

GATI LIMITED

CIN: L63011TG1995PLC020121

Regd. Office: Plot No.20, Survey No.12, Kothaguda, Kondapur, Hyderabad – 500084

Phone: +91 40-71204284 **Fax:** +91 40-23112318

Website: www.gati.com **Email:** investor.services@gati.com

RISK MANAGEMENT POLICY

(Effective from August 09, 2021)

INDEX

1. Document Control
2. Background
3. Legal Framework
4. Applicability
5. Underlying approach to risk management
6. Purpose of risk management
7. Objectives
8. Structure
9. Roles and Responsibilities
10. Composition of Risk Management Committee
11. Risk Management Frame Work
12. Risk Register
13. Risk Classification
14. Risk Appetite
15. Risk Likelihood Measurement
16. Risk Impact Measurement
17. Risk Categories
18. Annexures

1. Document Control:

1.1 Entity Name: Gati Limited

1.2 Document Name : Risk Management Policy

1.3 Change Record

Date	Author	Version	Change Reference
25-05-2021	T.S. Maharani	Version 1.0	Initial Version

1.4 Reviewer

Name	Position	Date Reviewed
Mukundan K V	Chief Assurance and Risk Officer	07-08-2021

1.5 Approver

Name	Position	Date Approved
Board of Directors	Board – Gati Limited	

GATI LIMITED

Risk Management Policy

2. Back Ground:

Gati Limited (“Gati” or “the Company”) is India’s pioneer in Express Distribution and Supply Chain Solutions. The Company offers specialized integrated logistics services across all over India including E-commerce Services. Benchmarked quality standards, standardized processes and operation excellence across all the services and facilities, have enabled the Company to emerge as the market leader in all these segments. Further, the Company is also engaged in Express Logistics, Air Freight, Warehousing Solutions, end-to-end logistics solutions through one of its subsidiary company. The Company is prone to inherent business risks like any other organization.

3. Legal framework:

As per the Regulation 21 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 as amended from time to time, have incorporated various provisions in relation to Risk Management policy, procedure and practices.

In line with the above requirements, it is therefore, required for the Company to frame and adopt a Risk Management Policy (“RM Policy”) of the Company.

RM Policy is framed with the objective of identification, evaluation, monitoring, controlling, managing and minimizing identifiable risks.

4. Applicability:

RM Policy applies to whole of the Company including subsidiaries, branches and functions.

5. Underlying approach to risk management:

Gati’s approach to risk management is described below:

- ❖ Adoption of an open and receptive approach to solve risks by the Board/ Risk Management Committee.
- ❖ Management and other employees and key volunteers implement policies approved by the Board/ Risk Management Committee under their advice.
- ❖ Making conservative and prudent recognition and disclosure of the financial and non-financial implications of risks.
- ❖ All employees are responsible for encouraging good risk management practice within their areas of work.
- ❖ Key risks will be identified by the Board/ Risk Management Committee/other employees and monitored on a regular basis.

6. Purpose of risk management

Gati is committed to high standards of corporate governance which encompasses good risk management to:

- ❖ **achieve sustainable business growth;**
- ❖ **protect the Company's assets;**
- ❖ **safeguard shareholder investment; ensure compliance with applicable laws and regulations; and**
- ❖ **avoid major surprises.**

RM Policy is intended to ensure that an effective risk management framework is established and implemented within the Company.

RM Policy complements and does not replace other existing compliance and operational excellence programs.

7. Objectives

The objectives of the RM Policy of the Company are:

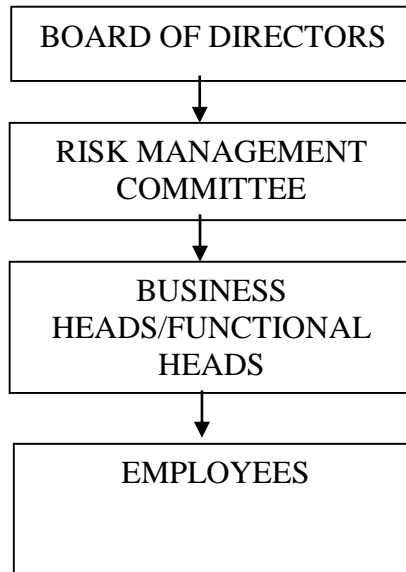
- ❖ The organization has a current, fair and comprehensive understanding of its risks.
- ❖ The organization's risks are within its risk criteria.
- ❖ The organisation develops and improves its ability to identify and manage existing and potential risks in a structured manner with minimum amount of disruption and cost.
- ❖ All decision making within the organization, whatever the level of importance and significance, involves explicit consideration of risks and the application of risk management to appropriate degree.

