Groww

Billionbrains Garage Ventures Limited

Risk Management Policy

(pursuant to Regulation 21(4) read with Part D of Schedule II of the SEBI LODR (Listing Obligations and Disclosure Requirement) Regulation, 2015)

Table of Contents

1. Purpose and Scope:

The **Risk Management Policy ("Policy")** has been framed in accordance with the provisions of Regulation 21 (4) and Part D of Schedule II of the SEBI (Listing Obligations and Disclosure Requirement) Regulation, 2015 (**"SEBI Listing Regulations"**).

The purpose of this Policy is to manage the risks involved in all activities of the Billionbrains Garage Ventures Limited (**"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.

All the words and expressions used in this Policy, unless defined hereafter, shall have meaning respectively assigned to them under the SEBI Listing Regulations and in the absence of its definition or explanation therein, as per the Companies Act, 2013 and the Rules, Notifications and Circulars made/issued thereunder, as amended, from time to time.

This Policy shall come into force from the date of listing of equity shares of the Company on the stock exchanges.

2. Objective

Risk Management is a structured process used to identify potential threats to an organisation and to define their strategy for eliminating or minimising the impact of the risks, as well as the mechanisms to effectively monitor, assess and evaluate the risks. The well-defined risk management process would provide confidence to its stakeholders that the Company's risks are known and adequately managed thereby enabling Management to focus on the Company's growth, strategy and value creation. The Company needs to assess which method best suits its objectives and its business.

In order to achieve the above objectives, the following needs to be ensured:

A. The risk process should be known and implemented across the business and critical support functions.
B. Risk management should be the responsibility of all the employees.
C. Risk management should be directly linked to the business performance of the Company and also the individual performance of the employees.
D. Each and every employee of the Company is responsible for identifying and managing the risks; and
E. Anticipate and respond to changing economic, social, political, technological, environmental and legal conditions in the external environment.

3. Risk Management Committee ("the Committee")

As per Regulation 21 of the SEBI Listing Regulations, the Risk Management Committee shall have minimum three members with majority of them being members of the board of directors, including at least one independent director. The Chairperson of the Risk management committee shall be a member of the board of directors and senior executives of the listed entity may be members of the committee.

The Risk Management Committee shall meet at least twice in financial year. The quorum for a meeting of the Risk Management Committee shall be either two members or one third of the members of the committee, whichever is higher, including at least one member of the board of directors in attendance.

This Policy and the Terms of Reference of Risk Management Committee are integral to the functioning of the Risk Management Committee and are to be read together. The Board has authority to reconstitute the Risk Management Committee from time to time as it deems appropriate.

4. Risk Management Process/Framework

The Company recognizes that entrepreneurial activities inherently involve the assumption of risks alongside potential reward opportunities. In this context, the Company is committed to operating within a structured risk management framework designed to identify, assess, and minimize potential risks. This framework supports informed decision-making by management, ensuring that risks are appropriately evaluated and managed in alignment with the Company's strategic objectives. An overview of the framework is provided as follows:

a. **Risk Identification:** Management identifies potential events that may positively or negatively affect the Company's ability to implement its strategy and achieve its objectives and performance goals. An illustrative list of such risks is outlined below as an **Annexure A**.

b. **Root Cause Analysis**: Undertaken on a consultative basis, root cause analysis enables tracing the reasons / drivers for existence of a risk element and helps developing appropriate mitigation action.

c. **Risk Scoring:** The risk scoring methodology helps in strengthening the overall resilience of the organization, safeguard its assets, ensure compliance with regulatory requirements, and protect its long-term stability. The Company shall incorporate structured risk scoring methodology based on the ratings of high, medium, and low risk is an essential element of the company's risk management policy. This approach facilitates a clear and systematic process for identifying, assessing, and prioritizing risks in accordance with their potential impact on the organization and the likelihood of their occurrence. Under this framework, risks are categorized into three distinct levels:

    1. **High-Risk**: These are risks that pose a significant threat to the company's operations, financial stability, or reputation. High-risk events are characterized by a high likelihood of occurrence and severe consequences if they materialize. As such, they require immediate attention and the implementation of comprehensive mitigation strategies. These risks must be managed with priority to prevent any potential disruption or loss, and resources should be allocated accordingly to address and reduce their impact.

    2. **Medium-Risk**: Risks falling into this category present moderate likelihood and impact. While not as urgent as high-risk items, they still necessitate careful monitoring and the development of appropriate preventive or corrective actions. These risks should be managed actively to reduce their likelihood or impact, with an emphasis on ongoing

evaluation and timely intervention to ensure they do not escalate into more critical issues.

3. **Low-Risk**: These are risks with a low probability of occurrence and limited potential impact on the organization. While low-risk items do not demand immediate action, they should still be subject to routine monitoring and periodic reassessment. Any necessary mitigation measures should be implemented in a cost-effective and proportionate manner, ensuring that the company remains prepared for even unlikely events.

By adopting this tiered risk scoring system, the company can optimize its resource allocation and focus efforts on the most pressing risks, ensuring that high-priority risks are addressed promptly and effectively.

d. **Risk Categorization:** The identified risks are further grouped in to (a) preventable; (b) strategic; and (c) external categories to homogenize risks.

   a. Preventable risks are largely internal to the Company and are operational in nature. The endeavor is to reduce /eliminate the events in this category as they are controllable. Standard operating procedures and audit plans are relied upon to monitor and control such internal operational risks that are preventable.

   b. Strategy risks are voluntarily assumed risks by the senior management in order to generate superior returns / market share from its strategy. The Company adopts a strategic approach to managing risks by either accepting or sharing the risk. This means that the Company may choose to accept certain risks as part of its business strategy, or it may opt to share the risk with external parties, such as partners or insurers. This system is designed to reduce the likelihood of identified risks materializing and to enhance the Company's ability to manage, control, and contain the impact of any risks that may occur.

   c. External risks arise from events beyond organization's influence or control. They generally arise from natural and political disasters and major macroeconomic shifts. Management regularly endeavours to focus on their identification and impact mitigation through 'avoid'/'reduce' approach that includes measures like business continuity plan / disaster recovery management plan / specific loss insurance / policy advocacy etc.

e. **Risk Prioritization:** Based on the composite scores, risks are prioritized for mitigation actions and reporting.

f. **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.

