TABLE OF CONTENTS

1. OBJECTIVE

1.1 GENERAL OBJECTIVE

Establish the methodological guidelines, roles, and responsibilities of the key actors for the Risk Management of Money Laundering, Terrorist Financing, and Financing of the Proliferation of Weapons of Mass Destruction (hereinafter ML/TF/FWMD).

1.2 SPECIFIC OBJECTIVES

- Guide entities in the definition and possible standardization of the rating criteria and methodologies that allow Grupo Aval to homogeneously consolidate their information.

- Empower entities' compliance units to lead the process of standardizing ML/TF/FWMD risk management.

- Define, share and adopt best practices to be implemented by entities, so that they are consistent with international recommendations such as the "Adequate management of risks related to money laundering, proliferation of weapons of mass destruction and terrorist financing" proposed by the Basel Committee (Bank for International Settlements – BIS), and those of other international organizations.

- Follow international guidelines and best practices, Grupo Aval guides its obligated and non-obligated entities so that within their policies, standards, processes and controls associated with the risk of money laundering and terrorist financing, they apply the recommendations issued by the Financial Action Task Force (FATF).

2. SCOPE

Ensuring the application of this policy is the responsibility of the Corporate Vice Presidency of Risk and Compliance of Grupo Aval, however, as it is a process inherent to the operation of the different business units of the organization, it is the responsibility of Grupo Aval and its subordinates to know, abide by and apply the guidelines established in this document, in accordance with the particular characteristics and regulations applicable to each of them.

3. GENERAL GUIDELINES

3.1 POLICIES

Grupo Aval has adopted the following policies on which the Money Laundering and Terrorist Financing and Financing of the Proliferation of Weapons of Mass Destruction Risk Management System (ML/TF/FWMD) of Grupo Aval and its subordinate entities is based and structured. Such policies are expressions of management for a fair and transparent presentation and assessment of such risks in the financial statements and other disclosures of Grupo Aval's Administrations and subordinate entities. This allows for an adequate identification of the controls that reasonably mitigate the identified risks.

3.1.1 General

- **Adopt and maintain a strong culture of ML/TF/FWMD risk.**
  Grupo Aval's management and its subordinates must take the lead in establishing a strong culture of risk management of Money Laundering and Terrorist Financing and

Financing of the Proliferation of Weapons of Mass Destruction. It must be guided and supported by appropriate guidelines and incentives for the professional and responsible behavior of all members of the entities. In this regard, it is the responsibility of each administration to ensure that there is a strong culture of ML/TF/FWMD risk management throughout the organization.

- **Implement and maintain a "ML/TF/FWMD Risk Management Framework".**
  Grupo Aval and its subordinates must develop, implement and maintain a framework that is fully integrated with their overall risk management processes. Within the frameworks established for risk management are: NTC ISO 31000:2018 Standard, SWOT Analysis and PCI Internal Capability Profile, selected by a variety of factors, including their nature, magnitude, general acceptance by both national and foreign regulatory bodies.

- **Ensure the Administration and Management of the ML/TF/FWMD Risk Management System.**
  Boards of directors and/or audit committees must establish, approve, and periodically review the "Money Laundering and Terrorist Financing Risk Management Framework." They must also supervise management to ensure that policies, processes, and systems are effectively implemented at all levels of decision-making.

- **Zero tolerance for the crime of Money Laundering and Terrorist Financing and Financing of the Proliferation of Weapons of Mass Destruction.**
  Entities must be committed to a "zero tolerance" policy against the crime of Money Laundering and Terrorist Financing and Financing of the Proliferation of Weapons of Mass Destruction, which promotes a culture of fighting it and allows them to conduct their business and operations with high ethical standards, in compliance with current laws and regulations.

- **Commitments of the Administration**
  The management of the entities must develop for the approval of their boards of directors, a clear, effective and robust management structure with well-defined, transparent and coherent lines of responsibility. The administrations of all entities are responsible for their consistent implementation and for maintaining throughout the organization policies, products, activities, processes and systems for the adequate management of the risk of ML/TF/FWMD.

- **Model of the three lines**
  Entities must structure the functions and responsibilities for the ML/TF/FWMD, and in general for all risks, following the methodology of the three lines, i.e., considering (i) management by the line of business, (ii) an independent ML/TF/FWMD risk management function, and (iii) an independent review, as established in the Framework for Integrated Risk Management.

  - **First Line**
    The first line is made up of the operational areas that manage the business (e.g. activities facing the public and in direct contact with customers). This means that ML/TF/FWMD risk governance recognizes that first line management is responsible for identifying, assessing, managing, and controlling risks inherent in the products, activities, processes, and systems for which it is responsible. This line must know and apply the policies and procedures, as well as have sufficient resources to effectively carry out these tasks.

- **Second Line**
  The second line assigns responsibilities to the unit led by the Compliance Officer in the obligated entities and the SARLAFT leader (or whoever takes his place) in the non-obligated entities, which must continuously monitor compliance with all ML/TF/FWMD Risk obligations by his entity. This involves validating compliance with regulations and analyzing anomaly reports so that they can communicate them to senior management or the board of directors and/or the audit committee of the entities. To this end, it must question the business areas using appropriate ML/TF/FWMD risk management tools, carrying out risk measurement activities and using ML/TF/FWMD risk information systems. The Compliance Officer in the obligated entities or the SARLAFT Leader (or whoever takes his place) in the non-obligated entities must be the contact for all issues in this matter of the internal and external authorities, including the supervisory authorities or the financial intelligence units (UIAF) or the jurisdictional authorities.

- **Third Line**
  The third line plays an important role in independently assessing the entity's ML/TF/FWMD risk management and controls, as well as the entity's processes and systems, reporting to the audit committee or a similar oversight body through periodic assessments of the effectiveness of compliance with the policies and procedures for the management of ML/TF/FWMD Risk. Those areas (usually internal audits) that must perform these reviews must be competent and properly trained and not participate in the development, implementation and operation of the risk/control structure. This review may be conducted by the audit or by personnel independent of the process or system being examined, but may also involve appropriately qualified external actors.

3.1.2 Risk identification and measurement

Administrations must ensure the identification and assessment of the ML/TF/FWMD risk found in all processes, products, activities and systems, considering the main activity of the entity, its structure and its regulatory scope (obligated or non-obligated subject), for the identification of inherent risks.

3.1.3 Control and mitigation

In the management and administration of SARLAFT/SAGRILAFT adopted by the entities, prevention and control measures must be applied to prevent them from being used as instruments for the concealment, handling, investment or use in any form of money or other assets, derived from criminal activities or intended for their financing, or to give the appearance of legality to criminal activities or related transactions and funds, thus ensuring an adequate control environment, structured through policies, processes, systems, internal controls and adequate monitoring of the effectiveness of control measures in terms of ML/TF/FWMD risk.

3.1.4 Monitoring

Entity management should implement a process to regularly monitor ML/TF/FWMD risk profiles and exposures to material losses associated with fines or penalties. Adequate information flows must be established to support the proactive management of ML/TF/FWMD risk by the different actors in the model.

3.1.5 Business flexibility and continuity

Entities must have the capacity for business adaptation and continuity plans to ensure the ability to operate in the face of material and/or reputational impacts and, in the event of events that call into question the ordinary course of business.

3.1.6 Report

- **Disclosure**
  Public information on entities should allow stakeholders to assess their approach to ML/TF/FWMD risk management.

- **New products or modification**
  Entities must guarantee prior to the launch or use of any product, the use of new business practices, including new service delivery channels and the use of new technologies or technologies in development for new or existing products, the modification of product characteristics, the incursion into a new market, the opening of operations in our jurisdictions and the launch or modification of distribution channels.

- **Updating customer information**
  Entities shall carry out the necessary procedures to periodically update the information provided by customers, depending on the level of risk, which may vary due to its nature (address, telephone number, activity, income, origin of resources, shareholders and/or beneficial owners, etc.), or when any concept needs to be clarified by the entity or by the competent authorities. In this way, the entity must maintain an update indicator, and monitor compliance constantly.

  In the case of persons belonging to the riskiest segments, such verification must be carried out at least annually.

  In jurisdictions other than Colombia, the most conservative regulation prevails between the local and the Colombian.

3.1.7 Training

The policies, standards and procedures established by the entities to prevent and control money laundering and terrorist financing, frame their compliance guidelines in this policy, therefore, it is the responsibility of the compliance units or whoever takes their place to ensure the due process of training of employees, as well as to ensure that they are included in the induction processes for new employees. The training may be given in person or virtually.

3.2 CORPORATE ML/TF/FWMD RISK MODEL

This corporate model guides the group's entities in the standardization of methodologies for managing ML/TF/FWMD Risk, ensuring that entities comply with the principles and regulations established by the control bodies of each country and mitigate ML/TF/FWMD risk.

With this model, Grupo Aval entities have the elements to manage ML/TF/FWMD risks in line with good practices, complying with the regulatory framework.

This requirement should be considered as a specific part of the general obligation of entities to have robust Risk Management programs in place to deal with all types of risks, including ML/TF/FWMD risks. In this context, having adequate policies and processes in place requires the implementation of additional effective measures. These measures must also be

proportionate and risk-dependent and informed by the entities' own assessment of ML/TF/FWMD risks (considering their core business and structure). ML/TF/FWMD[1].

3.2.1 Comprehensive system and integration of the components of the Program

The compliance program for the prevention of ML/TF/FWMD must allow its components to be related and consistent with each other. The axis that allows the system to be articulated is the risk matrix in which the risks/risk events/causes must be clearly identified, derived from the analysis of the external and internal contexts of each entity, their relationship with segmentation, controls and, finally, warning signs.

Once their contexts have been analyzed, each entity must prepare the segmentation and identify the risks/events/causes that should be input for the risk matrix. In addition, it must understand the causes why one segment represents greater exposure than another. The identification of risks from the context and the definition of segmentations lead the entity to summarize them in what is called the risk matrix, where the exposure to residual risk in each segment is quantified, applying defined methodologies for rating probabilities and impacts, and the effect of having effective controls that mitigate the inherent risk.

Finally, the results of the risk assessment recorded in the matrix help in the definition of the parameters to be calibrated in the transactional monitoring tools, always focused on the highest risk exposures observed in each defined segment.

The following diagram describes the interrelationship between the main components of the system, which allow visualizing the coherence between them:

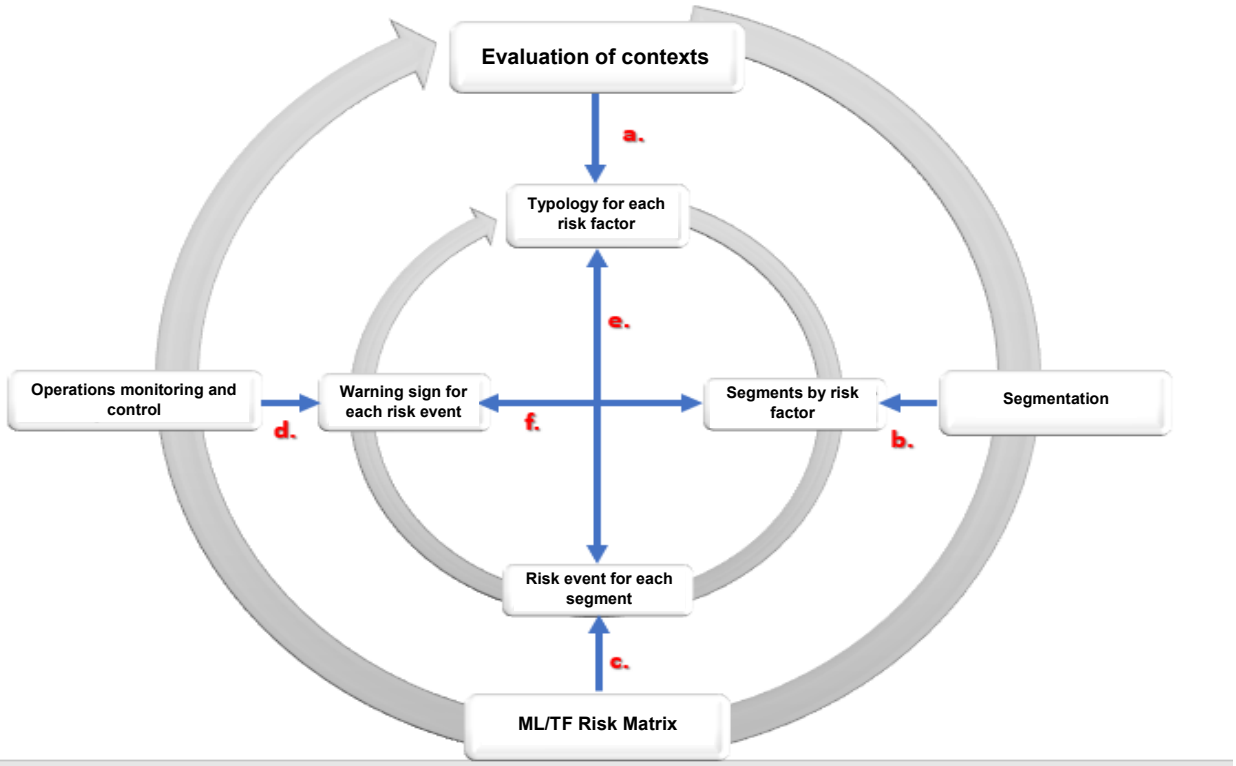


Illustration. Component integration model

[1] Author: Basel Committee on Banking Supervision - Source: "Adequate management of risks related to money laundering

An extension of how the integration of the system components proceeds is detailed in a separate document.

