks to which they are exposed, as well as the measures established to mitigate these risks.

The risk assessment should identify the sectors that have the highest exposure to ML/TF risk, both in the financial and non-financial sectors. Also, this assessment should determine the types of ML activities to which the country and region are exposed to, as well as identify the most common predicate offences.

It is also recommended for countries to establish a set of common alert signals (for example, customers whose profile is not consistent with their financial capacity; customers whom in a short period of time emerge as owners of important, new businesses; recurring transactions on behalf of third parties, etc.).

This information should be made available to all the competent authorities, so that they can strengthen the controls in the most sensitive areas to ML/TF risks.

III. BASIC REGULATORY FRAMEWORK FOR SUPERVISORS

An effective supervisory process requires an appropriate legal framework. Without a proper legal framework that grants adequate legal tools, it would be impossible to have an efficient supervisory process.

In this light, this document describes the components of the legal framework, including: the basic organizational structure for the supervisory authority, the supervisor's powers and minimum responsibilities regarding AML/CFT, coordination mechanisms with other national and international bodies, and the power to impose sanctions.

III.1. SUPERVISORY AUTHORITY

First, the scope of the term "supervisory authority or body" must be determined, since the regional assessment conducted for this paper shows that countries have different bodies carrying out functions in AML/CFT issues. In this paper, the term will not encompass all bodies involved in AML/CFT, but only the banking supervisor. In addition, and given that supervision of financial institutions includes various aspects[5], the current document will focus exclusively on the unit or area that carries out supervisory tasks in AML/CFT issues.

Thus, the objective of this section is not to determine the structure and/or powers that the banking supervisor should have in general, but only those related to the specific unit in charge of supervising AML/CFT (which will be referred to as 'specialized supervisor', or 'supervisor').

Therefore, when the paper mentions supervisory body or supervisor, the reference is to the body responsible for performing the supervisory process in AML/CFT matters.

It should be noted that the role of the supervisor must be in line with the FATF Recommendations 26 and 27[6].

Legal Framework for Supervisors

Supervisory Authority

III.2. Legal Framework
- III.2.1. Structure
- III.2.2 Human Recourses
- III.2.3. Physical Resources
- III.2.4. Powers
  - A) Regulatory Powers
  - B) Requirements for FII
  - C) Powers to Monitor and Control
  - D) Powers to Impose Sanctions

III.3. Coordination with Other Authorities

III.4. Sanctions
- III.4.1. Objective of the Sanction
- III.4.2. Opportunity
- III.4.3. Proportional Nature of the Sanctions

5 These include various risks that are regulated, monitored, and measured by the Supervisor.

6 A detail of FATF 40 Recommendations can be found at "Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems," FATF, 2013.

It is not the supervisor's responsibility to combat ML/TF crimes, or to investigate suspicious activities that may lead to AML/CFT crimes. This responsibility corresponds to the competent authorities designated for such purposes by national regulation.

III.2. LEGAL FRAMEWORK

Supervisors in AML/CFT matters must have an appropriate legal framework, covering aspects such as structure, responsibilities, resources, and powers that are commensurate to their responsibilities.

In addition, there must be a framework for the Supervisor to impose sanctions. To this end, sanctions must be regulated in such a way as to have a preventive and dissuasive role in cases of non-compliance with AML/CFT regulation.

III.2.1. Structure

The structure of the supervisory body must guarantee its technical independence[7], so that supervisors can determine the supervisory process they will apply to the financial system as a whole, as well as to each financial institution, with autonomy from a technical and operational point of view, and with sufficient resources for each case.

The special characteristics of ML/TF offences make the supervisory process in this matter differ from the procedures applied to other risks faced by these institutions (liquidity and market risks, among others).

This does not imply that a specific body must be created within the banking supervisor, but that the AML/CFT supervisory process should be developed by a specialized unit, team, or body, with the characteristics, powers and technical ability (specialization and experience) outlined below.

The powers and duties must be established by the country's legislation, bestowing the Supervisor with the powers to issue *regulations**, request and receive information, conduct inspections and assessments, make recommendations, and impose sanctions on non-compliance.

The resources that supervisors must have in terms of staff, their training, and data processing tools, must be equally contemplated.

III.2.2. Human Recourses

The supervisor must have sufficient human recourses, with the necessary expertise to carry out their duties and the required abilities in the prevention of ML/TF.

In turn, supervisors must be able to build multidisciplinary teams, so that the various tasks can be performed by staff members with specific know-how in each area.

It is not enough to simply have a certain number of staff members; but supervisors performing the tasks must be adequately trained and up to date on AML/CFT issues.

In this regard, it is important that the supervisory team has the ability to detect weaknesses in the processes applied by financial institutions, as well as detect the risks posed by products and services offered by financial institutions.

Furthermore, the supervisory team must receive ongoing training in this area, so that it is always up to date on ML/TF risks and methodologies, as well as their regulation, monitoring and control.

III.2.3. Physical Resources

As mentioned above, the supervisory process requires the use of appropriate technological tools to perform an effective analysis of information.

Therefore, it is necessary to ensure resources are budgeted in order to meet the above-mentioned requirements, mainly in regard to tools and training.

III.2.4. Powers

The supervisor must have the power to regulate[8], assess, supervise and impose sanctions on financial institutions, verifying compliance with AML/CFT requirements established in national regulation.

7 In addition to technical independence, the supervisor's opinion and/or actions should not be interfered by the country's political authorities nor the regulated industry, in order to ensure transparency.

8 This refers to the Regulatory Powers indicated in point III.2.4 (A)

Regulation must grant the supervisor the power to regulate, monitor, control and impose sanctions.

A) Regulatory Powers

Regulatory powers imply that the supervisor may have the power to pass regulation applicable to financial institutions, either as general mandates directed to all institutions or as *specific instructions** directed to a single institution or a group of institutions with the purpose of complying with the general regulation.

The supervisor must have sufficient powers to supervise financial institutions in regard to their AML/CFT systems, imposing obligations in accordance with the risks they are exposed to.

Furthermore, the Supervisor must be able to issue specific instructions to impose measures and corrective actions on each financial institution, attending to their characteristics and risks. For example, obligations may be imposed on specific transactions or services provided by an institution, which the supervisors considers as a risk not being mitigated by the institution.

Although the supervisor must have regulatory powers over financial institutions, in case these powers are not granted because of the legal provisions in a given country (according to the regional assessment, the regulatory powers can be distributed among various bodies), the supervisor must be able to establish recommendations and act in coordination with the authority that has the power to regulate.

B) Requirements for Financial Institutions

The ML/TF prevention systems required of financial institutions must incorporate the FATF Recommendations, in particular Recommendations 1, and 10 to 21. According to these Recommendations, the regulation of AML/CFT systems must include risk-based measures in regard to the following areas:

- General assessment of ML/TF risks (inherent and residual) to which the financial institution is exposed to, allowing the supervisor to identify the areas of the institution that face the highest risk and the mitigating measures to prevent such risks.
- Customer due diligence under the terms of FATF Recommendation 10.
- Enhanced Due Diligence, as applicable, for the following cases:
  - ~ High-risk customers
  - ~ Financial Institutions
  - ~ *Designated non-financial businesses and professions (DNFBPs)**
  - ~ *Politically Exposed Persons (PEPs)**
  - ~ Correspondent Banks
- Simplified Due Diligence can be applied in situations such as payment of salaries or payroll, *basic savings accounts**, among others, in order to promote financial inclusion.
- Record-keeping.
- Money or value transfer services.
- New technologies.
- Control of financial groups (consolidated supervision).
- Activities with jurisdictions that pose a high ML/TF risk.
- Reporting of transactions.
- Security in Information Technology (IT) systems.
- Audit Reports.
- Training.
- Information sharing mechanisms between banks.

The specific regulation developed in regard to the items described above will depend on the particularities and needs of each country. But in all cases, the regulator must ensure that the standard complies with the requirements of the FATF Recommendations.

In addition to the regulation requiring financial institutions to have AML/CFT systems in place, these institutions must also comply with requirements regarding Corporate Governance. An effective Corporate Governance ensures a smooth internal operation of the financial institution. It facilitates communication and control between the different areas of the institution, and provides transparency to their operations[9]. In this sense, reg-

9 It is recommended to follow the guidelines in the document: Regulatory and Supervisory Guidelines for Corporate Governance (ASBA, 2013).

ulation must provide guidelines on how financial institutions should be organized to conduct the management and control of their activities, regulating aspects such as:

- Structure of the institution (Board of Directors, Senior Management).
- Compliance. Regulation must consider the role of the Compliance Officer, as well as the allocation of resources and appropriate mitigating measures.
- Functioning of the committees.
- Monitoring practices and control of the business (regular internal reports).

Regarding the content of these norms, it is recommended to refer to the provisions set in the best practices in the field, which should be considered when establishing the specific regulations for each jurisdiction.

C) Powers to Monitor and Control

The power to control must be comprehensive and allow for an integral supervision of financial institutions, covering both the period prior to the beginning of operations, as well as throughout the course of the subsequent activities.

The supervisor must have the power to request information without restrictions, including those related to financial institution secrecy laws, which should not inhibit the work of the supervisor.

This information, in combination with the assessments derived from on-site inspections and off-site reviews, should be used to determine the financial institution's risk profile, as well as the level of compliance with applicable regulations. It will also be used to recommend the adoption of certain measures and to impose sanctions, in cases of non-compliance. Depending on the institution's risk profile, the supervisor must determine the frequency, scope, and nature of the supervisory process.

The power to control must allow the supervisor to carry out inspections in order to verify compliance with current regulation. The supervisor should also continuously monitor the work of the compliance officers, the effectiveness of the customer due diligence -and enhanced customer due diligence- processes through sampling, as well as supervise staff training and verify the effectiveness of the detection and reporting processes of suspicious transactions, among others.

The powers mentioned above must be established within the internal legislation, whether at the legal or regulatory level, considering the figure of the supervisor, its structure, responsibilities and functions.

