Corporate Risk Management Policy

This public version is an extract from the Corporate Risk Management Policy of Viña Concha y Toro S.A.

I Corporate Risk Management Policy

1. Metodological Framework

The Corporate Risk Management Policy ("the Policy") in this report is issued in compliance with the standards contained in the applicable local legislation, ISO 31000:2018 , COSO 2013 and the best practices of Corporate Governance for Open Stock Corporations, as defined by the Financial Market Commission ("CMF") in its General Standard N°461.

2. Purpose

The Policy seeks to establish the basic principles, processes, roles and responsibilities associated with Risk Management (Strategic, Operational, Financial Reporting and Compliance Risks), to both protect and create value for the Company and to assist in achievement of its objectives. It also seeks to reasonably ensure that any relevant risk is properly identified, managed in a timely manner and reported when necessary, while also generating valuable information to complement the decision making process.

3. Objectives

The main objectives of this Policy are:

- To specify the responsibility of Senior Management (Board of Directors, Directors' Committee, General Management and Corporate Management) in risk identification and its correct communication to all collaborators, in order to ensure proper risk management and its incorporation to the Company's various processes.

- To formally incorporate Risk Management in the Company's organizational culture, integrating it naturally in the day to day execution of business processes, by strengthening the current policies and procedures with a formal definition of responsibilities.

- To contribute to the Company's performance by seeking greater operational efficiency and responding adequately and in advance to undesired events.

- To anticipate potential events that have not yet occurred and ensure timely communication of those that have occurred, thus generating centralized risk databases that minimize the possibility of their recurrence.

4. Scope

This Policy applies to Concha y Toro Vineyards and all its subsidiaries, both national and foreign, and extends to all processes and business units[1]. Companies that do not consolidate in Concha y Toro Vineyards reporting manage their risks independently; nevertheless, there are risks which the parent company must anticipate or consider by the mere fact of participating in its ownership.

The Policy also extends to third parties that have a relationship with the Company, such as contractors, subcontractors and suppliers.

The Policy seeks to cover all types of risks in terms of their origin, nature and possible consequences.

The Policy should be read in conjunction with the applicable methodological framework as defined in point 1 above.

Finally, the methodologies established in this Policy are applicable not only to existing processes, but also to potential new processes or relevant projects of any kind.

5. Definitions

Risk: Defined as the possibility of occurrence of an event that may affect the strategy or the objectives of the company, favorably or unfavorably, which is measured according to its level of impact and probability of occurrence.

Impact: Represents the impact or set of consequences created if a risk were to occur.

Probability: Represents the possibility that a given event will occur.

Inherent Risk: It is the risk that affects achievement of the organization's objectives, **in absence of actions taken by management** to alter the probability or impact of the risk.

Residual Risk: Is the risk that affects the achievement of the organization's objectives and **that continues to exist** once the relevant management responses (controls) have been adopted and implemented.

Internal Risk: It is the business risk that depends on the management within the company, both at a general level and in each of its business areas.

[1] The Risk Management Policy extends to Joint Ventures in which the Company has control, as defined by Chile's Securities Law.

External Risk: It is risk that originates in the environment and influences or conditions the organization directly or indirectly and which has the potential to become a real threat for the company.

Strategic Risk: "A risk to the strategy or a risk created by the strategy", that is, any undesired event (risk) that may affect the fulfillment of the Company's strategy or of its strategic objectives. These risks can be uncertainties and are the key issues that concern the winery's Board of Directors.

Operational Risk: The possibility of failure in achieving performance, financial and operational objectives, or of protecting the Company's assets against possible losses.

Financial Reporting Risk: Risk of non-compliance in matters of presentation and disclosure of financial and non-financial information, both internal and external, covering reliability, transparency and other issues established by regulators, standardization bodies or by Company policies.

Regulatory Compliance Risk: Risks linked to non-compliance with the laws and regulations with which the Company must comply.

Preventive Control: Those controls that anticipate undesired events before they happen.

Detective Control: Are those controls that identify events at the time of occurrence.

