MONEY LAUNDERING, TERRORIST FINANCING AND FINANCING THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION RISK CORPORATE POLICY

2023

TABLE OF CONTENTS

1. PROCESS 4
2. OBJECTIVE 4
2.1 General Objective 4
2.2 SPECIFIC OBJECTIVES 4
3. SCOPE 4
4. GLOSSARY 4
5. REGULATIONS 11
6. GENERAL GUIDELINES 12
6.1 policies 12
6.1.1 Generalities 12
6.1.2 Risk Identification and Measurement 13
6.1.3 Control and Mitigation 13
6.1.4 Monitoring 14
6.1.5 Corporate Flexibility and Continuity 14
6.1.6 Report 14
6.1.7 Training 14
6.2 LAFT/FPADM Corporate Risk Model 15
6.2.1 Comprehensive System and Integration of Program Components 15
6.2. 2 Risk Assessment and Understanding 16
6.2.2.1 Risk Management 16
6.2.2.2 Knowledge of the Customer 16
6.2.2.3 Customer Profile 20
6.2.2.4 Knowledge of the Final Beneficiaries of the Legal Entities or Assimilated Structures 22
6.2.2.5 Internal and external context of the entities 24
6.2.2.6 Information Management 24
6.2.2.6.1 Record keeping 24
6.2.2.6.2 Updating the Information 25
6.2.2.6.3 Provide Information to Oversight Entities 25
6.2.2.6.4 Reporting of Suspicious Transactions by Regulated Entities 25
6.2.2.7 Blocking Assets 26
6.2.2.8 Use of Another Bank, Subsidiary Financial Institution of Aval Group to Perform Customer Due Diligence 26
6.2.3 Stages of the Model 28
6.2.3.1 Definition and/or Updating of Guidelines 28

6.2.3.2 LAFT/FPADM Risk Management in the Entity 28
6.2.3.3 Management Tracking 29
6.2.3.4 Definition of Improvement and Mitigation Plans 29
6.2.4 Adequate Governance Mechanisms 29
6.2.5 Model Actors 30
6.2.5.1 Grupo Aval Acciones y Valores S.A. Responsibilities 30
6.2.5.2 Responsibilities of Grupo Aval Entities 31
6.2.5.3 ATH Responsibilities 32
6.2.5.4 Roles and Responsibilities of the Board of Directors and/or Senior Management 32
6.2.6 LAFT/FPADM Risk on a Group Scale and in a Cross-Border Context 33
6.2.6.1 Global Customer Risk Management Process 34
6.2.6.2 Risk Management and Assessment 34
6.2.6.3 Consolidated Scale LAFT/FPADM Risk Policies and Procedures 35
6.2.6.4 Information Exchange within the Group 36
6.3 Transaction Monitoring System Agreement 38
6.3.1 Monitoring by Entities 38
6.3.2 Grupo Aval Monitoring 38
6.4 Management Model 38
6.4.1 Risk Identification 39
6.4.1.1 Segmentation of the LAFT/FPADM Risk Factors 39
6.4.1.2 LAFT/FPADM Risk Events 39
6.4.1.3 Risk Analysis 39
6.4.2 Risk Measurement 40
6.4.2.1 Inherent Risk 40
6.4.2.2 Probability of Occurrence 40
6.4.2.3 Magnitude of the Impact 40
6.4.2.4 Residual Risk 40
6.5 Dashboard 42
6.6 Definition of Improvement and Mitigation Plans 42

1. PROCESS

Control – SARLAFT

2. OBJECTIVE

2.1 GENERAL OBJECTIVE

Establish the methodological guidelines, roles and responsibilities of the key actors for the Risk Management of Money Laundering, Terrorist Financing and Financing the Proliferation of Weapons of Mass Destruction (hereinafter LAFT/FPADM, for its acronym in Spanish).

2.2 SPECIFIC OBJECTIVES

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

- Empower the compliance units within the entities to lead the process of standardization of LAFT/FPADM risk management.

- Define, share and adopt best practices to be implemented by the entities, so that they are consistent with international recommendations such as the “Sound management of risks related to money laundering and financing of terrorism” proposed by the Basel Committee (Bank for International Settlements - BIS), and those of other international organizations.

- Following international guidelines and best practices, Grupo Aval guides its regulated and non-regulated entities to apply the recommendations issued by the Financial Action Task Force (FATF) as part of their policies, standards, processes and controls associated with the risk of money laundering and terrorist financing.

3. SCOPE

Ensuring the application of this policy is the responsibility of Grupo Aval’s Senior Corporate Vice-Presidency of Risks and Compliance; however, since 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 subsidiaries to know, abide by and apply the guidelines established in this document, according to the particular characteristics and regulations applicable to each of them.

4. GLOSSARY

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

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

- **Geographic Areas:** places where the authorized commercial establishment of the individual or legal entity providing the service is located and the jurisdiction where its counterparties are located (cities or countries), where the transactions are traded or recorded either by origin or destination.

- **Shell bank:** is a financial institution that:

- Does not have a physical presence in the country where it is incorporated and licensed.
- It does not belong to a financial conglomerate that is subject to comprehensive and consolidated supervision by the Finance Superintendence of Colombia, SFC.
- It 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 client and/or the natural person on whose behalf a transaction is made. It also includes the natural person(s) who exercise effective and/or final control, directly or indirectly, over a legal person or other structure without legal status.

- **Customers:** any individual or legal entity or other structures similar to these, with whom the entity establishes and maintains a legal or contractual relationship for the supply of any product of their activity.

- **Employees:** individuals who are undertake to render a service to Grupo Aval or its subsidiaries, under continuous dependence or subordination and for remuneration.

- **Basel Committee (Basel Committee on Banking Supervision):** is the global organization that brings together banking supervisory authorities, whose objective is to strengthen the soundness of financial systems and the prudential regulation of institutions with the aim of improving financial stability; its main function is to act as an international forum for finding policy solutions and promulgating standards.

- **LAFT/FPADM Corporate Committee:** is the advisory group formed by the entities' Compliance Officers (Grupo Aval, 4 Banks, BAC, Corficolombiana and Porvenir), responsible for monitoring the strategic management of risks and formulating recommendations and good practices to manage the risks that affect the activity of the entities. The same committee shall be in charge of its amendment, adjustment or invitation.

- **External context:** 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 impact the organization's objectives; and (iii) relationships with people and organizations that may affect, be affected by, or perceive themselves to be affected by a decision or activity, and their perceptions and values.

- **Internal context:** the internal environment in which the organization seeks to achieve its objectives, which may include: (i) governance, organizational structure, roles and responsibilities; (ii) policies, objectives and strategies implemented to achieve them; (iii) capabilities, understood in terms of resources and knowledge (e.g. 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 relationships.

- **Transnational correspondence:** is the contractual relationship between two financial institutions, the first one called "correspondent institution" and the second one called "respondent institution". Lending companies must be located in different jurisdictions. "Correspondent institutions" are those entities that offer/provide certain services to other

financial institutions, and “respondent institutions” are those that use/receive the services contracted with the “correspondent institution”.

- **Due Diligence:** the principles of due diligence are risk-based,and describe what an institution should consider when entering into a customer relationship, to determine what type of activities it should undertake to get to know the customer. Due diligence is deepened according to the risk profile rating and may 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, regardless of the documentary policy established for each product, which will allow having an adequate reasonability about the origin and destination of the funds, compliance with the regulatory frameworks or the adoption of good practices in the prevention of LAFT/FPADM. Also known as enhanced measures.

- **Beneficiary Entity:** entities that receive a wire transfer from an ordering entity, either directly or through an intermediary entity, and deliver the funds to the beneficiary.

- **Intermediary Entity:** are those regulated entities in a serial or cover payment chain, which receive and transmit a wire transfer on behalf of the ordering financial entity and the beneficiary entity or another intermediary entity.

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

- **Entities:** for the purposes of this Policy, are the Banks, Corporations, Pension Fund Administrators (AFP’s), Trust Companies, General Deposit Warehouses, Brokerage Firms, and other regulated and non-regulated subordinates of Grupo Aval Acciones y Valores S.A., both in Colombia and abroad.

- **Risk Factors[1]:** agents generating risks of LAFT/FPADM/FPADM. For SARLAFT purposes, at least the following must be taken into account:

    - Customers/users
    - Products
    - Distribution channels
    - Jurisdictions

  Other risk factors may 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, support or sponsor terrorist individuals, groups or activities.

- **Financing of the Proliferation of Weapons of Mass Destruction or FPADM**: 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,

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

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 entity or an organization, as well as its branches and subsidiaries.

- **Financial Action Task Force for the Prevention of Money Laundering (FATF):** 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 derived from criminal activities to conceal their illicit origin and works closely with other entities involved in these issues, particularly its associate members and observers. The Basel Committee has observer status in the FATF.

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

- **Money laundering:** is the set of activities aimed at hiding the illicit origin or giving the appearance of legality to resources obtained from the execution of illicit activities.

- **International binding lists for Colombia:** lists of persons and entities associated with terrorist organizations that are binding under international law, including, but not limited to, the Resolutions 1267 of 1999, 1988 of 2011, 1373 of 2001, 1718 and 1737 of 2006 and 2178 of 2014 of the United Nations Security Council, to all those that succeed, relate to and complement them, and any other list adopted in the countries where the entities of the group are located.

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

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

- **Unusual Transactions:** are those transactions that meet at least one of the following characteristics:

    - It is not related to the customer's economic activity and no reasonable explanation has been found.
    - It is outside the parameters set by the entity and for which no reasonable explanation has been found.