The Supervisor must analyze the information obtained as a result of his inspection and monitoring activities, in order to determine the risk profile of each institution and evaluate their risk management system. Once this review is carried out, the Supervisor must indicate the level of compliance with current regulation, request corrective measures, and if applicable, impose the appropriate sanctions.

These aspects, together with the minimum AML/CFT standards, must be specially considered in the design of the Prevention system implemented by each State.

D) Powers to Impose Sanctions

The supervisor must be granted powers to impose sanctions on financial institutions and their personnel.

In addition, the Supervisor must be authorized to impose direct sanctions in cases of non-compliance and to verify whether financial institutions comply with the necessary mechanisms to correct the identified irregularities.

Chapter III.4 provides further details on sanctions, their proportionality and their role in AML/CFT systems; however, it is recommended for the power to impose direct sanctions to rest with the Supervisor.

III.3. COORDINATION WITH OTHER AUTHORITIES

According to FATF Recommendation 40, the supervisor must have the power to act in coordination with other supervisory authorities, both local as well as from other jurisdictions.

In contrast, the legal framework must require that information confidentiality be assured, and that the information is used for the sole purpose for which it was obtained.

The supervisor must have the power to enter into information sharing agreements with authorities from other jurisdictions, whenever this is necessary to effectively monitor institutions that comprise a financial group or conglomerate, or maintain some type of relationship with institutions from other jurisdictions.

III.4. SANCTIONS

Sanctions should not solely be a punishment, but also have a dissuasive or exemplary purpose for the rest of the financial system, and must be proportional to the identified non-compliance.

III.4.1. Objective of the Sanction

The importance of the sanctioning power over financial institutions lies in the dual role played by sanctions.

First, a sanction is a punishment for an identified non-compliance. In this case, it exclusively serves a punitive purpose. A sanction is applied solely to punish an action or omission.

Second, a sanction can act as a deterrent. That is, a sanction is applied so that an action or omission is not repeated in the future.

In this sense, sanctions can play an educational role, reaching the entire financial system and not only the entity being originally punished.

In addition, the ability to impose sanctions not only on financial institutions, but also on their senior staff (directors, managers, compliance officer) reinforces the dissuasive and educational role of sanctions.

With this purpose in mind, consideration should be given to making sanctions public, once these are definite. In this case, publicity will reinforce the role of the sanction, sending a clear message to the financial system.

For disclosure to third parties, the supervisors will be in the obligation of publishing on its website the sanction and it is recommended that the institution acts in the same manner.

The financial institution's Board of Directors must be made aware of the existence of the sanction through by recording the fact in the corresponding minutes.

III.4.2. Opportunity

The supervisor must be authorized to impose sanctions at any given moment when non-compliance by a financial institution is detected in matters of AML/CFT.

The supervisor can impose sanctions after completing the inspection process, and whenever non-compliance has been identified; but also in the case of delays in the presentation of regular or specific information.

III.4.3. Proportional Nature of the Sanctions

Sanctions must be proportionate to the severity of the identified non-compliance, taking into consideration the ML/TF risk involved. Existing extenuating or aggravating factors must be considered when imposing these sanctions.

Although it is considered that sanctions should range from simple warnings to monetary fines, as well as the revocation of operating licenses, the internal legislation of each country must be in charge of dictating the scope of sanctions.

The sanctions imposed on the institution's staff must be applied using the same criteria, considering the specific actions of the person receiving the sanction.

IV. SUPERVISION OF THE FINANCIAL SYSTEM ON ML/TF MATTERS

When discussing supervision, the document does not refer to the inspection process or a particular task, but to the various related activities serving a common purpose. Therefore, when referring to all related activities, the document is discussing the supervisory process.

The supervisory process detailed below does not seek to substitute the processes or manuals implemented by each country for the supervision of ML/TF issues. The process below was developed based on general guidelines, adaptable to any risk-based supervisory process in ML/TF issues.

Objective of supervising AML/CFT systems

The supervisory process should aim to protect the integrity of the financial system through the adoption of AML/CFT measures.

Thus, it is intended for financial institutions to be committed to combating ML/TF offences; through the promotion of a prevention culture based on regulatory compliance, as well as compliance with international standards and the implementation of best practices focused on the prevention, detection and control of transactions related to these crimes.

According to FATF Recommendation 1, countries should assess whether financial institutions effectively mitigate the ML/TF risks to which they are exposed.

Therefore, the supervisory process must set a higher standard than that established by regulatory compliance, aiming for financial institutions to have measures in place commensurate with the risks they face.

This does not mean that the supervisory process will not verify financial institutions' level of compliance with regulation, or monitor the formal aspects of the ML/TF prevention systems. Although these objectives should be considered part of the process, these are not the final objective in itself. The main objective is the effective mitigation of ML/TF risk to which institutions are exposed, which in turn will determine the scope and the tasks to be performed during the supervisory process.

Risk-Based Supervision

A risk-based supervisory process has two basic objectives:

a) To determine the risks faced by the system and the supervised institutions, i.e., to identify, measure, evaluate and control them; and

b) To determine if these risks are mitigated by the institutions' ML/TF prevention systems.

To comply with the provisions established in the previous paragraphs, it is recommended for each country to prepare a Risk Matrix that includes the aforementioned aspects (identification, measure, evaluation, and control of the ML/TF risk) affecting the financial system[10], as well as each financial institution[11].

IV.1. ASSESSMENT OF ML/TF RISK IN THE FINANCIAL SYSTEM

This section outlines the aspects that should be taken into consideration when assessing the inherent risk in the financial system. The assessment should be a tool that allows the supervisor to determine the ML/TF risk in the financial system as a whole, and to take appropriate measures.

10 The risks to which the financial system is exposed to must be assessed by a competent, national authority (point II.4 herein) with cooperation from the supervisor.

11 Annex I contains a model of a Risk Matrix that countries can use as a reference at this stage of the supervisory process.

IV.1.1. Risk factors to Consider

The Wolfsberg Group[12], in its "Guidance on a Risk Based Approach for Managing Money Laundering Risks", identifies the main risks to be addressed: i) Country Risk (or Geographic Risk); ii) Customer Risk; iii) Services Risk; and iv) Other Risks such as:

- Level of assets under management or volume of transactions undertaken;
- Regularity or duration of the relationship with the financial institution's customers;
- Familiarity with the jurisdictions where it operates; and
- Use by customers of intermediate corporate vehicles or other similar structures.

Implementation of a risk-based supervisory process will allow the institution to give priority to the major risk areas, and to effectively channel human and physical resources.

The various activities of the supervisory process described below, represent a risk-based approach implementation in each stage: therefore, this process should be considered in accordance with this principle.

IV.1.2. Methodology for Determining Risk

To determine ML/TF risk, the following aspects must be taken into consideration:

- ML/TF risk to which the country is exposed.
- ML/TF risk to which each activity sector is exposed.
- ML/TF risk to which the financial system is exposed.

The first two bullet points must be defined in the country's risk assessment, detailed in section II.4.

The risk assessment of the financial system must be performed by the supervisor, taking into consideration the individual risk of each financial institution in order to determine the aggregate risk profile of the financial system.

12 The Wolfsberg Group is formed by 11 international banks that have jointly developed a series of voluntary anti-money laundering standards known as the "Wolfsberbg Principles".

First, the supervisor must have knowledge, prior to the start of the supervisory process, about the typology of ML/TF offences and how criminal organizations may use financial institutions for this purpose. Furthermore, the supervisor's staff is required to be knowledgeable about the operational functioning and transactions usually conducted by the financial institution.

Second, the supervisor is required to understand the AML/CFT systems of each financial institution, and in particular their compliance culture. While this aspect will be further discussed in this document, the supervisor should be able to determine each financial institution's weaknesses given their characteristics.

The supervisor should analyze the financial institution's Risk Matrix or risk assessment to review and evaluate how risks are determined by the institution itself.

Once the financial institution's risk is identified and measured, the risk-mitigating measures must be assessed.

At this stage, the supervisor must analyze, from a formal point of view (review of policies and procedures), if the measures are commensurate to the risks faced by the financial institution, and if they are in line with the applicable national regulations.

Supervisors should determine whether the financial institution's AML/CFT system meets the following minimum requirements:

- It is appropriate to mitigate the risk to which the institution's is exposed.
- It meets regulatory requirements established in ML/TF regulations.
- It allows for the identification of transactions with a high ML/TF risk.
- Active involvement of the financial institution's Board of Directors and Management in the prevention of ML/TF offences.
- It requires effective customer due diligence and enhanced due diligence procedures to be in place.
- It provides for the control and monitoring of transactions.
- It is effective in the early detection of unusual or suspicious transactions.
- It has effective staff policies in place (control, selection, and training).

IV.1.3. Ongoing Updating of the ML/TF Risk Assessment

The dynamic nature of the financial industry (mainly with regards to products and services), the development of new ML/TF typologies, the changes in countries' economies and in the factors taken into consideration when assessing ML/TF risks, make the level of risk to which a financial system is exposed variable. Therefore, the ML/TF risk assessment must be regularly revised and updated.

For this purpose, it is recommended that at least once a year the various risk-determining factors be assessed, and the level of risk in the financial system be updated.

IV.2. ANNUAL SUPERVISORY PLAN FOR THE FINANCIAL SYSTEM

It is recommended for the supervisor to plan the supervisory process of the financial system by preparing an annual supervisory plan.

The annual supervisory plan must establish the activities that the supervisor must perform, including ongoing off-site surveillance of all institutions in the financial system, as well as routine on-site inspections.

Thus, the supervisor can control the entire financial system, monitoring all financial institutions as well as thoroughly controlling those considered most relevant.

IV.2.1. Risk-Based Supervision Planning

The planning must consider the risk to which the financial system is exposed as a whole, as well as the risk of each individual institution.