Business Process: Set of logically related activities that use the organization's resources to provide defined results with the goal of achieving business objectives.

Internal Control Area: This area is responsible for ensuring reasonable achievement of operational, financial reporting and compliance objectives, by monitoring activities on specific controls, supporting areas in the identification, prioritization and mitigation of risks. This area also assists in the design, development and maintenance of the internal control system, and in monitoring the implementation of corrective action plans.

Internal Control Committee: Composed of the Corporate Finance Manager, Corporate General Auditor, Overseas Financial Administrative Manager, Head of Internal Control and Internal Audit Coordinator. This Committee's goal is to review the status of risk matrices updating and action plan implementation, committed to by each responsible unit, and which allow risks that require higher priority to be managed opportunely. This Committee meets on a monthly basis on average.

Three Lines of Defense Model: This model provides a simple and effective way to improve communications in risk management and control by clarifying the essential functions and duties involved. This model helps ensure the continued success of risk management initiatives, increases clarity regarding risks and controls, and improves the effectiveness of risk management systems.

6. Principles

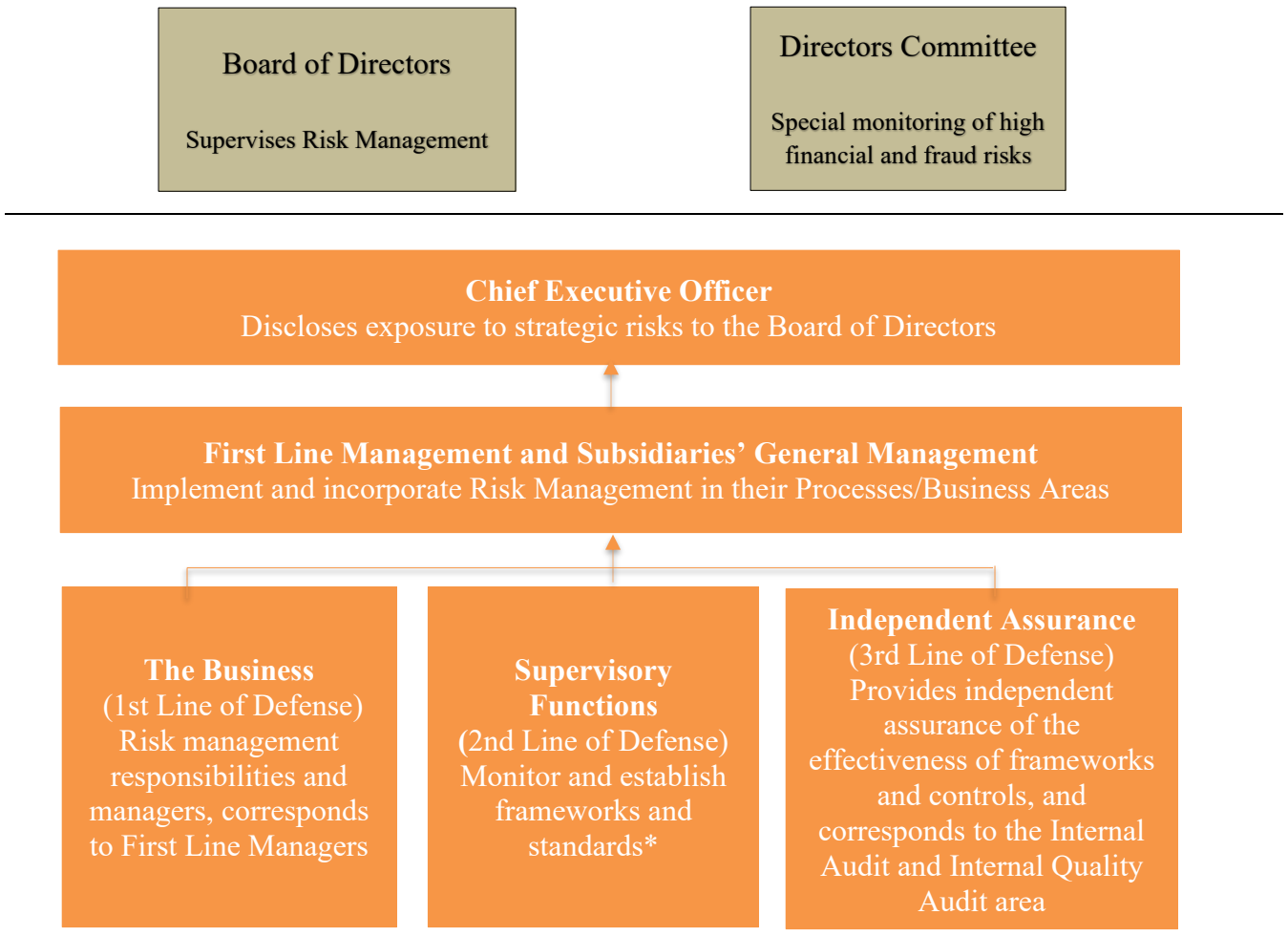
Concha y Toro's business is not risk free, especially considering the Company's vertical integration. The Company's operations extend across all stages, from production, processing and marketing to distribution of its products through subsidiaries in Chile and abroad or third party distributors.

