DOCUMENT INFORMATION

Approval Statement	**Board of Directors According to Minutes No. 355 dated 10-14-2020**

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

TABLE OF CONTENTS

1. PROCESS

Control - Corporate and Conglomerate Risk

2. OBJECTIVE

- Establish the policies, methodologies and procedures for the management of the Operational Risk Systems in Grupo Aval Acciones y Valores S.A. (hereinafter "the Entity"), in order to maintain exposure to the operational risks derived from the fulfillment of the entity's corporate purpose, within accepted levels.
- Strengthen the control environment in the processes through the application of the mechanisms defined for the management of operational risks.
- Establish the guidelines to identify, measure, control and monitor the operational risks of the Entity.
- Establish a unified language within the Entity to strengthen the culture of risk management in the Entity.
- Support processes in the identification of risks and controls.

3. SCOPE

This document governs the Entity's processes, in accordance with the analysis carried out by the Vice President of Corporate Risks. For this, the aspects stated in the Operational Risk Management from the Financial Superintendency of Colombia are used, with this being taken as a frame of reference. The update is the responsibility of the Vice President of Corporate Risks, the approval will be in charge of the Board of Directors. It is the duty of all employers to know, abide by and apply the provisions established in this document.

4. GLOSSARY

- **Risk acceptance:** informed decision to take a particular risk. Accepted risks may be subject to monitoring and review.

- **Basel Accords:** set of proposals for reform of banking regulation, prepared by the Basel Banking Committee to strengthen regulation, supervision and risk management in the banking sector. These measures seek to:
  - ✓ Improve the banking sector's ability to cope with shocks caused by financial or economic stress of any kind;
  - ✓ Improve risk management and good governance in banks; and
  - ✓ Strengthen the transparency and disclosure of banking information

- **Risk appetite:** defined as the amount of risk that the Entity considers appropriate to undertake in order to achieve its strategic objectives. This depends on multiple factors such as market conditions, the economy, the sector, the Entity's economic capacity, growth and strategic

objectives, and the institutional culture towards risk. Risk Appetite is expressed through the Risk Appetite Statement with a set of quantitative and qualitative metrics.

- **Ability:** it is the maximum amount of risk that the Entity can assume in relation to its capital, risk management, control capacities and regulatory restrictions. In this way, capacity is a "top-down" measure that is related to the resources that the Entity possesses (capital, liquidity, leverage, etc.).

- **Controls:** any measure taken by the Entity and other parties to manage risks and increase the probability of achieving the established objectives and goals.

- **COSO:** internal control framework. (COMMITTEE OF SPONSORING ORGANIZATIONS). Which establishes the principles for an effective internal control system.

- **Criteria for evaluating or measuring a Risk:** the terms of reference against which the importance of a risk is evaluated. The Risk Criteria are based on the objectives and the external and internal context of the organization. In addition, Risk Criteria can be derived from standards, laws, policies, and other requirements.

- **Risk Appetite Statement:** set of thresholds and restrictions on quantitative and qualitative risk metrics, respectively, that express the Entity's Risk Appetite.

- **Process / controls owner:** the person responsible for the governance of the process assigned to them, insofar as it ensures that its controls are executed, monitored and sufficient evidence is left of both tasks. They have a functional structure that addresses the process, its risks and controls within the Entities according to their internal policies. When the owner of the process / controls is mentioned in this document, it should be understood that the owner of the process has a group of people who together are in charge of ensuring and monitoring that the controls are executed as designed, in such a way that the responsibility of the owner of the process / controls involves all the actors involved in the process and not only the chief employee / manager / vice president of the same.

- **Event:** an incident or situation that occurs in a particular place during a certain time interval.

- **Loss events:** those incidents that generate operational risk losses for entities.

✓ Classification of operational risks

For the purposes of this chapter, operational risks are classified as follows:

- Internal Fraud: acts that have the result of defrauding, improperly appropriating property or breaching current regulations, laws or business policies in which at least one employee or third party hired to execute processes on behalf of the entity is involved.

- External Fraud: acts, carried out by a person external to the entity, that seek to defraud, misappropriate its assets or breach rules or laws, in which a third party outside the entity is involved.

- Labor relations and labor safety: acts that are incompatible with labor legislation or with agreements related to hygiene or safety at work, or that deal with the payment of claims for personal injury or cases related to diversity and / or discrimination in the workplace.