The supervisor should perform a general monitoring of all financial institutions in the system, and will focus on the institutions that are considered more relevant in terms of ML/TF risk (to determine the level of significance, the following aspects should be considered as a whole: volume of assets, number of customers handled by the financial institution, and the types of products and services offered, as well as the geographical zones where the institution operates, among other factors).

A general monitoring of the system involves analyzing the information from each financial institution in order to make an assessment to determine the risks to which each institution is exposed, the measures taken to mitigate risks, and their effectiveness (determining residual risk).

The individual monitoring (inspection process) is performed on financial institutions that have been selected based on their relevance within the system, and the monitoring procedures must be planned in accordance to the financial institution being supervised.

To determine which financial institutions to control specifically or more frequently, as deemed necessary, the following factors must be considered: the ML/TF risk of each financial institution, the measures applied to mitigate this risk (residual risk), and the relevance of the institution within the financial system.

Finally, the Supervisor must follow the annual supervisory plan, which should also be flexible to adapt to the findings identified during the general monitoring process.

In this sense, the plan should consider the possibility of conducting inspections on institutions that were not initially included in the individual monitoring plan, but which should be inspected as a result of relevant findings during the monitoring process of information regularly provided to the supervisor, or other elements that may have arisen during the investigation by competent authorities, or through reliable information published in the media.

IV.3. GENERAL MONITORING OF INSTITUTIONS IN THE FINANCIAL SYSTEM

A general monitoring of financial institutions involves performing an assessment of each institution, based on the supervisor's analysis of the information.

IV.3.1. Elements for the Assessment

The assessment is mostly conducted off-site. This process is independent from the inspection process; however, the tasks performed during this process will be useful for the inspections later performed on the supervised institution.

First, the supervisor must identify all the information gathered on the financial institution. The information to review includes:

- Audit reports (internal / external).
- Auditor's work papers.
- Prior supervisory process reports.
- A list of observations made during the previous inspection, the financial institution's committed action plan, and evidence of compliance with the plan.
- Information about the financial situation of the institution and other indicators about its operation, the risk trends in other areas, and its mitigating factors.
- Systematic reporting received from the financial institution.
- Unusual/ suspicious transaction reports.
- Sanctions imposed or in process of being imposed.

The monitoring process should also consider the following: reliable press releases about the entity; Board of Directors minutes; communications from other regulatory bodies; regulatory changes that may affect risk management; and sanctions; among others.

After reviewing this information, the supervisor must request further information from the financial institution in order to determine the following aspects:

- **Structure.** The size of the financial institution must be determined, as well as its organization and controls to ensure an effective Corporate Governance. The supervisor must be able to determine the number of employees, the number of branches, as well as the geographic areas where the financial institution operates (country, cities, neighborhoods).
- **Internal structure.** The supervisor must have knowledge about the financial institution's internal structure, particularly about the areas dealing with compliance (Compliance Officer and Compliance Committee), as well as the mechanisms for decision making and reporting.
- **Policies, procedures and risk assessments conducted by the financial institution.** The supervisor must understand all the elements of the institution's ML/TF risk management regime, as well as how this regime is integrated into the institution's integral risk management system.
- **Products and Services.** The supervisor must know and understand the products and services offered by the institution, given that most of the risks that institutions face are largely correlated to the characteristics of the products it offers and the services it renders.
- **Customers.** The supervisor must be able to determine the composition of the customer base. The supervisor should understand the risk profile assigned to customers (taking into consideration risk factors, such as type of customer, activity, products and services used, average amounts, geographical areas), as well as the total risk of the customer base.
- **Relevance.** The supervisor must identify the financial institution's relevance within the local financial system, both in general and in each sector. In order to do this, the supervisor must consider aspects such as the amount of assets under management, the number of customers, the products and services offered by the institution, as well as the jurisdictions where it maintains business relationships.
- **Economic Group.** The supervisor must have access to information about the economic group to which the financial institution belongs to, in order to identify and measure the internal and external risks to which the institution is exposed.
- **Jurisdiction.** The supervisor must take into consideration the institution's home jurisdiction, its customers' activities, as well as other institutions comprising the economic group, and in particular linkages to jurisdictions considered as high-risk by FATF.
- ***Correspondent Banks**** The supervisor must be aware of any correspondent relationship of the financial institution, whether reciprocal or not, as well as correspondent banking services provided and/or received.

IV.3.2. Information Regarding the Financial Institution Under Supervision

In order to perform the aforementioned assessment, the supervisor must have access to (or request the financial institution for access to), among others:

- General aspects of the financial institution's Corporate Governance (structure, Board of Directors and Committees' minutes, reports to the Board of Directors, among others).
- Up-to-date policies and procedures (general, "know-your-customer" (KYC), enhanced due diligence, correspondent banking, high-risk activities, etc.).
- Code of conduct.
- Risk Matrix prepared by the institution.
- The structure of the compliance function (its procedures); compliance committees (their bylaws, quorum, minutes of meetings, attendance).
- Reports on transaction monitoring (in response to alert triggers in the system).
- Reviews by the compliance function regarding the implementation of policies and procedures.
- Employee training and training for compliance staff, in particular.
- Procedures for reporting suspicious transactions.
- Audit reports (internal and/or external) related to ML/TF issues, among others.

This information will allow the supervisor to know if the institution's policies and procedures are suitable for the ML/TF risk to which it is exposed to.

IV.3.3. Analysis of Information Issued by the Supervised Financial Institution

The analysis of the documentation issued by the financial institution must be documented in minutes or work papers, including detailed information about the reviews conducted, the compliance testing, and other procedures applied. These reports must be properly written, and it is recommended for the information received and elaborated to be digitally stored with the highest safety standards possible.

IV.3.4. Background Information About the Financial Institution

Background information on the financial institution must be considered when planning the inspection.

The supervisor must take into consideration public information received from other jurisdictions where the institution operates (economic group), in order to identify information that may be relevant for the AML/CFT assessment.

IV.3.5. Public Information

Reliable media information must be taken into consideration, including, in the first place, information on ML/TF matters, but also information regarding the operations and business dealings of the institution.

IV.3.6. Previous Inspections of the Institution in ML/TF Matters

The supervisor must use reports and work papers from previous ML/TF supervisory processes. The background information about the financial institution may allow for certain aspects to only require an update (mainly aspects related to knowledge about the institution).

IV.3.7.Supervision in Other Areas

The supervisor must have access to information about the financial institution, resulting from supervisory processes in other areas.

In particular, the supervisor must consider information about the institution's senior management, its economic group, its corporate governance, and any other information relevant to the AML/CFT supervisory process.

Please note that the list presented below is not exhaustive. In each case, the supervisor must determine whether it is necessary to request all the information outlined below, or if additional information will be requested.

As an example, in the case of *superseding factors** that may have an impact on the financial institution (new lines of business, new senior management, specific transactions, among others), the supervisor may consider conducting interviews with key staff members in order to understand the current situation of the institution.

IV.3.8. Assessment of the Financial Institution

Once the information is analyzed, the supervisor must make an assessment about the institution. The assessment must consider the following factors:

a) The characteristics of the financial institution.
b) Its exposure to ML/TF risk.
c) The measures adopted by the financial institution to mitigate this risk.
d) An analysis regarding the suitability of the mitigating measures. The supervisor must also consider whether these measures are in line with applicable local regulations.

The supervisor should consider how convenient it would be for the assessment to remain confidential, even from the financial institution.

If the financial institution considers its mitigating measures to be adequate, the next step is to analyze (when the annual supervisory plan provides for conducting an inspection) whether these are effectively implemented.

If these measures are insufficient, —because the policies and procedures are not commensurate with the institution's business and risk level, and/or do not comply with regulations —,the following alternatives must be considered:

a. To notify the institution about the deficiencies that have been detected and request an action plan;
b. Include the financial institution (if it is not already included) among those to be immediately inspected in order to conduct a thorough assessment.

In both cases, the financial institution may present justifications. In addition, the supervisor may consider the possibility of imposing sanctions at this stage of the process.

IV.4. INSPECTION PLAN

The supervisor must prepare an inspection schedule, which establishes the order in which financial institutions that make up the financial system will be subject to the inspection process.

Two aspects must be taken into consideration when determining the priorities for the inspection schedule. On one hand, the supervisor should address the ML/TF risk in each financial institution, prioritizing control over those whose risk level is higher. On the other hand, supervisors should consider the relevance of the financial institution within the financial system.

The combination of these two factors will determine the order and frequency of the inspections. The inspection plan should cover all financial institutions in the system in a determined period of time, the latter will depend on the country's ML/TF risk.

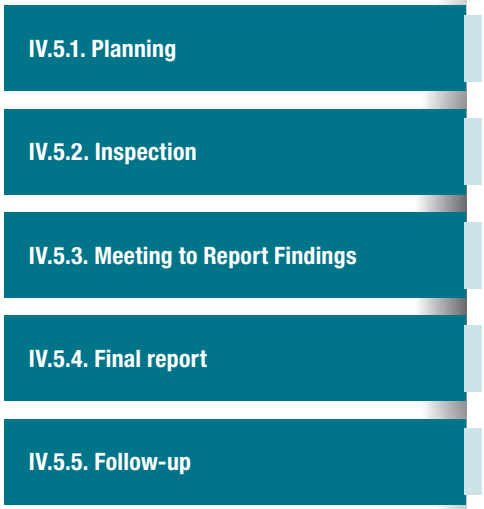
IV.5. INSPECTION PROCESS

The proposed inspection process consists of five clearly defined stages:

1. **Planning.** During this stage, the supervisor should determine the main focus of revision for each institution, according to its characteristics and ML/TF risk exposure. Once the key aspects to be evaluated have been defined, the supervisor must establish the inspection team and the estimated time to complete the inspection (stage 2).
2. **Inspection.** The activities planned in the previous stage are carried out. These activities are performed in the supervised financial institution's premises (on-site).
3. **Meeting to report findings.** The objective of this meeting is to communicate the financial institution about the findings during the inspection process. This meeting serves as a preview for the Final Report.
4. **Final Report.** The final report must include an executive summary covering the main conclusions, as well as a detailed report on the findings.
5. **Follow-up.** Based on the importance of the findings and the financial institution's response, the supervisor will determine a follow-up strategy that takes into consideration the deadlines and action plans set by the entity. The supervisor must continue monitoring the financial institution to ensure the implementation of the action plan.