Assuming risks is an essential part of the business; the Company consciously takes the appropriate amount of risks and manages them competently to find opportunities and ensure achievement of objectives.

Risks must be impartially evaluated. Risk Management includes the identification, analysis and evaluation of risks, appropriate and timely responses, and monitoring and reporting of these risks to provide assurance that objectives can be achieved.

7. Government

Concha y Toro winery has adopted the "Three Lines of Defense" model, which is summarized in the following diagram:



These are the areas: **Internal Control, Management Control areas (Commercial, Support Areas, Modeling and Reporting), Sustainability, Quality (Winemaking, Suppliers, and Productive Plants) and Safety.*

The Internal Control Area, as a second line of defense, monitors and evaluates the state of the controls, advises and accompanies the first line of defense in risk management. This area provides a reasonable degree of security regarding the development of objectives, effectiveness and efficiency of operations, reliability of financial information and compliance with applicable regulations and policies in force.

8. Responsibilities

The roles and responsibilities related to Risk Management include the following actors:

- The Board of Directors is responsible for the proper supervision of the Company's Risk Management. For these purposes it must:
  - Approve risk management policies, practices and methodologies.
  - Have knowledge of the adequate governance of Internal Control supervision and have direct supervision of the risk management responsibilities of First Line Management.

- The Chief Executive Officer, or his delegate, discloses to the Board of Directors the exposure to strategic risks and is responsible for the overall risk management culture, capabilities and practices to achieve the Company's strategy and objectives. The responsibilities of the General Manager include:
  - To assess the strategy considering risk tolerance and monitor risks.
  - To guide the development and performance of the Risk Management process, to ensure its appropriate delegation, and to communicate expectations and reporting requirements.

- First Line Management and Subsidiaries' General Management (or Finance Management if General Management does not exist) must report to General Management on the effective implementation and integration of the elements of risk management. They must also provide the necessary resources to effectively manage risk. They are responsible for identifying, evaluating, responding to, managing and reporting risks within their respective business areas, implementing appropriate treatments when risks exceed the defined tolerance level. In addition, they are responsible for keeping the policies, procedures and internal instructions formally updated.

- Corporate Finance Management, through its Internal Control area, monitors the development of Risk Management as part of its responsibilities in the second line of defense, and advises the Board of Directors, General Management, First Line Management and Subsidiaries' General Management on compliance of their respective supervisory responsibilities and evaluating the risk assessment they have performed. Internal Control advises on the establishment of risk management practices, conducts training and proposes improvements to the Risk Management process when necessary.