3.2.2 Risk assessment and understanding

3.2.2.1 Risk Management[2]

Sound risk management requires the identification and analysis of ML/TF/FWMD risks present in the entities, and the design and effective implementation of policies and procedures in line with the identified risks.

When conducting a comprehensive risk analysis to assess ML/TF/FWMD risks, entities should consider all relevant risk factors, at national and supranational level where applicable, sectoral, banking and commercial relationship, among other business lines, to determine their risk profile and the appropriate level of mitigation to be applied.

Therefore, know-your-customer policies and procedures, customer acceptance, customer identification and monitoring of business relationships and transactions (products and services offered) should take into account the risk assessment and the resulting risk profile of the entities.

3.2.2.2 Knowledge of the customer engaged by in person and virtual channels

Entities must design, develop and implement due diligence measures to know the people with whom they have civil, commercial or labor relationships based on the qualification of the risk profile.

The knowledge must be based on specific data on operations and transactions and other internal information collected by the entities, as well as on independent external information sources, such as national risk assessments and country reports prepared by international organizations, in accordance with the Instructions – Due Diligence Directive SARLAFT 4.0 and concepts that clarify it. Policies and procedures on customer acceptance, due diligence and ongoing monitoring should be designed and applied to new and old customers engaged through in person and virtual channels, to adequately control those identified inherent risks. Any resulting residual risk should be managed in line with the entities' risk profile established on the basis of their risk assessment3.

When assessing risk, in addition to the guidelines issued by both national and international control entities on the knowledge of the customer4 engaged through in person and nonvirtual channels, entities must take into account the following factors, considering the characteristics and nature of each business:

- The customer's background, occupation (including whether they hold a relevant position in the public or private sector), for enhanced due diligence,
- Their sources of income and wealth,
- Their country of origin and residence (where different),
- The products used,
- The nature and purpose of their accounts,

[2] Principle 15 of the Basic Principles for Effective Banking Supervision, September 2012. As well as Principle 6 of the Principles for enhancing corporate governance, October 2010.
[3] Author: Basel Committee on Banking Supervision -Source: "Adequate management of risks related to money laundering and terrorist financing" -January 2014.- Section II - chapter 1-a).
[4] External Circular 055 of 2016 Finance Superintendence of Colombia Title I Chapter XI Instructions Regarding the Management of the Risk of Money Laundering and Terrorist Financing - Parameters of Know-Your-Customer Procedures.

- Linked accounts, in cases of enhanced due diligence
- Commercial activities, and
- other customer-related risk indicators, to determine the level of total risk and the appropriate measures to be taken to manage those risks.

Those know-your-customer policies and procedures engaged in person and through virtual channels should require basic due diligence with all customers and enhanced or intensified due diligence as the level of risk associated with the customer varies. From the moment of their engagement, the potential customer must have a determined level of risk according to their characteristics and according to this, the corresponding due diligence must be applied. On a recurring basis, entities must monitor the customer to determine the change in their profile and if a change to a high risk occurs, they must have one month to update their data, applying the corresponding due diligence. In case of proven low-risk situations, simplified measures may be accepted, provided that the legislation allows it.

In the development of know-your-customer procedures engaged in person and through virtual channels, the obligated entities, as they have additional information, must comply with the corporate guidelines in accordance with the provisions of the Instructions for due diligence and concepts that clarify it, especially in relation to simplified due diligence in which at least the verification of identity must be done at the time of engagement with the following information: the type of identification document, the name, number and date of issuance of the identification document and request any other information they deem relevant**.** These legal exceptions and those that the law could implement do not exempt the obligated entities from carrying out the knowledge of their customers in accordance with the parameters established in the SARLAFT 4.0 Due Diligence Directive – Instructions, highlighting among the broad related typology, the following (for details refer to the standard):

- Operations carried out with multilateral organizations.
- The constitution of administrative trusts for the payment of pension obligations.
- In capitalization securities placed through mass marketing or network contracts, provided that the payment of the installments is made by direct deposit from a savings account, checking account or credit card, and that the customer has expressly authorized the transfer.
- Various types of insurance, such as those taken out by financial entities, insurance companies or pension fund management companies on behalf of their customers; Those relating to social security; Reinsurance contracts; insurance granted through public tender processes; Those taken through mass marketing or insurance banking provided that the payment of premiums is made through direct deposit from savings account, checking account or credit card, and that the customer has expressly authorized the transfer; Judicial; Health; Funeral policies.
- Savings accounts opened exclusively for the management and payment of pension liabilities.
- In the case of loans that are instrumented through a payroll loan, provided that these do not exceed 6 SMMLV and are granted to employees of companies that are previously engaged as a customer with the supervised entity granting the loan.
- The link to administrative entities of the general pension system in terms of mandatory contributions and severance.
- The link to severance administration entities in relation to the resources from said benefit.
- Savings accounts opened exclusively for payroll. Where other resources are handled in such accounts, this exception does not apply.
- Electronic savings accounts referred to in Article 2.25.1.1.1 of Decree 2555 of 2010.
- Savings accounts with simplified opening procedures.

Where risks are higher, banks should strengthen their measures to mitigate and manage those risks.

Decisions to establish or pursue business relationships with higher-risk customers (high or extreme) require the implementation of enhanced due diligence measures. The customer acceptance policy should also define the circumstances in which the entity does not accept a new business relationship or cancels an existing relationship.

Entities shall have a procedure for identifying and verifying their customers and, where appropriate, any person acting on behalf of them and any beneficial owners, where feasible. In general, entities should not establish a business relationship, or engage in any transaction, until the identity of the customer has been satisfactorily established and verified in accordance with FATF Recommendation 10. In line with Basel Basic Principle 29 and the FATF standards, procedures should also include taking reasonable steps to verify the identity of the beneficial owner. The entity must also verify that anyone acting on behalf of the customer is authorized to do so, and must verify that person's identity.

The identity of customers and beneficial owners, as well as of persons acting on their behalf, must be verified by means of reliable and independent documents, data or information. When using documents, the entity should bear in mind that the best documents for verifying identity are those that are most difficult to obtain illicitly or forge. Where sources of information other than documents are used, the entity should ensure that the methods (which may include checking references with other financial entities and obtaining financial statements) and sources of information are appropriate and consistent with the entity's policies and procedures and the customer's risk profile.

The bank may require customers to fill out a declaration of the identity and details of the beneficial owner, but it should not rely solely on such declarations. As with all elements of the know-your-customer process, the entity should also consider the nature and level of risk posed by a customer when determining the scope of applicable due diligence measures.

Under no circumstances should the entity avoid its customer identification and verification procedures just because the customer is unable to appear for an interview (customers not present). The entity must also take into account risk factors such as the reason why the customer has decided to open an account away from its headquarters or office, especially in another jurisdiction, when it has access to this information.

It is important to consider the relevant risks associated with customers from jurisdictions known for their strategic ML/TF/FWMD deficiencies and to conduct enhanced due diligence when required by the FATF, other international bodies or national authorities.

The first line of the entity must obtain all the information necessary to establish to its satisfaction the identity of the customer and that of any person acting on behalf of the customer and the beneficial owners, in accordance with the legislation in force (e.g. Habeas Data). While the entity is obliged both to identify its customers and to verify their identity, the nature and scope of the information required for verification depends on the risk assessment, including the type of applicant (natural person, legal entity, etc.) and the volume and intended use of the product and/or service requested (CDTs, etc.), savings accounts, loans, money orders, etc.). The specific requirements needed to verify the identity of natural persons are usually set out in national legislation or supervisory regulations or UIAFs. If the amount of the account is substantial, additional identification measures are advisable, which should be determined according to the level of total risk.

However, there are circumstances in which it would be permissible to complete the verification after establishing the business relationship, because it would be essential not to interrupt the normal course of business. In such circumstances, the entity should adopt appropriate risk management procedures with respect to the conditions and limitations under which the customer may use the business or contractual relationship prior to verification, as well as enshrine the requirement that officers put compliance with ML/TF risk management rules before the achievement of business goals.

In situations where the account has been opened, but verification problems arise in the course of establishing the commercial or contractual relationship that cannot be resolved, entities must block access to the product. In any case, the obligated entity should assess whether to proceed with the preparation of a suspicious transaction report (ROS) in cases where there are problems in completing the know-your-customer measures (subject to national legislation on the treatment of suspicious transactions, adequate management of risks related to money laundering and terrorist financing). In addition, where the checks raise suspicions or provide reasonable grounds to suspect that the future customer's assets or funds are derived from offences and crimes under ML/TF/FWMD scenarios, entities should not voluntarily agree to open accounts for those customers. In such situations, entities must prepare a ROS, notifying it to the competent authorities (UIAF), and ensure that the customer is not informed, even indirectly, that a ROS has been, is being or will be prepared.

If an entity has reason to believe that another entity has refused services to an applicant because it suspects unlawful activities of the customer, it should consider the classification of that applicant as high risk and apply enhanced customer and relationship due diligence procedures, the entity, in the case of an obligated entity, must assess whether to proceed with a suspicious transaction report (ROS) and/or not to accept the customer in accordance with its own procedures and risk assessments.

The entity must not open a product or conduct business with a customer who insists on anonymity or who provides a clearly fictitious name, nor should it open confidential numbered accounts, although a numbered account may offer greater confidentiality to the account holder, the account holder's identity must be verified by the entity and known to a sufficient number of employees to facilitate effective due diligence, especially if other risk factors indicate that the customer is a higher risk. The entity must ensure that its internal control, compliance, audit, and other oversight functions, in particular the Compliance Officer in the case of a SARLAFT-regulated or SARLAFT-leading entity (or whoever acts in their stead) in non-regulated entities, as well as the entity's supervisors, have full access to this information if necessary[5].

Finally, each entity must ensure the effective identity of potential customers through in person and virtual channels, at the time of engagement, using information from reliable and independent sources such as digital signature certificates, biometric systems, strong authentication mechanisms, among others.

- **Countries at higher risk**

Stricter and intensified procedures should be established with respect to operations that are entered into with natural and/or legal persons, or assimilated to legal persons, that process or are destined for, are related to or linked to countries where there is no cooperation or where the recommendations of the Financial Action Task Force (FATF) are not applied.

[5] **Source:** For the customer factor, the guidelines set out in the document "Adequate management of risks related to money laundering and terrorist financing" proposed by the Basel Committee (Bank for International Settlements – BIS) (January 2014) have been followed.