The following paragraphs describe the objectives and scope intended for each stage.

Structure of the Inspection Process



IV.5.1. Planning the Inspection Process

This is the first stage of the inspection process. In this stage, the supervisor will set the course for the whole process, determining which activities will be carried out and the resources that will be needed.

Although during later stages, mainly during inspection, the supervisor should act with certain flexibility with respect to the inspection plan, the provisions established during planning will pose a certain limit on activities performed in subsequent stages.

This stage has two essential objectives:

i) Based on the available information on the financial institution, the supervisor will determine the ML/TF risks to which it is exposed; and

ii) Outline the activities to carry out, as well as the resources needed for subsequent stages in the process.

The knowledge about the financial institution must allow the supervisor to determine the risks to which it is exposed. At this point, the supervisor must use information obtained from the institution's assessment during the general monitoring stage.

The knowledge about the supervised financial institution, also allows the supervisor to determine if the institution has ML/TF risk mitigating measures in place, and if these measures are appropriate.

The second objective is to define the steps to follow to evaluate or verify the previous point. This involves establishing the supervisory activities and resources needed to conduct them.

In view of these objectives, the supervisor must prepare a strategy that includes the revision of risks identified during the financial institution´s assessment (section 4.3.8). The strategy should specify the activities that must be performed in the subsequent stages of the supervisory process, mainly during the inspection.

At this point, the supervisor should establish the specific activities to be carried out during the inspection. The inspection plan must define the revision procedures, detailing the activities that will be carried out in each area, and assigning priorities and relevance to each activity.

In addition, the plan must establish the physical and human resources that will be needed, considering the participation of multi-disciplinary teams, according to the activities being conducted.

At this point, it is necessary to establish deadlines to apply the plan; these will serve as internal control measures for the supervisor.

Once the inspection begins, the strategy must be reviewed and adapted in accordance to the findings as the process is implemented.

IV.5.2. Inspection

The inspection is the core on-site activity. It consists of the supervisory teams performing activities to monitor compliance with regulation. These activities are conducted on the financial institution´s premises (headquarters and branches). During this stage, the aforementioned supervisory strategy is executed.

Given that the proposed supervisory process has a risk-based approach, it is during the inspection that this approach will be reflected by assigning more resources and efforts to control the areas that pose the greatest threats.

The inspection must verify whether the financial institution has an effective prevention system to mitigate the ML/TF risk to which it is exposed, and that the system is implemented effectively.

While the inspection process focuses on the institution's effective management and control of the ML/TF risk to which it is exposed, the supervisor must also verify compliance with applicable local regulation and international standards.

It is understood that the application of local regulation is not necessarily sufficient to mitigate the ML/TF risk facing the financial institution. Given that the goal of the supervisory process is to verify that risk is mitigated by the institution, the supervisor must prioritize an effective mitigation over a mere compliance with regulation in this matter.

Therefore, the supervisor should require financial institutions to mitigate the ML/TF risk, even when this requirement is more demanding than complying with applicable regulation. Thus, it is essential for the supervisor to have a specific regulatory power to impose obligations that are commensurate to the level of risk that each financial institution faces.

A) Elements to Assess

The assessment must allow the supervisor to verify whether financial institutions are adopting the FATF Recommendations. It is important to point out that the Supervisor is responsible for requiring financial institutions to implement policies and procedures that will allow them to prevent ML/TF. However, it is not the role of the Supervisor to search or investigate people involved in ML/TF offences.

The following paragraphs describe the basic and general elements that should be evaluated during an inspection[13].

Inspection and Aspects to Assess

- **A.i. Structure of the organization**
- **A.ii. Policies and Procedures. Internal Control**
- **A.iii. Customer Due Diligence Procedures**
- **A.iv. Staff policies and Training**
- **A.v. Products - New Technologies – Distribution Channels and Channels to Acquire New Customers**
- **A.vi. Financial Group and Consolidated Supervision**
- **A.vii. Monitoring of Transactions**
- **A.viii. Data Processing Tools**
- **A.ix. Reporting**
- **A.x. Independent Review of the ML/TF Prevention System**

13 Notwithstanding other aspects the supervisor may deem necessary to inspect in specific cases.

A.i) Organizational Structure

The supervisor should determine the level of involvement of the Board of Directors in the financial institution's management of ML/TF risk. For example, the supervisor must analyze whether the Board approves the compliance structure, its policies and procedures, if the Board receives information on ML/TF issues, and if so with what frequency, among others.

A specific analysis must be carried out regarding the compliance structure to determine whether it is appropriate for the size and the risks of the financial institution.

If the financial institution has specific committees to deal with AML/CFT issues, the supervisor must review their integration, functioning (frequency of meetings), activities, degree of involvement in ML/TF risk management, as well as the degree of specialization of its members. In addition, the supervisor should review the Committee's minutes and monitor the aspects mentioned above.

Regarding the Compliance Officer, the supervisor should evaluate whether:

- He/she has the necessary training for the role.
- He/she has sufficient authority and independence within the financial institution's structure (the Compliance Officer position must be included in the category of senior management).
- He/she has the necessary resources (human and technological) to carry out this function.
- He/she has sufficient authority to access information from all areas in the financial institution, without restrictions.
- He/she has direct and adequate channels of communication with the Board of Directors.

The supervisor must review the level at which the Compliance function is established within the institution's organizational structure, its independence from the risk-taking areas, its assigned responsibilities, its scope of action (i.e. whether it refers solely to the bank, its branches, or the financial group), how many human resources have been assigned to this function, and the available data processing tools to monitor transactions, among others.

The supervisor must consider whether the Compliance Officer function covers a group of entities (corporate compliance officer). In these cases, supervisors should evaluate the Officer's position within the group, his/her powers (which must be commensurate to the position), as well as whether he/she has appropriate human and material resources to develop this activity.

Another aspect that should be analyzed includes the tasks assigned to the Compliance Officer, as well as their effective implementation.

The following elements should be reviewed:

- Annual compliance report (and any other regular report pursuant to a country's regulations).
- Plan of activities and its execution.
- Training plan for the institution's staff.
- Activities related to the monitoring, analysis, and reporting of transactions (according to the policies and procedures of each institution and the applicable local regulations).
- Assessment of new products, services, and technologies used by the institution.

The supervisor must ensure that the financial institution has an organization structure in accordance with the best corporate governance practices, and that the compliance area and the compliance officer have the necessary independence and resources to carry out their responsibilities.

A.ii) Internal Control Policies and Procedures

The supervisor must verify that policies and procedures comply with regulation requirements and that these are effective for risk mitigation regarding the relevant activities to be reviewed during the institution's inspection.

In addition, the supervisor should verify the effective implementation of the institution's policies and procedures set for the prevention of ML and TF offences.

These policies and procedures must have been approved by the institution's Board of Directors and communicated to the entire personnel. The supervisor must control and assess whether the following requirements are met, as a minimum:

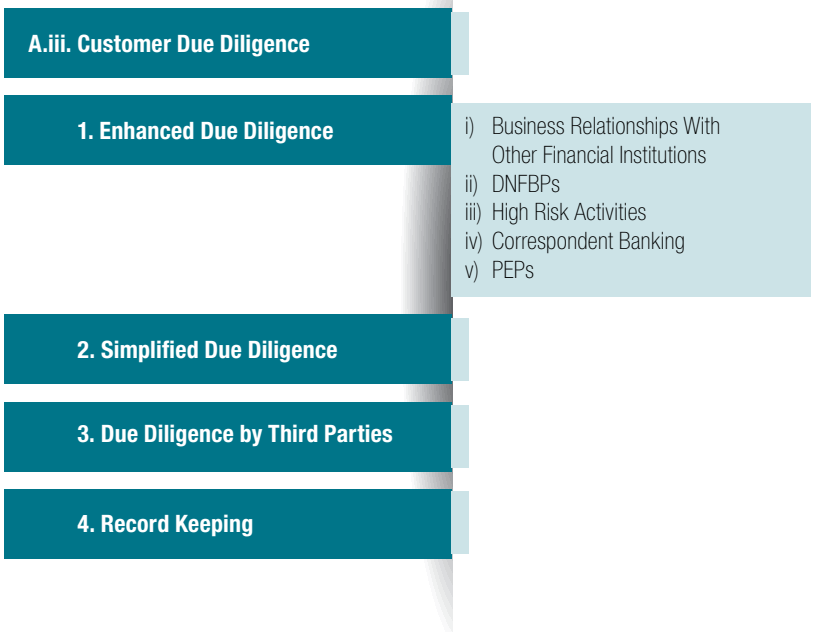
- Compliance with regulatory requirements in the prevention of ML/TF offences.
- Active involvement of the financial institution's Board of Directors and Senior Management in AML/CFT issues.
- Role of the Compliance Officer and the specific committee on AML/CFT issues.
- Role and responsibilities of the various areas of the financial institution.
- Established effective procedures for Customer Due Diligence and Enhanced Due Diligence, as well as restrictions on certain types of customers.
- Established Provider Due Diligence policies.
- Record keeping and updating information.
- Control and monitoring of transactions, in accordance with the risks to which the financial institution is exposed.
- Identify high-risk ML/TF transactions, and detect in a timely manner alert signs of suspicious transactions.
- Establish provisions in regard to systematic transaction reports.
- Have effective personnel policies in place (control and training).
- Set up provisions regarding the updating of policies and procedures.

Supervisors must verify that financial institutions have a Conduct Code, and if so, if the Code contains provisions in reference to AML/CFT matters.

A.iii) Customer Due Diligence Procedures.