  In the case of identification and analysis of user transactions (individuals or legal entities 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 the entities.

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

- **Suspicious transactions**: a suspicious transaction is 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 clients, or on transactions of its users that, due to their number, the amounts traded or their particular characteristics, may reasonably

lead to suspicion that they are using the entity to transfer, manage, take advantage of or invest money or resources derived from criminal activities or destined to their financing.

- **Host Country:** country in which an affiliate of a foreign domiciled entity is located. Entities that are classified in this way must comply with the LAFT/FPADM regulations applicable in that country, and in the event that Colombian regulations are more rigorous, they must comply with the most complete regulations.

- **Home Country:** country in which a parent company is domiciled, from where the best practices in LAFT/FPADM management for the subsidiaries under the parent company originate.

- **Higher-risk countries:** higher-risk countries are those included in the FATF lists of non-cooperating countries and higher-risk jurisdictions.

- **Politically Exposed Person (PEPs)[2]:** public servants of any system of nomenclature and classification of jobs of the national and territorial public administration will be considered PEP, when they have assigned or delegated functions of: issuance of rules or regulations, general direction, 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 individuals who are responsible for the direction or management of resources in political movements or parties.

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

- **Foreign PEPs:** are those persons who perform important public functions in another country. Foreign PEPs include: (i) heads of state, heads of government, ministers, undersecretaries or secretaries of state; (ii) members of congress or parliament; (iii) members of supreme courts, constitutional courts or other high judicial instances whose decisions do not normally admit appeals, except in exceptional circumstances; (iv) members of courts or boards of directors of central banks; (v) ambassadors, chargés d'affaires and senior officials of the armed forces; and (vi) members of the administrative, management or supervisory bodies of state-owned enterprises.

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

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

- **STR**: is the Suspicious Operation Report that every compliance officer or official responsible for natural or legal persons must send to the Financial Analysis Unit - UAF when, in the exercise of their activity or functions, they detect an operation suspicious of money laundering or financing of terrorism, which should be reported.

[2] Decree 830 of July 26, 2021

- **Risks Associated with Money Laundering and Terrorist Financing (LAFT/FPADM)[3]:** are the risks through which the LAFT/FPADM risk materializes; these are: reputational, legal, operational and contagion.

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

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

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

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

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

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

- **Residual Risk:** resulting level of risk after applying controls.

- **SAGRILAFT:** is the LAFT/FPADM integral risk management and self-control system established in Chapter X of the Basic Legal Circular applicable to entities required by the Superintendence of Companies.

- **SARLAFT:** the 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 possible threats to the Entities in the practice of criminal conducts that seek to channel resources from criminal activities and in particular to reduce the exposure to the risk of LAFT/FPADM.

- **Segmentation:** is the process by which elements are separated into homogeneous groups within them and heterogeneous groups between them. The separation is based on the recognition of significant differences in their characteristics (segmentation variables).

- **Services:** are all those interactions of the entities subject to inspection and surveillance by the Superintendence of Finance of Colombia with persons or structures without legal status 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

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

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:** is the transaction carried out by an individual or legal entity called originator, through an entity authorized in the respective jurisdiction to make national and/or international transfers, by means of electronic or accounting processes, so that a sum of money is placed at the disposal of an individual or legal entity called beneficiary, in an entity authorized to carry out this type of operation. The originator and the beneficiary may be the same person.

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

- **Users:** are those individuals or legal entities or structures without legal status to whom, without being customers, the entity provides a service.

- **Related Parties:** are those that meet any of the criteria set forth in Article 2.39.3.1.2 of Decree 2555 of 2010.

  a) Control, subordination and/or corporate group: the individual, legal entity or investment vehicle 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 corporate group in accordance with the definition of Article 28 of Law 222 of 1995, or the regulations that amend, supersede or add to them.

  b) Significant stake: a significant stake is held by a person or persons who meet any of the following conditions:

     – The shareholder(s) or beneficial owner(s) of ten percent (10%) or more of the shareholding in any entity of the financial conglomerate. Non-voting shares will not be counted for this purpose.
     – Legal entities in which any entity of the financial conglomerate is the beneficial owner of ten percent (10%) or more of the shareholding. Non-voting shares will not be counted for this purpose.

- Legal entities in a subordinate position with respect to those defined in item i. of this paragraph. Subordination situations shall be those provided for in Articles 260 and 261 of the Code of Commerce. Non-voting shares will not be counted for this purpose.

5. REGULATIONS

Regulations used in the development of Money Laundering and Terrorist Financing Corporate 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 the Financing of Terrorism.
  - Basic Legal Circular of the Finance Superintendence of Colombia (External Circular 100-000005 of 2017) in its Chapter X Self-control and LA/FT Risk Management and Report of Suspicious Transactions to the UIAF.
  - External Circulars 100-00004/21 and 100-000016/20 of the Superintendence of Companies - Self-control and LAFT/FPADM Risk Management System. - Mandatory Reporting of Information to the UIAF.
  - Decree 830 of 2021 “whereby some articles are amended and added to Decree 1081 of 2015, as related 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 located abroad.
  - Basel Committee: Guideline for “Sound management of risks related to money laundering and financing of terrorism”. Bank for International Settlements - BIS (January 2014).
  - FATF: List of relevant recommendations.
  - New FATF Recommendations (including their interpretative notes), among others:
    - R. 1: Assessing risks & applying a risk-based approach
    - R. 2: National cooperation and coordination
    - R. 9: Financial institution secrecy laws
    - R. 10: Customer due diligence
    - R. 11: Record keeping
    - R. 12: Politically Exposed Persons (PEP)
    - 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 subsidiarias
    - R. 20: Reporting of suspicious transactions
    - R. 26: Regulation and supervision of financial institutions
    - R. 40: Other forms of international cooperation

6. GENERAL GUIDELINES

6.1 POLICIES

Grupo Aval adopts the following policies on which it bases and structures the Risk Management System for Money Laundering and Terrorist Financing and Financing the Proliferation of Weapons of Mass Destruction (LAFT/FPADM) of Grupo Aval and its subsidiaries. Such policies are management's expressions of a fair and transparent presentation and assessment of such risks in the financial statements and other disclosures of the Administrations of Grupo Aval and its subsidiaries. This allows for an adequate identification of the controls that reasonably mitigate the identified risks.

6.1.1 Generalities

- **Adopt and maintain a solid culture of the risk of LAFT/FPADM**
  Grupo Aval's management and its subsidiaries must take the lead in establishing a solid risk management culture for Money Laundering and Terrorist Financing and Financing the Proliferation of Weapons of Mass Destruction. Said culture should 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 a strong LAFT/FPADM risk management culture exists throughout the organization.

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

- **Ensure the Administration and Management of the LAFT/FPADM Risk Management System**
  The 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 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 the Financing the Proliferation of Weapons of Mass Destruction, which promotes a culture to fight against it and allows them to conduct their business and operations with high ethical standards, in compliance with the laws and regulations in force.

- **Management Commitments**
  Management of the entities must develop a clear, effective and robust management structure with well-defined, transparent and coherent lines of responsibility for approval by their Boards of Directors. Management of all Entities are responsible for its consistent implementation and for maintaining throughout the organization policies, products, activities, processes and systems for the adequate management of LAFT/FPADM risk.

- **Three Lines Model**
  Entities should structure the roles and responsibilities for LAFT/FPADM, and in general for all risks, following the three-line methodology, that is, considering (i) management by line of business, (ii) an independent LAFT/FPADM risk management function, and (iii) an independent review, as established in the Comprehensive Risk Management Framework.

  - **First Line**
    The first line is the operational areas that manage the business (e.g. public-facing activities and direct contact with customers). This means that the governance of the LAFT/FPADM risk recognizes that front-line management is responsible for identifying, assessing, managing and controlling the risks inherent to the products, activities, processes and systems for which it is responsible. This line must understand and apply the policies and procedures and have sufficient resources to effectively perform these tasks.

  - **Second Line**
    The second line assigns responsibilities to the Unit headed by the Compliance Officer in the regulated entities and the SARLAFT Manager (or whoever acts as such) in non-regulated entities, which must continuously monitor compliance with all obligations in terms of LAFT/FPADM Risk by its entity. This involves validating compliance with regulations and analyzing anomaly reports so that they can be reported to senior management or to the Board of Directors and/or the Audit Committee of the entities. To this end, it must question the business areas using appropriate LAFT/FPADM risk management tools, carrying out risk measurement activities and using LAFT/FPADM risk management information systems. The Compliance Officer in the regulated entities or the SARLAFT Leader (or whoever acts as such) in the non-regulated entities, must be the contact for all matters in this area for internal and external authorities, including supervisory authorities or financial intelligence units (UIAF) or jurisdictional authorities.

  - **Third Line**
    The third line plays a key role in independently assessing LAFT/FPADM risk management and controls, as well as the entity's processes and systems, reporting to the Audit Committee or similar oversight body through periodic assessments of the effectiveness of compliance with LAFT/FPAMD risk management policies and procedures. Those areas (usually internal audits) that are to perform these reviews must be competent and duly trained and not participate in the development, implementation and operation of the risk/control structure. This review may be performed by the audit or by staff independent of the process or system under review, but may also involve suitably qualified external parties.

6.1.2 Risk Identification and Measurement

Management must ensure the identification and evaluation of the LAFT/FPADM risk found in all processes, products, activities and systems, considering the main activity of the entity, its structure and its regulatory scope (regulated or non-regulated subject), for the identification of inherent risks.