3.2.2.3 Customer profile

While the customer identification and verification process takes place at the beginning of the relationship or before a banking or financial transaction is made, the entity must use that information to identify the potential customer and determine their risk profile and the level of due diligence to be applied. The purpose of the relationship or the banking or financial transaction, the volume of assets and the volume of operations of the customer, as well as the regularity or duration of the relationship, are examples of information commonly collected. Therefore, the entity should have due diligence policies and procedures with its customers that are sufficient to develop risk profiles of specific customers or certain categories of customers. The information obtained for this purpose must be determined by the level of risk associated with the customer's business model and activities, as well as the financial products or services demanded by the customer.

These risk profiles facilitate the level of due diligence to be applied to potential customers, establish special monitoring rules and determine the deadline for updating data. Customer risk profiles make it easier for the entity to subsequently determine whether the customer or category of customers poses a high risk and requires the implementation of enhanced ML/TF/FWMD risk management measures and controls.

The profiles must also reflect the entity's knowledge of the purpose and nature of the commercial relationship or occasional banking or financial transaction, the volume of activity envisaged, the type of operations and the sources of funds, income or wealth of the customer, as well as other similar considerations. Any significant information obtained about the customer's activity or conduct should be used to update the entity's assessment of the risk presented by the customer.

The first line in the entity must verify the identification of the customer, as well as any other information and documentation collected as a result of the Customer Relationship Management (CMR) activity. Such information may include copies or records of official documents (such as passports, identity cards, driver's licenses), account files (e.g., records of financial transactions), and business correspondence, including the results of any analyses conducted, such as risk assessments and inquiries made to ascertain the background and purpose of business or contractual relationships and activities and FWMD.

General Know-Your-Customer Policies for PEPs

This category of customers for Grupo Aval entities requires the implementation of particular controls both at the time of engagement, and during the development of the commercial or business relationship, considering that the connotation of PEP suggests some more notable and sensitive risks than those of customers without this attribute. These risks are mainly framed in the possibility or ease of appropriating State resources, embezzling and diverting public funds for private interests or to finance political campaigns, groups outside the law or other structures or forms of association such as foundations, non-profit organizations that have been created with the intention of concealing or giving the appearance of legality to ML/TF/FWMD operations.

Consequently, this requires entities to implement enhanced or intensified due diligence measures when establishing and maintaining business relationships with this category of customers.

For this purpose, it is important to determine the scope of the name of PEPs in Grupo Aval, considering as such the natural persons who are classified as:

- Local PEPs
- Foreign PEPs

It is important to mention that for the categories of PEPs of international organizations and foreigners, officials at intermediate or lower levels are excluded.

Likewise, people who have a conjugal relation, de facto, or de jure with politically exposed national or foreign persons, as well as their relatives up to the second degree of consanguinity, first of affinity and first civil, are classified as PEPs.

The minimum time to maintain the status of PEPs will be tied to the period in which the third party occupies their position and the time after the separation, resignation, dismissal, or any other form of disengagement established in the different regulations that Grupo Aval companies must comply with.

In order to engage a potential customer who has the status of PEP or legal entity whose beneficial owners have the status of PEP, entities must carry out the following due diligence procedures:

- Have mechanisms in place to identify them, such as: Inclusion of this information in know-your-customer and counter-party forms, through the use of questions and self-statements from potential customers about their potential PEP status, the purchase of information from database providers, or the establishment of internal lists through the collection of information for public use, among others.

- PEP quality verification must be carried out prior to the start of the business relationship, to provide for more demanding procedures. Exceptions should not be allowed in the delivery of information and/or documentation by the applicant.

- It will be essential in the engagement process to focus the attention of the commercial team on the origin of the wealth and the origin of the PEP funds, for this each entity must leave a record through verifiable means of the activity, profession or trade from which the resources come and obtain a copy of the income tax return, assets or revenue before the tax authority of the country where he or she resides.

- At the time of engaging a potential customer with PEP quality, an interview must be carried out in person or by digital means, leaving a record of it. For entities obligated by the Superintendence of Companies, it is not required.

- Have senior level approval to continue with the business relationship. For this purpose, each entity must determine the highest level responsible for the knowledge and approval of the PEPs' business relationship.

In addition to applying the normal know-your-customer procedural measures, senior management approval must be obtained for customer engagement or to continue the business relationship, adopt measures to establish the origin of resources; provide for more demanding procedures for engagement; and to carry out continuous and intensified monitoring of the commercial relationship. It should be noted that the concept of senior management does not include the Compliance Officer.

When it is known that a customer or beneficial owner acquires the conditions to be a PEP, under the terms indicated in this policy, they must be marked as such in the systems, request the update of data whenever their level of risks increases, and collect the documents that correspond to this new condition.

The collaborators responsible for managing the commercial relationship with these people must strive to ensure that their information is updated, therefore, the periodicity established for the updating of customers with this condition will be at least annually or earlier if there are circumstances that do merit it.

During the term of the business relationship with a Politically Exposed Person, the owner of the business relationship must monitor the customer's transactional activity to detect warning signs and manage them, especially they must take steps to determine the origin of the funds from such transactions.

For its part, the compliance team of each entity must establish the transactional profile of the PEP customer, carry out special monitoring and/or centralized evaluations of the operations carried out by this type of customer, as well as of legal entities that are commercial companies, trust funds, foundations or other structures where PEPs are linked as beneficial owners or controlling parties.

3.2.2.4 Knowledge of the beneficial owners of structures without legal personality and of legal persons, shareholders and/or associates.

Knowing the current and potential customer in each of the entities implies knowing their identity, for this purpose data must be obtained that allows each of the current or potential customers to be individualized, determine the economic activity carried out by the customer and that constitutes the origin of their funds, as well as establish the origin and volume of the funds of which the customer is the owner.

The identification of the beneficial owner who directly holds more than 5% of the share capital, contribution or participation of the potential customer in structures without legal personality and of legal entities, as well as of the shareholders and/or associates of legal entities or other structures of a similar nature, must be carried out to the extent that due diligence allows, so that the entity is satisfied that the beneficial owner is known and that it meets the characteristics included in the definition.

The knowledge of the beneficial owners of structures without legal personality and of legal entities, as well as of the shareholders and/or associates of legal entities, must be obtained in the procedures for engagement and updating customers or in those cases where, due to risk monitoring, the need to update such information is detected as part of the enhanced due diligence actions.

Entities may have the tools, forms or questionnaires they consider necessary to identify the beneficial owner of their customers, legal persons or similar structures. In the case of companies in Colombia with the following structures: Limited Partnership, Sole Proprietorship and Limited Liability Companies, the information of the beneficial owners may be obtained from the certificate of existence and legal representation in force for the company. For those types of companies where such information is not available, it may be requested from the customer or obtained through public or private sources after a risk analysis of the integrity and reliability of said source.

If the entities have doubts about the veracity of the information declared in the forms, they may apply reasonable measures for such identification that allow more information to be obtained. Likewise, it must establish measures in accordance with the information obtained that determine if the beneficial owner is a Politically Exposed Person, in which case they must adopt measures to establish the origin of the wealth and the origin of the funds of the latter

and thus, necessarily apply intensified continuous monitoring and according to the exposure to risk carry out due diligence.

In the case of Legal Entities such as Trusts, Private Foundations, Non-Profit Entities, whose beneficial owners cannot be identified by corporate participation, a minute or statement signed by the customer's representatives must be obtained, detailing the beneficial owner or owners.

In order to engage entities with complex corporate structures, i.e., those that have multiple legal structures in their direct and indirect composition, and generate opacity or difficulty in obtaining information from the natural persons who hold ownership or control of the company, it will be necessary to obtain satisfactory evidence on the identity of the beneficial owners of said companies. Such evidence is understood to be those public or private documents of incorporation where their names and identification numbers are visible or, failing that, the delivery of a written certification from the beneficial owner of their ownership in the entity and its controlling shareholders.

In those cases in which the information cannot be obtained by a public or private document, because the customer reserves such information for objective reasons and the owner of the commercial relationship accounts for very particular situations of the customer (i.e. personal security reasons, etc.), this information must be documented and obtained by any other verifiable means. In the latter case, approval must be obtained from a higher-ranking collaborator defined by each entity, who will make the decision on the potential customer's engagement after consulting their risk profile.

In the case of legal entities or similar structures where the final or controlling beneficiary cannot be definitively identified through other means; and only when a natural person is not identified, the entities may consider obtaining the information of the natural person who holds the legal representation and management of the company. However, potential legal entity customers who:

- Aspire to be part of banks or mass or retail segments, that is, when they do not have the quality of corporate or business customers.
- Intend to acquire products in foreign currency or others classified as high risk by the entity.
- Have been classified in the engagement process as customers with a High ML/TF/FPWMD risk profile.
- Are companies or corporate vehicles that involve beneficiary companies in different countries, generating difficulty in following the traceability of money and the availability of information.
- Have a constitution time of less than one (1) year.

If the potential customer or owner of the majority interest is a company listed on the Colombian Stock Exchange and/or other stock exchanges that do not correspond to High Risk jurisdictions, and is subject to availability of information and disclosure requirements, which lead to ensuring adequate transparency of the beneficial owner or is a majority-owned subsidiary of a company, may be exempted from the delivery of the beneficial ownership information, and consequently it will not be necessary to identify and verify the identity of their beneficial owners, since the relevant identification data if required during the business relationship may be obtained from a public registry of the customer or from other reliable sources. In other words, this does not mean that listed companies do not have to identify their beneficial owners, but that they are assumed to already do so and that information about them is already available elsewhere.

In no case will companies with bearer shares or whose shareholding composition includes associates who issue bearer shares or with the possibility of issuing bearer share certificates, as well as companies that allow shareholders or nominal directors, be accepted as customers. In that case, it will be necessary to require them to disclose that they are nominal, and the identity of the person who nominated them, keeping that record. Nor are they susceptible of engaging Shell Banks as customers.

In the case of legal structures, such as cooperatives; employee funds; foundations; NGOs and the like, the people who occupy a position in senior management must be identified, without prejudice to identifying the founders or managers and the main donors or contributors.

Regarding trusts, it is necessary to understand the structure of the trust business, who holds the status of settlor, who is the contributor and the beneficiary of the funds of the trust business.

For the identification of the beneficial owner of structures without legal personality, the know-your-customer procedure involves identifying and taking reasonable steps to verify the identity of the beneficial owners.

3.2.2.5 Internal and external context of entities

The entities of the group must establish their internal context in accordance with the theoretical framework established by Grupo Aval in terms of the ISO 31000:2018 Standard, SWOT Analysis and the evaluation of the Internal Capacity Profile – PCI, whichever generates the most value to the Entity in its expert opinion; likewise, the evaluation of the external context is carried out by Grupo Aval in a transversal way for all the entities that are part of the group. Entities must complement the evaluation of the previous contexts by considering the particularities of their operation.

The internal and external context is optional for obligated entities and those not obligated by the Superintendence of Companies, since it is not required as a rule.

3.2.2.6 Information management

3.2.2.6.1 Record keeping

- The entity must ensure that all required information is recorded in the context of the know-your-customer system and must include:
  - The registration of the documents provided to the bank when verifying the identity of the customer or the beneficial owner, and
  - the transcription in the entity's own IT systems of the relevant Customer Due Diligence (CDD) information contained in such documents or obtained by other means.

- The entity should develop and enforce clear rules on the records that must be maintained to document due diligence performed on customers and individual transactions. These rules should take into account any regulated privacy measures.

- They must include a definition of the types of information and documentation in the records, as well as the period of retention of these physical records, which must be in accordance with legal and regulatory requirements, from the termination of the commercial or contractual relationship. After this time, its electronic reproduction must be guaranteed.

- Even if accounts are terminated, in the event of an ongoing investigation or litigation, all records must be retained until the closure of the proceedings or in accordance with legal and regulatory requirements. Keeping complete and up-to-date records is essential to enable the entity to monitor its relationship with its customer, to understand the customer's recurring business and activities and, if necessary, to provide an audit trail in the event of disputes, legal action or inquiries or investigations that could lead to regulatory action or criminal prosecution.

- Adequate records should be maintained documenting the assessment process related to the ongoing analysis and monitoring and the conclusions drawn, so as to demonstrate the entity's compliance with the know-your-customer requirements and its ability to manage ML/TF/FPWMD risk.