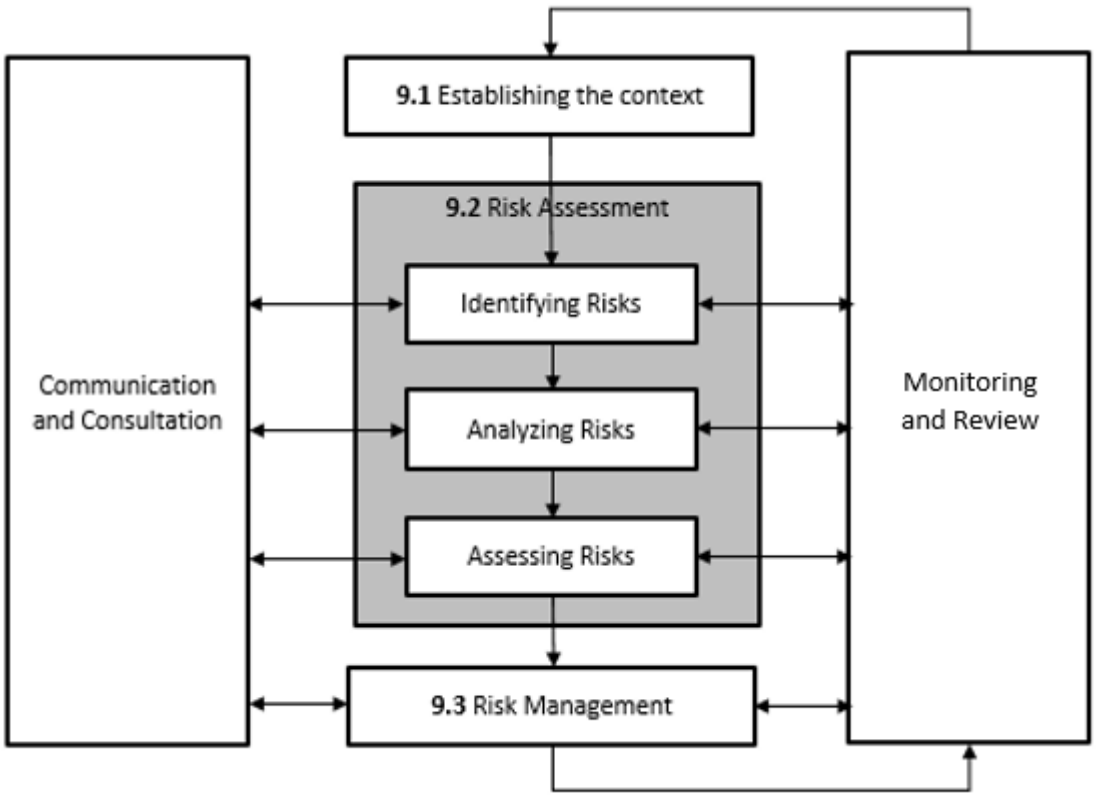
- The Internal Audit and Internal Quality Audit areas, are the Third Line of Defense, and provide an independent opinion regarding effectiveness of the risk management framework and controls.

Any deviation from this Policy must be formally approved by the Internal Control Committee.

II The Risk Management Process

9. Risk Management

Risk management is a structured approach to managing uncertainty surrounding a threat (occurrence of an event), through a sequence of activities that include risk identification, analysis and evaluation, then establishing strategies to handle risk using management resources. The following figure illustrates the risk management process[2]:



The various actions of the Risk Management process, i.e. 9.1 Establishing the Context, 9.2 Risk Assessment and 9.3 Risk Management, are explained in detail below.

[2] Process according to ISO 31000:2018

9.1 Establishing the Context

Corporate Finance Management, through its Internal Control area, together with General Management, must establish the context for risk management at a strategic level and update it annually. This activity comprises the following assessment:

Strategic SWOT Analysis[3]: Sources of Risk, Weaknesses, Opportunities, Threats.
Identification of Regulations: Market, Voluntary Standards, Environmental, Food, Accounting Standards, among others.
Review of the accepted risk level and risk tolerance.