The success or failure of the institution's ML/TF prevention system depends in great measure on the effective implementation of the *Customer Due Diligence (CDD)** procedures.

Structure of the Supervision Process



The supervisor must pay special attention for the effective evaluation of this aspect of the AML/CFT system. This evaluation must be conducted through sampling, considering the level of risk of the customer portfolio. In this sense, sampling must be directed towards customers who have higher-risk characteristics.

The sample must be representative of both the customer portfolio managed by the financial institution and the high-risk customers (according to the risk assigned by the institution, which must be reviewed during the inspection).

The sampling process must consider the following steps:

- Define the population of interest.
- Define the variable of interest (customer risk) and the methodology for selecting samples (simple random sample, stratified sampling, cluster sampling).
- Collecting information.
- Review the resulting sample and calculate the desired statistics.

The supervisor must review that the basic customer information is in order and up-to-date, in accordance with regulatory requirements and the institution's policies.

The aspects to be reviewed must include[14]:

- The correct identification of the customer, conducted prior to the beginning of the business relationship.
- Identification of the customer's economic activity.
- Identification of the customer's source of funds. The supervisor must review whether the funds being managed in the supervised account correspond to the stated financial activity of the customer (source of the funds).
- Correct identification of the final beneficiary. Special attention must be given to cases where legal structures are used.
- The purpose and character of the business relationship.
- The supervisor must control that the customers' risk rating is correct (high, medium, low). In order to do this, the following risk factors must be determined:
  - ~ Customer's economic activity.
  - ~ Amounts transacted.
  - ~ How long ago did the business relationship start and the type of services provided by the financial institution.
  - ~ Geographical areas to which the customer is linked.
  - ~ Legal structure adopted by the customer (trust, partnership, corporation, etc.).
  - ~ Other risk factors: Politically Exposed Persons (PEPs), Designated non-financial Businesses and Professions (DNFBPs).
  - ~ Review listings (United Nations, *Office of Foreign Assets Control**, among others).
- The supervisor should review whether the customer's transactional profile is correctly assigned and updated. In order to verify the assignation of the transactional profile, the following must be analized:
  - ~ Volume of funds managed by the customer.
  - ~ Stated economic activity.
  - ~ Net Worth.
  - ~ Volume of revenue or income.
  - ~ Financial information.
  - ~ Nature of the relationship, meaning the purpose of the account or link between the customer and the financial institution.

The supervisor must review that information is properly documented, when applicable.

A lack of customer information (identification data, economic activity, and sources of the funds), as well as incorrect risk ratings, should be considered as a serious fault by the institution.

Specific customers, given their characteristics and risks, must be particularly considered and may require a differential treatment in regards to due diligence. See Enhanced Due Diligence.

The supervisor should keep in mind that the supervisory team will require advanced training when analyzing issues such as customer's risk ratings, as

14 Customer information and other elements to be reviewed must at least comply with the requirements contained in the applicable FATF Recommendations.

well as evaluating the adequacy of explanations for the customer's source of funds.

*1. Enhanced Due Diligence (EDD)**

The supervisor should assess the implementation of the EDD process, at least in the cases outlined in the following paragraphs. This assessment should take place regardless of its implementation on customers that the financial institution has ranked as high risk (according to the risk factors such as geographical area where the customer operates, economic activity, volume of transactions, amounts transacted, among others).

i) Business Relationships With Other Financial Institutions

The supervisor must determine if the financial institution provides services to other financial operators. These services may not necessarily amount to correspondent banking. In this case, Enhanced Due Diligence (EDD) must be conducted to determine the risk profile of the financial institution receiving the services (activity, amounts transacted, risks, level of control), and the nature of the services being provided. The supervisor must monitor any related accounts and identify fund movements between these accounts.

A specific analysis must be conducted about the risk of such business relationship, as well as the mitigating measures taken to reduce such risk.

ii) Designated Non-Financial Businesses and Professions (DNFBPs)

The institution must identify the customers regulated for AML/CFT purposes.

According to the applicable regulations, the institution must identify the regulated activities (regulated agents) or customers requiring enhanced due diligence procedures[15].

Financial institutions must ensure that customers in this category have prevention policies in place, according to local requirements and procedures for handling third-party funds.

In these reviews, the supervisor should verify that the financial institution complies with these regulations, and that the institution has identified on its own other activities it considers require Enhanced Due Diligence.

Institutions should consider the risk posed by customers that have regulated activities. Also, the supervisor shall review if the financial institution has adequate control measures in place (identification, control of funds, and activity monitoring).

The supervisor must review whether the financial institution has implemented appropriate procedures to identify cases where customers manage third-party funds. And that once identified, these third-parties are monitored in order to determine the final beneficiary of the transaction and the source of the funds.

iii) Higher-Risk Activities

The institution must specifically define the conditions, areas or activities considered to be high-risk, in accordance to risk parameters such as:

- Economic activity.
- Managing third-party funds.
- Significant amounts (according to the institution).
- Managing large volumes of cash.
- Geographical areas where the customer operates, etc.

For example, this category includes activities such as:

- Real estate agents.
- Car dealerships.
- Charity or non-for-profit organizations.
- Hotels.
- Car rentals.
- Casinos.
- Schools.
- Public notaries and persons authorized to attest validity, among others.

Once customers in this category are identified, the supervisor must control that the financial institution has a special know-your-customer system (KYC) in place, as well as a system for monitoring and following-up its transactions.

15 It must at least include the persons and/or activities indicated in FATF Recommendation 22.

iv) Correspondent Banking

Policies must establish the nature of cross-border correspondent banking and the applicable requirements to operate with these financial institutions (especially when associated with ML/TF).

During the inspection, the supervisor must verify whether the financial institution has carried out the following tasks:

- Have sufficient information about the financial institutions with which the supervised institution has any type of relationship [minimum identifying information such as: bylaws or partnership agreement, significant shareholders (considering those that exceed ten percent of capital), key personnel, tax identification number].
- Assess the policies and procedures applied to detect ML/FT transactions.
- Document the respective AML/CFT responsibilities of each financial institution.
- Obtain approval from senior management before establishing new correspondent relationships.
- Ensure ongoing monitoring of transactions with the correspondent bank.
- Analyze the correspondent bank's home jurisdiction, as well the jurisdictions or regions where it is active.

The supervisor must control that financial institutions do not maintain correspondent relationships with shell banks, and that these banks do not use supervised institutions directly or indirectly.

v) Politically Exposed Persons (PEPs):

The supervisor must identify the PEP accounts kept by the financial institution, whether national or international.

In regard to PEPs, the supervisor should analyze the following elements:

- Compliance with formal account requirements (i.e. the application of EDD procedures) to ensure that it has adequate information about the customer and persons related to the customer.
- Checking of lists (national or international).
- Source of funds and ongoing monitoring of the account.
- Jurisdictions where the activity of the PEP customer takes place.
- Account authorization and approval procedure.

It is especially relevant to establish the source of funds of a PEP account, as well as the use of the account.

The supervisor must analyze if the funds in the account are duly justified, and if the services provided to the PEP customer are reasonable and justified.

As in previous cases, the supervisor must verify the effective monitoring of transactions performed by a PEP customer.

2. Simplified Due Diligence

According to FATF Recommendations 1 and 10, institutions should be allowed to apply simplified due diligence procedures in situations of lower ML/TF risk.

If the financial institution applies simplified due diligence measures, then the supervisor must control the following aspects:

- That the financial institution has taken appropriate measures to assess and measure the risks to which it is exposed to.
- Factors taken into consideration when assessing risk (types of customers, countries, geographical areas, particular products, thresholds, etc.).
- The supervisor must verify that the risk assessment is kept up to date.
- The financial institution must document the risk assessment performed, so that it can present the results to the supervisor, and appropriately support the financial institution's processes.
- Monitoring of customers where simplified measures were applied.
- The existence or use of alerts to indicate the need to change the transactional profile of customers to which the institution applied simplified measures.

If the conditions mentioned above are not met, the supervisor must require the implementation of regular or enhanced due diligence measures, if applicable.

3. Due Diligence by Third Parties

If the supervised financial institution delegates its due diligence process to third parties, following the consideration and approval of the supervisor, the latter must verify that:

- There is a formal agreement in which the financial institution delegates the due diligence process to the third party, the agreement establishes the obligations and responsibilities of each party and the obligation of confidentiality. Nevertheless, the responsibility of the due diligence process rests with the financial institution.
- The financial institution has immediate access to information gathered through the due diligence process. It must at least have access to the following information: a) customer identification and final beneficiaries; b) economic activity of the customer; c) purpose and characteristics of the business relationship with the customer.
- The third party must be duly regulated in the jurisdiction where it provides the service and it should use AML/CFT procedures in accordance with the best practices and international standards. The supervisor must verify that the financial institution has reviewed the policies and procedures implemented by the third party.

When a financial institution outsources its due diligence process to a third party that is part of the same financial group, the aforementioned requirements must be met, but the supervisor can be more flexible regarding the control of regulations applicable to the third party.

4. Record Keeping

Financial institutions should keep records of transactions and customer information in accordance to FATF Recommendation 11 (Record keeping).

The supervisor should verify that the financial institution complies with all requirements related to record keeping. The supervisor should:

- Control that the financial institution maintains records of all transactions conducted by or through the institution.
- Control that the records held by the institution is sufficient to allow for a reconstruction of individual transactions (including the amounts and types of currency involved, intervening parties, etc.).
- Control that the institution maintains all records obtained from customers and those produced by the institution through the application of the customer due diligence process.
- Review that the financial institution has appropriate contingency plans, allowing it to protect and access all information in case of a disruption or system failure. To achieve this, the following aspects must be analyzed:
  - ~ That the contingency plans are in writing and have been approved by the institution's senior staff; also that they are duly communicated to the staff involved in their implementation.
  - ~ That the measures allow information to be recovered in its entirety and in a period no greater than 24 hours.
  - ~ That the plans include adequate security measures (location of servers, back-ups, access control, security passwords, etc.).
- Verify whether the financial institution has a designated person responsible for the information.
- Control that the records remain legible and complete.