6.1.3 Control and Mitigation

In the management and administration of SARLAFT/SAGRILAFT adopted by the entities, prevention and control measures must be applied to prevent being used as instruments for the concealment, handling, investment or use in any form of money or other assets from criminal activities or intended for their financing, or to give the appearance of legality to criminal

activities or related transactions and funds, thereby ensuring an adequate control environment, structured through policies, processes, systems, internal controls and adequate monitoring of the effectiveness of LAFT/FPADM risk control measures.

6.1.4 Monitoring

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

6.1.5 Corporate Flexibility and Continuity

Entities must have the business resilience and continuity plans to ensure the ability to operate in the face of material and/or reputational impacts and events that jeopardize the ordinary course of business.

6.1.6 Report

- **Disclosure**
  Entities' public information should enable stakeholders to assess their approach to LAFT/FPADM risk management.

- **New products or modification**
  Entities must ensure 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 under development for new or existing products, the modification of product features, the entry into a new market, opening operations in our jurisdictions and the launch or modification of distribution channels.

- **Update customer information**
  Entities shall carry out the necessary diligence to periodically update, according to their risk level, the information provided by customers, that by their nature may vary (address, telephone, activity, income, origin of resources, shareholders and/or beneficial owners, etc.), or when required to clarify any concept by the entity or by the competent authorities, in this way the entity must maintain an update indicator, and monitor compliance on an ongoing basis.

  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 of the local and Colombian regulations shall prevail.

6.1.7 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 acts as such) to ensure the due training process for employees, as well as to ensure that they are part of the induction processes for new employees. Trainings may be imparted in-person or virtually.

6.2 LAFT/FPADM CORPORATE RISK MODEL

This Corporate model guides the group's entities in the standardization of methodologies to manage the LAFT/FPADM risk, ensuring that the entities comply with the principles and regulations set forth by the oversight bodies of each country and mitigate the LAFT/FPADM risk.

With this model, Grupo Aval's entities have the elements to manage LAFT/FPADM risks in line with good practices, complying with the regulatory framework.

This requirement should be considered a specific part of the general obligation for entities of having robust Risk Management programs in place to address all types of risks, including LAFT/FPADM risks. In this context, having appropriate policies and processes in place requires the implementation of additional effective measures. These measures should also be proportionate and risk-based, and informed by the entities' own assessment of LAFT/FPADM risks (considering their core business and structure). LAFT/FPADM[4].

6.2.1 Comprehensive System and Integration of Program Components

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

Once their contexts have been analyzed, each entity should prepare the segmentation and identify the risks/events/causes that should be input to the risk matrix. In addition, they should understand the reasons 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 risk matrix, where the residual risk exposure is quantified in each segment, applying defined methodologies of probability and impact qualification, and the effect of having effective controls to 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, showing the coherence between them.

[4] Author: Basel Committee on Banking Supervision -Source: "Sound management of risks related to money laundering and financing of terrorism".

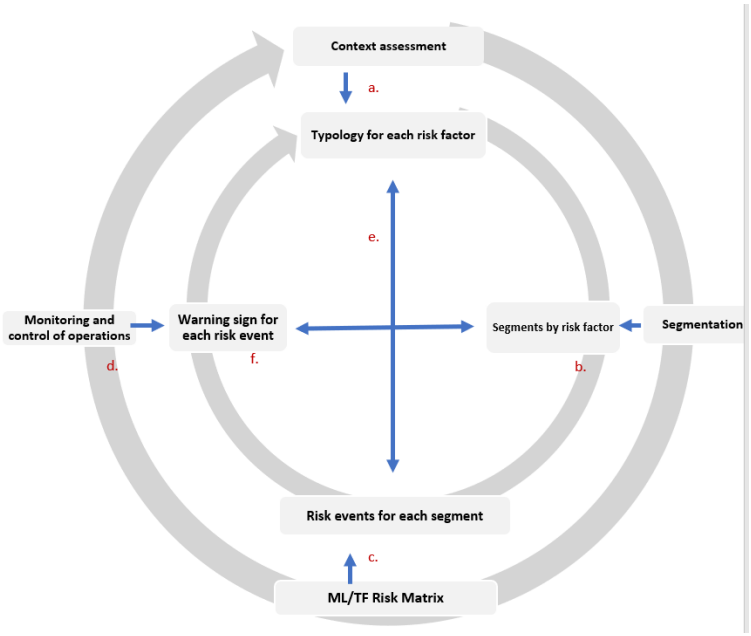


Illustration. Component integration model

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

6.2. 2 Risk Assessment and Understanding

6.2.2.1 Risk Management[5]

Sound risk management requires the identification and analysis of LAFT/FPADM risks present in the entities and the design and effective implementation of policies and procedures commensurate with the identified risks.

When conducting a comprehensive risk analysis to assess LAFT/FPADM risks, entities should consider all relevant risk factors, nationally and supranationally where applicable, sectoral, banking and business relationship, among other lines of business, to determine their risk profile and the appropriate level of mitigation to be applied.

Thus, policies and procedures regarding knowing your customer, customer acceptance, customer identification and monitoring of commercial relationships and operations (products and services offered) must take into account the risk assessment and the resulting risk profile of the entities.

6.2.2.2 Knowledge of the Customer

Entities must design, develop and implement due diligence measures to know the persons with whom they have relationships of a civil, business or employment nature based on the rating of the risk profile.

Knowledge should 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,

[5] Principle 15 of the Core Principles for Effective Banking Supervision, September 2012. As well as Principle 6 of the Principles for Enhancing Corporate Governance, October 2010.

as indicated in the Instructions - Due Diligence Directive SARLAFT 4.0 and concepts that clarify it. Policies and procedures for customer acceptance, due diligence and ongoing monitoring should be designed and implemented to adequately control these identified inherent risks. Any resulting residual risk should be managed in line with the risk profile of the entities established from their risk assessment[6].

When assessing risk, in addition to the guidelines issued by national and international control entities on knowing your customer[7], entities must take into account the following factors, based on 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 extended due diligence;
- Their sources of income and wealth;
- Their country of origin and country of residence (when different);
- The products used;
- The nature and purpose of their accounts;
- Their linked accounts, in cases of extended due diligence;
- Their business activities, and
- Other risk indicators related to the customer, to determine the level of total risk and the appropriate measures to be taken to manage those risks.

Such know-your-customer policies and procedures should require basic due diligence on all customers and expanded or enhanced due diligence as the level of risk associated with the customer varies. From the moment they are engaged by the company, potential customers must have the level of risk determined according to their characteristics and the corresponding Due Diligence must be applied accordingly. Entities must monitor the customer on a recurring basis to determine the change in their profile and if there is a change to a high risk, they will have a month to update the data, applying the corresponding due diligence. In the case of proven low-risk situations, simplified measures may be accepted, provided that the legislation allows it.

In the development of the know-your-customer procedures, the regulated entities, to the extent they have additional information, must comply with the corporate guidelines in accordance with the Due Diligence Instructions and concepts that clarify them, especially with regard to the simplified due diligence in which, as a minimum, identity verification must be performed at the time of engagement with the following information: the type of identification document, the name, number and date of issue of the identification document and request any other information they deem relevant. These legal exceptions and those that the law may implement do not exempt the regulated entities from knowing their customers in accordance with the parameters established in the Instructions - Due Diligence Directive SARLAFT 4.0, highlighting among the wide typology related, the following (for details please refer to the standard):

- Transactions with multilateral organizations.
- Establishing management trusts to pay pension obligations.
- In capitalization securities placed through mass marketing or network contracts, provided that the payment of installments is made through direct discount from a savings account, checking account or credit card, and that the customer has expressly authorized the transfer.

[6] Author: Basel Committee on Banking Supervision -Source: "Sound management of risks related to money laundering and financing of terrorism" - January 2014 - Section II - Chapter 1-a).
[7] External Circular 055 of 2016 Superintendence of Finance of Colombia Title I chapter XI Instructions related to money laundering and terrorist financing risk management - Parameters for know-your-customer procedures.

- Various types of insurance, such as those taken out by financial institutions, insurance companies or pension fund management companies on behalf of their customers; those related 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 discount from a savings account, checking account or credit card, and that the customer has expressly authorized the transfer; legal policies; health policies; funeral policies.
- Savings accounts opened exclusively for the management and payment of pension liabilities.
- In the credits that are instrumented through pay loans provided that these do not exceed 6 SMMLV and are granted to employees of companies that are previously engaged as a client with the supervised entity granting the credit.
- Affiliation with entities that manage the general pension system with respect to mandatory contributions and severance payments.
- Affiliation with entities that manage severance payments in connection with the resources derived from such benefit.
- Savings accounts opened exclusively for payroll payments. When other resources are managed 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.

When risks are higher, entities should strengthen their measures to mitigate and manage those risks.

Decisions to establish or continue business relationships with higher-risk (high or extreme) customers require 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 their customers and any beneficial owner, as far as practicable. In general, entities should not establish a business relationship, or conduct any transaction, until the identity of the customer has been satisfactorily established and verified in accordance with FATF Recommendation 10. Consistent with Basel Core Principle 29 and FATF standards, procedures should also include taking reasonable measures to verify the identity of the beneficial owner. The entity must also verify that any person acting on behalf of the customer is authorized to do so, and must verify the identity of that person.

