GLOTTIS LIMITED

RISK MANAGEMENT POLICY

Framed under Regulation 17(9)(b) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015

CIN: U63090TN2022PLC151443
Registered Office: New No.46, Old No.311, 1st Floor, Thambu Chetty Street, Chennai, Tamil Nadu, India, 600001

RISK MANAGEMENT POLICY

1. INTRODUCTION

The Companies Act, 2013 emphasizes the requirement of risk management policy for the Company. Section 134(3)(n) of the Companies Act, 2013 requires that the report by the Board laid at the general meeting shall include a statement on the development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company shall be included in the Board's report.

The Audit Committee of the Company is required to evaluate the internal financial controls and risk management systems of the Company pursuant to Section 177(4)(vii) of the Companies Act, 2013; and the Independent Directors shall satisfy themselves that the systems of risk management are robust and defensible.

Regulation 17(9)(a) of SEBI (Listing Obligation and Disclosure Requirements) Regulations, 2015 (**"Listing Regulations"**), inter alia, mandates laying down the procedures for risk assessment and minimization. Further Regulation 17(9)(b) of the Listing Regulations, provides the Board shall be responsible for framing, implementing and monitoring the risk management plan for the company.

The Board of Directors (**"the Board"**) of Glottis Limited (**"the Company"**) has adopted the following policy and the Board may amend this policy from time to time. In case of any subsequent amendments to the Listing Regulations which makes any of the provisions in the Policy inconsistent, the provisions of the prevalent Listing Regulations shall prevail.

2. OBJECTIVE OF POLICY

The key objectives of this policy include the following:

- Develop a risk culture that encourages all employees to identify risks, associated opportunities/gains and respond to them with effective actions
- Develop both proactive and reactive mechanism for risk management
- Identify and manage existing/new risks in a planned and coordinated manner.
- Develop an incident response management framework to manage the risks that may materialize.
- To adopt best Risk Management practices leading to shareholder value creation and increased stakeholder confidence.

3. DEFINITIONS

"Company" means Glottis Limited.

"Risk" means a probability or threat of damage, injury, liability, loss, or any other negative occurrence that may be caused by internal or external vulnerabilities; that may or may not be avoidable by pre-emptive action.

"Risk Management" is the process of systematically identifying, quantifying, and managing all risks and opportunities that can affect achievement of a corporation's strategic and financial goals.

"**Senior Management**" means officers/personnel of the Company who are members of its core management team comprising all members of management one level below the chief executive director or managing director or whole-time director or manager, including the functional heads and shall specifically include company secretary and chief financial officer.

Words and expressions used and not defined in this Policy shall have the meaning ascribed to them in the Listing Regulations, the Securities and Exchange Board of India Act, 1992, as amended, the Securities Contracts (Regulation) Act, 1956, as amended, the Depositories Act, 1996, as amended, or the Companies Act and rules and regulations made thereunder.

4. RISK MANAGEMENT POLICY & FRAMEWORK

Risk is the potential for failure or loss of value or the missed opportunity for value creation / strategic competitive advantage resulting from either a certain action or a certain inaction.

Controlling risk is essential in any business by having processes to ensure safeguarding of assets and compliance with appropriate regulatory frameworks. However, risks may also have to be taken consciously to explore untapped business opportunities in line with the corporate strategy to optimize maximum potential stakeholder's value and to improve their confidence.

Classification of Risks:

A. Internal risks:

The internal risks i.e. Financial / Operational / Preventable / Compliance risks arising from within the organization that are controllable and need to be eliminated or avoided. The examples are:

- Governance, organizational structure, roles and accountabilities.
- Policies, objectives and the strategies that are in place to achieve them;
- Contractual compliances;
- Operational efficiency;
- Credit and liquidity risk;
- Human resource management;
- Hurdles in optimum use of resources;
- Culture and values;
- Suppliers risk;
- Customers risk;
- Technology related risks, including but not restricted to cybersecurity risks;
- Physical risk – that is risk of damage/breakdown to the assets of the company.
- Legal risks
- Compliance risks
- Reputational risks

B. External risks

External risks come up due to economic events that arise from outside of an institution's control. It arises from the external events that cannot be controlled by any an institution, cannot be forecasted with reliability, are normally beyond its control, and it is therefore difficult to reduce the associated risks. The examples are :

- Statutory/ regulatory changes/ changes in government policies;
- Market conditions/ trends;
- Economic environment;
- Political Environment;
- Fluctuations in trading activities;
- Foreign exchange rate risk;
- Factors beyond the company's control (including act of God, epidemic, pandemic, war, etc) which significantly reduces demand for its business and/or affects its operations.