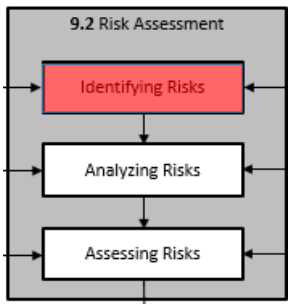
9.2 Risk Assessment

Risk assessment is the general process of risk identification, risk analysis and risk evaluation. This risk assessment must be carried out by First Line Management (i.e. management directly dependent on the parent company's General Management or a subsidiary's General Management) for each area. This review must be carried out at least annually or in the event of any relevant change which affects processes managed by those Managements.

The method to be used for risk assessment is qualitative analysis, which must be applied using the Cause - Impact methodology, explained in the following points and defined in ISO 31010.

9.3.1 Risk Identification

The purpose of risk identification is to find, recognize and describe risks that could help or prevent an organization from achieving its objectives. The identification of risks should be carried out for both internal and external risks to the process.

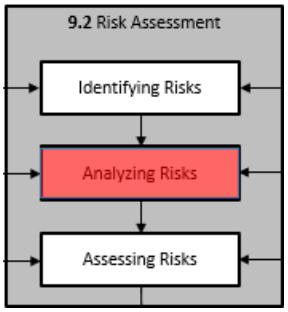


(i) **Internal risks**: Identification will be based mainly on the analysis of the activities documented in the flowchart, which must faithfully represent the process's current functioning, evaluating for each activity what events could affect them and considering different combinations of events, such as: errors in the input data, in the processing and recording of information, in the estimates or criteria, in calculations, errors of omission, among others.

(ii) **External risks:** An analysis must be made based on the sources of risk, context, applicable legal regulations, emerging risks, among others.

[3] Specific analysis for Risk Management, not equivalent to regular SWOT analysis.

9.3.2 Risk Analysis



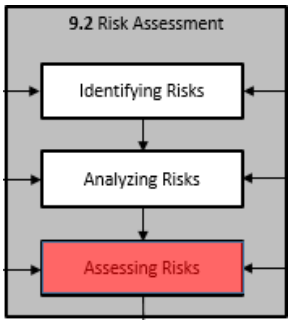
The objective of risk analysis is to understand the nature of the risk and its characteristics, including, where appropriate, the level of risk involved. Risk analysis involves a detailed examination of uncertainties, sources of risk, impacts, consequences, probabilities, events, scenarios, controls and their effectiveness.

Since a risk can have multiple causes and impacts, and can affect more than one objective, an assessment must be made of how these risks impacts the different categories of company objectives:

Levels of inherent risk are defined according to the following scale:

Very Low	Low	Medium	High	Very High

9.3.3 Risk Assessment



Risk assessment, according to ISO 31000, consists in comparing the results of the risk analysis with the established tolerance criteria. If the result is higher than the accepted tolerance, the following actions must be taken:

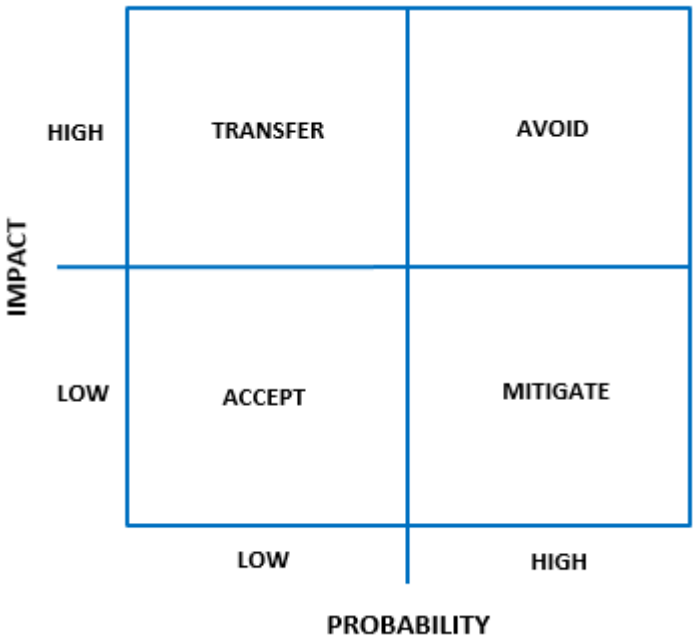
a) Conduct additional analysis to better understand the risk
b) Reconsider objectives of the process
c) Evaluate risk treatment options
d) If the result is equal or lower than the accepted tolerance level, existing controls must be maintained
e) Maintain existing controls, if established tolerance level is not exceeded