- Clients, products and business practices: involuntary or negligent breach of a professional / business obligation towards clients or events derived from the nature or design of a product.

- Damages to physical assets: losses derived from damages or losses to physical assets of the entity as a result of natural disasters, acts of terrorism, vandalism or other events.

- Technological failures: events or changes caused by failures of hardware, software, telecommunications or public services that may affect, in addition to the internal operation of the entity, the provision of service to customers.

- Execution and administration of processes: errors in the processing of operations or in the management of processes, as well as in relationships with commercial counterparts and suppliers.

Additionally, for each type of operational risk event, the entity must establish, as a minimum, the subcategories indicated in section 3.2.5.4 of chapter XXIII of the Basic Accounting and Financial Bulletin (CBCF, for the Spanish original).

- **Risk factors:** risk factors are understood to be sources that generate operational risks that may or may not **generate** losses. Risk factors are human resources, processes, technology, infrastructure and external events.

  These factors should be classified as internal or external, as indicated below:

  ✓ Internal

  - Human Resources: the set of people directly or indirectly linked to the execution of the entity's processes.

    Direct relationship is understood to be one based on an employment contract in the terms of current legislation.

    Indirect relationship refers to those people who have a legal relationship with the entity for the provision of services, different from a relationship that originates in an employment contract.

  - Processes: the interrelated set of activities for the transformation of input elements into products or services, to satisfy a need.

- Technology: the set of tools used to support the entity's processes. Includes: hardware, software and telecommunications.

- Infrastructure: the set of supporting elements for the operation of an organization. Others include: buildings, workspaces, storage, and transportation.

✓ External

These are situations associated with the force of nature or caused by third parties, which are beyond the control of the entity in terms of their cause and origin.

- **Indicator (KRI):** Quantitative metrics for the material risks to which the entity is exposed, which reflect its Risk Profile and which allow its control and monitoring.

- **Risk Appetite Reports:** these include the periodic analysis of the Risk Profile and the action plans established to keep it within the corresponding thresholds.

- **Impact:** this is the loss (monetary or non-monetary) generated by the materialization of a risk, which can be measured qualitatively and quantitatively.

- **Operational Risk Manual:** this is the document that contains the policies, methodologies and procedures applicable in the development, implementation and monitoring of the ORM System.

- **Risk Appetite Framework:** this includes guidelines, organizational models and policies that establish both principles, roles and responsibilities; as criteria that determine the guidelines in which the Entity's risk culture is specified and common standards of cross-sectional application to various areas are defined.

- **Internal Control Reference Framework:** refers to the framework used by the management to evaluate the effectiveness of the design and operation of its internal control system. In the case of Grupo Aval, the Internal Control Reference Framework is COSO in accordance with the guidelines of the Superintendency, established in the basic legal bulletin.

- **Risk Profile:** the exposure to current and potential risks inherent in the development of the business plan.

- **Losses:** economic quantification of the occurrence of an operational risk event, as well as the expenses derived from its attention.

✓ Gross Loss: a loss before recoveries of any kind.

✓ Net Loss: the loss is understood after taking into account the effects of recoveries. Recovery is an independent event, related to the gross loss event, which does not necessarily take place in the same period for which funds or economic flows are received.

- **Probability:** The possibility that a risk materializes. Qualitative or quantitative analysis can be used to determine probability.

- **Processes:** A set of interrelated activities, which transform input elements into results or output elements and generate added value.

- **Person Responsible for Information - RES:** the executive for whom the information was created in order to perform their functions in the business and who has the responsibility of managing it, classifying it and evaluating the risks that may affect it.

- **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.

- **Operational Risk (RO, for the Spanish original):** the possibility that the entity may incur losses due to deficiencies, failures or inadequate functioning of the processes, technology, infrastructure or human resources, as well as due to the occurrence of external events associated with them. Includes legal risk.

- **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. It applies to all activities and includes third parties who act on behalf of the entity with respect to outsourced processes and / or activities.

- **Operational Risk Management (ORM) System:** a set of elements such as policies, procedures, documentation, organizational structure, operational risk event registry, control bodies, technological platform, information disclosure and training, through which the supervised entities identify, measure, control and monitor operational risk.

- **Tolerance:** the acceptable level of the variation or deviation from the risk appetite that the Entity is willing to assume while pursuing its objectives. It serves as a warning to avoid reaching undesired levels of risk exposure and / or your maximum risk-taking capacity.