3.2.2.6.2 Updating Information

Entities must ensure that the records maintain their reliability, validity and periodic relevance and that the information is updated with Customer Due Diligence. Other competent authorities, law enforcement agencies or financial intelligence units may make effective use of that information to carry out their own functions in the context of ML/TF/FPWMD. In addition, keeping information up to date helps the entity effectively monitor anomalous or suspicious activity on products.

3.2.2.6.3 Provision of information to the control entities

The entity must be able to demonstrate to the control entities, at their request, the adequacy of its ML/TF/FPWMD risk assessment, management and mitigation systems; of its customer acceptance policy; of its procedures and policies on customer identification and verification; of its continuous monitoring processes and procedures for reporting suspicious transactions, as well as of all measures taken in the context of the prevention of ML/TF/FPWMD.

3.2.2.6.4 Reporting of suspicious transactions by obligated entities

- The process for identifying, investigating and reporting suspicious transactions to UIAF should be clearly specified in the policies and procedures of the entities and communicated to all staff through regular training programs. These policies and procedures should provide employees with a clear description of their duties, as well as instructions for the analysis, investigation, and reporting of such activities within the entity, as well as guidelines on how to make such reports.

- Procedures should be in place to assess whether the entity's regulatory obligations under the suspicious activity reporting regimes require reporting the transaction to the UIAF and/or the competent supervisory authorities, if applicable. These procedures should reflect the principle of confidentiality (at least legal confidentiality), ensuring that the investigation proceeds quickly and that reports are prepared and notified in a timely manner, incorporating the information. The Compliance Officer should seek prompt notification when funds or other assets are suspected to be derived from criminal activity.

- Once an account or relationship is suspected, in addition to reporting suspicious activity, the entity must ensure that timely measures are taken to adequately mitigate the risk of the entity being used in criminal activities. These measures may include reviewing the risk rating of the customer or account or the relationship as a whole. Appropriate action may require moving the matter in question to the appropriate decision-making level to determine how to manage the relationship, taking into account any other relevant factors, such as cooperation with the authorities.

3.2.2.7 Asset blocking

- Terrorist financing has similarities with money laundering, but it also shows singularities that entities must take into account: the funds used to finance terrorist activities can come from criminal activities or from legal sources and the nature of the financing sources can vary depending on the type of terrorist organization. In addition, it should be noted that the amounts of transactions associated with terrorist financing can be very small.

- The entity must be able to identify and comply with the decisions to block funds adopted by the competent authority and under no circumstances must it maintain relationships with designated entities or individuals (e.g., terrorists, terrorist organizations), in accordance with the relevant national laws (Colombian and countries where subordinate entities are held) and the applicable American legislation related to money laundering and terrorist financing.

- Customer Relationship Management (CRM) must allow the entity to detect and identify possible terrorist financing transactions, providing a more accurate knowledge of its customers and the transactions they carry out. When developing its customer acceptance policies and procedures, the entity must refrain from business relationships with entities or individuals linked to terrorist groups. Before establishing a business relationship or engaging in an occasional transaction with new customers, the entity must check whether they are listed on known or suspected terrorist lists published by the competent authorities (national and international). Similarly, ongoing monitoring should verify that current customers are not listed in those same listings.

- All entities must have systems in place to detect prohibited transactions (such as transactions with entities designated in the relevant UN Security Council Resolutions (UNSCR) or in national sanctions lists). Terrorist detection is not a risk-sensitive due diligence measure, so it should be performed regardless of the risk profile attributed to the customer. To detect terrorists, the entity may adopt automatic detection systems, but it must ensure that these systems are fit for purpose[6].

3.2.2.8 Use of another bank, subordinate financial entity of Grupo Aval to perform customer due diligence

In some countries, entities are permitted to use other banks, financial institutions or other entities to perform customer due diligence without exempting the entities from liability. These mechanisms can take a variety of forms, but in essence, they usually involve one of the following situations:

Reliance on third parties:

a. Identify the customer and verify their identity using reliable and independent documents, data or information.

b. Identify the beneficial owner to the extent possible and take reasonable steps to verify their identity, so that the financial entity is satisfied that it knows who the beneficial owner is. In the case of persons and legal structures, financial entities must understand the customer's ownership and control structure.

[6] Author: Basel Committee on Banking Supervision Document: Adequate management of risks related to money laundering and terrorist financing- Chapter 5 and 6-January 2014.

When they rely on another bank or financial institution to practice certain aspects of CDD, entities must assess the reasonableness of that resource. In addition to ensuring the existence of legal capacity to formalize the resource, the relevant criteria for its evaluation include:

a. The bank, financial entity or other entity (as permitted by national law) used must be as closely regulated and supervised as the bank, use comparable requirements for consumer identification during account opening and have a prior relationship with the customer who opens an account with the bank.

b. The bank-entity and the other entity must formalize in writing an agreement or pact recognizing the bank-entity's resource to the processes with Due Diligence with the Customer of the other financial entity.

c. The entity's procedures and policies should document that resource and establish appropriate controls and procedures for evaluating that relationship.

d. A third party may be required to certify to the entity that it has implemented its ML/TF/FPWMD risk management program and that it carries out Customer Due Diligence substantially equivalent to that of the bank or consistent with the bank's obligations.

e. The bank-entity must take due account of unfavorable public information about the third party, such as being subject to coercive measures due to deficiencies or violations in the field of ML/TF/FPWMD.

f. The entity should identify and mitigate any additional risks posed by relying on a multitude of third parties (a chain of resources) rather than maintaining a direct relationship with a single entity.

g. The entity's risk assessment must consider the delivery of resources to third parties as a potential risk factor.

h. The entity must periodically review the other entity to ensure that the other entity continues to perform Customer Due Diligence as thoroughly as the entity. To this end, the entity must obtain all the information and documentation of the Customer Due Diligence from the bank, financial institution or entity to which it resorts and evaluate the due diligence carried out, including its comparison with local databases to ensure compliance with local regulatory requirements.

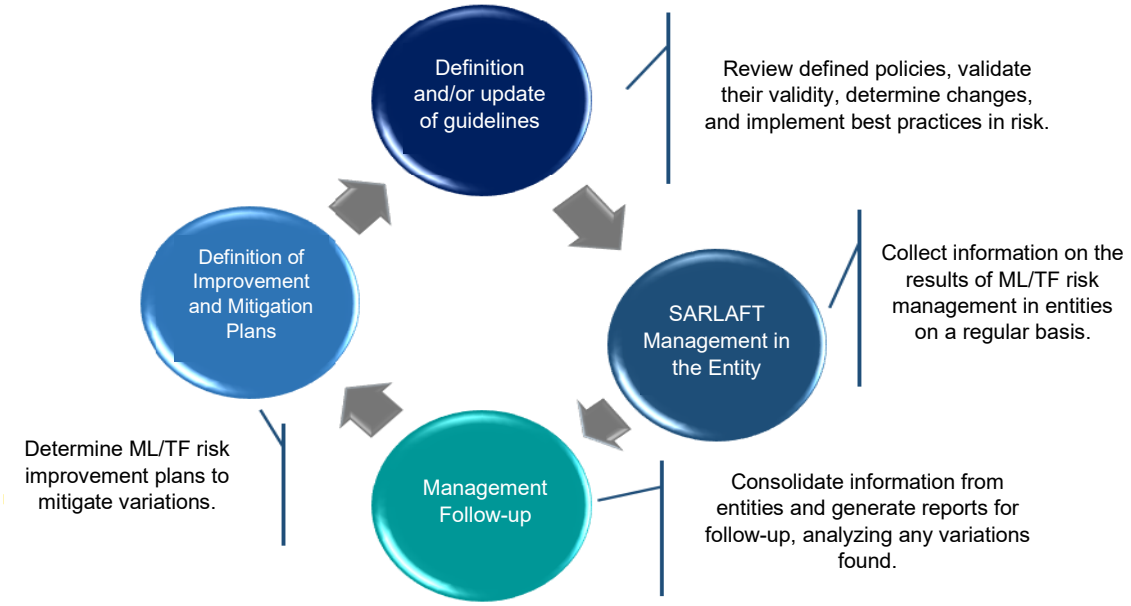
i. Entities must consider ceasing their use of entities that do not carry out adequate Customer Due Diligence on their customers or fail to comply with requirements and expectations.

Banks with subsidiaries or branches outside the home jurisdiction may use the financial group to introduce their customers to other parts of the group. In countries that allow this cross-border use to subsidiaries, entities that entrust the identification of customers to other parts of the group must ensure that the above assessment criteria are in force. It is specified that the FATF40 standards allow countries to exclude country risk from this assessment if the financial entity is subject to group-wide ML/TF/FPWMD rules and supervised at the group level by its financial supervisor[7].

[7] Author: Basel Committee on Banking Supervision Document: Adequate management of risks related to money laundering and terrorist financing- Annex 1.

3.2.3 Stages of the model

The "Corporate ML/TF/FPWMD Risk Management Model" consists of four stages, which are defined to direct and unify the criteria for managing ML/TF/FPWMD Risk in Grupo Aval and its subordinate entities, stages that are related in a cyclical and continuous manner, according to the following diagram:



3.2.3.1 Definition and/or updating of guidelines

The Corporate Vice Presidency of Risk and Compliance of Grupo Aval proposes corporate guidelines aimed at complying with applicable regulations, considering the different jurisdictions and types of entities that make up the Group. Through the ML/TF/FPWMD Corporate Committee, the feasibility of these guidelines is analyzed and best practices to strengthen the system are jointly identified.

3.2.3.2 ML/TF/FPWMD risk management in the entity

Each entity adapts the ML/TF/FPWMD Risk Management model in accordance with the regulations of its industry and jurisdiction, as well as corporate guidelines. When there are changes in the Corporate guidelines, the Compliance Officer in the case of obligated entities or the SARLAFT Leader (or whoever takes his place) in non-obligated entities, guides and executes their implementation within their entity.

3.2.3.3 Management monitoring

Each entity must fill out the SARLAFT Monitoring Reports as applicable, with the information on its ML/TF/FPWMD risk management; these reports are the input to assess in a consolidated manner the risks to which the entities are exposed.

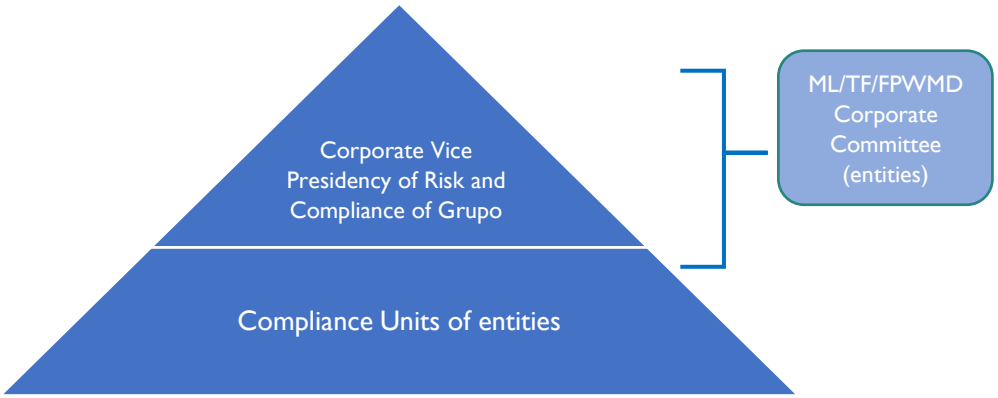
Management information is consolidated and a monitoring report is prepared and presented to the Grupo Aval LAFT/FPADM Corporate Monitoring Committee.

3.2.3.4 Definition of improvement and mitigation plans

Each entity must ensure that a process of continuous improvement of the System is maintained. Grupo Aval, together with the entities through the sessions of the ML/TF/FPWMD Corporate Committee, identify regulatory changes or components of the system that require improvement/modification, to comply with legal requirements and to promote adequate and efficient risk management.

3.2.4 Proper governance mechanisms

The model defines the following actors who participate in the stages of the model and have specific roles.