9.4 Risk Management

The purpose of risk management is to select and implement options to address risk. Risk management involves an iterative process of:

- Formulating and selecting risk mitigation (treatment) options
- Planning and implementing risk mitigation
- Evaluating the effectiveness of such treatment
- Deciding if the residual risk is acceptable
- If residual risk is not acceptable, evaluating and implementing new mitigation measures

Mitigation strategies include: (1) **Transferring** the risk; (2) **Avoiding** the risk (i.e., eliminating its probability or impact to zero); (3) **Mitigating** the risk's negative impact; and (4) **Accepting** the possible consequences of a particular risk with an informed decision, as long as the risk is withing tolerable levels, as defined in this Policy.



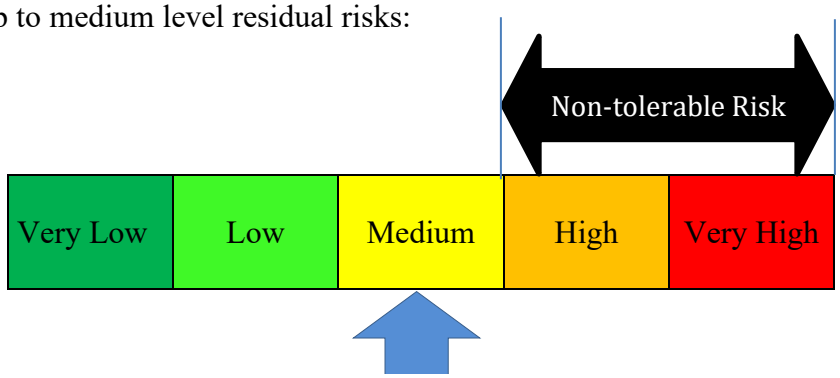
The time frame and level of prioritization for implementing mitigation is defined in the next point of this document (10.1 Accepted Risk Level).

In the case of identified risks that exceed the established tolerable risk level, and whose mitigation requires an increase in the budget, these should be channeled through the Internal Control Committee.

10 Accepted Risk Level and Risk Tolerance

10.1 Accepted Risk Level

The accepted risk level is defined as the risk the Company is willing to assume; the Company has defined that it can assume up to medium level residual risks:



Accepted Risk Level

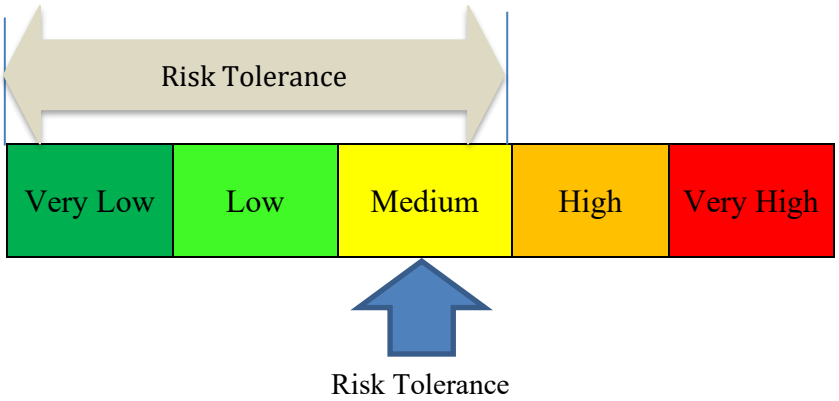
This implies that Very High and High level risks must be mitigated as a matter of priority, according to the following diagram:

Residual Risk Level	Implementation Priority
Very High	Very High
High	High
Medium	Medium
Low	N/A
Very Low	N/A

If a longer period of time is deemed necessary, this requirement should be channeled through the Internal Control Committee, explaining the reasons why a definitive improvement cannot be implemented or, in its absence, a compensatory control while this implementation is being completed. In the event an action plan is not carried out opportunely, the maximum period indicated in the table above will automatically be considered as the expiration date, starting from the date on which the opportunity for improvement or of unmitigated risk was reported.