- **Operational Risk Unit (URO, for the Spanish original):** the area or position, designated by the Legal Representative of the entity, responsible for managing the ORM system.

5. REGULATIONS

- Framework: Chapter XXIII Basic Accounting and Financial Bulletin of the Superintendency of Finance.

Other Regulations:

- ISO 31000 standard
- Basel Accord

6. RESPONSIBILITIES

6.1 ORGANIZATIONAL CONTEXT OF GRUPO AVAL

Grupo Aval Acciones y Valores S.A.'s corporate purpose is the purchase and sale of shares, bonds and securities of entities belonging to the financial system and of other commercial entities.

In development thereof, the Company may acquire and negotiate all kinds of securities freely circulating in the market and securities in general; promote the creation of any type of company that complements or is related to the corporate purpose; represent individuals or legal entities engaged in activities similar or complementary to those indicated in the preceding paragraphs; acquire or grant monetary loans with or without interest, give as collateral or in administration their movable or immovable property, issue, endorse, acquire, accept, collect, deny, cancel or pay bills of exchange, checks, promissory notes, or any other securities, or accept or offer them as payment and execute or celebrate exchange contracts of all manifestations, modalities or related, parallel and / or additional activities.

In order to have an adequate control environment, the Entity has adopted COSO as a reference framework.

6.2 LEADERSHIP AND COMMITMENT

This chapter describes the commitments of the organizational structure with the Operational Risk Management System, for the fulfillment of the policies, functions and responsibilities that employees must assume for the implementation, and monitoring of the risk mitigation activities assigned to them. The system policies and functions are listed below:

6.2.1 Management Commitment

The President of Grupo Aval, through the Vice President of Corporate Risks, is committed to the implementation and development of the ORM System in terms of compliance with policies, objectives and strategies to strengthen the risk culture that the administration of the ORM System implies.

6.2.2 Operational Risk Management Policies

The operational risk management Policies of the ORM System are based on the organizational context in which the Entity is located and are framed within the following policies:

Strategic Policy

Operational Risk management is aimed at creating and strengthening a Risk culture through training and raising awareness of all the Entity's employees, which allows for the identification of risks and controls that may arise in the development of the activities of its processes. For this, it is important to have a constant flow of information among all areas of the Entity, strengthening the reporting culture and supporting the mitigation of potential risks.

Governance Policy

The management and control bodies and other collaborators of the Entity have functions defined in the ORM System, evidencing their role and specific responsibilities in each of the System stages, ensuring their compliance and alignment with its objectives.

Independence Policy

The URO as an independent area and maintaining its impartiality, has access to all the information it deems necessary for the execution of each of the stages of the ORM System and especially for recording operational risk events.
For the development of its functions, the URO has personnel with experience and trained in operational risk management and with sufficient resources. This Unit is in charge of the Corporate Risks and Conglomerate Standards Management, with a high organizational level and decision-making capacity.

Disclosure Policy

The URO generates the operational risk profile, its evolution, and the changes that occur in the implemented controls. The results of the progress of each of the ORM System stages are at all times available for consultation by the members of the Risk and Audit Committee, for their respective feedback and continuous improvement.

Business Continuity Policy

The Business Continuity Policies are established in the "Business Continuity Manual", which are based on actions that seek to mitigate the impacts of events that interrupt the Entity's normal operation.

6.3 LINES OF DEFENSE AGAINST RISK

Grupo Aval has established the principle of the three lines of defense in accordance with the COSO framework.

The Entity structures its functions and responsibilities in the face of the risks that it is exposed to, following the scheme of the three lines of defense, that is, considering (i) management by line of business, (ii) an independent risk management function, and (iii) an independent review.

First Line of Defense

The first line of defense lies with each of the areas or employees of the Entity responsible for the development of its corporate purpose (e.g., the activities facing the public that are in direct contact with clients and the back office processes necessary to attend to their needs). This means that such areas or employees are primarily responsible for identifying, evaluating, managing, monitoring and reporting the risks inherent in the activities, processes and systems for which they are responsible. Those who make up this line of defense must know their activities and processes, and have sufficient resources to effectively carry out their tasks.

Second Line of Defense

This line of defense is made up of the URO. It is independent from the first line, it monitors compliance with all obligations regarding Operational Risk, it is responsible for defining the methodology for managing this risk, as well as the identification of the right tools for this purpose.