The participation of the actors in the model has two fronts: in execution and in supervision, according to the detail of the following table of actors and responsibilities:

Actor	Responsibilities	
	Execution	Supervisory
Grupo Aval ML/TF/FPWMD Corporate Committee	• Define the guidelines that they deem appropriate, both for Grupo Aval and for the subordinate entities, for the improvement of the SGR. Validate the Management of the SGR through the consolidated reports that are presented periodically. As a result of this review, it proposes the generation or modification of corporate guidelines that may affect one or all of the entities of the Conglomerate, as required.	• Know the Risk Management carried out by the entities. • Know the risk events in the entities that make up the group and the action plans carried out to mitigate them.
ML/TF/FPWMD Risk Executive Committee entities	• Define the schedule of meetings to be held during the current year. • Hold monthly meetings to report on the latest developments in the ML/TF/FPWMD risk processes in each entity. • Determine and review, when required, the general policies of the model.	• Know the status of risk management for each of the entities. • Review the ML/TF/FPWMD risk methodology established at the corporate level.

Actor	Responsibilities	
	Execution	Supervisory
	• Review regulatory issues that may affect ML/TF/FPWMD risk and make them known for enforcement action. • Establish guidelines for improvement in ML/TF/FPWMD risk processes. • Share good practices used in the market	
Grupo Aval Corporate Vice Presidency of Risk and Compliance.	• Design and maintain ML/TF/FPWMD risk monitoring report formats. • Report the current status of ML/TF/FPWMD Risk Management in the entities to the Audit Committee of Grupo Aval. • Establish guidelines in accordance with the best practices defined in the Committee. • Keep the SGR policies updated in accordance with the guidelines given by Grupo Aval.	• Receive and consolidate information on the different risks of the entities to generate periodic monitoring reports. • Establish deviations from the principles and convene when it deems it necessary to make adjustments.
Compliance areas of the entities	• Submit a Management Report in accordance with the applicability of the requirements, taking into account the main activity of the entity, its structure and regulatory approach (obligated entity quarterly and non-obligated semi-annually). • Participate monthly in the ML/TF/FPWMD Executive Risk Committee entities • Adopt and socialize the best practices received from Grupo Aval.	• Analyze and monitor the entity's daily operations ensuring the application of ML/TF/FPWMD risk.

3.2.5 Actors of the model

3.2.5.1 Responsibilities of Grupo Aval Acciones y Valores S.A.

Ensure the efficient management of the Risk of Money Laundering, Terrorist Financing and Financing for the Proliferation of Weapons of Mass Destruction by its subsidiaries.

3.2.5.2 Responsibilities of Grupo Aval entities

- Manage the ML/TF/FPWMD risk under its sole responsibility in accordance with the defined internal policies and the applicable regulations in force.

- The entity must continuously monitor all business relationships and transactions, as this is an essential aspect of sound and effective ML/TF/FPWMD risk management. The scope of this monitoring must be based on the risk identified in the risk assessment carried out by the entity in its know-your-customer work. It should strengthen the monitoring of high-risk customers or transactions and maintain cross-cutting surveillance of products or services to identify and mitigate emerging risk patterns.

- All entities must have systems in place to detect unusual or suspicious transactions or patterns of activity (according to their type and size considering the characteristics of their business). When designing scenarios to identify such activities, the entity should consider the customer risk profile developed in accordance with the Due Diligence Directive.

- The entity must implement robust due diligence policies and procedures for customers who are identified as high-risk as detailed in this Policy.

- An entity should ensure that it has integrated information management systems, commensurate with its size, organizational structure or complexity, based on materiality and risk criteria, that provide business units (e.g., relationship managers) and risk and compliance officers (including research personnel) with the appropriate information necessary to identify, analyze and effectively track customer accounts.

  The systems used and the information available must facilitate the tracking of those customer relationships by lines of business and include all available information about that customer relationship, including transaction history, documentation omitted from account opening, and significant changes in the customer's behavior or business profile, as well as anomalous transactions made through a customer account.

- The entity must check its customer database(s) when there are changes in the sanctions lists. The entity should also regularly check its customer database(s) to detect PEPs and other high-risk accounts and perform due diligence on them.

- Prepare the monitoring report on the current status of the ML/TF/FPWMD Risk under the format designed by Grupo Aval, and deliver it one month after the cut-off.

- Financial entities must submit to Grupo Aval, in Excel format, the report on the identification and management of alerted, unusual and suspicious transactions sent to the Finance Superintendence, with the periodicity indicated in External Circular 018 of 2022.

- Manage for consolidated reporting purposes to Grupo Aval the 5 x 5 consolidation matrix, with the risk levels according to the methodology established by Grupo Aval.

- Inform Grupo Aval in a timely manner about risk events that occur and that have a high impact category.

- Follow the guidelines established by the ML/TF/FPWMD Corporate Committee.

- Build public and investor confidence; avoiding being used for ML/TF/FPWMD, ensuring that the reputation, seriousness and transparency of the business is maintained.

- Refrain from doing business with persons (natural or legal) whose ethics are or have been questionable, since their relationship can affect the good image of the entity in the market, exposing the brand and assets.

- Apply the rules against the ML/TF/FPWMD and adopt appropriate controls to avoid sanctions that may be imposed by supervisory and control authorities on financial entities or bank employees.

- With respect to commercial relations and transactions with natural and legal persons and financial entities in countries listed as at higher risk by the FATF, jurisdictions under greater surveillance, the special procedures established by the supervised entities must

contemplate, among other measures, the application of intensified know-your-customer measures and monitoring of those commercial and transactional relationships with natural and legal persons.

- For countries listed by the FATF as high-risk jurisdictions (countries), it should be tended not to have trade relations.

- Comply with the other obligations established by law in accordance with their industry, jurisdiction and supervisory entity.

3.2.5.3 AVC responsibilities

AVC is the technological support of the electronic channels of Grupo Aval's banks, since it has a central data processing system, which allows it to support the financial operations that are carried out through them and can analyze the transactions made by users, being the provider of information to the banks and to the UIAF at the time it is required.

For this reason, AVC in its ML/TF/FPWMD risk model must:

- Track international card transactions through this channel, identifying unusual behavior according to the transactional level of bank users.

- The AVC Compliance Officer must report suspicious transactions to the compliance officers of the relevant entities (as required) and to the UIAF, as the case may be, for such action as they deem necessary.

- Report to Grupo Aval banks the transactions made during the immediately preceding month by debit and credit cards issued by Grupo Aval banks, within the first ten days of each month, in the amounts determined for this purpose.

- Report to the control entities (committees, board of directors, etc.) the statistics of the ROS reported to the UIAF.

3.2.5.4 Roles and responsibilities of the Board of Directors and/or Senior Management

- Effective ML/TF/FPWMD risk management requires appropriate governance mechanisms. In particular, the requirement for the Board of Directors and/or Audit Committee to approve and monitor policies on risk, risk management and compliance is entirely relevant in the context of ML/TF/FPWMD risk. The Board of Directors and/or the Audit Committee must have a clear understanding of the ML/TF/FPWMD risks. Information on the ML/TF/FPWMD risk assessment should be communicated to the Board of Directors and/or Audit Committee in a timely and complete, understandable and accurate manner, in order to enable it to make informed decisions.

- The Board of Directors should allocate explicit competencies with real regard to the governance structure of the entity to ensure the effective management of policies and procedures. The Board and/or senior management shall appoint a Compliance Officer for obligated entities or a SARLAFT Leader (or whoever takes his/her place) for non-obligated ML/TF/FPWMD entities with adequate preparation to assume the general competencies of that function and with the necessary status and authority within the entity

so that the issues raised in this policy receive the necessary attention of the Board, senior management and business lines[8].

3.2.6 ML/TF/FPWMD risk at Group level and in a cross-border context

When a financial group such as Grupo AVAL operates in other jurisdictions, solid ML/TF/FPWMD risk management is required, which implies taking into account the legal requirements of the host countries. Given the risks, Grupo AVAL must apply the ML/TF/FPWMD risk policies and procedures in force in accordance with Colombian legislation at the Group level, with consistent application and supervision.

In turn, the policies and procedures in branches and subsidiaries, while taking into account local business patterns and the requirements of the host jurisdiction, should support and be consistent with the general policies and procedures for the entire Group. In cases where the requirements of the host jurisdiction are stricter than those of Grupo AVAL, the Group's policy should allow the branch or subsidiary to adapt and apply the local requirements of the host jurisdiction.

At the Group and subsidiary level, the minimum guidelines established by the Finance Superintendence of Colombia must be followed[9]:

Obligated entities in Colombia that are in the situations provided for in articles 260 of the Code of Commerce and article 28 of Law 222 of 1995 may carry out the engagement of customers through the entity of the Group that establishes a contractual relationship and binds them for the first time, as long as the following rules are complied with:

- The responsibility for carrying out all the necessary steps to confirm and update the information, at least annually, will correspond to the obligated entity that the Group designates for this purpose or, failing that, to the parent company.

- The Group may maintain the design of the single form for customer engagement in physical or digital format, which contains, at least, all the information requirements required in the SARLAFT 4.0 Due Diligence Directive – Instructions, as well as the information required with respect to all the products offered by the Group's entities. Likewise, the form must contain a stipulation in which the customer expressly and unequivocally authorizes its submission to the other entities of the same Group to which it is successively engaged. In any case, it will be up to the entity with which the potential customer intends to engage to determine what information, in addition to the minimum required in the SARLAFT 4.0 Due Diligence Directive – Instructions, must be provided to carry out its engagement.

- The responsibility for updating the additional information to the minimum will be borne by each of the entities with which the customer has a contractual relationship, without prejudice to compliance with the other ML/TF/FPWMD risk regulations.

- It is the permanent obligation of each of the obligated entities that make up the Group to include the modifications and request the additional information that, as a result of the evaluation and monitoring of the risk factors, each of them has determined as relevant and necessary to control the risk of ML/TF/FPWMD.

[8] Author: Basel Committee on Banking Supervision -Source: "Adequate management of risks related to money laundering and terrorist financing" -January 2014.- Section II - chapter 1-b)

[9] External Circular 027 of 2020 Part I Title IV Chapter IV - numeral 4.2.2.2.1.3 Knowledge of the customer in financial conglomerates

3.2.6.1 Global process for managing customer risk

Consolidated ML/TF/FPWMD risk management involves establishing and managing a process for coordinating and implementing policies and procedures for the entire group, which establishes a systematic and comprehensive benchmark for managing the risks of the different national and international operations of the entities. In this context, the design of the policies and procedures outlined in this policy is not only aimed at strict compliance with all relevant legislation and regulation, but also at the more general objective of identifying, monitoring and mitigating risks across the group.

- Every effort should be made to ensure that the Group's ability to obtain and analyze information in accordance with this global policy and procedures is not impaired as a result of changes to local policies or procedures as may be required by local legal requirements. In this regard, the entity must have a robust system for the exchange of information between the parent company and all its branches and subsidiaries. Finally, where the minimum regulatory or legal requirements of the home and host countries differ, the offices or subsidiaries located in the host jurisdictions will apply the strictest rules.

- In the development of know-your-customer procedures, entities are not required to demand the engagement request form or interview the potential customer whenever it is any of the operations, products or services found in the numeral Risk Assessment and Understanding - Know the Customer. In any case, the entities, as they have additional information, must comply with the instructions given by Grupo Aval. These exceptions do not exempt obligated entities from carrying out know-your-customer knowledge in accordance with the parameters established in the SARLAFT 4.0 Due Diligence Directive – Instructions.

- It is also understood that under the FATF rules, if the host country does not allow the proper application of these standards, the Compliance Officer must inform the home supervisors (SFCs).

- It is recognized that the implementation of ML/TF/FPWMD procedures across the Group is more challenging than that of many other risk management processes, given the particularities between jurisdictions in which it operates. For effective group-wide monitoring and for the purposes of ML/TF/FPWMD risk management, it is essential that, without prejudice to appropriate legal safeguards, entities are allowed to exchange information about their customers with their parent companies. This applies to both branches and subsidiaries.

3.2.6.2 Risk assessment and management

The entity should have a thorough understanding of all risks associated with its customers across the group, individually or by category, and should document and regularly update that information, in line with the level and nature of risk in the group.