Institutions should maintain records (of transactions and customer information) for at least five years.

A.iv) Personnel Policies and Training

During the inspection, the supervisor should at least control that the following requirements are met:

- Compliance with personnel recruitment policies. The supervisor must assess whether these policies are implemented, in particular regarding new personnel during the last year.
- Monitoring of personnel, with emphasis on job positions in areas considered "critical", due to the risk they face. The supervisor must access and review the monitoring process, which must include aspects such as net worth of employees and use of paid leave.

- The supervisor should control that staff is duly trained (according to the risk in each area of the financial institution), and that training is properly documented. To verify the training provided to the institution's staff, it is recommended that the supervisor have access to the course syllabus, tests, certificates, as well as the contracts with organizations or individuals who provided the training sessions.
- Special attention must be given to the training of the financial institution's Compliance Officer. In this respect, the supervisor may conduct interviews to verify the level of training acquired by the Officer.
- The supervisor will need to control the existence of a Training Plan, its compliance, and the staff approving the courses. In this regard, the supervisor must control that the financial institution develops ongoing staff training programs, covering current applicable regulation, internal policies, the institution's systems and procedures. The institution should also have a system to evaluate the training provided to employees. The supervisor should review the methods used by the institution to communicate its policies, verifying that all staff has access to them.
- The supervisor should review whether the training plan includes all staff, the frequency of training (it should be at least annual), and if the institution has training tailored towards new staff (an initial training must be provided to new personnel), compliance staff, operations staff, or front-line staff members directly dealing with the public.

Regardless of the above, the supervisor may consider the possibility of testing or holding interviews with staff members (of any of the areas of the financial institution) in order to verify the degree of training on AML/CFT matters.

A.v) Products - New Technologies – Distribution Channels and Channels to Acquire New Customers

The supervisor must understand the operation and scope of the products offered by the financial institution. The supervisor must require institutions to conduct an internal assessment/control of the products offered, performed and documented by the compliance area. This assessment must be reviewed by the supervisor.

The supervisor must determine the level of risk entailed by the offered products. To achieve this, the supervisor shall conduct a comprehensive assessment covering the following aspects:

- Inherent risk of the product and/or service.
- Characteristics of the customers that have access to these products and services.
- Areas or regions where the product is offered.

Thus, products will be assigned a risk level based on: i) the risk of the service in itself; ii) the risk of customers accessing the service; and iii) the geographical risk associated to the service.

Once the risk of a product is determined, the supervisor should ensure that the institution treats the product according to its risk level.

1. New Technologies

The supervisor should verify that the financial institutions adequately control ML/TF risk related to the use of new technologies. To do this, the supervisor must control that the financial institution performs the following tasks:

- Identify, assess, measure and control the ML/TF risk that may arise in relation to the development of new products and services based on new technologies, prior to the launch of such products.
- Monitor the use of products and services with new technologies.
- Control transactions that do not require the physical presence of customers (considering aspects such as: relevant amounts, recurring originators and/or beneficiaries, etc.).

The supervisor must have appropriate human and material resources to understand and analyze the products related to these technologies, so that supervisors can determine if the risk is properly mitigated by the institution.

*2. Channels to Attract Customers and Distribution Channels**

The supervisor must review the various channels used by the financial institution, in order to assess potential threats. Supervisors must particu-

larly consider the cases where new customers are acquired through third parties; or through the use of non-traditional channels (new technologies).

Customers are considered to be attracted by third parties when the customer is able to access the service provided by the financial institution indirectly, that is, without the need to physically visit the institution.

In these cases, the following aspects must be taken into consideration:

- The supervisor should control the link between the financial institution and the third party (usually by reviewing the contract).
- Supervisors should determine the responsibilities of each party. This is regardless of the fact that the ultimate responsibility lies on the supervised institution.
- The supervisor must ensure that the financial institution is able to control that the third party correctly applies AML/CFT procedures.
- The supervisor must ensure that the financial institution has the necessary tools to monitor the activity of customers managed by third parties.

The supervisor must be able to access and monitor the third party directly, in order to verify whether the third party adequately complies with the procedures established by the institution.

In all cases, the third party is required to verify the identity of customers, as well as their source of the funds (consideration must be given to the possibility of setting thresholds and/or maximum limits to the use of these services).

A.vi) Financial Group and Consolidated Supervision

The supervisor must know the Financial Group to which the financial institution belongs. In addition, the supervisor must know the jurisdictions where it operates, as well as the services it provides.

The supervisor must have access to information that would allow him to evaluate the level of compliance in AML/CFT matters, especially with respect to the group's entities that deal directly with the supervised institution. The supervisor must verify whether the Financial Group applies equivalent measures to those adopted by the financial institution, especially in regard to due diligence measures.

The supervisor must make efforts to exchange information with supervisory authorities in the various jurisdictions in which the entity operates (for example through the signing of Memorandums of Understanding, among other mechanisms).

Countries should consider and promote the possibility of the Supervisor participating in Supervisory Colleges, thus encouraging consolidated supervision[16].

A.vii) Monitoring of Transactions

The institution must monitor its transactions. It is recommended that this study be conducted selectively, covering different periods of time (the seasonality of transactions must be considered, as it could affect the amounts and number of transactions).

The following aspects must be monitored, among others:

- The transactions linked to risk factors (customers, jurisdictions, amounts, products or services).
- Transactions outside a customer's transactional profile, which must be detected through alerts set by the institution (the following point refers to the alert systems). The supervisor must ensure that the institution controls these transactions and that these are duly justified. If the justification is not sufficient, the institution must provide explanations.
- Random customer transactions or selected randomly, which the financial institution considers to be within the customer's profile, in order for the supervisor to verify that in fact this is the case.
- Transactions using new technologies. In particular, the supervisor must control the amounts of the transactions, as well as the accumulated total amount per customer.

16 In regard to this point, it is recommended to follow the recommendations of the Association of Supervisors of Banks of the Americas: *"Best Practices Guide and Recommendations for the Regulation and Supervision of Financial Conglomerates," ASBA, 2011.*

A.viii) Data Processing Tools

The supervisor should evaluate that the data processing system is in accordance with the financial institution's profile, taking into consideration the following aspects:

- Risk the institution is exposed to.
- Transactions conducted through the institution, considering: customers, products, services, geographical areas involved in money transfers.
- Size of the financial institution.
- Complexity of transactions.

The features that the system must satisfy and that the supervisor should assess include:

- Maintain and update, as well as allow data to be consulted regarding the records in each customer identification file.
- Categorize the various types of transactions or financial products that financial institutions offer to their customers or users, based on the criteria set by the financial institution itself, in order to detect potential unusual transactions.
- Detect and monitor transactions conducted in a single account or by the same customer or user.
- Implement an alert system that contributes to the detection, monitoring, and analysis of potential unusual and suspicious transactions, which takes into consideration, at least, the information provided by the customer at the start of the business relationship, the historical records of the transactions made by the customer, the transactional behavior, the average balances and any other parameter that may provide further information for the analysis of this type of transactions.
- Place together in a consolidated database the various accounts and contracts from a single customer, in order to comprehensively monitor and track his balances and transactions.
- Retain historical records of potential unusual and suspicious transactions.
- Serve as a means for the financial institution's personnel to report to the designated internal area about potential unusual or suspicious transactions, in a safe, confidential, and auditable manner.
- Maintain security schemes of the processed information, to ensure the integrity, availability, auditability and confidentiality of the data.
- Execute an alert system for transactions intended to be conducted with individuals linked to terrorism or its financing, or other illegal activities, as well as with politically exposed persons. The supervisor should analyze whether these system alerts are appropriately set. To do this, the supervisor should consider the number of transactions flagged and the institution's response. The supervisor must verify that these are effectively analyzed and dismissed, when appropriate.

A.ix) Reporting

Reporting should be considered from two perspectives. First, internal reporting that meets regulatory requirements (such as regulations on corporate governance and *systematic transaction reports "STR"**). Second, reporting of unusual and suspicious transactions detected by financial institutions.

1. Periodic and Regulatory Reporting

Financial institutions should have adequate information systems in order to prepare management reports appropriate to the nature of the ML/TF risks they are exposed to. These management reports must be structured in accordance to the report recipients. The frequency and contents of these reports shall also depend on the recipients.

Supervisors must review two types of reports:

a) Internal/Operational:
   - ~ Reports related to the institution's corporate governance: periodic reports and evaluations directed to the Board of Directors and Committees.
   - ~ Alert analysis reports.

b) Reports sent to the supervisor.
   - ~ Modifications in senior management.
   - ~ Changes in the internal structure of corporate governance.
   - ~ Internal and external audit reports, and any other required report.

The supervisor must verify that these reports are effectively prepared and that their content corresponds to the actual situation of the financial institution.

The supervisor must also verify that the recipient of the report (in case of internal reports) acts accordingly, when applicable, and in line with the content of the report.

The supervisor must analyze the methodology and procedures to prepare reports to determine whether these are effective. In addition, the supervisor must control that the internal reporting channels work adequately.

In this regard, it is necessary to verify the existence of proper documentation and safeguarding of the reports prepared by the institution.

2. Unusual[17] and/or Suspicious Transactions Reports. Implemented Process

Unusual transactions detected by the financial institution through its alert systems — whether identified by data processing or through monitoring of areas providing customer services— must be reported to the unit responsible for assessing these transactions.