Third Line of Defense

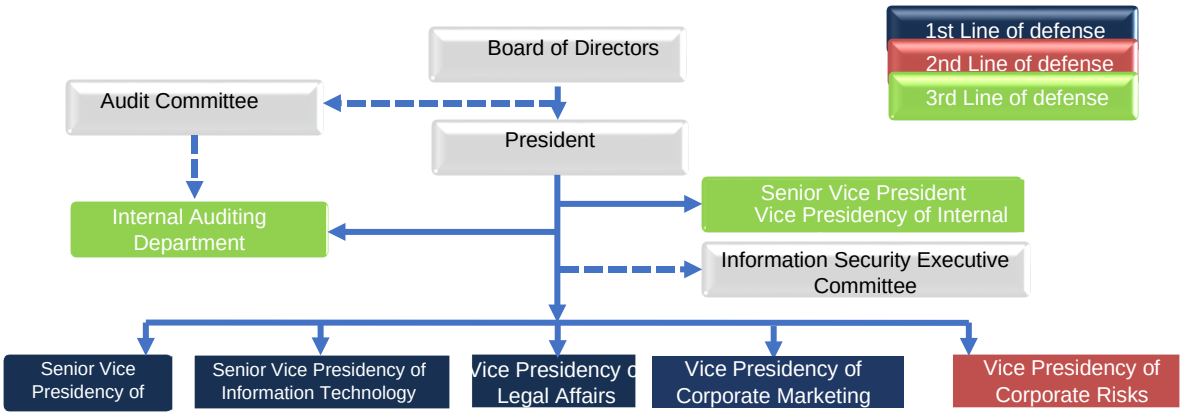
The third line of defense is made up of the Internal Auditing Department and it is responsible for carrying out the independent evaluation of the Operational Risk management in the entity, as well as the processes and systems that comprise it, reporting to the Audit Committee.

This review can be carried out by the audit staff or by personnel independent of the process or system under examination, but it can also involve suitably qualified external actors. These provide an objective assurance on the effectiveness of risk management to the Board of Directors and / or Audit Committee, ensuring that key business risks are being properly managed and that the internal control system implemented is being operated effectively.

6.4 ORGANIZATIONAL FUNCTIONS, RESPONSIBILITIES AND AUTHORITIES

The ORM System compliance process requires the supervision of the Entity's senior management, the control bodies and the establishment of the roles and responsibilities applicable to each and every one of the employees.

The following is the organizational structure of the ORM System:



Board of Directors

Notwithstanding the functions assigned in other provisions, the ORM System must contemplate at least the following functions in charge of the Board of Directors or body that acts in its stead:

- Approve the Operational Risk Management Manual, and its updates.
- Monitor and make a statement on the entity's operational risk profile. The foregoing is in accordance with the Risk Management Framework of Grupo Aval .
- Request the necessary measures to adjust the operational risk profile, when it is outside the levels set by the Board of Directors. The foregoing is in accordance with the Risk Management Framework of Grupo Aval.
- Provide the necessary resources to implement and maintain the ORM System in an effective and efficient manner.

Audit Committee

The Committee, as a support body for the Board of Directors in relation to the supervision of the internal control system, and in relation to the ORM System, performs the following functions:

- Evaluate compliance with the Policy and request the adoption of the necessary measures when breaches are identified. These will be evidenced through the reports on the periodic evaluation of the ORM System presented by the Internal Auditing Department, according to its annual work plan.
- Know and discuss the reports presented by the Vice President of Risks on the Grupo Aval ORM System.

President of Grupo Aval

Without prejudice to the responsibilities assigned in other provisions, the functions of the President are:

- To approve the presentation and submit to the consideration and approval of the Board of Directors, the Operational Risk Management Manual and its subsequent updates.
- Ensure effective compliance with the policies established in the Operational Risk Manual.
- Know the reports on the periodic evaluation of the ORM System, carried out by the control bodies.
- Designate the area or position that will act as responsible for the implementation and monitoring of the ORM System - (Operational Risk Unit - URO).
- Be informed through the Vice Presidency of Corporate Risks about the evolution of Grupo Aval's Operational Risk.
- The President, through the Vice Presidency of Corporate Risks and the heads of the other areas of Grupo Aval, must develop and ensure that the strategies are implemented to strengthen the culture in the management of this risk in the entity.
- Adopt the necessary measures to adjust the operational risk profile, when it is outside the levels set by the Board of Directors. The foregoing, within the Risk Management Framework of Grupo Aval.