10.2 Risk Tolerance

The guiding principle is not to assume risks above the Accepted Risk Level. Assuming that due diligence has been carried out to manage the identified risks, this Policy understands that exceptions may occur, in which cases it is possible, with the appropriate information, to responsibly assume greater risk. Tolerance to residual risks is allowed up to a medium level, and it can be assumed as long as the cost of implementing the risk response is greater than the effect associated with the identified risk. The event's occurrence probability during the period under analysis must also be considered (a minimum 1-year period):



When cases associated with higher risk levels (High or Very High) also have a high implementation cost, even higher than the possible effect of the identified risk, and considering the risk's occurrence probability, these cases should escalate to the Internal Control Committee, which will proceed to evaluate possible treatments. If the Internal Control Committee is unable to resolve a case, it should then be escalated to CEO and finally to the Company's Directors' Committee, which may communicate the case or cases under analysis to the Board of Directors so it may evaluate risk treatment options (explained in point 9.3).

12 Risk Communication and Monitoring

12.1 Risk Management Monitoring Frontline Management

As noted in Chapter 7 and 8 of this document, Frontline Managers (the Management) are primarily responsible for properly managing risks, this, in terms of monitoring of Risk Management implies the following:

- They must implement monitoring controls on risk management, that is, reports or measures that allow them to know the status of the operation of the controls or mitigation measures that operate

within their processes, managing corrective actions when a non-operational control or mitigation measure is reported.

- The management must ensure that adequate action plans are in place to mitigate risks when they are not tolerable, or when weaknesses are reported from audits executed by the Corporate Internal Audit or External Audits area.
- The management must ensure that action plans are implemented in a timely manner, and that they actually operate, monitoring the status of these at least monthly.
- The management must report to the Internal Control and Corporate Internal Audit area the status of the action plans at least quarterly, providing supporting evidence when implemented.

12.2 Consolidated Risk Management Reports (Second Line of Defense)

Every quarter Internal Control must generate a Risk Management report, which must be presented to the Internal Control Committee. The report must include the residual risks heat map and the status of action plans in progress to mitigate risks that are out of tolerance range. In addition, the report must contain the status of overdue action plans or those which have not yet been defined by the responsible Manager. Finally, in cases where it has not been possible to mitigate risks these must be reported, to propose corrective actions.

Residual Risk Level	Requires Immediate Corrective Action
Very High	YES
High	YES
Medium	NO
Low	NO
Very Low	NO

Updating the risk and control matrices, as well as the follow-up of implementation of action plans, mainly those associated with high and very high residual risks, has been carried out jointly by the Internal Control and Internal Audit areas.

Likewise, in accordance with the guidelines defined in this policy, a re-evaluation of high and very high residual risks was carried out for the executed and pending action plans of each manager, allowing the segregation of those actions that had to be dealt with immediately.

On an annual basis, Internal Control provides training to employees holding positions of responsibility on the risk management matters addressed in this Policy.

As described in this document, the process of updating risk matrices is responsibility of the first line of defense, with support and advice from Internal Control.

13 Modification Log

Version 00 – Date of Creation: November 2020

- The "Corporate Risk Management Policy" document is created.

Version 01 - Date Modified: August 2022

- In 1. Methodological Framework, General Standard No. 461 is modified.
- Chapter 12.1 Risk Management Monitoring is incorporated in Frontline Management.
- Chapter 12.2 Consolidated Risk Management Reports (Second Line of Defense) is updated.
- Updated Figure 1 indicated in Appendix 1.3 Determination of the Risk Level.
- The first paragraph annex 2 "Risk mitigation through control activities" is updated.

Modified / Reviewed by: Leslie Silva, Head of Internal Control
Paula Alemparte, Compliance Lawyer