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

   - Required action(s).
   - Required resources.

- Responsibilities.
- Timing.
- Performance measures and.
- Reporting and monitoring requirements.

The mitigation plan may 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.

Therefore, it is drawn with adequate precision and specificity to manage identified risks in terms of documented approach (accept, avoid, reduce, share) towards the risks with specific responsibility assigned for management of the risk events.

g. **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 assessments throughout the year.

h. **Risk Response Strategies**: There are various 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.

i. **Risk Reporting**: Periodically, key risks are reported to the 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 carries 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.

j. **Risk Management Measures**: The Company shall adopt various measures to mitigate the risk arising out of various areas described above, including but not limited to the following:

- A well-defined organization structure;
- Defined flow of information to avoid any conflict or communication gap;

- Hierarchical support personnel to avoid work interruption in absence/ non-availability of functional heads;
- Discussion and implementation on financial planning with detailed business plans;
- Detailed discussion and analysis of periodic budgets;
- Employees training and development programs;
- Internal control systems to detect, resolve and avoid any frauds;
- Systems for assessment of creditworthiness of existing and potential contractors/subcontractors/ dealers/vendors/ end-users; and
- Redressal of grievances by negotiations, conciliation and arbitration.

5. Roles and responsibilities:

Responsibility holders	Responsibilities
Board of Directors	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: a. Ensure that the organization has proper risk management framework. b. Define the risk strategy, key areas of focus and risk appetite for the company. c. Approve various risk management policies including the code of conduct and ethics. d. Ensure that senior management takes necessary steps to identify, measure, monitor and control these risks.
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: a. Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company. b. Monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems. c. 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. d. Keep the Board of directors of the Company informed about the nature and content of its discussions, recommendations and actions to be taken. e. Review the appointment, removal and terms of remuneration of the Chief Risk Officer (if any).
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.

6. Business Continuity Plan

The objective of the Business Continuity Plan is to support the business process recovery in the event of a disruption or crisis. This can include short or long-term crisis or other disruptions, such as fire, flood, earthquake, explosion, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, Epidemic and Pandemic and other natural or man-made disaster.

7. Policy review and amendment:

The policy shall be reviewed once every two years by the Risk Management Committee. Any changes or modification to the Policy shall be recommended by the Committee and be placed before the Board of Directors for approval.

Any subsequent amendment/modification in the Act or the rules framed thereunder or the SEBI Listing Regulations and/or any other laws in this regard shall automatically apply to this Policy.

8. Version Control:

Sr. No.	Versions	Approval date	Approved by
1	Version 1	April 22, 2025	Board of Directors

Annexure A

Risk Identification: various internal and external risks associated with the Company which can be identified, including but not limited to, are:

a. **Macroeconomic Risk:** any adverse macro-economic situation may have direct correlation on borrower companies ability on revival process and debt servicing.

b. **Liquidity Risk:** The lack of liquidity in the market could affect the Company's liquidity.

c. **Operational Risk:** The operational risk can result from a variety of factors, including failure to obtain proper internal authorisations, improperly documented transactions, failure of operational and information security procedures, computer systems, software or equipment, fraud, inadequate training and employee errors.

d. **Reputational Risk:** Reputational Risk is the current or prospective risk of business, earnings and capital arising from adverse perception of the Company on part of counterparties, shareholders, investors or regulators.

e. **Legal, Regulatory, Statutory and Compliance Risk:** Risk arising out of a change in laws and regulations governing the business or non-compliance of any existing laws and regulations.

f. **Competition Risk:** The industry in which the Company operates is growing at a rapid pace and is exposed to tremendous competition. Entry of new players may increase the competition.

g. **Business Continuity Risk:** Incidents like fire, natural calamity, breakdown of infrastructure, acts of terrorism etc., may result in the risk of loss of data which can adversely affect the Company's financial results.

h. **Force Majeure Risks:** Force Majeure risks constitute an unprecedented macro-economic shock, pushing the economy into a recession of uncertain magnitude and duration. Pandemic and resultant lockdowns were such risks.

i. **Cyber/ Information Technology Risk:** Risk of financial loss, disruption or damage to the reputation of an organisation resulting from the failure or compromise of cyber resources/ information technology. Cyber threats include phishing attacks, malware attacks, ransomware attacks etc. and can result in to loss of data, control over information systems and could result into adverse impact on the operations.

j. **Data Protection Risk:** Data Protection Risk includes failure of data storage device resulting in the loss of transactional data. It also includes corruption of data caused due to data rot causing business processes to fail.

k. **Money Laundering Risk:** Negative publicity; damage to corporate reputation and loss of goodwill; legal and regulatory sanctions; an adverse effect on the bottom line, are all possible consequences of an organisation's failure to manage the risk of money laundering.

l. **Crisis Management Risk:** Crisis management risk is the identification of threats to an organisation and its stakeholders, and the methods used by the organisation to deal with the threats arising on account of unpredictability of global events.

m. **Succession planning risk:** Succession planning risk is the chance that a critical role will become vacant and cannot be filled satisfactorily before the vacancy has unacceptable impact on the organisation.

n. **Criticality of the risks:** Criticality of the risks is based on the consequence of failure of managing the risk.