Vice Presidency of Corporate Risk

- Review and submit to the President's consideration, the Operational Risk Management Manual and its updates, for approval by the Board of Directors.
- Ensure effective compliance with the policies established in the Operational Risk Management Manual.
- Present periodic reports to the President and the Audit Committee on the evolution and relevant aspects of the ORM System.
- Follow up on the stages and elements established in the ORM System.
- Develop and ensure that strategies are implemented to strengthen the culture of operational risk management in the entity.
- Evaluate the reports presented by the Operational Risk Unit.
- Ensure that the procedures for operational risk management are implemented, including the reporting of operational risk events, assuring compliance with the criteria of integrity, availability and confidentiality of the information contained therein.
- Inform the Audit Committee and the President in a timely manner about any important event that affects the operational risk of the entity.

Operational Risk Unit (URO, for the Spanish original)

The functions of the Operational Risk Unit correspond to the Corporate Risk Management and Conglomerate Standards. For this purpose, it has the Operational Risk Department and the support of the Operational Risk Analyst. Its responsibilities are to:

- Define the methodologies, instruments and procedures necessary for the adequate management of the Entity's operational risks, in accordance with the volume and complexity of the operations carried out.
- Develop operational risk measurement models that allow the Entity's risk profile to be established.

- Develop and implement the reporting system, internal and external, of the entity's operational risk.
- Monitor the risk profile of the entity and report it to the Vice Presidency of Corporate Risks.
- Coordinate the collection of information to feed the record of operational risk events and manage it.
- Assist the processes in the identification of their risks and controls.
- Request the necessary action plans from the processes to keep risks within accepted levels and carry out follow-up.
- Design and execute the entity's training programs related to the ORM System.
- Support the identification of risks when the process owner considers it and during the implementation or modification of any process, product, service or channel, as well as in cases of merger, acquisition, transfer of assets, liabilities and contracts, among others.
- Report every six months to the Vice President of Corporate Risks, the evolution and relevant aspects of the ORM System.
- Design and propose to the Vice Presidency of Corporate Risks the Operational Risk Management Manual, as well as its updates, for later presentation to the President of Grupo Aval and the Board of Directors.

Process Owners and Other Employees

- Keep the processes under their responsibility documented and updated. To achieve this, they must have clearly defined, disclosed and understood procedures.
- Strict compliance with the guidelines and policies defined in this Manual, as well as the management procedures.
- Know clearly the activities that make up the process, its objective, its frequency of execution and classification within the process map.
- Have adequate policies and processes to select their staff, in order to guarantee high ethical and professional principles.
- Provide induction and training programs to employees in order to ensure that they have the competencies for the proper execution of the activities under their responsibility.
- Participate in the stage of Identification, Measurement, Control and Monitoring of Operational Risk.
- Keep the staff updated on their obligations and responsibilities, which must include within their scope the possible risk factors to which the employees are exposed when fulfilling their responsibilities.
- Identify the operational risks and controls of the processes carried out in the development of their functions.
- Know the rules that govern their process, in order to identify legal and compliance risks in accordance with the terms and definitions in this manual.
- Define the action plans where there is room to mitigate risks outside the accepted levels, in accordance with the periodicity and methodology defined by the URO and in any case at least once in a six-month period.
- Ensure self-management, self-control and self-regulation in the execution of their activities, and inform the URO in a timely manner of changes that occur in its activities and that may modify the current operation and therefore the risks identified.

- Carry out the evaluation of their operational risks with the standards defined by the URO.
- Adequately and timely report risk events in the form defined by the URO and the fields must be filled out in their entirety. If they become aware of a materialized risk event that is not their responsibility, they must notify the URO to request the event report from the appropriate person.
- Verify the implementation of the controls that are part of the processes in the area and update the rating in the operational risk matrix. In case of changes in both the controls and the risks of the process, notify them to the URO.
- For those risks whose exposure at a residual level is outside the Entity's risk appetite and expresses its agreement with said level, the RES must carry out a Risk Acceptance process, in accordance with the protocols defined by the URO. The URO will present in its reports the summary of those risks that this situation presents.
- Report to the URO potential situations that indicate possible new risks in their process.
- Include the URO in the disclosure of new documents or changes in the processes carried out through the Organization and Methods area, in order to update the ORM System matrices and implement and schedule continuity tests if the change requires it.
- Participate in the training and activities defined by the URO to strengthen the ORM System.
- For processes that in the identification of operational risks and due to their probability or impact are considered critical risks and that also may cause the interruption of the normal operation of business, the processes will be responsible for documenting their contingencies in the corresponding internal documents. However, together with the URO, an assessment of inclusion in the Entity's business continuity strategy must be carried out, under the Continuity policies that are published in the manual of said Management system.

