Sula Vineyards Limited (SVL)

Risk Assessment and Management Policy

Commercial SOP #	
Version	1
Issued On	February 23, 2022
Effective From	February 23, 2022

Contents

1. Introduction

Pursuant to Regulation 17(9) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("SEBI Listing Regulations") and Section 134(3) of the Companies Act, 2013, this Risk Assessment and Management Policy ("Policy") establishes the philosophy of Sula Vineyards Limited ("Company"), towards risk identification, analysis and prioritization of risks, development of risk mitigation plans and reporting on the risk environment of the Company. The purpose of this Policy is to define, design and implement a risk management framework across the Company to identify, assess, manage and monitor risks. Aligned to this purpose is to identify potential events that may affect the Company and manage the risk within the risk appetite and provide reasonable assurance regarding the achievement of the Company's objectives. This will present a wide approach to ensure that key aspects of risk that have a wide impact are considered in its conduct of business.

Accordingly, the board of directors of the Company ("Board") has adopted this policy at its meeting held on February 23, 2022.

2. Scope

This Policy is applicable to all the functions, departments and geographical locations of the Company.

3. Definition

Risk is an event which can prevent, hinder or fail to further or otherwise obstruct the enterprise in achieving its objectives. A business risk is the threat that an event or action will adversely affect an enterprise's ability to maximize stakeholder value and to achieve its business objectives. Risk can cause financial disadvantage, for example, additional costs or loss of funds or assets. It can result in damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities. Risk is the product of probability of occurrence of an event and the financial impact of such occurrence to an enterprise.

4. Objectives

The objective of this Policy is to manage the risks involved in all activities of the Company, to maximize opportunities and minimize adversity. This Policy is intended to assist in decision making processes that will minimize potential losses, improve the management of uncertainty and the approach to new opportunities, thereby helping the Company to achieve its objectives.

The objectives of the Policy can be summarized as follows:

(a) To safeguard the Company's and its subsidiaries'/ joint ventures' property, interests, and interest of all stakeholders;
(b) To manage risks with an institutionalized framework and consistently achieving desired outcomes;
(c) To protect and enhance the corporate governance;
(d) To implement a process to identify potential / emerging risks;
(e) To implement appropriate risk management initiatives, controls, incident monitoring, reviews and continuous improvement initiatives;
(f) Minimize undesirable outcomes arising out of potential risks; and
(g) To align and integrate views of risk across the enterprise.

5. Components of Risk Management System

The risk management system in the Company has the following key features:

(a) Active board of directors, committee and senior management oversight;
(b) Appropriate policies, procedures and limits;
(c) Comprehensive and timely identification, measurement, mitigation, controlling, monitoring and reporting of risks;
(d) Appropriate management information systems at the business level;
(e) Comprehensive internal controls in accordance with current regulations; and
(f) A risk culture and communication framework

6. Risk Governance

Risk governance signifies the way the business and affairs of an entity are directed and managed by its Board and executive management.

The Company can conduct risk management effectively by having an appropriate risk governance structure and well-defined roles and responsibilities.

7. Risk Management Framework

The risk management committee formed by the Board shall periodically review the risk assessment and management policy of the Company and evaluate the risk management systems so that management controls the risk through a properly defined network.

Heads of departments shall be responsible for implementation of the risk management system as may be applicable to their respective areas of functioning.

8. Risk Management Process

Conscious that no entrepreneurial activity can be undertaken without assumption of risks and associated profit opportunities, the Company operates on a risk management process /framework aimed at minimization of identifiable risks after evaluation to enable management to take informed decisions.

Broad outline of the framework is as follows:

(a) Risk Identification: Management identifies areas that may positively or negatively affect the Company's ability to implement its strategy and achieve its objectives and performance goals. The identification process is carried out in such a way that an expansive risk identification covering operations and support functions are put together and dealt with.

Risks can be identified under the following broad categories:

(i) Internal risks include:

- Strategic Risk: Competition, inadequate capacity, high dependence on a single customer/vendor.
- Business Risk: Project viability, process risk, technology obsolescence/ changes, development of alternative products.
- Finance Risk: Liquidity, credit, currency fluctuation.
- Environment Risk: Non-compliances to environmental regulations, risk of health to people at large.
- Personnel Risk: Health & safety, high attrition rate, incompetence.
- Operational Risk: Process bottlenecks, non-adherence to process parameters.
- Reputation Risk: Brand impairment, product liabilities.

- Regulatory Risk: Non-compliance to statutes, change of regulations.
- Technology Risk: Innovation and obsolescence.
- Information and Cyber Security Risk: Cyber security related threats and attacks.