When assessing the risk associated with a customer, the entity should identify all relevant risk factors, such as customers and users, products, distribution channels and jurisdictions, the use of products and services, and establish criteria to identify high-risk customers. These criteria must be applied throughout the bank-entity, its subsidiaries and branches and in subcontracted activities. Customers who pose a high risk of ML/TF/FPWMD to the entity should be identified using these same criteria across the group. Customer risk assessments should be applied in the same way across the group or at least be consistent with the risk assessment at group level.

Taking into account the differences in risks associated with different categories of customers, the Group's policy should recognize that customers included in the same category may pose different risks in different jurisdictions. The information obtained in the assessment process should be used thereafter to determine the level and nature of the Group's total risk and to facilitate the design of appropriate controls within the Group to mitigate those risks. Mitigating factors may include additional customer information, closer monitoring, more frequent updates of personal data, and visits by the bank's staff to the customer's home.

Compliance and internal audit staff for entities, in particular the Compliance Officer for obligated entities or a SARLAFT Leader (or whoever takes his or her place) for non-obligated entities, should assess compliance with all aspects of their group's policies and procedures, including the effectiveness of centralized CDD policies and requirements to exchange information with other group members and respond to queries from the parent company.

3.2.6.3 ML/TF/FPWMD risk policies and procedures on a consolidated scale

- The entity must ensure that it understands the extent to which the ML/TF/FPWMD risk legislation allows it to use the procedures applied by other banks-entities (e.g. within the same group) when a business is being recommended. The bank-entity should not use presenters who are subject to less stringent rules than those governing its own ML/TF/FPWMD risk procedures. Accordingly, entities should monitor and assess the ML/TF/FPWMD risk standards in force in the jurisdiction of the recommending bank-entity.

- An entity may use a presenter who is part of the same financial group and may consider giving a higher degree of reliability to the information provided by the financial group, provided that the latter is subject to the same rules as the entity and that the application of these requirements is monitored at group level. However, the bank-entity adopting this approach should ensure that it obtains the customer information provided by the recommending entity, as it may be required to submit this information to the UIAF if a transaction involving the referred customer is determined to be suspicious.

- The Group's parent must have access to relevant information to enforce the Group's ML/TF/FPWMD risk policies and procedures. Each office and subsidiary of the group should be able to comply with the minimum ML/TF/FPWMD risk and accessibility policies and procedures applied by the parent company and defined in accordance with the Committee's guidelines.

- Customer acceptance policies, Customer Due Diligence and record keeping must be implemented through the consistent application of policies and procedures across the organization, with precise adjustments to account for differences in risk by business lines or geographical areas of activity. In addition, it is recognized that it may be necessary to use different methods of collecting and retaining information in different jurisdictions to accommodate local regulatory requirements or relative risk factors. However, these methods should be consistent with the group-wide standards outlined above.

- Regardless of its location, each office and subsidiary must establish and maintain effective policies and procedures commensurate with the risks present in the jurisdiction and in the entity. This local monitoring should be complemented by a robust process of information exchange with the parent and, where appropriate, with other branches and subsidiaries in relation to accounts and activities that may pose a higher risk.

- In order to effectively manage the ML/TF/FPWMD risks arising from such accounts, the bank-entities should integrate that information based not only on the customer, but also

on its knowledge of the beneficial owners), the customer and the funds concerned. The entity should monitor on a consolidated basis the relationships, balances and significant activities with customers, regardless of whether the accounts are held on the balance sheet, off the balance sheet, as assets under management or under adequate management of risks related to money laundering, terrorist financing and FPWMD.

- Entities with national and international activity must appoint a Compliance Officer for obligated entities or a SARLAFT Leader (or whoever takes his/her place) for non-obligated entities. This Officer is responsible, as part of overall risk management, for creating, coordinating and evaluating at group level the implementation of a single ML/TF/FPWMD risk strategy (including mandatory policies and procedures and authorization to issue orders to all domestic and international branches, subsidiaries and subordinate entities).

- The role of the Compliance Officer for obligated entities or a SARLAFT Leader (or whoever takes his/her place) for non-obligated entities includes the continuous monitoring of compliance with all ML/TF/FPWMD risk requirements, both national and international, throughout the group. Therefore, the group's ML/TF/FPWMD risk manager should ensure (including by conducting regular on-site visits) that the ML/TF/FPWMD risk requirements are met throughout the group. If necessary, it should be empowered to issue orders or take appropriate action throughout the group.

3.2.6.4 Exchange of information within the Group

- Entities should monitor the coordination of the exchange in accordance with the legal rules for the exchange of information in each jurisdiction. Subsidiaries and branches should be required to proactively provide the parent company with information on high-risk customers and activities that is relevant for the purposes of global ML/TF/FPWMD risk standards and to respond in a timely manner to requests for account information from the parent. The parent entity's rules for the Group as a whole should include a description of the process to be followed in all establishments to identify, monitor and investigate possible anomalous circumstances and to report suspicious activity.

- The entity's Group-wide policies and procedures should take into account issues and obligations related to data protection at local level and to privacy legislation and regulation. They must also take into account the different types of information that may be shared within the group and the requirements for storing, retrieving, sharing/distributing, and disposing of that information.

- The Group's overall ML/TF/FPWMD risk management function should assess the potential risks posed by the activities reported by its branches and subsidiaries and, where appropriate, assess the Group-wide risks posed by a given customer or category of customers. It should also have policies and procedures in place to check whether other branches or affiliates maintain accounts for the same customer (including those of parties related to that customer or within the same group). The parent entity should also have comprehensive policies and procedures in place on account relationships that are considered to be high risk or that have been associated with potentially suspicious activity, including referral procedures and guidelines on restrictions on account activities, including closure where appropriate.

- In addition, the parent company and its branches and subsidiaries must, in accordance with their respective national laws and at the request of financial intelligence agencies, supervisory authorities or other authorized authorities, cooperate with requests for information on customers that they require in their work to combat ML/TF/FPWMD. The

parent bank must be able to require all its branches and subsidiaries to compare their files with certain lists or requests to verify the presence of individuals or organizations suspected of collaborating and instigating Money Laundering and Terrorist Financing and to notify the matches.

- The parent entity should be able to report to its supervisors, upon their request, on its overall customer risk management process, its assessment and management of ML/TF/FPWMD risks, its ML/TF/FPWMD risk policies and procedures on a consolidated scale and its information exchange systems within the group.

- In the case of transnational correspondent relationships, the obligated entities must establish mechanisms that allow them to[10]:

    - Obtain the approval of senior officials before establishing transnational correspondent relationships;
    - Gather sufficient information about the represented establishment that allows them to fully understand the nature of their businesses, including whether it has been subject to sanctions or intervention by the control authority for money laundering or terrorist financing, as well as any other information that allows them to establish a transnational correspondent relationship with transparency for both parties.
    - Determine that the entity has controls in place to prevent and control money laundering and terrorist financing;
    - Document each entity's respective ML/TF/FPWMD responsibilities.
    - Apply stricter procedures for monitoring such relationships.
    - Ensure that the represented establishment complies with know-your-customer measures.
    - The instructions contained in this paragraph must also apply with respect to natural or legal persons who intend to acquire fixed assets of an entity.
    - Comply with any obligation, in accordance with applicable regulation.

- **Securities transactions and insurance activities:** The application of ML/TF/FPWMD risk management controls in mixed financial groups raises additional issues that may be unrelated to deposit-taking and lending operations. Mixed groups should be able to monitor and exchange information on the identity of customers and on their transactions and accounts across the group, and to be vigilant about customers using their services in different sectors.

  Differences in the nature of activities and in the patterns of relationships between banks and customers in each sector may require or justify variations in the ML/TF/FPWMD risk requirements required for each sector. Entities in the financial sector should be aware of these differences when cross-selling products and services to customers from different business units, and appropriate ML/TF/FPWMD risk requirements should be applied to the relevant sectors[11].

3.3 TRANSACTION MONITORING SYSTEM AGREEMENT

3.3.1 Monitoring by entities

Entities must have a monitoring system in place that is commensurate with their size, activities and complexity, as well as with the risks present in the entity. When using a system where

[10] External Circular 055 of 2016 Finance Superintendence of Colombia Title I Chapter XI Instructions Regarding the Management of the Risk of Money Laundering and Terrorist Financing - Know the Customer by Groups.
[11] "Adequate management of risks related to money laundering and terrorist financing" proposed by the Basel Committee (Bank for International Settlements – BIS (January 2014).

information is initiated, processed, reported or stored for the management of ML/TF/FPWMD risk, this system should allow for trend analysis of transaction data to identify unusual transactions.

In particular, this system should be able to provide reliable information to senior management on certain crucial aspects, including changes in the profile of transactions made by customers. The updated, complete and reliable know-your-customer information provided by the customer must be incorporated to prepare the customer profile. The IT system must allow the entity to have a centralized repository of information (i.e., organized by customer, product, group entities, transactions made during a certain time interval, etc.). Without being required to have a single file per customer, entities must rate their customers according to risk and manage alerts with all the relevant information at their disposal. An IT monitoring system should use appropriate parameters based on national and international experience on ML/TF/FPWMD methods and risk management. The parameters used should reflect and take into account the specific risk situation of the entity.

The monitoring system should allow it to determine its own criteria for additional follow-ups, and be a source for the preparation of Suspicious Transaction Reports (ROS) or adopt other measures to minimize risk. The Compliance Officer for obligated entities or a SARLAFT Leader (or whoever takes his/her place) for non-obligated entities must have access to the Monitoring system. The parameters of the Monitoring System must allow the generation of alerts on anomalous transactions, in which case they must also be subject to subsequent evaluation by the Compliance Officer.

The internal audit should also evaluate the Monitoring System and the ML/TF/FPWMD Risk Management System to ensure that it is adequate and that the first and second lines of the Monitoring System and Risk Management System use it effectively and forward the result to the Compliance Officer[12].

3.3.2 Monitoring of Grupo Aval

Grupo AVAL has reporting mechanisms including a dashboard that allow it to know first-hand the risk management at the level of the entities that make it up. The analyses are carried out from the point of view of entities that are obligated by the Finance Superintendence, the Superintendence of Companies and non-obligated entities.

3.4 MANAGEMENT MODEL

The Corporate Management model generally comprises the following phases:

Identification	Measurement	Control	Monitoring
• Entities shall apply the three risks focused on ML/TF/FPWMD • Each of the entities performs identification of causes and controls.	• Risk assessment • Generation of the Group's risk profile	• Improvement plans and their follow-up • Identify controls and assess their design and effectiveness	• Generation of reports of different instances • Share relevant events and best practices • Review of control execution

3.4.1 Risk identification

[12] Source: "Adequate management of risks related to money laundering and terrorist financing" proposed by the Basel Committee (Bank for International Settlements – BIS (January 2014).

Entities shall identify the three risks to be used for:
- Money laundering
- Terrorist financing
- Financing of the proliferation of weapons of mass destruction

It should be taken into account that any inclusion, modification or elimination of the risks set forth above, which arises as a result of the natural evolution of the business and current regulations, must be reported to the Corporate Compliance and SOX Management of Grupo Aval indicating: Risk Reference / Risk / Cause Reference / Cause / Exchange Rate (Inclusion, modification or elimination) / Suggested change / Justification.

3.4.1.1 Segmentation of ML/TF/FPWMD risk factors

Entities that hold the status of obligated entities must segment, at least, each of the risk factors according to the particular characteristics of each of them, ensuring that the defined analysis variables guarantee the achievement of the characteristics of homogeneity within the segments and heterogeneity between them. The segmentation of the risk factors will be included in the risk control matrix, which includes the risk factor, segmentation of the a priori models, segment number and segment detail in accordance with the scope of the standard for Grupo Aval's obligated entities.

3.4.1.2 ML/TF/FPWMD risk events

Its objective is to capture information on the identified risk events, based on expert judgment, on the internal and external context, on information on market typologies and trends and on the evolution of the business itself.

3.4.1.3 Risk analysis

These are the attributes associated with each of the risk events, taking into account the defined causes, ML/TF/FPWMD typologies associated with the risk event, warning signs, which must include at least the internal and external context options for entities obligated by the SFC.