Breach of Established Rules and Procedures. Administrative sanctions for non-compliance with the provisions of this document will be applied in accordance with the provisions of the Internal Work Regulations, without prejudice to any legal sanctions that may apply.

ORM System Management Support Areas

Some areas are an important source for the adequate management of the ORM System in the Entity. Due to the execution of their activities and support to the other processes, they present relevant information which is input for the URO, to review the risks and controls identified in the processes. This information will be supported and agreed by SLAs signed by the areas, in order to agree on the minimum parameters in the supply of information to the URO.

- The Technology area must inform the URO and the Organization and Methods Directorate when it makes changes to the technological infrastructure, in order to update the established processes and continuity strategies.

- The events or incidents that are reported to the IT area must be notified to the URO to analyze whether an operational risk event report and any adjustment in the ORM System matrix should be made.

- The Organization and Methods area will include the URO in the disclosure list of creation, modification, elimination, of the different documents of the processes (Manuals, policies, procedures, others) so that it can carry out the process of updating the SARO matrix.

- The Internal Auditing Department may send the reports generated by its audit plan in the processes, in order to show failures in the controls and that require updating the ORM System matrix.

- If the Legal Department has received reports from external entities and that in its judgment considers appropriate to communicate to the URO, it must send the communication to make adjustments to the risks and controls where applicable.

- If the Regulatory Risk Management which leads the information Security and Cybersecurity system has incident reports form the entity, they must notify the URO, for their management from operational risk.

Internal Auditing Department

Notwithstanding the functions assigned in other provisions to the Internal Auditing Department, the latter must periodically evaluate, according to its annual work plan, the ORM system in order to determine possible weaknesses in the internal control system and request the required action plans. Likewise, it will report the results of the evaluation to the Operational Risk Unit to the Vice Presidency of Corporate Risks, the Presidency and the Audit Committee.

7. GENERAL GUIDELINES

7.1 STAGE I - IDENTIFICATION OF OPERATIONAL RISKS

The specific objective of this stage is the identification of the inherent risks based on the process map or the methodology that the URO determines for the Entity.

7.1.1 Identification of Risk Factors and Operational Risks

The identification of risk factors and loss events is carried out according to the provisions of the regulatory references and the glossary of this document.

7.1.2 Risk Identification Methodology

- The determination of the risks inherent in a process will be carried out by the owner of the process with the support of the URO, based on the knowledge of the process and identifying the possible causes that may affect the fulfillment of the objectives and strategy of Grupo Aval.

- Those who participate in the risk identification phase must rely on reliable information and have a good knowledge of the processes and the Entity. Apart from experience, it is recommended to have the documentary support provided by management and audit reports, findings from surveillance and control entities, plans, diagnoses, regulations and standards, surveys, checklists, statistical data and event records.

- Risk identification should answer the following cycle of questions:

Figure No. 1

- When carrying out the analysis, both the operational risks that have already been presented and the potential risks must be taken into account.

- Risk identification will be carried out based on the protocols defined by the URO.

- Once the risks that could originate operational risk events in a process have been identified, the information must be recorded in the risk matrix defined by Grupo Aval.

- Prior to the implementation or modification of any process, product, service or channel, as well as in cases of merger, acquisition, transfer of assets, liabilities and contracts, etc., the risks are identified in order to foresee the control scheme that can mitigate their impact upon their materialization.

7.1.3 Inherent Risk Profile

This corresponds to the result of the identification of the risks inherent to the execution of the activity without taking into account the effect of the controls carried out by the process.