(ii) External risks include:

- Sectoral Risk: Unfavorable consumer behavior in relation to the relevant sector etc.
- Sustainability Risk: Environmental, social and governance relates risks.
- Political Risk: Changes in the political environment, regulation/ deregulation due to changes in political environment.

(b) Root Cause Analysis: Root cause analysis enables tracing the reasons / drivers for existence of a risk element and helps developing appropriate mitigation action.

(c) Risk Scoring: An analysis of all internal processes and support functions is done to determine the likelihood and impact of risk elements. Likelihood of occurrence of a risk element within a finite time is scored based on analysis of event logs drawn from the past. Impact is measured based on a risk element's potential impact on cost, revenue, profit etc. should the risk element materialize.

(d) Risk Categorisation:

The identified risks are further grouped in to (a) High; (b) Medium; and (c) Low risks.

- High Risk - Represents critical control weaknesses requiring prompt action to mitigate information systems or business process vulnerabilities. Adequate compensating controls do not exist to mitigate risk exposure or may not be sufficient given the impact of a risk occurrence should it occur.
- Medium Risk - Represents moderate control weaknesses requiring near-term management focus to strengthen existing controls. Some compensating controls are present but additional controls are necessary to further mitigate risk exposure.
- Low Risk - Represents minor control weaknesses requiring management focus to enhance existing controls. Compensating controls are present to mitigate exposure (or if not the impact of a risk occurrence is minor) but opportunities exist to enhance controls or improve operating efficiency.

(e) Risk Mitigation Plan:

Management develops appropriate responsive action on review of various alternatives, costs and benefits, with a view to managing identified risks and limiting the impact to tolerance level. Risk mitigation plan drives policy development as regards risk ownership, control environment timelines, standard operating procedure, etc.

Risk mitigation plan is the core of effective risk management. The mitigation plan covers:

(i) Required action(s);
(ii) Required resources;
(iii) Responsibilities;
(iv) Timing;
(v) Performance measures; and
(vi) Reporting and monitoring requirements

The mitigation plan also covers (i) preventive controls - responses to stop undesirable transactions, events, errors or incidents occurring; (ii) detective controls - responses to promptly reveal undesirable transactions, events, errors or incidents so that appropriate action can be taken; (iii) corrective controls - responses to reduce the consequences or damage arising from crystallization of a significant incident.

(f) Risk Monitoring:

It is designed to assess on an ongoing basis, the functioning of risk management components and the quality of performance over time. Staff members are encouraged to carry out self-assessments throughout the year.

(g) Options for dealing with risk:

Tolerate – If we cannot reduce the risk in a specific area (or if doing so is out of proportion to the risk) we can decide to tolerate the risk; i.e., do nothing further to reduce the risk.

Transfer – Here risks might be transferred to other organizations, for example by use of insurance or transferring out an area of work.

Terminate – This applies to risks we cannot mitigate other than by not doing work in that specific area. So, if a particular project is of very high risk and these risks cannot be mitigated, we might decide to cancel the project.

(h) Risk reporting:

Periodically, key risks are reported to the Board or risk management committee with causes and mitigation actions undertaken/ proposed to be undertaken.

The internal auditor carries out reviews of the various systems of the Company using a risk-based audit methodology. The internal auditor is charged with the responsibility for completing the agreed program of independent reviews of the major risk areas and is responsible to the audit committee which reviews the report of the internal auditors on a quarterly basis.

The statutory auditors carry out reviews of the Company's internal control systems to obtain reasonable assurance to state whether an adequate internal financial controls system was maintained and whether such internal financial controls system operated effectively in the company in all material respects with respect to financial reporting.

On regular periodic basis, the Board will, on the advice of the audit committee, receive the certification provided by the CEO and the CFO, on the effectiveness, in all material respects, of the risk management and internal control system in relation to material business risks.

(i) Risk Management Measures adopted in general by the Company:

The Company has adopted various measures to mitigate the risk arising out of various areas described above, including but not limited to the following:

(i) A well-defined organization structure;
(ii) Defined flow of information to avoid any conflict or communication gap;
(iii) Hierarchical support personnel to avoid work interruption in absence/ non-availability of functional heads;
(iv) Discussion and implementation on financial planning with detailed business plans;
(v) Detailed discussion and analysis of periodic budgets;

(vi) Employees training and development programs;
(vii) Internal control systems to detect, resolve and avoid any frauds;
(viii) Systems for assessment of creditworthiness of existing and potential contractors/subcontractors/ dealers/vendors/ end-users;
(ix) Redressal of grievances by negotiations, conciliation and arbitration; and
(x) Defined recruitment policy.