C. Disruptive risks:

These are the anticipated or unanticipated events which may result in disruption of the operations of firm or existence of its current business model and Innovations to business models that disrupt the existing paradigm. The examples are:

- Supply Chain Disruptions;
- E-commerce Growth;
- Fuel Price Volatility;
- Environmental Concerns;
- Labor Shortages;
- Market Consolidation;

- Technological Obsolescence;
- Customer Expectations;

4.Risk Management Process

The aggregate level and types of risk the Company is willing to assume within its risk capacity to achieve its strategic objectives and business plan shall be as per its risk appetite. The risk management process involves the following phases:

- Risk identification
- Risk Analysis
- Risk Assessment
- Risk Mitigation/Treatment
- Implementation
- Monitoring and Review
- Risk Reporting

4.1 Risk Identification

This involves continuous identification of events that may have a negative impact on the company's ability to achieve goals. The company has adopted a robust risk identification process keeping in view the key activities/ focused areas of company's business for the purpose of risk assessment. Identification of risks, risk events and their relationship are based on the basis of discussion with the senior management and analysis of related data/ reports, previous internal audit reports, past occurrences of such events etc. The identification of risk by the company is broadly based on the internal and external risk factors:

Category of Risk	Examples
Financial Risks	· Financial misstatements/ improper accounting or financial reporting. · Unavailability of funding and cash flow; · Change in credit limit affecting availability of funds; · Market conditions on lending / borrowing of funds; · Loan repayment schedules not adhered; · Changes in the applicable laws and environment related to funding, investment norms, including raising of funds from international market;
Operational	· Business disruption; · Delay in implementation of project/ plan; · Inefficient use of resources/increased product/ service cost; · Physical property/damage/disruption; · Accidents / force majeure events, change in management, etc. · Limited availability of manpower and resources;
Sectoral	· Product development and engineering activities; · Limited number of customers including government customers; · Third Party suppliers for our key components, materials; · Inability to implement business strategies; · Cyclical demand and vulnerable to economic downturn; · Competition with certain key players in the industry; · Regulatory approvals and licenses for business; · Changes in the energy industry and governmental energy
Information	· Leakage of key/sensitive non-public information; · Rumors in the market and / or related trading in the securities of the Company; · Data Privacy challenges;

Technology related	· Disruption of IT operations; · Server issues; · Phishing, data leakage, hacking, insider threats, etc.
Strategic Risks	· Reduction in business vitality (due to change in business strategy, customer spending patterns, changing technology, etc.); · Loss of intellectual property and/or trade secrets; · Competition for talent; · Negative impact to reputation/loss of trust mark.
Compliance Risks	Violation of laws or regulations governing areas including but not limited to:
	· Environmental;
	· Employee health & safety;
	· Labour laws;
	· Product quality/safety issues ;
	· Local tax and statutory laws.
	· Prosecution, fines, investigations, inquiries; litigation including class actions.
Reputational Risks	Media communication by employees other than authorised personnel viz., the Board of Directors/Managing Directors • Timely response to statutory/ regulatory queries/ requirements.

4.2 Risk Analysis

Risk analysis involves:

- consideration of the causes and sources of risk;
- the trigger events that would lead to the occurrence of the risks;
- the positive and negative consequences of the risk;
- the likelihood that those consequences can occur.

Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be considered.

4.3 Risk Assessment

Management considers qualitative and quantitative methods to evaluate the likelihood and impact of identified risk elements. Likelihood of occurrence of a risk element within a finite time is scored based on polled opinion or from analysis of event logs drawn from the past. Impact is measured based on a risk element's potential impact on revenue, profit, balance sheet, reputation, business and system availability etc. should the risk element materialize. The composite score of impact and likelihood are tabulated in an orderly fashion. The Company has assigned quantifiable values to each risk element based on the "impact" and "likelihood" of the occurrence of the risk on a scale of 1 to 4 as follows.

Impact	Risk Level	Likelihood
Minor	1	Low
Moderate	2	Medium
High	3	High
Critical	4	Critical

4.4 Risk Mitigation/Treatment

Risk mitigation/treatment involves selecting one or more options for modifying risks and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are tolerable;
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

Based on the Risk level, the company should formulate its risk management strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Following framework shall be used for risk treatment:

1. ***Risk Avoidance (eliminate, withdraw from or not become involved)***
   Risk avoidance implies not to start or continue with the activity that gives rise to the risk.

2. ***Risk Reduction (optimize - mitigate)***
   Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied.

3. ***Risk Sharing (transfer - outsource or insure)***
   Sharing, with another party, the burden of loss or the benefit of gain, from a risk.