The supervisor should:

- Analyze the adequacy of the reporting system and its correct operation.
- Analyze the internal process for the detection and reporting of unusual and/or suspicious transactions. This process must be adequate and correctly implemented, so that the detected transactions are promptly notified to the person responsible for compliance. The reporting channel must allow employees to send reports directly to the designated area for processing (FIU/ Supervisor) without them being held responsible when senior management does not send reports explaining the reasons for dismissing the identified transactions.
- Review that the process ensures the confidentiality of the final report *(tipping off*)*.
- Identify the key staff members in this process and assess aspects such as: their AML/CFT training; knowledge of the system and channels for reporting unusual or suspicious transactions; and their hierarchical level within the institution.
- Ensure that the individuals in charge of preparing these reports are not conditioned by potential conflicts of interest. For example, that the decision to prepare a report is not influenced by a relationship with the customer (by relationship we refer to business as well as personal relationships).
- Analyze transactions detected by being outside a customer's risk profile, but which the institution decided not to report. The supervisor should evaluate whether the justification for the transaction (reason for dismissal) was appropriate, and if in each case the processes were carried out as established (reporting channel, analysis, decision-making capacity of the person who dismissed the case, among others).

A.x) Independent Review of the ML/TF Prevention System.

1. Internal Audit

The ML/TF prevention system must be assessed on a regular basis by the institution's internal auditor. The internal audit function must have staff with knowledge in this field and their reports must be directly communicated to the Board of Directors or Audit Committee.

The internal auditor is responsible for the ongoing assessment and monitoring of the institution's internal controls and compliance with ML/TF risk management policies. In addition, the internal auditor must follow up on the findings made by the supervisor in previous inspections.

The supervisor must review the internal audit plans to ensure these are sufficient and complete, their scope and the areas covered, among other issues.

The supervisor should also verify the timely correction of the observations made by the audit function.

17 Only when applicable, according to the local regulations in each jurisdiction.

2. External Audit

The supervisor must control that the financial institution's AML/CFT system is reviewed by an independent external auditor. This report must be sent to the supervisor.

Before analyzing the auditor's report, it is recommended for the supervisor to assess whether the external auditor is duly qualified to conduct and evaluation of the institution's policies, systems and procedures to manage the risk of ML and TF. To do this, it is recommended that the Supervisor keep a Registry of Auditors in this field, through which the supervisor can monitor the adequacy and independence of the auditors.

Regarding the report, the supervisor must analyze at least the following aspects:

- Whether the report covers the financial institution's ML/TF risk and whether it assesses the measures established to mitigate this risk.
- Whether it includes a review of the systems used to conduct transactions, as well as the transactions themselves.
- Whether it includes a revision of the procedures for detecting unusual or suspicious transactions, and whether these are adequate and suitable based on the reality and risk of the financial institution.

In case the audit report contains observations, the supervisor must follow up on the measures taken by the financial institution to correct these observations. When applicable, the supervisor should take the appropriate actions (request further information, conduct a limited inspection to confirm the observations, apply sanctions, among others).

The supervisor must consider the possibility of requesting the Auditor to provide the audit working papers, in order to expand the analysis presented in the report.

B) Interviews

If interviews are conducted, they must allow the supervisor to gain an understanding of the financial institution's situation in terms of its activity, as well as the involvement of its staff in ML/TF issues.

It is recommended to have predefined questionnaires to be used as a guide. This implies that the supervisor should be flexible when using the questionnaire, adapting it to the specific case ahead.

The supervisor must set up meetings with staff members responsible for, or involved in, managing this risk, for example: the compliance area, the commercial area, back-office, and the internal auditors, among others.

C) Working Papers

It is recommended that the working papers be stored in digital files, as well as in binders accessible to the supervisory team reviewing this risk. The regulations of each country shall determine how long these files must be kept for.

It is recommended that working papers be kept confidential. Although the conclusions must be shared (and the institution may present justifications), the working papers related to the supervisory process should remain reserved.

IV.5.3. Meeting to Report Findings.

The meeting to report findings is conducted once the inspection is completed.

The purpose of this meeting is for the supervisor to present the financial institution with the findings obtained during the inspection process. The supervisor must determine who should participate in this meeting.

Regarding the participants representing the financial institution, it is recommended that at least one member of the Board of Directors is present, as well as members of the Compliance Committee, the Internal Auditor, and the Compliance Officer.

During the presentation, the supervisor should describe the findings and listen to the opinions and feedback from the institution.

If the institution requires it, the supervisor should consider a granting a reasonable period following the meeting so that the institution can prepare its comments in writing and/or eventually prepare a defense on the observations.

The meeting should be documented through minutes and signed by all participants.

IV.5.4. Final Report

After the meeting to report findings, the supervisor must be able to determine whether the prevention system for ML/TF is effective for the management of risk of the supervised financial institution.

The supervisor must consider the risks identified by the financial institution, as well as the risks identified before and during the inspection.

The objective of the final report is to reflect the situation of the institution in two aspects: a) in regards to regulatory compliance; and b) in regards to the institution's exposure to ML/TF risks.

Therefore, its contents must clearly reflect these two aspects. In this way, the report will be useful for the financial institution as well as for the supervisor.

A) Contents

The final report must include an executive summary of the activities performed, the main conclusions, as well as a detailed report of the findings.

If weaknesses have been found in the implemented AML/CFT system, these must be documented in the final report.

The contents of the report must at least consider the following aspects:

- Whether the AML/CFT system set by the financial institution is adequate for the mitigation of all its risks to which the institution is exposed.
- Whether the Board of Directors and Senior Management are aware of the ML/TF risks facing the institution, and are duly involved in implementing and complying with the prevention system and the applicable regulations.
- Whether the policies and procedures are in line with the regulatory requirements.
- Whether the internal controls are appropriate (monitoring, reporting) for the business (structure, size, complexity, risks).
- The Compliance Officer must have the necessary training and recourses to undertake his/her tasks in line with the risk and size of the financial institution.
- Whether the staff has training, and information about the internal ML/TF policies and procedures.
- If the External Auditor conducts an assessment of the controls set by the financial institution, to determine whether these are adequate for the risks that the institution faces.

If weaknesses are found in the AML/CFT system, it is recommended that these are categorized and rated according to their severity.

This rating must reflect the level of importance that the financial institution must give to correcting these weaknesses (priority/non-priority). Also, the supervisor must establish deadlines for the institution to remedy these weaknesses (the deadlines may be discussed with the financial institution).

B) Findings Letter

Once the final report is completed, a findings letter must be prepared and communicated to the institution in writing, indicating the deadline for the institution to respond (Action Plan as indicated below).

Although the objective of this letter is not to impose sanctions, in case the inspection has identified instances of non-compliance the letter would mention these. It is recommended for the financial institution to be informed that sanctions will be applied as a result of non-compliance[18].

The findings letter must be received by the institution's Board of Directors and transcribed in the Books of Minutes of the Board.

C) Corrective Action Plan

The supervisor must request the financial institution to prepare and submit an action plan to remedy the identified weaknesses.

The action plan must designate a person responsible for the compliance of the plan and include deadlines to remedy each weakness.

This plan must be approved by the supervisor, who may make observations or request modifications.

18 Both the penalty and the sanction process will depend on the internal regulation of each jurisdiction.

IV.5.5. Follow-up

This is the last stage of the inspection process and is part of the ongoing monitoring conducted by the supervisor, which in turn is part of the general supervisory tasks performed on regulated financial institutions (see general monitoring of institutions in the financial system, point IV.3).

A follow-up strategy must be defined in accordance to the severity of the identified observations/ weaknesses.

A) Scope. Tasks to Develop

The financial institution's follow-up must consider two aspects. In the first place, the supervisor must monitor the compliance of the action plan presented by the financial institution. To do this, the supervisor must request progress reports describing the execution of the action plan; the supervisor must have the power to verify these reports through on-site visits.

It is recommended for this monitoring to be reinforced by reviewing both External and/or Internal Audit reports, when necessary, and conducting on-site visits if necessary. The need to conduct specific on-site visits must be considered depending on the severity of the weaknesses detected during the process.

Secondly, the supervisor must conduct a general monitoring of the financial institution as part of the annual supervisory plan. This plan covers the revision of periodic information provided by the institution, the review of audit reports, monitoring media news on the institution, and assessment of any information relevant to ML/TF.

V. GLOSSARY:

- **Basic savings accounts**

These are accounts opened by residents, in which deposits cannot exceed an established amount and the end-of-month balance does not exceed an established limit.

- **Control sub-systems (also known as self-regulatory bodies)**

According to FATF, these entities represent a profession (for example, lawyers, notaries, other independent legal professionals or accountants, etc.), and are made up of members from that profession; these bodies play a role in regulating the persons that are qualified to enter and exercise the profession, and also perform certain supervisory or monitoring functions. For example, it would be normal for this body to enforce regulations to ensure that all persons exercising the profession maintain high ethical and moral standards.

- **Correspondent Banking**

According to the FATF definition, the term correspondent banking refers to a financial institution that provides financial services to another institution.

Large international banks typically act as correspondent banks for thousands of banks worldwide. The respondent banks may receive a wide range of services, including cash processing (e.g. accounts that accrue interests in several currencies), international wire transfers, check processing, payable-through accounts, and foreign exchange services.

- **Customer Due Diligence**

This is a process by which a financial institution obtains, updates, and maintains information about current and potential high-risk customers, as a key component of the ML/TF prevention program.

- **Designated Non-Financial Businesses and Professions (DNFBPs)**

According to FATF, Designated non-financial businesses and professions refers to:

a) Casinos
b) Real estate agents
c) Dealers in precious metals
d) Dealers of precious stones
e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or professionals employed within professional firms. This group does not refer to 'internal' professionals that are employed by other types of businesses, nor professionals working for government agencies, who may already be subject to AML/CFT measures.
f) Trust and Company Service Providers refers to all persons or businesses that provide any of the following services to third parties:
   - ~ acting as a formation agent of legal persons;
   - ~ acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
   - ~ providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
   - ~ acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; acting as (or arranging for another person to act as) a nominee shareholder for another person.

- **Distribution channels and channels to attract customers**

The distribution channels and the channels to attract customers refer to channels used by the institution to attract new customers and initiate a

business relationship with them. For example, some distribution channels include branches, financial correspondents, new technologies, etc.