9. Responsibility for Risk Management

Responsibility holder	Responsibilities
Board	The Company's risk management architecture is overseen by the Board and the policies to manage risks are approved by the Board. Its role includes the following: • Ensure that the organization has proper risk management framework • Define the risk strategy, key areas of focus and risk appetite for the company • Approve various risk management policies including the code of conduct and ethics • Ensure that senior management takes necessary steps to identify, measure, monitor and control these risks
Audit Committee	The Audit Committee assists the Board in carrying out its oversight responsibilities relating to the Company's (a) financial reporting process and disclosure of financial information in financial statements and other reporting practices, b) internal control, and c) compliance with laws, regulations, and ethics (d) financial and risk management policies. Its role includes the following: • Setting policies on internal control based on the organisation's risk profile, its ability to manage the risks identified and the cost/ benefit of related controls; • Seeking regular assurance that the system of internal control is effective in managing risks in accordance with the Board's policies. • Ensure that senior management monitors the effectiveness of internal control system • Help in identifying risk, assessing the risk, policies / guidance notes to respond its risks and thereafter frame policies for control and monitoring.
Risk Management Committee	The Risk Management Committee, as constituted by the Board, is the key committee which implements and coordinates the risk function as outlined in this policy on an ongoing basis. Its role includes the following: • Formulation of a detailed risk management policy which shall include: (a) a framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Risk Management Committee; (b) measures for risk mitigation including systems and processes for internal control of identified risks; and (c) business continuity plan; • Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company; • Monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems; • Periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity, and recommend for any amendment or modification thereof, as necessary; • Keep the Board of directors of the Company informed about the nature and content of its discussions, recommendations and actions to be taken; • Review the appointment, removal and terms of remuneration of the Chief Risk Officer (if any);

	• To implement and monitor policies and/or processes for ensuring cyber security; and any other similar or other functions as may be laid down by Board from time to time and/or as may be required under applicable law, as and when amended from time to time, including the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015.
Head – Risk & Assurance	The Head – Risk & Assurance shall ensure that high standard are sustained in the auditing process and towards this, shall: • Formulate an Annual Internal Audit Plan in consultation with management. • Implement the Annual Internal Audit Plan, special tasks or projects requested by the CFO and Audit Committee and the Chairperson. • Issue periodic reports on a timely basis to the Senior Management, CFO and Audit Committee summarizing results of audit activities. • Keep the Audit Committee informed of emerging trends and developments in internal auditing and information systems auditing practices and give recommendations for necessary revisions in Internal Audit Charter. • Assist in the investigations and examination of significant suspected fraudulent activities and notify the CFO and Audit Committee of the results. • Ensure control improvements are identified and corrective action recommended to the management based on an acceptable and practicable time frame. • Ensure through tracking that management implements the agreed control improvements on a timely basis, performing such follow-up work as Internal Audit deems necessary to ensure the improvements are adequate, effective and timely. • Ensure whistle-blower programs and trainings are adequately undertaken to educate the organisation employees and appropriate reporting to CFO & Audit Committee. • Ensure Standard Operating Procedures (SOP) and Delegation of Authority (DOA) are drafted and followed for critical and key activities / functions.

10. Business Continuity Plan

Please refer to the BCP policy document.

11. Communication and Consultation

Appropriate communication and consultation with internal and external stakeholders should occur at each stage of the risk management process as well as on the process as a whole.

12. Disclaimer Clause

The risks outlined above are not exhaustive and are for information purposes only. Management is not an expert in assessment of risk factors, risk mitigation measures and management's perception of risks. Readers are therefore requested to exercise their own judgment in assessing various risks associated with the Company.

13. Periodical Review and Effectiveness

Effectiveness of risk management framework is ensured through periodical review of this Policy, provided that such review should be undertaken at least once in two years. As the risk exposure of any business may undergo change from time to time due to the changing industry dynamics, evolving complexity and continuously changing environment, the updation and review of this Policy will be done as and when required, by the risk management committee to ensure it meets the requirements of legislation and the needs of organisation.

In the event of any conflict between the Companies Act, 2013 or the SEBI Listing Regulations

or any other statutory enactments and the provisions of this Policy, the Regulations shall prevail over this Policy. Any subsequent amendment/modification in the SEBI Listing Regulations, in this regard shall automatically apply to this policy.

14. Approval

The Board will be the approving authority for the company's overall risk management system. The Board will, therefore, approve this Policy and any amendments thereto from time to time.

Sr. No.	Name	Signature
1.	Bittu Varghese – CFO	
2.	Chaitanya Rathi – COO	