7.2 STAGE II - MEASUREMENT OF OPERATIONAL RISKS

The specific objective of this stage is to measure the level of Operational Risk, for which a qualitative measurement will be carried out, and when there is data on Operational Risk events, this will be carried out quantitatively. For this, the following guidelines are established:

- Frequency of Operational Risk is measured with a one-year horizon.
- Impact and probability scales are determined to measure risks.
- The inherent risk profile will be made based on the judgment of people familiar with the Entity's processes, for which the Delphi method scheme is applied.
- When there is sufficient information on operational risk events, the assessment of probability and qualitative impact is adjusted using the basis of the materialized events as a tool. These events will be crossed with the qualitative Operational Risk matrix to adjust the profile of the main valuation.
- In order to carry out an adequate assessment of the risks, the impact and probability of both qualitative and quantitative variables are evaluated, under the criteria defined in the Methodological Risk Annex A-R_corporative-8.

7.3 STAGE III - CONTROL

In order to mitigate the materialization of operational risks to which the Entity is exposed in the execution of its operations, prevention and control measures must be applied. These measures are aimed at reducing the probability of occurrence and / or the impact on should it materialize. For ORM System purposes, it is understood that the operational risk matrix includes those key controls that really mitigate the risk. During this stage the following are established:

- Methodology to define the control measures for operational risks.
- Control measures on each of the operational risks.
- Measures to ensure business continuity.
- The entity's residual risk profile.

Notwithstanding the foregoing, the Entity decides whether to transfer, mitigate, accept or avoid risk, in cases where this is possible. When deciding to accept the risk, the protocols defined by the URO must be followed.

The use of certain measures, such as the contracting of insurance or outsourcing of both natural and / or legal persons, and that proceed to the development of the Entity's activities, may be a source of other operational risks, which must be in turn administered.

For that, the entity must: (i) carry out a risk analysis to determine the processes and / or activities to be outsourced; (ii) understand the operational risk associated with outsourced processes and / or activities; (iii) have effective policies to incorporate risks derived from outsourcing into its strategy; and (iv) determine within the outsourced processes and / or activities those that are considered critical.

7.3.1 Evaluation of Controls

In the evaluation of the controls, two criteria are taken into account: Coverage and Opportunity. As a result of the combination of these criteria, the control efficiency is determined.

- Control coverage

The purpose of this phase is to evaluate the control with respect to the risk that is being mitigated. During the risk and control exercises, the experience of the work team and the best practices must be taken into account to determine whether the defined controls are aimed at reducing the probability of occurrence on the one hand, or the impact of the assessed risk on the other. Otherwise, new or complementary controls should be established.

- Control opportunity:

This is the rating given to the level of execution of the control in the process.

The sum of the coverage and the opportunity determine the efficiency of the control:

- If the control is not running
- If the control is running in the process, but does not meet all the parameters established in the process design
- If the control is running in the process according to the parameters established in its design

The characteristics of the control evaluation are found in the Operational Risk Methodological Annex.

7.3.2 Residual Risk Profile

In this phase, the effect of the controls on the inherent risk profile is taken into account, the calculation of impact and probability of occurrence is carried out automatically and shows the residual risk levels for the processes. The generation of the residual risk profile includes:

- The assessment of the existing controls in each process.
- Review of materialized events.

7.4 STAGE IV - MONITORING AND REVIEW OF THE ORM SYSTEM

Every six months the URO monitors the inherent and residual risk profiles, as well as the materialized events, in which the assessment of new processes, new controls and redesign of current controls is reviewed.

Likewise, the evolution of external or internal variables that could be generating a greater probability of occurrence or financial impact is taken into account.

The URO's semi-annual report must include at least:

- Composition and Rating of Risks (Analysis report carried out on the factors and classes of Operational risk events identified in the matrix).
- Results of the changes generated by updating the Operational Risk matrix, by new processes, controls, application of treatment plans or remediation against the profile.
- Statistical Reports of Operational Risk Events.
- Analysis and Monitoring of Treatment Plans.
- Risk acceptance report.
- Results of the execution of the training program.

In the process of monitoring and follow-up of the risk profiles, the descriptive and prospective indicators referenced in the Operational Risk Methodological Annex are also used as sources, verifying the behavior and carrying out the assessment of these in the cases that apply.

These indicators focus on observing the control management and the materialization of events over time. They can be classified into control or performance indicators (related to results of the procedure).

7.5 OPERATIONAL RISK EVENTS RECORD

Operational Risk events are an indispensable source of information for the proper management of the ORM System. For this purpose, the Entity has a record of operational risk events which must be updated and its administration is the responsibility of the URO.