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 keep in mind that the best documents for verifying identity are those that are most difficult to obtain illegally or to forge. Where sources of information other than documents are used, the entity should ensure that the methods (which may include reference checks with other financial institutions 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 entity may require customers to complete a declaration on the identity and details of the beneficial owner, although it should not rely solely on such declarations. As with all elements of the know-your-customer process, an entity should also consider the nature and level of risk posed by a customer when determining the scope of applicable due diligence measures.

In no case 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 should also take into account risk factors such as the reason why the customer has decided to open an account far from its headquarters or office, especially in another jurisdiction, when accessing this information.

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

The entity's front line 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 of the beneficial owners, in harmony with current legislation (e.g., Habeas Data). While the entity is obliged to both identify its customers and verify their identity, the nature and extent of the information required for verification depends on the risk assessment, including the type of applicant (individual, legal entity, etc.) and the volume and intended use of the product and/or service requested (CDTs, savings accounts, credits, transfers, etc.). The specific requirements necessary to verify the identity of individuals are usually set out in the national or regulatory legislation of the supervisors or UIAF. If the amount of the account is substantial, additional identification measures are advisable and should be determined based on the total risk level.

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, and to demand that officers put compliance with LA/FT risk management regulations before the achievement of business goals.

In situations where the account has been opened but verification problems arise in the course of establishing the business or contractual relationship that cannot be resolved, entities must block access to the product. In any case, the regulated entity must assess whether to proceed with the preparation of a suspicious transaction report (STR) in cases where there are problems in completing the know-your-customer measures (subject to national legislation on the treatment of suspicious transactions. Sound management of risks related to money laundering and financing of terrorism). In addition, when the verifications raise suspicions or provide reasonable grounds to suspect that the assets or funds of the future customer derive from infractions and crimes included in LAFT/FPADM assumptions, the entities should not voluntarily accept opening accounts for such customers. In such situations, Entities must prepare a STR, notifying the competent authorities (UIAF), and ensure that the customer is not informed, even indirectly, that a STR has been, is being or will be prepared.

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

The entity should not open a product or conduct business with a customer who insists on anonymity or who provides an obviously fictitious name, or numbered confidential accounts; although a numbered account may offer greater confidentiality to the account holder, the identity of the account holder should 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 regulated entity or SARLAFT Manager (or whoever acts as such) in non-regulated entities, as well as the entity's supervisors, have full access to this information if necessary.[8]

Finally, each entity must ensure that potential customers are effectively identified at the time of the engagement by using information from reliable and independent sources such as digital signature certificates, biometric systems, and strong authentication mechanisms, among others.

- **Higher-risk Countries**

Stricter and enhanced procedures should be established with respect to operations entered into with individuals and/or legal entities, or persons assimilated to legal entities, that process or have destination, are related or linked to countries where there is no cooperation or where the recommendations of the Financial Action Task Force - FATF - are not applied.

6.2.2.3 Customer Profile

While the customer identification and verification process takes place at the beginning of the relationship or prior to a banking or financial transaction, the entity must use this information to identify the potential customer and determine his risk profile and the level of due diligence to be applied. The purpose of the banking or financial relationship or transaction, the volume of the customer assets and transactions, as well as the regularity or duration of the relationship, are examples of information commonly collected. Thus, the entity must have customer due diligence policies and procedures that are sufficient to develop risk profiles for specific customers or certain categories of customers. The information obtained for these purposes 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 enable the entity to subsequently determine whether the customer or category of customers poses a high risk and requires the implementation of enhanced LAFT/FPADM risk management measures and controls.

The profiles should also reflect the entity's knowledge of the purpose and nature of the business relationship or occasional banking or financial transaction, the anticipated volume of activity, the type of transactions and the customer's sources of funds, income or wealth, 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., financial transaction records) and business correspondence, including the results of any analysis performed, such as risk assessment and inquiries made to ascertain the background and purpose of business or contractual relationships and activities and FPADM.

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

General Know-Your-Customer Policies for Politically Exposed Persons (PEPs)

This category of customers for Grupo Aval entities requires the implementation of particular controls both at the time of the engagement and during the development of the commercial or business relationship, considering that the PEP connotation suggests some more notable and sensitive risks than those of customers without this attribute. These risks are mainly framed in the possibility or feasibility of appropriating State resources, embezzlement and diversion of public funds for private interests or to finance political campaigns, illegal groups 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 LAFT/FPADM operations.

The foregoing consequently 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 designation of PEPs in the Grupo Aval, considering as such the individuals that are classified as PEPs:

- 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, persons who have a marital, de facto or de jure partnership with local or foreign politically exposed persons, as well as their relatives up to the second degree of consanguinity, first degree of affinity and first degree of civil status, are also classified as PEPs.

The minimum time to maintain the PEP's condition will be tied to the period in which the third party occupies its position and the time after the departure, 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 is a PEP or a legal entity whose beneficial owners are PEPs, entities must carry out the following due diligence steps:

- Have mechanisms to identify them, such as: Inclusion of this information in the know-your-customer and counterparty forms through the use of questions and self-declarations by the potential customer about their possible PEP status, purchasing information from database providers or establishing internal lists through the collection of information for public use, among others.

- Verification of the PEP status should be carried out prior to the start of the business relationship in order to provide for more stringent procedures. No exceptions should be allowed in the provision of information and/or documentation by the applicant.

- It will be essential in the engagement process to focus the attention of the business team on the source of wealth and the origin of the PEP's funds. To this end, each entity must provide evidence through verifiable means of the activity, profession or trade from which the resources originate and obtain a copy of the declaration of income, assets or revenues from the tax authority of the country in which it resides.

- At the time of engaging a potential customer with PEP status, an interview must be conducted in person or by digital means, leaving a record of it. This is not required for

entities regulated by the Superintendence of Companies.

- 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, approval from senior management must be obtained for customer engagement or to continue the business relationship, take steps to establish the origin of resources; provide for more stringent engagement procedures; and 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 meets the conditions to become a PEP, in the terms set forth in this policy, they must be marked as such in the systems, request updating of data whenever their risk level increases and collect the documents that correspond to this new status.

Employees responsible for managing the business relationship with these people must ensure that their information is updated, therefore, the frequency established for updating customers with this condition will be at least annually or earlier if circumstances warrant it.

During the duration of the business relationship with a Politically Exposed Person, the owner of the business relationship must monitor the customer's transactions to detect warning signs and manage them, especially by taking measures to determine the origin of the funds of such transactions.

In turn, the Compliance team of each entity shall establish the transactional profile of the PEP customer, conduct special monitoring and/or centralized evaluations of the operations carried out by this type of customers, as well as of the legal entities that are commercial companies, trust funds, foundations or other structures where PEPs are linked as beneficial owners or controlling entities.

6.2.2.4 Knowledge of the Beneficial Owners of the Legal Entities or Assimilated Structures

Knowledge of the current and potential customer in each of the entities implies knowing their identity. To this end, data must be obtained to identify each of the current or potential customers, determine the economic activity carried out by the customer and the origin of its resources, as well as to establish the origin and volume of the resources of which the customer is the holder.

It is the duty of the entities in the knowledge of the structures without legal status and of legal entities, as well as of the shareholders and/or associates of legal entities or other structures of a similar nature, to identify (obtain the information of names and surnames, document type and number) the beneficial owner who directly has more than 5% of the share capital, contribution or participation of the potential client who has control of the company or assimilated structure to the extent that due diligence permits, so that they are convinced that the beneficia owner is known and meets the characteristics included in the definition.

Knowledge of the beneficial owners of structures without legal status and legal entities, as well as shareholders and/or associates of legal entities, shall be obtained in the procedures for engaging and updating customers or in those cases in which, 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 deem necessary to identify the beneficial owner of their customers, legal entities or similar structures, in the case of companies in Colombia with the following structures: Limited Partnerships, Joint Stock Companies, Sole Proprietorships and Limited Liability Partnerships, information of the beneficial owners may be obtained from the same Certificate of Existence and Legal Representation in force for the company. For companies where such information is not available, it may be requested from the customer or obtained through public or private sources, subject to a risk analysis on the integrity and reliability of such source.

If the entities have doubts as to the veracity of the information declared in the forms, they may apply reasonable measures for such identification to obtain more information; they must also establish measures in accordance with the information obtained to determine whether 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 its funds and apply intensified continuous monitoring and, in accordance with the risk exposure, perform due diligence.

In the case of legal entities such as trusts, private foundations and non-profit institutions, whose beneficial owners cannot be identified due to corporate participation, a statement or declaration signed by the customer's representatives must be obtained, detailing the beneficial owner or owners.

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 to obtain the information of the individuals that own or control the company, it will be necessary to obtain satisfactory evidence on the identity of the beneficial owners of such companies. This is understood to mean public or private incorporation documents where their names and identification numbers are visible or, failing that, the delivery of a written certification from the beneficial owner about its ownership at the entity and its controlling companies.

In cases where 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 business relationship is aware of very particular situations of the customer (e.g. personal security reasons, etc.), said information must be documented and obtained by any other verifiable means, in the latter case, approval must be obtained from a senior employee assigned by each entity, who will make the decision on the potential customer's relationship after consulting their risk profile.

In the case of legal entities or similar structures where the beneficial owner or controller cannot be identified through other means, and only when an individual cannot be identified, entities may consider obtaining information from the individual who is the legal representative and manager of the company; nevertheless, those potential legal customers will not be eligible to be exempted from the information on the beneficial owner and leave in its place the information of the officer who holds the legal representation who:

- Aspire to be part of banks or mass or retail segments, i.e., when they are not corporate or business customers.
- Intend to acquire products in foreign currency or other products catalogued as high risk by the entity.
- Have been categorized in the engagement process as customers with a High LAFT/FPADM risk profile.
- Companies or corporate vehicles that involve beneficiary companies in different countries, making it difficult to follow the traceability of the money and the availability of information.
- Have been incorporated for less than one (1) year.