3.4.2 Risk measurement

The measurement model is based on the measurement through Heat maps of the Inherent and Residual Risk of the entities and the Group. Heat maps make it possible to establish the most relevant risks to which entities are exposed, taking into account the criteria of probability and impact. Colorimetry allows prioritizing risks that require immediate attention, and its scales are in accordance with the nature, complexity and volume of the operations of Grupo Aval's entities. Refer to the ML/TF/FPWMD Corporate Risk Management Model.

3.4.2.1 Inherent risk

Inherent Risk is the level of risk inherent to the activity, assuming that there are no controls to mitigate it; that is, the susceptibility that ML/TF/FPWMD events could considerably affect Grupo Aval and its subordinate entities, individually or in aggregate, assuming that there are no internal controls.

It is important to indicate that the analysis and evaluation of the Inherent Risk for each of the ML/TF/FPWMD risks is the responsibility of the owner of the process in validation and accompaniment by the Compliance Officer, but of the process owners. For the assessment

of inherent risk, they are classified into low, moderate, high and extreme categories, according to the Probability of Occurrence (PO) and the Magnitude of Impact (MI).

3.4.2.2 Probability of occurrence

The evaluation of the Probability of Occurrence of the risk materializing without the consideration of the controls is measured with the following scale in both Occurrence and Frequency, where only one of the two criteria must be selected for the evaluation of each risk, the one of greater relevance to the risk evaluated. Thus, each of these two elements is evaluated with a weight of 100%. Both Occurrence and Frequency are rated into five levels between 1, 2, 3, 4 or 5

3.4.2.3 Magnitude of impact

The assessment of risk and each associated cause without consideration of controls is measured with a scale that includes four (4) factors (Legal, Reputational, Operational, and Contagion) that must be rated between 1, 2, 3, 4, or 5. Each factor has a different weight within the magnitude of impact.

3.4.2.4 Residual risk

Identification of key controls

The management (first line) of each entity should assess whether it has controls in place that are designed to adequately manage ML/TF/FPWMD risks. Those controls that effectively and efficiently mitigate risks and causes and are identified as relevant to include in the risk matrices, will be referred to as "key controls". Controls can be of two types: automated or manual and can have two functions: to prevent or to detect.

In any case, the following aspects must be considered for the identification of key controls:

- ✓ A preventive control shall be considered to be one that has the purpose of preventing errors, omissions or irregularities.
- ✓ A detection control will be considered to be one that allows errors to be detected at the time they occur.
- ✓ A preventive control shifts the probability of occurrence since the focus of this type of control is to prevent the risk from materializing.
- ✓ Detection controls will displace the magnitude of the impact, considering that once the risk has materialized, it is necessary to focus on reducing its impact.
- ✓ A control will not be able to mitigate both probability and impact at the same time.
- ✓ For the qualification of controls that are transversal, that is, that are mitigating different risks, it is qualified only once, that is, its effectiveness rating will be the same in all the processes and causes in which it is associated.
- ✓ Controls must be implemented that manage both the likelihood and impact of inherent risk.
- ✓ Once the effectiveness of the control is rated, its rating is averaged to reduce the inherent risk per risk, resulting in the residual risk.
- ✓ Adequate identification and documentation of controls must be carried out, achieving adequate coherence between Risk-Cause-Control.

Control effectiveness evaluation

Grupo Aval and in joint work with the subordinates that participate in the ML/TF/FPWMD Corporate Committee, have defined different factors to carry out the evaluation of the control,

each with a different weighting depending on its effect on the effectiveness of the control. Their rating have defined weights measured through scales 1, 2 or 3.

It has been defined that the maximum degree of mitigation of a control is 85% on each risk.

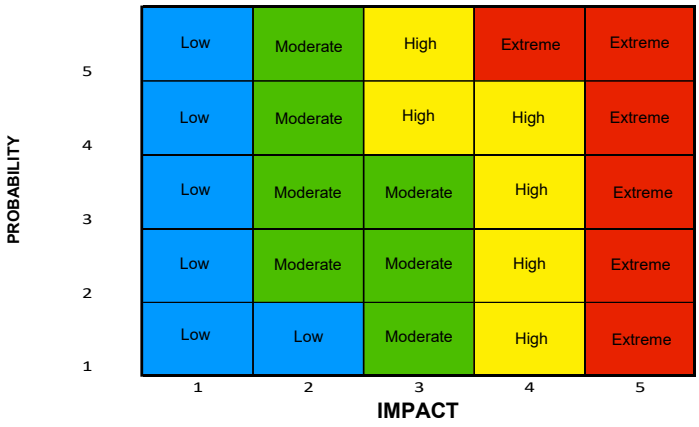
Residual risk result
Based on the "Inherent Risk" ratings and the factors that determine the "Effectiveness of Control", and subtracting from these two criteria, the Residual Risk is derived. Consequently, Residual Risk is determined by:

RIPO: Inherent risk rating of probability of occurrence
ECPO: Rating effectiveness control of probability of occurrence
RIMI: Inherent risk rating of magnitude of impact
ECMI: Rating effectiveness control of magnitude of impact
RIPO – (RIPO*ECPO%)
RIMI – (RIMI*ECMI%)

In order to obtain a more acid rating of the residual risk derived from the overall effectiveness of the associated controls, the maximum rating weighting of these controls is applied, depending on the result of the rated factors.

Heat Map

The measurement model is based on measuring through heat maps the inherent and residual risk of the entities and the Group. Heat maps make it possible to establish the most relevant risks to which entities are exposed, taking into account the criteria of probability and impact. Colorimetry allows prioritizing risks that require immediate attention, and its scales are in accordance with the nature, complexity and volume of the operations of Grupo Aval's entities.



	Impact Level
Extreme	5
High	4
Moderate	3
Low	1 and 2

3.5 DASHBOARD

An indicator is an instrument that provides quantitative evidence about whether a certain condition exists or certain results have been achieved or not. If they have not been achieved, it allows the evaluation of the process carried out. A performance indicator, for example, provides us with quantitative information regarding the achievement of the objectives of a program, it can cover quantitative or qualitative aspects.

Grupo Aval defines indicators of the risk management of ML/TF/FPWMD, based on the good practices carried out by the entities, which are summarized through dashboards that must be reported to Grupo Aval periodically.

3.6 DEFINITION OF IMPROVEMENT AND MITIGATION PLANS

The follow-up reports are analyzed by the ML/TF/FPWMD Corporate Committee, in order to determine the control points to be strengthened, review the relevant changes and seek action plans aimed at mitigating such changes. These action plans are agreed upon by the Committee to be implemented in the entities and in Grupo Aval, in accordance with the projected schedules for each case.

In addition, the reports provide information on the state of risk management of each of the entities and the new developments that may arise in the period, which provides the Committee with tools to define changes in the methodology and/or adapt prevention practices to mitigate risk.

4. GLOSSARY

- **Senior Management:** They are the people responsible for directing, executing and supervising the operations of the entity under the direction of the Board of Directors.

- **Risk Appetite:** The level of risk that the entity is willing to accept or assume, to achieve its strategic objectives and business plan.

- **Geographical Areas:** Place where the authorized commercial establishment of the natural or legal person providing the service is located and the jurisdiction where its counterparts are located (cities or countries), where the operations are transacted or registered either by their origin or destination.

- **Shell Bank:** It is a financial entity that:
  - Has no physical presence in the country in which it is incorporated and is licensed.
  - Does not belong to a financial conglomerate that is subject to comprehensive and consolidated supervision by the Finance Superintendence of Colombia (SFC).
  - Is not subject to inspection, surveillance and/or control or an equivalent degree of supervision, by the supervisor of the jurisdiction where it is domiciled or incorporated.

- **Beneficial Owner:** Natural person(s) who ultimately owns or controls, directly or indirectly, a customer and/or the natural person on whose behalf a transaction is made. It also includes the natural person(s) who exercises effective and/or final control, directly or indirectly, over a legal person or other structure without legal status**.**

- **Customers:** Any natural or legal person and structures without legal status with which the entity establishes and maintains a contractual or legal relationship for the supply of any product of its activity.

- **Collaborators:** Individuals who are obliged to provide a service to Grupo Aval or its subordinates, under continuous dependence or subordination and through remuneration.

- **Basel Committee (Basel Committee on Banking Supervision):** It is the global organization that brings together banking supervisory authorities, whose objective is to strengthen the soundness of financial systems and prudential regulation of entities with the purpose of improving financial stability. Its primary function is to act as an international forum for finding policy solutions and issuing standards.

- **ML/TF/FPWMD Corporate Committee**: It is the advisory group made up of the Compliance Officers of the entities (Grupo Aval, 4 Banks, Corficolombiana and Porvenir), responsible for monitoring the strategic management of risks and formulating recommendations and good practices for the management of risks that affect the activity of the entities. Its modification, adjustment or invitation will be responsibility of the same committee.

- **External Context:** It is the external environment in which the organization seeks to achieve its objectives, which may include: (i) the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; (ii) key drivers and trends that have an impact on the organization's objectives; and (iii) relationships with people and organizations that may affect, be affected, or perceive themselves as affected by a decision or an activity, and their perceptions and values.

- **Internal Context:** It is the internal environment in which the organization seeks to achieve its objectives, which may include: (i) governance, organizational structure, functions and responsibilities; (ii) policies, objectives and strategies implemented to achieve them; (iii) capabilities, understood in terms of resources and knowledge (i.e. capital, time, people, processes, systems and technologies); (iv) information systems, information flows and decision-making processes (both formal and informal); (v) the culture of the organization; (vi) standards, guidelines and models adopted by the organization; and (vii) forms and extent of contractual relations.

- **Transnational Correspondent:** It is the contractual relationship between two financial entities, the first called "correspondent establishment" and the second "represented establishment". Credit entities must be located in different jurisdictions. "Correspondent establishments" are entities that offer/provide certain services to other financial entities and "represented establishment" are those that use/receive the services contracted with the "correspondent establishment".

- **Due Diligence:** The principles of due diligence are risk-based and describe what an entity should consider when initiating a relationship with the customer, to determine what kind of activities it should carry out to know the customer. Due diligence is deepened based on the rating of the risk profile and can consider levels such as Simplified Due Diligence, Due Diligence, Extended Due Diligence, and Enhanced Due Diligence.

- **Extended or Enhanced Due Diligence:** In addition to the above, it contemplates deepening the knowledge of the customer in certain types of customers or activities, for which the entity will request additional information, independent of the documentary policy established for each product, which will allow for adequate reasonableness regarding the origin and destination of the funds, compliance with regulatory frameworks or the adoption of good practices in the field of ML/TF/FPWMD prevention. It is also known as enhanced measures.

- **Beneficiary Entity:** These are those entities that receive an electronic transfer from an entity that makes the order, directly or through an intermediary entity and provides the funds to the beneficiary.

- **Intermediary Entity:** These are those entities obliged in a serial chain or coverage payment chain, which receive and transmit an electronic transfer on behalf of the financial entity making the order and the beneficiary entity or other intermediary entity.

- **Parent Entity:** It is the entity that controls or exercises dominant influence in its subordinate entities. It provides management, administration and/or controls over its strategy and/or operation.

- **Entities:** For the purposes of this Policy, they are the banks, corporations, pension fund administrators (AFPs), Trust Companies, General Deposit Warehouses, Commission Agents, and others, obligated and non-obligated, subordinated to Grupo Aval Acciones y Valores S.A., both in Colombia and abroad.

  Risk Factors[13]: These are the agents that generate the risk of ML/TF/FPWMD. For the purposes of SARLAFT, at least the following must be considered:
  - Customers/Users
  - Products
  - Distribution channels
  - Jurisdictions

  Other risk factors can be considered, which will be identified from the process of evolution of the internal and external context.

- **Terrorist Financing:** is the set of activities aimed at channeling licit or illicit resources to promote, pay for or sponsor terrorist individuals, groups or activities.

- **Financing of the Proliferation of Weapons of Mass Destruction or FPWMD:** It is any act that provides funds or uses financial services, in whole or in part, for the manufacture, acquisition, possession, development, export, transfer of material, fractionation, transport, transfer, deposit or dual use for illegitimate purposes in contravention of national laws or international obligations, when the latter is applicable.

