Corporate Risk Management Policy

I Corporate Risk Management Policy

1. Methodological Framework

This Corporate Risk Management Policy ("the Policy") is issued in compliance with the standards contained in the applicable local legislation, ISO 31000:2018[1], COSO 2013[2] and the good practices of Corporate Governance for Open Corporations, issued by the Financial Market Commission ("CMF") through General Rule No. 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), thus allowing to protect and create value for the Company, helping to achieve its objectives. It also seeks to reasonably ensure that any relevant risk is duly identified, managed in a timely manner and reported when necessary, generating valuable information to complement decision making.

3. Objectives

The main objectives of this Policy are:

- To make explicit the responsibility of Senior Management (Board of Directors, Directors' Committee, General Management, Corporate Management), in the identification of risks, as well as their adequate communication to all collaborators for their proper management and incorporation in the various processes of the Company.
- To formally incorporate Risk Management into the organizational culture, integrating it into the day-to-day execution of business processes in a natural way, through the strengthening of the current Policies and Procedures, with a formal definition of responsibilities.
- Contribute to the Company's performance, through the search for operational efficiencies, responding adequately and in advance to undesired events.
- Anticipate potential events that have not yet occurred and communicate in a timely manner those that have occurred, thus generating centralized risk databases to minimize the possibility of recurrence.

[1] Risk Management – Principles and Guidelines, International Organization for Standardization (ISO 31000:2018)

[2] COSO: Committee of Sponsoring Organizations to the Treadway Commission (COSO 2013)

4. Scope

This Policy applies to Viña Concha y Toro S.A. and all its domestic and foreign Subsidiaries, covering all processes and business units[3]. Companies that are not consolidated in Viña Concha y Toro manage their risks independently, without prejudice to those risks that the parent company itself must foresee or consider by the mere fact of participating in its ownership.

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

The Policy is intended 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 defined in point N°1.

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

5. Definitions

Risk: It is defined as the possibility of the occurrence of an event that may impact the company's strategy or objectives, favorably or unfavorably, which is measured in terms of its level(s) of impact(s) and probability of occurrence.

Impact: Represents the effect or set of consequences of a risk if it were to occur.

Probability: Represents the possibility of a given event occurring.

[3] The Risk Management Policy extends to Joint Ventures in which the Company has control, as defined by the Securities Market Law..

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

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

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

External Risk: It is the one that comes from the environment and that influences or conditions the organization directly or indirectly, and may even become a real threat to the company.

Strategic Risk: "Risk to the strategy or risk created by the strategy", i.e. any undesired event (Risk) that may affect the fulfillment of the company's strategy or strategic objectives. These risks can be uncertainties and are the key issues that concern the vineyard's Board of Directors.

Operational Risk: These are those that point to the risk of non-compliance with performance, financial and operational objectives, and the protection of its assets against possible losses.

Financial Reporting Risk: Risk of non-compliance in matters of presentation and disclosure of internal and external financial and non-financial information, including aspects of reliability, transparency and other concepts established by regulators, standardization bodies or company policies.

Regulatory Compliance Risk: Risks related to non-compliance with laws and regulations to which the company is subject.

Preventive Control: Controls that anticipate undesirable events before they happen.

Detective Control: Controls that identify events at the time they occur.

Business Process: A set of logically related activities that use the organization's resources to provide defined results, in order to achieve business objectives.

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

Internal Control Committee: It is composed of the Corporate Finance Manager, Corporate General Auditor, Overseas Financial Administrative Manager, Head of Internal Control and Internal Audit Coordinator. The purpose of this committee is to review the status of updating the risk matrices, the status of implementation of action plans committed by each responsible, allowing the risks that require higher priority to be managed in a timely manner. This committee meets on an average monthly basis.