If the potential customer or owner of the controlling 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 information availability and disclosure requirements that are conducive to ensuring adequate beneficial ownership transparency or is a majority-owned subsidiary of a company, it may be exempted from providing beneficial ownership information, and therefore 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, can be obtained from a public record of the customer or 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 supposed to already do so and that information about them is already available elsewhere.

Under no circumstances will companies with bearer shares or whose shareholding composition includes associates issuing bearer shares or with the possibility of issuing bearer share certificates be accepted as customers, as well as companies that allow nominee shareholders or directors, in which case it will be necessary to require them to disclose that they are nominees, and the identity of the person who nominated them, keeping that record. Shell banks are also not eligible to be engaged as customers.

In the case of legal structures, such as cooperatives; employee funds; foundations; NGOs and others, the persons occupying a position in senior management should be identified, without prejudice to identifying the founders or managers and the main donors or contributors.

With respect to trusts, it is necessary to understand the structure of the trust business, who is the settlor, who is the contributor and who is the beneficiary of the trust funds.

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

6.2.2.5 Internal and external context of the entities

In accordance with the provisions of the SARLAFT Internal and External Context Assessment Instructions, group entities 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 Internal Capability Profile - ICP assessment, whichever generates the most value for the Entity in its expert opinion; likewise, the external context assessment is carried out by Grupo Aval transversally for all the entities that are part of the group. Entities must complement the evaluation of the above contexts considering the particularities of their operation.

The internal and external contexts are optional for the entities regulated by the Superintendence of Companies and those not regulated, since it is not required by law.

6.2.2.6 Information Management

6.2.2.6.1 Record keeping

- The entity must ensure the recording of all information required in the context of the know-your-customer system and must include:
    - The record of the documents provided to the bank when verifying the identity of the customer or the beneficial owner; and

- The transcription into 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 apply clear rules on the records to be kept to document the due diligence performed on customers and individual transactions, these rules should take into account any regulated privacy measures.

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

- Even when accounts are closed, in the event of an ongoing investigation or litigation, all records must be retained until the closing of the proceeding 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 business and recurring 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 kept to document 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 LAFT/FPADM risk.

6.2.2.6.2 Updating the Information

Entities should ensure that records maintain their reliability, currency and periodic relevance and update the information with Customer Due Diligence. Other competent authorities, law enforcement agencies or financial intelligence units may make effective use of such information to perform their own functions in the context of LAFT/FPADM. In addition, keeping the information up to date helps the entity to effectively monitor anomalous or suspicious activity in the products.

6.2.2.6.3 Provide Information to Oversight Entities

The entity must be able to demonstrate to supervisory authorities, upon request, the adequacy of its systems for assessing, managing and mitigating LAFT/FPADM risks; of its customer acceptance policy; of its procedures and policies on customer identification and verification; of its ongoing monitoring processes and procedures for reporting suspicious transactions, as well as of all measures adopted in the context of LAFT/FPADM prevention.

6.2.2.6.4 Reporting of Suspicious Transactions by Regulated Entities

- The process for identifying, investigating and reporting suspicious transactions to the UIAF should be clearly specified in the entity's policies and procedures and communicated to all personnel 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, and guidelines on how to make such reports.

- There should be procedures in place to assess whether the entity's regulatory obligations under identified suspicious activity reporting regimes require reporting the transaction to

the UIAF and/or relevant supervisory authorities, as applicable. These procedures should reflect the principle of confidentiality (at least legal confidentiality), ensuring that the investigation is carried out promptly and that reports are prepared and reported in a timely manner, with all the information. The Compliance Officer should require prompt reporting when there is a suspicion that funds or other assets may be derived from criminal activity.

- Once an account or relationship is suspected, in addition to reporting the suspicious activity, the entity must ensure that timely measures are taken to adequately mitigate the risk of the entity being used in criminal activity. These measures may include reviewing the risk rating of the customer or account or the relationship as a whole. Appropriate action may require escalating the matter 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.

6.2.2.7 Blocking Assets

- Terrorist financing has similarities with money laundering, but also exhibits singularities that entities must take into account: the funds used to finance terrorist activities may come from criminal activities or from licit sources, and the nature of the sources of financing may vary according to the type of terrorist organization. Moreover, it should be noted that the number 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 should it maintain relations with designated entities or individuals (e.g., terrorists, terrorist organizations), in accordance with the relevant national legislation (Colombian and of countries where it has subsidiaries) and applicable U.S. legislation related to money laundering and terrorist financing.

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

- All entities must have systems in place to detect forbidden transactions (such as transactions with entities designated in relevant United Nations Security Council Resolutions (UNSCRs) or national sanctions lists). Terrorist screening is not a risk-sensitive due diligence measure, so it should be performed regardless of the risk profile attributed to the customer. For the purpose of detecting terrorists, an entity may adopt automatic detection systems, but it must ensure that such systems are fit for purpose[9].

6.2.2.8 Use of Another Bank, Subsidiary Financial Institution of Aval Grupo to Perform Customer Due Diligence

In some countries, entities are allowed to use other banks, financial institutions or other entities to perform customer due diligence without exempting the entities from liability. These

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

mechanisms can take various forms, but, in essence, they usually involve one of the following situations:

Third party resource:

a. Identify the customer and verify its 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 institution is satisfied that it knows who the beneficial owner is. In the case of individuals and legal structures, financial institutions should understand the ownership and control structure of the customer.

.

When relying on another bank or financial institution to perform certain aspects of CDD, Entities should assess the reasonableness of such reliance. In addition to ensuring the existence of legal capacity to formalize the resource, the relevant criteria for its evaluation include:

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

b. The bank-entity and the other entity must enter into a written agreement acknowledging the bank-entity's resource to the other financial institution's Customer Due Diligence processes.

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

d. A third party may be required to certify to the institution that it has implemented its LAFT/FPADM risk management program and performs Customer Due Diligence substantially equivalent to that of the bank or consistent with the bank's obligations.

e. The bank-entity should give due consideration to unfavorable public information about the third party, such as being subject to enforcement action due to LAFT/FPADM deficiencies or violations.

f. The entity should identify and mitigate any additional risk 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 should consider the delivery of resources to third parties as a potential risk factor.

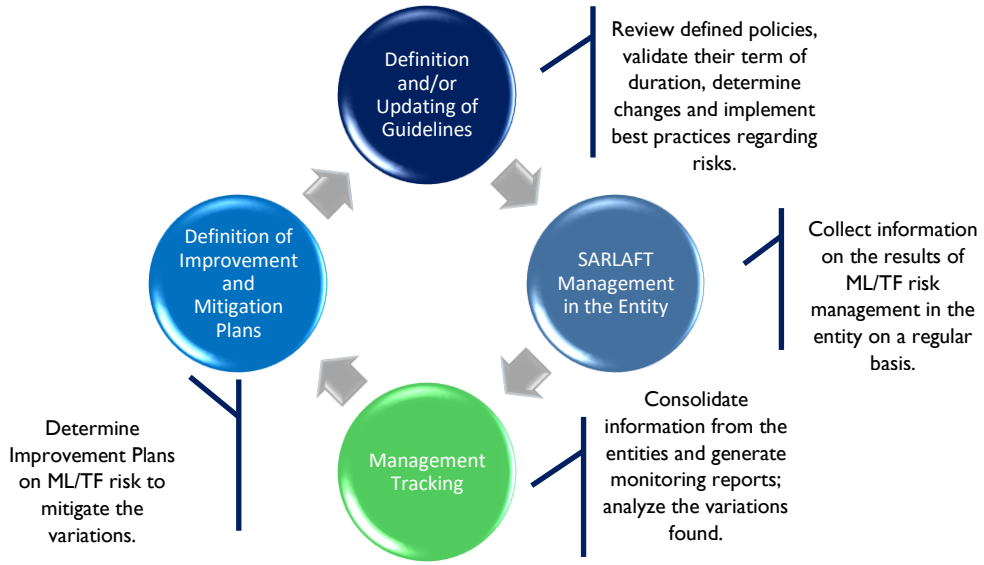
h. The entity should periodically review the other entity to ensure that it continues to practice Customer Due Diligence as thoroughly as itself. For this purpose, the entity should obtain all Customer Due Diligence information and documentation from the bank, financial institution or entity used and assess the due diligence performed, including cross-checking against local databases to ensure compliance with local regulatory requirements.

i. Entities should consider terminating their resource to entities that do not practice adequate Customer Due Diligence on their customers or fail to meet 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 of subsidiaries, entities that entrust the identification of customers to other parts of the group must ensure that the above assessment criteria are in place. It should be noted that FATF 40 standards allow countries to exclude country risk from this assessment if the financial institution is subject to group-wide LAFT/FPADM standards and supervised at the group level by its financial supervisor[10].

6.2.3 Stages of the Model

The "LAFT/FPADM Risk Corporate Management Model" should consist of four stages which are defined to direct and unify the LAFT/FPADM risk management criteria in Grupo Aval and its subsidiary entities, stages that are related in a cyclical and continuous manner, according to the following diagram:



6.2.3.1 Definition and/or Updating of Guidelines

Grupo Aval's Senior Corporate Vice-Presidency of Risks and Compliance proposes the corporate guidelines aimed at complying with applicable regulations, considering the different jurisdictions and types of entities that make up the Group. The LAFT/FPADM Corporate Monitoring Committee analyzes the feasibility of these guidelines and jointly identify best practices to strengthen the system.