- **Group:** Refers to one or more entities subordinated by one or an organization, as well as its branches and subsidiaries.

- **Financial Action Task Force for the Prevention of Money Laundering (FATF):** It is an intergovernmental body that develops international standards and promotes policies to protect the international financial system against money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. This group defines money laundering as the recycling of funds from criminal activities to conceal their illicit origin and works closely with other entities involved in these issues, in particular with its associate members and observers. The Basel Committee has observer status in the FATF.

- **Jurisdiction:** Scope or territory in which an authority or power is exercised.

- **Money Laundering:** It is the set of activities aimed at concealing the illicit origin or giving the appearance of legality to resources obtained as a result of the execution of illicit activities.

- **Binding International Lists for Colombia:** Those lists of persons and entities associated with terrorist organizations that are binding under International Law, including, but not limited to, United Nations Security Council Resolutions 1267 of 1999, 1988 of 2011, 1373 of 2001, 1718 and 1737 of 2006 and 2178 of 2014, to all those that succeed, relate and

[13] **Definition of customer, user and product** - Basic Legal Circular Part 1-Title 1- Chapter 1 of the Finance Superintendence of Colombia - Instructions Relating to the Management of the Risk of Money Laundering and Terrorist Financing - Point 1 Definitions.

complement it, and any other list that is adopted in the countries where the entities of the group are located.

- **Risk Matrix:** It is a tool that facilitates a holistic risk assessment.

- **Monitoring:** Stage where the evolution of the inherent and residual risk profile and in general of the SARLAFT must be compared and monitored.

- **Unusual Operations:** These are those operations that meet at least one of the following characteristics:
  - It is not related to the customer's economic activity and for which no explanation has been found that is considered reasonable.
  - It is outside the parameters set by the entity and for which no explanation has been found that is considered reasonable.

  In the case of identifying and analyzing the transactions of users (natural or legal persons to whom, without being customers, the entity provides a service), the entities must determine which of these are relevant, taking into account the risk to which they are exposed and based on the criteria previously established by them.

  The operations alerts generated by the monitoring system can be evaluated by business (first line) or compliance (second line) areas, and facilitate the identification of unusual operations. They can lead to unusual operations, which in turn can lead to suspicious transactions.

- **Suspicious Transactions:** It constitutes a suspicious transaction on any relevant information on the management of assets, liabilities or other resources, the amount or characteristics of which are not related to the economic activity of its customers, or on transactions of its users that, due to their number, the amounts traded or the particular characteristics of the same, may reasonably lead to suspect that they are using the entity to transfer, handle, take advantage of, or invest money or resources from criminal activities or intended for their financing.

- **Host Country:** Country in which a subsidiary of an entity domiciled abroad is located. Entities that are classified in this way must comply with the ML/TF/FPWMD regulations applied by that country, and in the event that Colombian regulations are more rigorous, they must comply with the most complete regulations.

- **Country of Origin:** Country in which a parent company is domiciled, where the best practices in ML/TF/FPWMD administration for the subsidiaries that are under it come from.

- **Higher Risk Countries:** Higher risk countries are those contained in the FATF lists of non-cooperative countries and high-risk jurisdictions.

- **Politically Exposed Person (PEPs):**[14] Public servants of any system of nomenclature and classification of jobs in the national and territorial public administration will be considered as PEPs, when they have been assigned or delegated functions of: issuance of rules or regulations, general management, formulation of institutional policies and adoption of plans, programs and projects, direct management of assets, money or securities of the State, administration of justice or administrative sanctioning powers, and

[14] Decree 830 of July 26, 2021

individuals who are in charge of directing or managing resources in political movements or parties.

The status of Politically Exposed Persons (PEP) will be maintained over time during the exercise of the position and for two (2) more years from the separation, resignation, dismissal or declaration of non-subsistence of the appointment, or any other form of dismissal, or termination of the contract.

- **Foreign PEPs:** These are those people who perform prominent functions in another country. Foreign PEPs are: (i) heads of state, heads of government, ministers, undersecretaries or secretaries of state; (ii) congressmen or parliamentarians; (iii) members of supreme courts, constitutional courts or other high judicial bodies whose decisions are not normally appealable, except in exceptional circumstances; (iv) members of tribunals or boards of directors of central banks; (v) ambassadors, chargés d'affaires and senior officials of the armed forces, (vi) members of the administrative, management or supervisory bodies of state-owned enterprises, and (vii) legal representatives, directors, deputy directors and/or members of the boards of directors of international organizations.

  In no case do these categories include officials at intermediate or lower levels. In addition, foreign PEPs are considered during the period in which they hold their positions and during the two (2) years following their separation, resignation, dismissal, or any other form of dismissal.

- **Products**: These are the legally authorized operations that can be carried out by supervised entities through the execution of a contract (i.e. checking or savings account, insurance, investments, CDT, drafts, debt issuance, purchase and sale of securities, trust businesses, etc.).

- **ROS:** It is the Suspicious Transaction Report that every compliance officer or responsible official of natural or legal persons must send to the Financial Analysis Unit - UIAF when, in the exercise of its activity or functions, it detects a suspicious transaction of money laundering or terrorist financing, which should be reported.

- **Risks Associated with Money Laundering and Terrorist Financing (ML/TF/FPWMD):**[15] These are the risks through which the risk of ML/TF/FPWMD materializes; these are: reputational, legal, operational and contagion.

  - **Reputational Risk:** It is the possibility of loss incurred by an entity due to discredit, bad image, negative publicity, true or not, with respect to the entity and its business practices, which causes loss of customers, decrease in income or legal proceedings.

  - **Legal Risk:** It is the possibility of loss incurred by an entity when it is sanctioned or forced to compensate damages as a result of the breach of rules or regulations and contractual obligations.

    Legal risk also arises as a result of failures in contracts and transactions, derived from malicious actions, negligence or involuntary acts that affect the formalization or execution of contracts or transactions.

[15] **Risk Definitions** - Basic Legal Circular Part 1-Title 1- Chapter 1 of the Finance Superintendence of Colombia-: Instructions Relating to the Management of the Risk of Money Laundering and Terrorist Financing - Point 1 Definitions

- **Operational Risk:** It is the possibility of incurring losses due to deficiencies, failures or inadequacies, in human resources, processes, technology, infrastructure or due to the occurrence of external events. This definition includes legal risk.

- **Risk of Contagion:** It is the possibility of loss that an entity may suffer, directly or indirectly, due to an action or experience of a related party. The related party is the related or associated party and includes natural or legal persons or structures without legal personality that have the possibility of exerting influence over the entity.

- **Inherent Risk:** It is the level of risk inherent to the activity, without taking into account the effect of the controls.

- **Residual Risk**: It is the level resulting from the risk after applying the controls.

- **SAGRILAFT:** It is the system of self-control and management of the comprehensive risk of money laundering and terrorist financing applicable to entities obligated by the Superintendence of Companies.

- **SARLAFT:** Money Laundering and Terrorist Financing Risk Management System is the integrated set of policies, procedures, infrastructure, controls, training and disclosure that seeks to respond to the possible threats that entities are used for the practice of criminal conduct that seeks to channel resources from criminal activities and in particular reduce exposure to the risk of ML/TF/FPWMD.

- **Segmentation:** It is the process by which the separation of elements into homogeneous groups within them and heterogeneous among them is carried out. Separation is based on the recognition of significant differences in their characteristics (segmentation variables).

- **Services:** These are all those interactions of entities subject to inspection and surveillance by the Finance Superintendence of Colombia with persons or structures without legal personality other than their customers.

- **Red Flags and Early Red Flags:** are the facts, situations, events, amounts, quantitative and qualitative indicators, financial ratios and other information that the entity determines as relevant, from which it can infer timely and/or prospectively the possible existence of a fact or situation that escapes what the entity, in the development of SARLAFT/SAGRILAFT, has determined as normal.

  These signals must consider each of the risk factors and the characteristics of its operations, as well as any other criteria that the entity deems appropriate

- **Third Parties and Intermediaries (TPI):** any third party (individual or legal entity) used by Grupo Aval and/or its subsidiaries, directly or indirectly, to carry out a transaction on a particular or periodic basis for the purpose of selling the products or services of Grupo Aval and its subsidiaries or to purchase goods and/or services for Grupo Aval and its subsidiaries. Intermediaries can be defined as independent organizations or individuals acting on behalf of the entity and over which the entity has a controlling influence. These partners often perform day-to-day business activities, such as obtaining licenses, permits or other authorizations, and are involved in business development. Intermediaries –e.g., business development consultants, sales representatives, customs agents, lawyers, accountants– are usually local allies who have a strong knowledge of local customs and business practices and an extensive personal network.

- **Transfer:** It is the transaction carried out by a natural or legal person called the payer, through an entity authorized in the respective jurisdiction to make domestic and/or international transfers, through electronic or accounting movements, in order for a sum of money to be made available to a natural or legal person called the beneficiary in an entity authorized to carry out this type of operation. The payer and the payee can be the same person.

- **Financial Information and Analysis Unit (UIAF):** It is an entity attached to the Ministry of Finance and Public Credit of Colombia, its mission is to protect national security in the economic field, based on investigation and innovation processes through the prevention and detection of criminal activities, related to the crimes of Money Laundering and Terrorist Financing.

- **Users:** These are those natural or legal persons or structures without legal personality to which, without being customers, the entity provides a service.

- **Related Parties:** They are those who meet any of the criteria set forth in article 2.39.3.1.2 of Decree 2555 of 2010.
  a) Control, subordination and/or business group: the natural person, legal person and investment vehicle that presents a situation of control or subordination with respect to an entity of the financial conglomerate directly or indirectly, in the cases provided for in Articles 260 and 261 of the Code of Commerce, or belongs to the same business group in accordance with the definition of Article 28 of Law 222 of 1995, or the rules that modify, replace or add to them.

  b) Significant participation: A significant participation is held by any person or persons who meet any of the following conditions:
     - The equity participant or beneficial owners of ten percent (10%) or more of the participation in any entity of the financial conglomerate. For this purpose, shares without voting rights will not be counted.
     - Legal entities in which any entity of the financial conglomerate is the beneficial owner of ten percent (10%) or more of the participation. For this purpose, shares without voting rights will not be counted.
     - Legal persons that are subordinate to those defined in the first bullet of this paragraph. Situations of subordination shall be those provided for in Articles 260 and 261 of the Code of Commerce. For this purpose, shares without voting rights will not be counted.

5. REGULATION

Regulations used in the development of Money Laundering and Terrorist Financing Risk Management:

- **Colombia:**
  - Basic Legal Circular of the Finance Superintendence of Colombia, (External Circular 29 of 2014), Part I General Instructions Applicable to Supervised Entities Title IV Duties and Responsibilities Chapter IV: Instructions Relating to the Management of the Risk of Money Laundering and Terrorist Financing.
  - Basic Legal Circular of the Superintendence of Companies (External Circular 100-000005 of 2017) in its Chapter X Self-control and Management of ML/TF Risk and Report of Suspicious Transactions to the UIAF.

- Decree 830 of 2021 "by which some articles are modified and added to Decree 1081 of 2015, in relation to the regime of Politically Exposed Persons (PEP)".

- **International:**
  - Regulations in relation to the administration of Money Laundering and Terrorist Financing that apply to entities abroad.
  - Basel Committee: Guideline for "Adequate Management of Risks Related to Money Laundering and Terrorist Financing". Bank for International Settlements – BIS (January 2014).
  - FATF: List of relevant recommendations.
  - New FATF recommendations (including its interpretative notes), including:
    - R.1: Risk assessment and implementation of a risk-based approach
    - R.2: National cooperation and coordination
    - R. 9: Legislation on the professional secrecy of financial entities
    - R. 10: Customer Due Diligence
    - R. 11: Record keeping
    - R. 12: Politically Exposed Persons (PEPs)
    - R. 13: Correspondent banking
    - R. 15: New technologies
    - R. 16: Wire transfers
    - R. 17: Reliance on third parties
    - R.18: Internal controls, and foreign branches and subsidiaries
    - R.20: Suspicious transaction reporting
    - R. 26: Regulation and supervision of financial entities
    - R. 40: International cooperation