To achieve the above objectives, the Company aims to the following:

- ❖ The identification and management of risk is integrated in the day to day management of business;
- ❖ Risks are identified, assessed in the context of Company's risk appetite for risk and their potential impact on the achievement of objectives, continuously monitored and managed to an acceptable level;
- ❖ The escalation of risk information is timely, accurate and gives complete information on the risks to support decision making at all management levels;
- ❖ Risk is primarily managed by the business and support functions transacting the business which gives rise to the risk; and
- ❖ All employees actively engage in risk management within their own areas of responsibility and in a well co-ordinated manner across all functions.

8. Structure

The organizational structure for risk management is as follows:



9. Roles and Responsibilities

The risk management roles and responsibilities will be as follows:

<p>Board of Directors</p>	<ul style="list-style-type: none"> ❖ Reviews and approves Risk Management policy, plan including Information/Cyber Security of the Company; ❖ Review the Company's risk governance structure, risk assessment and risk management practices and guidelines, procedures for risk assessment and risk management; ❖ Reviews adequacy and effectiveness of business risk management; ❖ Reviews and approves assurance plans on risk management frame work; ❖ Monitor (including addressing escalations) business risk reporting;
<p>Risk Management Committee</p>	<ul style="list-style-type: none"> ❖ Frame, implement and monitor the Risk Management Plan and Policy of the Company, which shall include: - <ol style="list-style-type: none"> a) A framework for identification of internal and external risks specifically faced by the entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risk), information, cyber security risks or any other risk as me determine by the Committee. b) Measures for risk mitigation including systems and processes for internal control of identified risks. 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;

	<ul style="list-style-type: none"> ❖ 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; ❖ Keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken; ❖ The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee. ❖ Adopting polices, systems for maintaining information/cyber security of the Company from preventing of global hacking incidents, losing of sensitive, confidential data etc; ❖ Set the tone and influence the culture of risk management within the Company. This includes: <ul style="list-style-type: none"> • communicating the Company’s approach to risk • determining what types of risk are acceptable and which are not, setting the standards and expectations of staff with respect to conduct and probity ❖ Periodically review the approach to risk management and approve changes or improvements to key elements of its processes and procedures; ❖ Escalate risks to Board; ❖ Monitor business risk reporting; ❖ Setting strategic plans and objectives for risk management and risk minimization; ❖ Oversee maintenance, updation and review Risk Registers from time to time; ❖ Framing guidelines, policies and processes for monitoring and mitigating risks;
<p>Functional / Departmental Heads</p>	<ul style="list-style-type: none"> ❖ Responsible for identifying risks; ❖ Responsible for preparing risk profile; ❖ Responsible for managing risk by implementing mitigation plans; ❖ Escalate Risks to Risk Management Committee; ❖ Responsible for compliance at all relevant levels; ❖ Determination/approval of mitigation plans; ❖ Identify, review and monitor risks of each business vertical and functions of the Company including strategic, financial, operational, currency, work place environment, safety & information security, regulatory and reputational risk periodically; ❖ Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company; ❖ implementation of the risk management policy, including evaluating the adequacy of risk management systems;

	<ul style="list-style-type: none"> ❖ Implementingsystems for maintaining information/cyber security of the Company from preventing of global hacking incidents, losing of sensitive, confidential data etc; ❖ Maintenance of Risk Registers ❖ Quality assurance on risk management process; ❖ Provide adequate information in a timely manner to the Board /Risk Management Committee on the status of risks and controls. ❖ To work with Chief Assurance & Risk Executive for Risk workshops or other methods to identify, assess, evaluate, mitigate and manage risks at acceptable levels and seek guidance from time to time and maintain, review and update risk register from time to time.
<p>Chief Assurance & Risk Executives/Group CIO</p>	<ul style="list-style-type: none"> ❖ To co-ordinate meeting of Risk Management Committee at least twice in a year; ❖ To conduct various periodic workshops for each business verticals of the Company regarding the risk faced by them, creating awareness of RM Policy and reporting the same to the Risk Management Committee; ❖ Tests compliance at all relevant levels; ❖ Scopes audit work based upon significance of risk to the business and based on the audit plan approved by Audit Committee; ❖ Assist Functional/Departmental Heads to maintain and Update Risk Registers from time to time; ❖ Special investigations requested, if any; ❖ Creating awareness and educating all employees across the Company about the importance of Information Security & IT Risk Management; ❖ Taking measures to mitigate / minimize Security risks by selecting and implementing appropriate tools and processes; ❖ Responsible for compliance of all laws related to IT
<p>Employees</p>	<ul style="list-style-type: none"> ❖ Implement policies on risk management and internal control; ❖ Identify and evaluate the fundamental risks faced by the Company; ❖ Identify risks for escalations; ❖ Re-assess risks on a periodic basis; ❖ Ensure to develop 'Risk culture' in all decision making within the organization; ❖ Educate themselves with Risk Management Policy; ❖ Escalation Process and Risk appetite of the organization and ensure compliance; ❖ Exercise reasonable care to prevent loss, to maximize opportunity and to ensure that the operations, reputation and assets are not adversely affected.