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

6. Principles

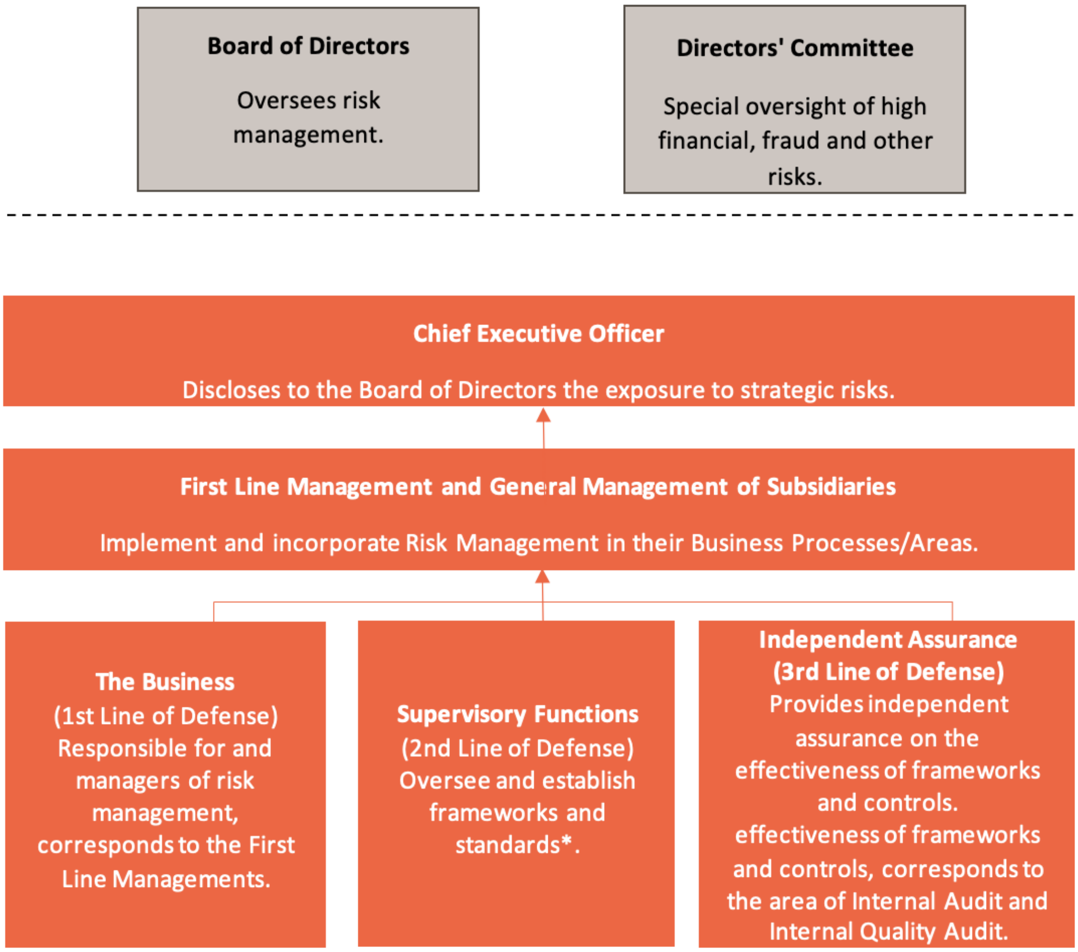
Viña Concha y Toro's business is not free from risk, especially considering that the Company is vertically integrated. Indeed, it participates in all stages of production, processing and marketing and distribution of its products through subsidiaries in Chile and abroad or third party distributors.

Assuming risks is an essential part of doing business, so the Company consciously takes the appropriate amount of risks and manages them competently to achieve the related opportunities and ensure the fulfillment of objectives.

Risks must be assessed in an unbiased manner, Risk Management includes the identification, analysis and evaluation of risks, the appropriate and timely response, monitoring and reporting of these to provide assurance that objectives can be achieved.

7. Governance

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



Corresponds to the areas of: **Internal Control, Management Control areas (Commercial, Support Areas, Modeling and Reporting), Sustainability, Quality (Oenological, Suppliers, Production Plants), Safety.*

The Internal Control Area, as the second line of defense, monitors and evaluates the status of controls, advises and accompanies the first line of defense in risk management, providing a reasonable degree of assurance as to 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 encompass the following stakeholders:

- The Board of Directors is responsible for the proper supervision of the Company's Risk Management. For these purposes:
    - Approving the Policies, practices and methodologies thereof;
    - Approving the adequate governance of the Internal Control supervision and the direct supervision of the risk management to the First Line Managements.

- The Chief Executive Officer or his delegate discloses to the Board of Directors the strategic risk exposure and is responsible for the overall Risk Management culture, capabilities and practices to achieve the Company's strategy and objectives. The General Manager's responsibilities include:
    - Evaluate strategy within risk tolerance, maintaining oversight of risk.
    - Guide the development and performance of the Risk Management process and appropriate delegation, as well as communicating expectations and reporting requirements.