The operational risk events record must comply with the following guidelines:

- The record must contain all operational risk events that have occurred and that:
- Generate losses and affect the entity's income statement.
- Do not generate losses and therefore do not affect the entity's income statement.
- The losses defined in accordance with the previous item, when they affect the income statement, must be recorded in expense accounts in the period in which the loss materialized.
- Recoveries for operational risk when they affect the income statement must be recorded in income accounts in the period in which the recovery took place.
- The required income and expense accounts are defined by the Superintendency in the respective Single Catalog of Financial Information (CUIF, for the Spanish original).
- Report all events, whether or not they generate losses. All the Entity's personnel are responsible for reporting operational risk events or ensuring that they are reported.

- The reporting of Operational Risk events is carried out through the form established by the URO, these must be reported through the mechanism defined for said Unit or, otherwise, to the Vice President of Corporate Risks.
- The Operational Risk events generated by the Technological factor (hardware, software, telecommunications) must be reported to the Technical Support area of Grupo Aval, with a copy to the URO, so that the failure correction management can be carried out. Later, Technical Support must report the solution to the process that reported the event and to the URO.
- Once the event is reported to the URO, the latter will proceed to carry out the investigation and analysis of the Operational risk event, so that together with the process owner, the record can be completed in the minimum fields stated in the previous section.
- The operational risk events that are reported are intended to review possible measures that tend to improve the process control environment. Non-compliance activities will be treated in accordance with the provisions of Grupo Aval's Code of Ethics and Conduct.
- Records of events on operational losses must be comprehensive and include all activities and exposures.
- The minimum fields to fill out in the Record of Operational Risk Events are:

Name	Description
Reference	Internal code that relates the event sequentially.
Event start date	Date the event starts.
	Day, month, year, hour.
Event end date	Date the event ends.
	Day, month, year, hour.
Discovery date	Date the event is discovered.
	Day, month, year, hour.
Accounting record date	Date on which the loss for the event is recorded in the accounting records.
	Day, month, year, hour.
Recovery date	Date on which the money used to address an operational risk event is fully or partially recovered.
	Day, month, year, hour.
Currency	Foreign currency in which the event is materialized.
Gross amount	The amount of money (legal currency) to which the gross loss amounts.
Total amount recovered	The amount of money recovered by direct action of the entity. Includes amounts recovered by insurance.
Amount recovered by insurance.	This corresponds to the amount of money recovered by the coverage through insurance.
Amount of other recoveries	This corresponds to the amount of money recovered by mechanisms other than coverage through insurance.
Net amount of recoveries	The amount of money (legal currency) to which the loss amounts taking into account the total amount recovered.
Operational risk type	This specifies the type of risk, according to the classification indicated in the glossary of this document.
Product / service affected	Identify the affected product or service.
Catalog accounts affected	Identifies the accounts of the Single Catalog of Financial Information for Supervision Purposes "(CUIF) affected.
Process	Identify the affected process.
Type of loss	Identify the type of loss, in accordance with that indicated in Stage III - Record of operational risk events

Name	Description
Description of the event	Detailed description of the event.
	- Customer care or service channel (when applicable)
	- Geographical area
Business lines	Identification according to the classification adopted by the SFC, these lines are indicated in the event report format.

7.6 DISCLOSURE OF INFORMATION

The Operational Risk Management Manual approved by the Board of Directors is published by the Organization and Methods area on the Entity's shared resource.

7.7 TRAINING

This is an essential requirement for both current employees and in the induction of new employees, training in the ORM System is carried out. That is why the entity organizes training sessions and these include aspects related to operational risk management and business continuity, in order to ensure that the policies and procedures of the ORM System are adequately known by all employees.

Grupo Aval carries out at least one annual training session for current employees and is focused on providing knowledge in the mechanisms and tools required for the adequate management of Operational Risk.

These programs are supported by the attendance record for induction and participation record for current employees, in addition there is an evaluation or workshop to measure the knowledge acquired by the employees.

When, by virtue of a contractual relationship, there are third parties that perform functions of the entity, training is carried out on the relevant aspects of the ORM System.
This activity should be led by the URO with the support of the Administrative and Human Talent area.

The training program has the evaluation of the results obtained, which allows to determine the effectiveness of the program.