6.2.3.2 LAFT/FPADM Risk Management in the Entity

Each entity adapts the LAFT/FPADM Risk Management model according to the regulations of its industry and jurisdiction, as well as corporate guidelines.

[10] Author: Basel Committee on Banking Supervision Document: Sound management of risks related to money laundering and financing of terrorism- Annex 1.

When there are changes in the Corporate guidelines, the Compliance Officer in the case of Regulated Entities or the SARLAFT Manager (or whoever acts as such) (in Non-regulated Entities) guides and executes its implementation within the entity.

6.2.3.3 Management Tracking

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

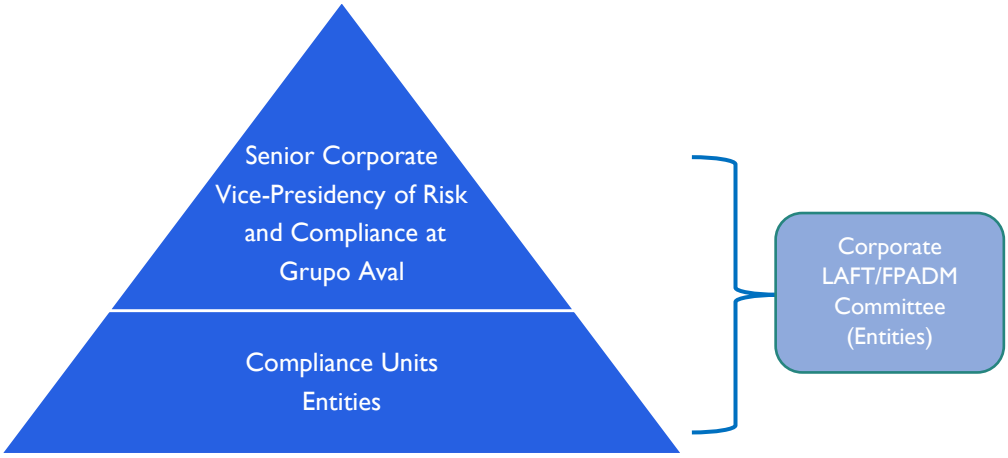
Management information is consolidated and a monitoring report is prepared and presented to the Grupo Aval LAFT/FPADM Corporate Monitoring Committee.

6.2.3.4 Definition of Improvement and Mitigation Plans

Each entity must ensure that it maintains a process of continuous improvement of the system. Grupo Aval, working together with the entities through the LAFT/FPADM Corporate Monitoring Committee sessions, identifies regulatory changes or components of the system that require improvement/modification to comply with legal requirements and to ensure adequate and efficient risk management.

6.2.4 Adequate Governance Mechanisms

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



Actor participation in the model has two fronts: in execution and in supervision, as detailed in the following table of actors and responsibilities:

Actor	Responsibilities	
	Execution	Supervision
Corporate LAFT/FPADM Committee Grupo Aval	• Define the guidelines deemed appropriate, both for Grupo Aval and for the subsidiaries, to improve the SGR. Monitor the SGR Management carried out by the entities through the consolidated	• Understand the Risk Management conducted by the entities. • Understand the risk events in the entities that make up the group and

Actor	Responsibilities	
	Execution	Supervision
	reports that are presented periodically. As a result of this review, propose the generation or modification of corporate guidelines that may affect one or all of the entities of the Conglomerate, as required.	the action plans carried out to mitigate them.
LAFT/FPADM Risk Executive Committee - Grupo Aval - Entities	• Define the schedule of meetings to be held during the year. • Conduct monthly meetings to report on developments in the LAFT/FPADM risk processes in each entity. • Determine and revise, when required, the general policies of the model. • Review regulatory issues that may affect LAFT/FPADM risk and publicize them for enforcement action. • Establish guidelines for improvement in the LAFT/FPADM risk processes. • Share best practices used in the market	• Understand the risk management status of each of the entities. • Review the LAFT/FPAMD risk methodology established by at a corporate level.
Corporate Senior Vice-Presidency of Risks and Compliance at Grupo Aval.	• Design and maintain LAFT/FPADM risk monitoring report formats. • Report the current status of LAFT/FPADM Risk Management in the entities to Grupo Aval's Vice-Presidency of Risk and to Grupo Aval's Corporate LAFT/FPADM Monitoring Committee. • Establish guidelines in accordance with the best practices defined by the Committee. • Maintain updated SGR policies in accordance with the guidelines issued by Grupo Aval.	• Receive and consolidate information on the different entity risks in order to generate periodic monitoring reports. • Establish deviations from the principles and convene when deemed necessary to make adjustments.
Entity compliance areas	• Submit Quarterly Management Report according to applicability requirements, taking into account the entity's main activity, structure and regulatory approach (regulated, quarterly, and non-regulated entity, biannually). • Participate monthly in the LAFT/FPADM Risk Executive Committee Entities • Adopt and disseminate best practices received from Grupo Aval.	• Analyze and monitor the daily operations of the entity ensuring the application of LAFT/FPADM risk.

6.2.5 Model Actors

6.2.5.1 Grupo Aval Acciones y Valores S.A. Responsibilities

- Ensure the efficient management of the Risk of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction by the Banks, Corficolombiana, Porvenir and their subsidiaries.

6.2.5.2 Responsibilities of Grupo Aval Entities

- Manage the LAFT/FPADM risk under its full responsibility in accordance with the internal policies defined and applicable regulations in force.

- The entity should continuously monitor all business relationships and transactions, as this is an essential aspect of sound and effective LAFT/FPADM risk management, the extent of this monitoring should be in accordance with the risk identified in the risk assessment conducted by the entity in its know-your-customer work. It must reinforce the monitoring of customers or higher risk transactions and maintain cross-sectional oversight of products or services in order 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 shall consider the customer's risk profile prepared in accordance with the Due Diligence Directive.

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

- The entity shall 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., relations managers) and risk and compliance officers (including investigative staff) with the timely information needed to identify, analyze and effectively follow up on customer accounts.

  Systems used and information available shall facilitate the tracking of these customer relationships by business line and include all available information about that customer relationship, including transaction history, documentation omitted at account opening and significant changes in the customer's behavior or business profile, as well as anomalous transactions effected through a customer account.

- The entity must cross-check its customer database(s) when there are changes in the sanction lists. The entity shall also periodically check its customer database(s) for PEPs and other high-risk accounts and perform due diligence on them.

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

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

- For purposes of the consolidated report to Grupo Aval, handle the 5 × 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 LAFT/FPADM Corporate Committee.

- Promote public and investor confidence; avoid being used for LAFT/FPADM and ensure that the reputation, seriousness and transparency of the business are maintained.

- Refrain from doing business with individuals or legal entities whose ethics are or have been questioned, since their involvement may affect the entity's reputation in the market, exposing the brand and assets.

- Enforce anti-LAFT/FPADM regulations and adopt appropriate controls to avoid sanctions that may be imposed by supervisory and oversight authorities on financial institutions or bank employees.

- With respect to business relationships and transactions with individuals and legal entities and financial institutions in countries listed as higher risk by the FATF, jurisdictions under increased surveillance, the special procedures established by the supervised entities must include, among other measures, the application of intensified measures of knowing the customer and monitoring those business and transactional relationships with individuals and legal entities.

- For countries listed by the FATF as High-risk Jurisdictions (countries), it is recommended not to have business relations.

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

6.2.5.3 ATH Responsibilities

ATH is the technological support for Group Aval's banks' electronic channels, since it has a central data processing system that supports the financial transactions carried out through these channels and can analyze the transactions made by users, providing information to the banks and the UIAF when required.

For this reason, ATH in its LAFT/FPADM risk model must:

- Monitor international card transactions through this channel, identifying unusual behavior according to the transactional level of the banks' users.

- The ATH Compliance Officer must report suspicious transactions to the Compliance Officers of the corresponding Entities (as necessary) and to the UIAF, as the case may be, in order for them to take the measures 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 oversight bodies (committees, board of directors, etc.) the statistics of the STRs reported to the UIAF.

6.2.5.4 Roles and Responsibilities of the Board of Directors and/or Senior Management

- Effective LAFT/FPADM risk management requires appropriate governance mechanisms. In particular, the requirement that the Board of Directors and/or Audit Committee approve and oversee risk, risk management and compliance policies is highly relevant in the context

of LAFT/FPADM risk. The Board of Directors and/or the Audit Committee should have a clear understanding of the LAFT/FPADM risks. Information on LAFT/FPADM risk assessment should be communicated to the Board of Directors and/or Audit Committee in a timely, complete, understandable and accurate manner, in order to enable them to make informed decisions.

- The Board of Directors should assign explicit competencies taking into account the governance structure of the entity to ensure the effective management of policies and procedures. The Board and/or senior management should appoint a Compliance Officer for regulated entities and/or a SARLAFT Manager for non-LAFT/FPADM regulated entities with the appropriate background to assume the general responsibilities of this function and with the necessary status and authority within the Entity to ensure that the issues raised by this officer receive the necessary attention from the Board, senior management and the business lines[11].

6.2.6 LAFT/FPADM Risk on a Group Scale and in a Cross-Border Context

When a Financial Group such as Grupo Aval operates in other jurisdictions, sound LAFT/FPADM risk management is required, which implies taking into account the legal requirements of the host countries. Given the risks, Grupo Aval must apply the LAFT/FPADM risk policies and procedures in force in accordance with Colombian legislation at group level, with consistent application and supervision throughout the group.