- The First Line Management and General Management of the Subsidiaries (or Finance Management where it does not exist) must report to the General Management on the effective implementation and integration of the elements of risk management (first line of defense), in addition to providing the necessary resources to effectively manage the risk. They are also responsible for identifying, assessing, responding to, managing and reporting on risks within their business areas, implementing appropriate treatments for these where risks exceed the defined tolerance. In addition, they are responsible for maintaining formally updated internal policies, procedures and instructions.

- The Corporate Finance Management, through the Internal Control area, monitors the development of Risk Management as part of its responsibilities in the second line of defense, advising the Board of Directors, General Management, First Line Managers and General Managers of Subsidiaries in the fulfillment 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 Quality Internal Audit area, as the Third Line of Defense, provides an independent opinion on the effectiveness of the risk management framework and the effectiveness of 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 manage the uncertainty related to a threat (occurrence of an event), through a sequence of activities that include the identification, analysis and evaluation of the risk, and then establish strategies for its treatment, using management resources.

The following is a detailed explanation of the activities that make up the Risk Management process, i.e.: 9.1 Establishment of the Context, 9.2 Risk Assessment and 9.3 Risk Management.

[4] Process according to ISO 31000:2018

9.1 Establishing the Context

The Corporate Finance Management, through its Internal Control area, together with the General Management, must establish the context for risk management at the strategic level, which must be updated annually. In this activity, the following evaluation must be performed:

- Strategic SWOT [4]Analysis: Weaknesses, Opportunities, Threats, Risk Sources.
- Identification of Regulatory Requirements: Market, Voluntary Standards, Environmental, Food, Accounting, among others.
- Review of the accepted level of risk 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 each area or First Line Management (direct dependence of the General Management of the parent company or General Management of Subsidiaries). This review must be carried out at least annually or in the event of any relevant change affecting the processes managed by these Managements.

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

9.3 Risk Management or Treatment

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 options
- Plan and implement risk mitigations
- Evaluate the effectiveness of such treatment
- Decide whether the residual risk is acceptable
- If not acceptable, evaluate and implement new mitigation measures

Mitigation strategies include: (1) Transferring the risk, (2) Avoiding the risk (i.e.,

[4] Specific analysis for Risk Management, not equivalent to SWOT Analysis.

eliminating its probability or impact to zero), (3) Mitigating the negative impact of the risk, and (4) Accepting the possible consequences of a particular risk through an informed decision, as long as it is at tolerable levels, as indicated in this Policy.

The deadlines and level of prioritization for implementing mitigation are defined in the following point of this document (10.1 Accepted Risk Level).

For those identified risks that are above the tolerable risk appetite, and that the mitigation requires an increase in the budget, this must be channeled through the Internal Control Committee.

10.Level of Accepted Risk and Risk Tolerance

10.1 Accepted Risk Level

The level of risk accepted is defined as the risk that the Company is willing to assume, for which the Company has defined that it can assume up to medium level residual risks.

In the event that the action plan is not delivered in a timely manner, a compensatory control is required while this implementation is being finalized. In the event that the action plan is not delivered in a timely manner, the maximum period indicated in the table above, counted from the date on which the improvement opportunity or unmitigated risk was reported, will automatically be considered as the expiration date.

10.2 Risk Tolerance

The guiding principle is not to assume risks above the Accepted Risk Level, assuming that due diligence has been performed to manage the identified risks, this Policy understands that there may be exceptions, for which it is possible to assume a higher risk in an informed and responsible manner, for which there is a tolerance to residual risks up to medium level, which can be applied as long as the cost of implementing the risk response is greater than the impact associated with the identified risk, also considering the probability of occurrence of the event during the period under analysis (at least 1 year).

In the event that there are cases associated with higher level risks (High or Very High) associated with a high implementation cost, even higher than the possible impact related to the identified risk, considering its probability, they should be escalated to the Internal

Control Committee to evaluate their treatment. If the Internal Control Committee cannot resolve it, it should be escalated to the General Management, and finally to the Directors' Committee, who may communicate to the Board of Directors the case or cases under analysis to evaluate the treatment options explained in point 9.3.