▪ Enhanced Due Diligence

This is a process by which a financial institution obtains, updates, and maintains additional information than that required during a regular Customer Due Diligence process. This process is usually implemented on current and potential high-risk customers, as a key component of the institution's prevention program for ML/TF prevention program.

▪ Financial Institutions

The term means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

- Acceptance of deposits and other repayable funds from the public.
- Lending.
- Financial leasing.
- Money or value transfer services.
- Issuing and managing means of payment. (e.g. credit and debit cards, checks, traveler's checks, money orders and bankers' drafts, electronic money).
- Financial guarantees and commitments.
- Trading in:
  - ~ money market instruments (checks, bills, certificates of deposit, derivatives etc.);
  - ~ foreign exchange;
  - ~ exchange, interest rate and index instruments;
  - ~ transferable securities;
  - ~ commodity futures trading.
- Participation in securities issues and the provision of financial services related to such issues.
- Individual and collective portfolio management.
- Safekeeping and administration of cash or liquid securities on behalf of other persons.
- Otherwise investing, administering or managing funds or money on behalf of other persons.
- Underwriting and placement of life insurance and other investment related insurance.
- Money and currency changing.

▪ Instructions

Refers to orders and/or indications directed to one or more specifically identified institutions, which are considered binding for the institutions.

▪ Politically Exposed Persons (PEPs)

According to the FATF definition, foreign PEPs are individuals who hold or have been entrusted with prominent public offices in another country, for example a Head of State or Government, high-level politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Domestic PEPs are individuals who hold or have been entrusted with prominent public functions within the country, for example a Head of State or Government, high-level politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Persons who are or have been entrusted with a prominent function in an international organization, refers to members of senior management, i.e., directors, deputy directors and members of the Board or similar functions.

The definition of PEPs does not cover individuals who hold positions in middle management or more junior positions than the categories mentioned above.

▪ Regulations

These are rules that in the legal hierarchy are inferior to the Law, which are issued by competent authorities, with the purpose of detailing the contents of laws.

▪ Shell Bank

According to the definition provided by FATF, shell banks are banks that have no physical presence in the country where they are incorporated and licensed, and are not affiliated to any financial services group that is subject to effective consolidated supervision. The term "physical presence" means

that the headquarters and senior management is located within the country. The existence of a local agent or a low-level staff does not constitute physical presence.

- **Superseding Factors**

In this document, superseding factors refers to changes occurred in a financial institution, after the last supervisory process has taken place.

- **Systematic transaction reports**

These are transaction reports that financial institution systematically prepare in compliance with national regulation. For example, reporting wire transfers that exceed USD$ 1,000; cash transactions in amounts exceeding USD$ 10,000; etc.

- **Tipping – off**

This refers to disclosing the fact that a Suspicious Transaction Report or information about a third party is being delivered.

- **UN and OFAC lists**

This are lists of terrorists and/or terrorist organizations issued by the United Nations (UN) and the Office of Foreign Assets Control (OFAC).

ANNEX I

RISK MATRIX TEMPLATE

RISK MATRIX[19]

	Level of ML/TF Risk	Weighting % (b)	HIGH	MEDIUM	LOW	Total/ Bank (a)
	Inherent Risk factor		3	2	1	
1	High and growing customer base in various geographic areas (H); increase of customer base due to acquisition of other banking institutions (M); customer base stable, with little variation (L). **A growing customer base implies a growing inherent ML/TF risk.**	The weight for each factor must be determined.				
2	Number of branches. **The higher the number of branches, the greater the risk of smurfing (using many people to make small bank transfers), structuring.**					
3	High number of private banking accounts or correspondent accounts offering services to areas considered to be high risk according to reliable international sources (FATF, UN, etc.) (H); Low number of private banking accounts or correspondent accounts from low risk areas (M); Does not offer correspondent banking services and has very few private banking customers (L). **Private banking is considered high risk because of the specialized attention offered to these customers.**					
4	High percentage (>60%) of foreign accounts with high activity of international transfers (H); Moderate amount (30%-59%) of foreign accounts with international transfers (M); Very few foreign accounts (<30%) and with a low volume of international transactions (L). **Banks with many foreign accounts represent a greater risk in monitoring these accounts, as well as the contact with customers.**					
5	High number of fund transfers from **"non-customers (remittances)". The supervisor should determine a threshold amount. This can depend on the number of transfers performed annually by the entity. The supervisor should also determine the percentage of international transfers from remittances.**					
6	High percentage of customers considered high risk, according to the customer's risk matrix (above 40%) (H), medium percentage of high risk customers (20%) (M), low percentage of high risk customers (8%) (L). **The higher the percentage of high risk customers, the higher the inherent risk of wrongful use of the services provided.**					

19 This Risk Matrix applies for assessing the institution's inherent risk, given that the controls put in place by the institution must be incorporated to assess the residual risk.

	Level of ML/TF Risk Inherent Risk factor	Weighting % (b)	HIGH 3	MEDIUM 2	LOW 1	Total/ Bank (a)
7	High amounts of cash transactions (H), moderate amounts of cash transactions (M), low amounts of cash transactions (L). **Banks with high movements of cash represent a high money laundering risk given that this type of transactions are a characteristic seen at global scale.**					
8	High volume of transfers with geographical areas considered high-risk according to reliable sources (H), medium volume of transactions with high-risk geographical areas (M), low volume of transactions with geographical areas considered to be high-risk (L). **Reliable sources that designate high-risk countries are used to determine if a bank has a high number of transactions with these specific countries.**					
9	Banks with branches in border zones, free-trade zones (H), banks with branches in socially diverse metropolitan areas (M), banks with branches located in high-income areas (L). **Banks with branches in border zones**					
10	Banks with manual systems for reporting cash (SQL) and monitoring transactions (H), automatic systems for reporting cash transactions, but without ML/TF monitoring (M), automatic systems for monitoring cash and transactions (L). **Banks that do not have automatic systems represent a higher risk for monitoring unusual transactions.**					
11	Bank with high volume of STR, medium volume of STR, low volume of STR. **The higher the number of STR, the higher the bank's risk appetite. The higher the risk appetite, the higher the probability of ML/TF.**					
12	Very little training, frequency less than once per year (H), only one training in ML/TF per year (M), various trainings in ML/TF per year (L). **Trained staff is aware of the inherent ML/TF risks. Non-trained staff are not aware of such risk.**					
13	High rotation of senior management, as well as staff from the compliance area (H), low rotation of key and compliance staff, but high rotation of key staff in branches (M), low rotation of staff in the whole institution (L). **There is no stability in the compliance area, leading to poor controls and high degree of vulnerabilities.**					
14	High percentage of corporate loans in the lending portfolio (H), moderate percentage (M), low percentage (L). **A high percentage increases the risk of transactions with non-cooperating countries.**					
15	Regional products that allow a customer from a country in which the group operates to conduct transactions in another country in the region. **These products represent a high-risk for the entity, as it does not know the customer and has to trusts that the due diligence procedure has been performed in the country where the individual is customer.**					
x	Other factors	Total weighting must add up to 100%			Total	

- **Low-risk if total sum is between 15-40**
- **Medium-risk if total sum is between 41-71**
- **High-risk if total sum is between 72-100**

The significance given to the weighting may increase the specific risk factor.

REFERENCES:

http://www.fatf-gafi.org/

Caribbean Financial Action Task Force (CFATF)

http://www.cfatf.org/

Council of Europe - Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)

http://www.coe.int/t/dghl/monitoring/moneyval/

Middle East & North Africa Financial Action Task Force (MENAFATF) http://www.menafatf.org/

OFAC issues a list of countries with sanctions for various reasons, including drug trafficking, and ML/TF. This list can be found at:

http://www.treas.gov/offices/enforcement/ofac/programs/

The United Nations issues a list of countries that have been given sanctions, embargoes or similar measures. This list can be found at:

http://www.tid.gov.hk/english/import_export/uns/uns_countrylist.html

Members of the Working Group

Comision Nacional Bancaria y de Valores, Mexico
Mrs. Paulina Morfin Cedeño
(President of the Working Group)

Superintendencia de Bancos e Instituciones Financieras, Chile
Mrs. Jessica Bravo Perea

Superintendencia de Bancos y Seguros, Ecuador
Mr. Galo Díaz Gómez

Federal Deposit Insurance Corporation, United States of America
Mrs. Lisa Arquette

Financial Action Task Force / Bank of Jamaica
Mrs. Maurene Simms

Superintendencia de Bancos y de Otras Instituciones Financieras, Nicaragua
Mrs. Jacqueline Gómez Guerrero

Superintendencia de Bancos, Panama
Mrs. Marisol Sierra Vargas

Superintendencia de las Instituciones del Sector Bancario, Venezuela
Mr. Lucas Martín Serrano

Consultant

Mr. Leonardo Costa Franco

Technical Secretariat

Ms. Pamela Afcha Mallo
Mr. Ricardo Toranzo Gutiérrez

General Secretariat

Association of Supervisors of Banks of the Americas
Mr. Rudy V. Araujo Medinacelli

MISSION

Contribute to the strengthening of bank regulation and supervision and financial system stability in the Region by actively sharing information and disseminating knowledge; providing support and services that lead to increased technical capacity and leadership; supporting the adoption and implementation of sound supervisory practices; and promoting timely and relevant international dialogue.

OBJECTIVES

a. Promote and maintain close communication among the Association's Members, in order to facilitate co-operation among them, and to promote the improvement of their respective capabilities;
b. Provide its members with a high-level discussion forum for the exchange of information, ideas, techniques, experiences and knowledge over their scope of competence;
c. Promote and carry out research and analysis on financial regulation and supervision as well as financial stability;
d. Organize and conduct systematic and permanent training programs as well as technical cooperation amongst its Members;
e. Promote cooperation and exchange relationships with non-member bank supervisors, with financial standard setting institutions, with international and multilateral technical cooperation institutions, with other organizations with similar objectives and with organizations representative of the supervised entities; and
f. In general, to carry out every activity related to its purposes.