In turn, policies and procedures in branches and subsidiaries, while taking into account local business patterns and the requirements of the host jurisdiction, should follow 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, group policy should allow the branch or subsidiary to adapt and apply the local requirements of the host jurisdiction.

At the group or subgroup level, entities must follow the minimum guidelines established by the Superintendence of Finance of Colombia[12]:

The regulated entities in Colombia that are in the situations stipulated in articles 260 of the Code of Commerce and article 28 of Law 222 of 1995, may engage customers through the group entity that establishes a contractual relationship and engages them for the first time, provided that the following rules are observed:

- The responsibility for taking all necessary steps to confirm and update the information at least annually, shall correspond to the regulated entity that the group designates for such purpose or, in its absence, to the parent company.

- The group may maintain the design of the single customer engagement form in physical or digital format, containing, at least, all the information requirements demanded in the Instructions - Due Diligence Directive SARLAFT 4.0, as well as the information required regarding all the products offered by the entities of the group. Likewise, the format must contain a stipulation in which the customer expressly and unequivocally authorizes its referral to the other entities of the same group to which it is successively linked. In any case, it will be up to the entity with which the potential customer intends to be engaged to determine which information, in addition to the minimum required in the Instructions - Due Diligence Directive SARLAFT 4.0, must be provided to complete the engagement.

[11] Author: Basel Committee on Banking Supervision -Source: “Sound management of risks related to money laundering and financing of terrorism” - January 2014 - Section II - Chapter 1- b)
[12] External Circular 027 of 2020 Part I Title IV Chapter IV - numeral 4.2.2.2.1.3 Know Your Customer in financial conglomerates

- The responsibility to update the additional information to the minimum shall be the responsibility of each of the entities with which the customer maintains a contractual relationship, without prejudice to compliance with other LAFT/FPADM risk regulations.

- It is the permanent obligation of each of the regulated entities that make up a 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 LAFT/FPADM.

6.2.6.1 Global Customer Risk Management Process

Consolidated LAFT/FPADM risk management involves establishing and administering a process of coordination and application of policies and procedures for the entire group, which establishes a systematic and integral reference point for managing the risks of the different national and international transactions of the entities. In this context, the design of the policies and procedures outlined in this policy are not only aimed at strict compliance with all relevant legislation and regulations, but the more general objective of identifying, monitoring and mitigating risks throughout 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 needed by local legal requirements. In this regard, the entity must have a robust information exchange system between the parent company and all its branches and subsidiaries. Finally, when 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 stricter standards.

- In the development of the procedures for knowing the customer, the entities are not obliged to require the application form or conduct an interview with the potential customer when dealing with any of the operations, products or services listed in the section Evaluation and Understanding of Risks - Knowing your Customer. In any case, as additional information becomes available, the entities must comply with the instructions issued by Grupo Aval. These exceptions do not release the regulated entities from knowing their customers in accordance with the parameters established in the Instructions - Due Diligence Directive SARLAFT 4.0.

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

- It is understood that the implementation of LAFT/FPADM procedures across the Group is more challenging than many other risk management processes, given the particularities of the jurisdictions in which it operates. For effective group-wide monitoring and LAFT/FPADM risk management purposes, it is essential that, subject to appropriate legal safeguards, entities are allowed to exchange information on their customers with their parent companies. This is applicable to both subsidiaries and affiliates.

6.2.6.2 Risk Management and Assessment

The entity should have a comprehensive understanding of all risks associated with its customers throughout the group, individually or by category, and should document and periodically 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 outsourced activities. Customers that pose a high LAFT/FPADM risk 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 group-wide risk assessment.

Considering the differences in risks associated with different categories of customers, group policy should recognize that customers in the same category may pose different risks in different jurisdictions. The information obtained in the assessment process should then be used to determine the level and nature of the group's overall risk and to facilitate the design of appropriate controls within the group to mitigate those risks. Mitigating factors may include additional customer information, closer follow-ups, more frequent updates of personal data, and visits by entity personnel to the customer's home.

The compliance and internal audit staff of the entities, in particular the Compliance Officer for Regulated Entities and/or a SARLAFT Manager (or whoever acts as such) for Non-regulated entities, should assess compliance with all aspects of their group's policies and procedures, including the effectiveness of centralized CDD policies and requirements for sharing information with other group members and responding to parent company inquiries.

6.2.6.3 Consolidated Scale LAFT/FPADM Risk Policies and Procedures

- The entity should ensure that it understands the extent to which the LAFT/FPADM risk legislation allows it to rely on procedures applied by other bank-entities (e.g. within the same group) when recommending business. The bank-entity should not use underwriters who are subject to less stringent standards than those governing its own LAFT/FPADM risk procedures. Accordingly, entities should monitor and assess the LAFT/FPADM risk standards in force in the jurisdiction of the recommending bank-entity.

- The entity may use an underwriter that is part of the same financial group and may consider granting a higher degree of reliability to the information provided by the underwriter, provided that the underwriter is subject to the same standards as the Entity and that the application of these requirements is monitored at the group level. However, the bank-entity adopting this approach should ensure that it obtains the customer information provided by the recommending entity, as this information may be required to be forwarded to the UIAF if a transaction involving the recommended customer is determined to be suspicious.

- The group's parent company must have access to relevant information in order to enforce the group's LAFT/FPADM risk policies and procedures. Each office and subsidiary of the group must be able to comply with the minimum LAFT/FPADM 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 should be implemented through consistent application of policies and procedures throughout the organization, with appropriate adjustments to account for differences in risk by business lines or geographic areas of activity. In addition, it is acknowledged that different methods of collecting and retaining information may be necessary in different jurisdictions to accommodate local regulatory requirements or relative risk factors. However, these methods must be consistent with the group-wide standards outlined above.

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

- In order to effectively manage LAFT/FPADM risks from such accounts, the bank-entities must integrate this information based not only on the customer, but also on their knowledge of the beneficial owners of the customer and of the funds in question. The Entity should monitor relationships, balances and significant activities with customers on a consolidated basis, regardless of whether the accounts are held on-balance sheet, off-balance sheet, as assets under administration or in Sound management of risks related to money laundering and financing of terrorism and FPADM.

- Entities with national and international activity must appoint a Compliance Officer for Regulated Entities and/or a SARLAFT Manager (or whoever acts as such) for Non-regulated Entities. This Officer is responsible, as part of overall risk management, for creating, coordinating and assessing group-wide implementation of a single LAFT/FPADM risk strategy (including mandatory policies and procedures and authorization to issue orders to all domestic and international branches, affiliates and subsidiaries).

- The role of the Compliance Officer for Regulated Entities and/or a SARLAFT Manager (or whoever acts as such) for Non-regulated Entities includes the continuous monitoring of compliance with all LAFT/FPADM risk requirements, both national and international, throughout the group. Thus, the group's LAFT/FPADM risk manager must ensure (including by conducting periodic on-site visits) that LAFT/FPADM risk requirements are met throughout the group. If necessary, they should be empowered to give orders or take appropriate action throughout the group.

6.2.6.4 Information Exchange within the Group

- Entities should oversee the coordination of the exchange in accordance with the legal information exchange standards of each jurisdiction. Subsidiaries and branches should be required to proactively provide the parent company with information on high-risk customers and activities relevant to the global LAFT/FPADM risk standards and to respond in a timely manner to requests for account information from the parent company. The parent entity's group-wide standards should include a description of the process to be followed in all establishments to identify, monitor and investigate possible anomalous circumstances and report suspicious activities.

- The entity's group-wide policies and procedures should take into account local data protection issues and obligations and privacy legislation and regulation. They should also consider 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 LAFT/FPADM 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 particular customer or category of customers. It should also have policies and procedures in place to check whether other branches or subsidiaries hold accounts for the same customer (including those of parties related to that customer or belonging to the same group). In addition, the Parent Company should have comprehensive policies and procedures for account relationships that are considered high risk or have been associated with potentially suspicious activity, including

procedures for referrals to more senior management and guidelines for restrictions on account activity, including account 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 may require in their efforts to combat LAFT/FPADM. The parent bank should be able to require all its branches and subsidiaries to check their files against certain lists or applications to verify the presence of individuals or organizations suspected of aiding and abetting Money Laundering and Terrorist Financing and to report matches.

- The parent company should be able to report to its supervisors, upon request, on its overall customer risk management process, its assessment and management of LAFT/FPADM risks, its LAFT/FPADM risk policies and procedures on a consolidated basis, and its intra-group information sharing systems.

- In the case of transnational correspondent relationships, the regulated entities must establish mechanisms that allow them to[13]:

  - Obtain approval from senior management before entering into transnational correspondent relationships;
  - Gather sufficient information about the respondent institution to allow them to fully understand the nature of its business, including whether it has been subject to sanctions or intervention by the oversight authority for money laundering or terrorist financing, as well as any other information that allows the establishment of a transnational correspondent relationship with transparency for both parties.
  - Determine that the entity has controls to prevent and control money laundering and terrorist financing;
  - Document the respective responsibilities of each institution with respect to LAFT/FPADM.
  - Apply stricter procedures to monitor such relationships.
  - Ensure that the respondent institution complies with the know your customer measures.
  - The instructions contained in this section should also be applied with respect to individuals or legal entities that intend to acquire fixed assets from an entity.
  - Comply with any obligation, in accordance with the applicable regulation.