4. ***Risk Retention (accept and budget)***
   Involves accepting the loss, or benefit of gain, from a risk when it occurs. Risk retention is a viable strategy for risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

4.5 Implementation

This involves execution of the risk mitigation strategies or treatments that have been identified and planned during the risk management process. It ensures that risk responses are put into action and integrated into daily operations. Key aspects of Implementation are as follows:

- Action Plan Execution: Turning the risk treatment plan into concrete steps, with clear timelines and milestones.
- Resource Allocation: Ensuring that necessary resources (budget, personnel, technology, etc.) are allocated to carry out the actions effectively.
- Assigning Responsibilities: Designating specific roles or teams to take ownership of different tasks involved in the implementation process.
- Execution: Put the risk mitigation strategies into action according to the action plan.

4.6 Monitoring and Review

Monitoring and Review is a critical and ongoing phase in the risk management process that ensures effectiveness, relevance, and continuous improvement of risk mitigation strategies. After implementing risk treatment plans, organizations must regularly monitor the performance of these strategies and review whether they are

successfully addressing identified risks. This phase not only helps assess the current state but also ensures that risk management processes adapt to evolving threats and challenges.

At this stage, it is essential to regularly monitor the implementation process, identify any emerging risks, assess the effectiveness of the risk mitigation strategies, and make necessary improvements to the strategies as required.

4.7 Risk Reporting

Periodically, key risks are reported to the Board 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.

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 Managing Directors and the Chief Financial Officer (CFO) on the effectiveness, in all material respects, of the risk management and internal control system in relation to material business risks.

The Board shall include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company.

5. RESPONSIBILITIES FOR RISK MANAGEMENT

The Management shall be responsible for framing, implementing and monitoring the risk management policy for the company. The audit committee shall review risk management systems on an annual basis and ensure that adequate risk management systems are in place. Every staff member of the Organization is responsible for the effective management of risk including the identification of potential risks. Risk management processes should be integrated with other planning processes and management activities. Few accountabilities are as follows:

- **Directors**: Directors are accountable for ensuring that a risk management system is established, implemented and maintained in accord with this policy. Assignment of responsibilities in relation to risk management is the prerogative of the Managing Director.

- **Senior Executives:** Senior Executives are accountable for strategic risk management within areas under their control including the devolution of the risk management process to operational managers. Collectively the Senior Executives are responsible for identification of risk, Allocation of priorities, development of Strategic plans for risk management and monitoring.

- **Senior Managerial Personnel & Branch Heads:** Senior Managerial Personnel & Branch Heads are a accountable to the Management of the Company for Implementation of this policy within their respective areas of responsibility, reporting on the status, Ensuring compliance with risk assessment procedures

- **Chief Financial Officer and Accounting & Finance Head**: In addition to the functions as an Office Head, this officer will be accountable for the Organization financial stability and will ensure that a risk management plan is completed for each commercial venture. Advice will be sought, as required, from the concerned internal functional head on risk management issues in relation to these matters.

- **Internal Audit/Risk Manager:** The Internal Audit will be accountable for the implementation of this policy in key areas of the Organization. The Internal Audit will provide advice to the relevant Directors/Officers on risk management matters pertaining to the Organizations' financial stability and to occupational health and safety and workers' compensation issues and any other matter as may be required.

- Company Secretary/Compliance Head: The Company Secretary/Compliance Head shall be responsible for ensuring, among other things, timely submission of all information, returns, filings etc., conduct of Board and Committee Meetings, responding to regulators etc. He/She shall also be aware of any modifications/amendments to applicable regulations at all times.

- Legal Team: the legal team shall be responsible to ensure that all Agreements entered into by the Company are in compliance with extant regulations/laws of the land and prevent entering into a transaction which is or may be determined to be void or unenforceable in whole or with respect to a material part; ensure that the basis of representations or investigations if any, are not misleading or false or which fail to disclose material facts or circumstances

- Information Technology team; The IT team shall be responsible to oversee the assessment, identification, and mitigation of IT risks, including the adequacy of controls and incident response plans, develop and enforce policies and procedures to protect the Company's digital assets from cyber threats
-

6. REVIEW OF THIS POLICY

This Policy shall be reviewed by the Board periodically, at least once a year, including by considering the changing industry dynamics and evolving complexity and basis a risk report to be submitted by the management on an annual basis

7. BUSINESS CONTINUITY PLAN

Business continuity plan refers to maintaining business functions or quickly resuming them in the event of a major disruption, in other words, a disaster management plan. The Company shall formulate a business continuity plan as may be required for protecting the interest of the Company in the event of happening/ occurrence of any unforeseen events that may affect the business of the Company.

Such business continuity plan may vary from time to time depending on Company's need and the risk management strategy being adopted by the company at such time. The business continuity plan may, among other things, focus on protecting the assets and personnel of the Company in the event of a disaster event which affects day to day operations of the company's business. The business continuity plan may be reviewed and amended by the Board from time to time, as they may deem fit. The Company shall test the effectiveness of its Business Continuity Plan on an annual basis and table the report to the Board for information.

Effective Date: 29.01.2025