- **Securities transactions and insurance activities:** the application of LAFT/FPADM risk management controls in mixed financial groups raises additional issues that may be unrelated to those specific to deposit-taking and lending operations. Mixed groups should be able to monitor and exchange information on the identity of customers and their transactions and accounts within the group as a whole, and be aware of customers using their services in different sectors.

  Differences in the nature of the activities and patterns of relationships between banks and customers in each sector may require or justify variations in the LAFT/FPADM risk requirements for each sector. The banking group should be aware of these differences when cross-selling products and services to customers from different business units, and the appropriate LAFT/FPADM risk requirements should be applied to the corresponding sectors[14].

[13] External Circular 055 of 2016 Superintendence of Finance of Colombia Title I Chapter XI Instructions regarding money laundering and terrorist financing risk management - Know your customer by groups.
[14] "Sound management of risks related to money laundering and financing of terrorism" proposed by the Basel Committee (Bank for International Settlements - BIS (January 2014).

6.3 TRANSACTION MONITORING SYSTEM AGREEMENT

6.3.1 Monitoring by Entities

Entities must have a monitoring system in accordance with their size, activities and complexity, as well as with the risks present in the entity. When using a system where information is initiated, processed, reported or stored for LAFT/FPADM risk management, this system should allow trend analysis of transaction data in order to identify unusual transactions.

In particular, this system must be able to provide senior management with reliable information on certain crucial aspects, including changes in the profile of transactions carried out by customers. The customer profile should incorporate up-to-date, complete and accurate customer knowledge information provided by the customer. The IT system must enable the entity to have a centralized information repository (i.e. organized by customer, product, group entities, transactions carried out during a certain period of time, etc.). Without being required to have a single file per customer, entities must rate their customers based on risk and manage alerts with all relevant information at their disposal. An IT monitoring system should use appropriate parameters based on national and international experience on LAFT/FPADM methods and risk management. The parameters used should reflect and take into account the entity's specific risk situation.

The monitoring system should allow the entity to determine its own criteria for further follow-up, and be a source for the preparation of Suspicious Transaction Reports (STRs) or take other measures to minimize risk. The Compliance Officer for Regulated Entities and/or a SARLAFT Manager for Non-regulated Entities must have access to the Monitoring system. The parameters of the monitoring system must generate alerts on anomalous transactions, in which case they must also be subject to subsequent evaluation by the Compliance Officer.

Internal audit should also evaluate the monitoring system and the LAFT/FPADM risk management system to ensure that it is adequate and that the first and second line are using it effectively, and forward the result to the Compliance Officer[15].

6.3.2 Grupo Aval Monitoring

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

6.4 MANAGEMENT MODEL

In general, the corporate management model comprises the following phases:

[15] Source: "Sound management of risks related to money laundering and financing of terrorism" proposed by the Basel Committee (Bank for International Settlements - BIS) (January 2014).

Identification	Measurement	Oversight	Monitoring
• Entities shall apply the three risks focused on LA/FT/FPADM • Each entity performs identification of risks, causes and controls	• Risk assessment • Generation of the group risk profile	• Improvement plans and monitoring thereof • Identify controls and evaluate their design and effectiveness	• Generate reports to the different instances • Share relevant events and best practices • Review control execution

6.4.1 Risk Identification

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

It must be taken into account that any inclusion, modification or elimination of the aforementioned risks, 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: Reference Risks / Risk / Reference Cause / Cause / Exchange Type (Inclusion, modification or elimination) / Suggested change / Justification.

6.4.1.1 Segmentation of the LAFT/FPADM Risk Factors

Entities acting as regulated entities must segment, as a minimum, each of the risk factors according to the particular characteristics of each of them, ensuring that the analysis variables defined guarantee homogeneity within the segments and heterogeneity among them. The segmentation of risk factors will be included in the risk control matrix which includes the risk factor, segmentation of a priori models, segment number and segment detail according to the scope of the standard for Grupo Aval's regulated entities.

6.4.1.2 LAFT/FPADM Risk Events

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

6.4.1.3 Risk Analysis

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

6.4.2 Risk Measurement

The measurement model is based on measuring the Inherent and Residual Risk of the entities and the group through heat maps. The heat maps make it possible to establish the most relevant risks to which the entities are exposed, taking into account the criteria of probability and impact. The colorimetry prioritizes the 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 Corporate LAFT/FPADM Risk Management Model Instructions.

6.4.2.1 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 probability that LAFT/FPADM events could significantly affect Grupo Aval and its subsidiaries, 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 LAFT/FPADM risks is the responsibility of the process owner with validation and monitoring by the Compliance Officer, as well as of the process owners.
To assess inherent risks, they are classified into low, moderate, high and extreme categories, according to the Probability of Occurrence (PO) and Magnitude of Impact (MI).

6.4.2.2 Probability of Occurrence

The Probability of Occurrence assessment of the risk materializing without consideration of the controls is measured with the following scale in both Occurrence and Frequency, where only one of the two criteria should be selected to assess each risk, that of greater relevance to the risk assessed. Thus, each of these two elements is assessed with a weight of 100%. Both Occurrence and Frequency are rated in four levels ranging from 1 to 5.

6.4.2.3 Magnitude of the 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 from 1, 2, 3, 4 or 5. Each factor has a different weight within the magnitude of impact.

6.4.2.4 Residual Risk

Identification of key controls

The administration (first line) of each entity should assess whether it has controls in operation (i.e., in use) that are designed to adequately manage LAFT/FPADM 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: prevention or detection.

In any case, the following aspects should be taken into account when identifying key controls:

- ✓ A prevention control shall be considered as that which has the purpose of preventing errors, omissions or irregularities.
- ✓ A detection control is considered to be that which allows errors to be detected at the time they occur.

- ✓ A prevention control shifts the probability of occurrence since the focus of this type of control is to prevent the risk from materializing.
- ✓ Detection controls will shift the magnitude of the impact, considering that once the risk has materialized, it is necessary to focus on reducing its impact.
- ✓ A control cannot mitigate both probability and impact.
- ✓ Rating controls that are transversal, i.e., that are mitigating different risks, is done only once, i.e., their effectiveness rating will be the same in all the processes and causes where they are associated.
- ✓ Controls should be implemented to manage both the likelihood and the impact of inherent risk.
- ✓ Once the effectiveness of the control has been rated, its rating is averaged to reduce the inherent risk by risk, resulting in the residual risk.
- ✓ The proper identification and documentation of controls must be carried out, achieving adequate coherence between Risk-Cause-Control.

Assessing the Effectiveness of the Control

Grupo Aval, working together with the subsidiaries that participate in the LAFT/FPADM Corporate Committee, have defined different factors to perform the assessment of control, each with a different weighting depending on its effect on the effectiveness of the control; their ratings have defined weights measured through scales 1, 2 or 3.

The maximum mitigation level of a control has been defined as 85% for each risk.

Result of Residual Risk

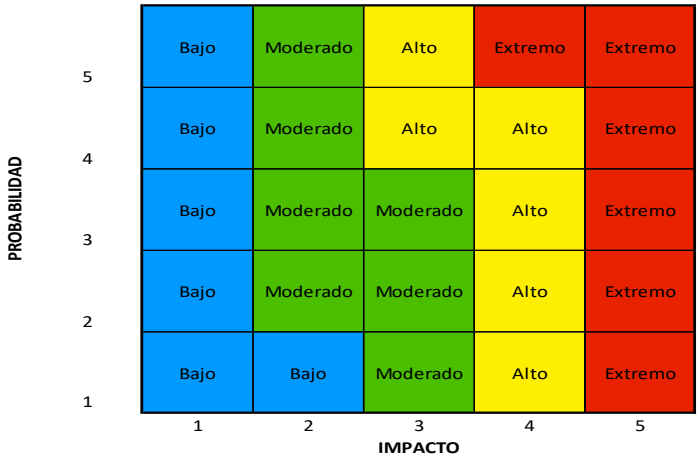
Based on the “Inherent Risk” ratings and the factors that determine the “Effectiveness of Control”, and the subtraction of these two criteria, the Residual Risk is derived. Consequently, Residual Risk is determined by:

IRPO: Inherent risk of probability of occurrence rating
EPOC: Effectiveness of probability of occurrence control rating
IRMI: Inherent risk of magnitude of impact rating
EMIC: Effectiveness of magnitude of impact control rating
IRPO – (IRPO*EPOC%)
IRMI – (IRMI*EMIC%)

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

Heat Map

The measurement model is based on measuring the inherent and residual risk of the entities and the group through heat maps. The heat maps make it possible to establish the most relevant risks to which the entities are exposed, taking into account the criteria of probability and impact. The colorimetry prioritizes the 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.



	Nivel de Impacto
Extremo	5
Alto	4
Moderado	3
Bajo	1 y 2

6.5 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, the process can be evaluated. A performance indicator, for example, provides quantitative information on the achievement of a program's objectives and can cover quantitative or qualitative aspects.

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

6.6 DEFINITION OF IMPROVEMENT AND MITIGATION PLANS

Monitoring reports are analyzed by the Corporate LAFT/FPADM Committee (Grupo Aval) entities, in order to determine the control points to be strengthened, review relevant changes and seek action plans to mitigate such changes. These action plans are approved by the committee to be implemented by the entities and Grupo Aval, in accordance with the projected schedules for each case.

In addition, the reports provide information on the risk management status of each of the entities and any new developments that may occur during the period, which gives the Committee the tools to define changes in the methodology and/or adapt prevention practices to mitigate risk.

Translation

The translation of this policy corresponds to a free translation from the original in Spanish.