10. Composition of Risk Management Committee:

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. Following shall be permanent invitees:

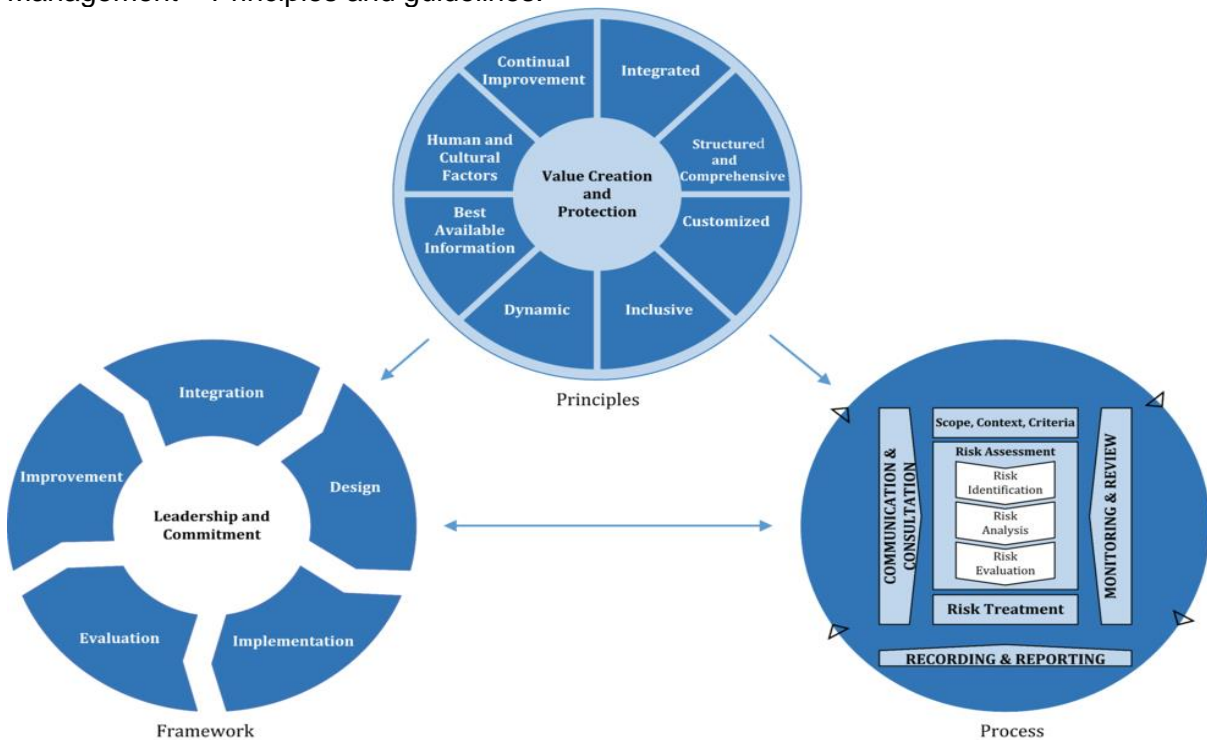
- Chief Financial Officer
- Chief Information Officer
- Chief Assurance & Risk Executive

The Board of Directors may re-constitute the composition of the Risk Management Committee, as it may deem fit, from time to time.

The terms of reference of the Risk Management Committee as may be approved by the Board of Directors is attached as **Annexure 1**. Any changes in the term of reference shall automatically apply in RM Policy.

11. Risk Management Frame Work

The Company will follow a broad risk management frame work as envisaged in ISO 31000 Risk Management – Principles and guidelines.



12. Risk Register

The Risk Register is the main risk management tool for monitoring the risk management process within the project. It lists the ranked risks and references the associated risk action plans. Keeping the risk register up to date is the responsibility of the CEO / Functional Heads. Format of the Risk Register is attached as **Annexure - 2**.

New risks will be identified and entered into the Risk Register and if required risk action plans developed and referenced in the Register. Risks that have been managed, avoided or are no longer relevant can be removed from the Risk Register. The associated risk action plans will also be deleted from the Risk Register. Risk Register shall be placed before the Risk Management Committee meeting.

13. Risk Classification

For effective management risks will be classified in to various baskets based on the broad nature of risks. An indicative classification of risks is as under:

- a. **Strategic**: Risks associated with an organization's inability to formulate and/or execute a successful business strategy largely having to do with the future growth plans of the company such as plans to enter new markets, launch new products, and form new alliances. For example: Acquisitions and Divestitures; Key Person / Succession Planning; Capital Planning / Allocation; Research and Development; Brand and Marketing; Pricing; Customer Demands; Customer Concentration; Product; Technology.
- b. **Governance**: Risks related to the structure, policies, procedures and authorities in which the key directions and decisions of the Company are overseen. For example: Independence and Oversight; Ethics; Corporate Social Responsibility; Delegation of Authority; Shareholder Relations; Stakeholder Activism; Corporate Policy, etc.
- c. **Financial**: Some examples of Financial risks as applicable to Gati are:-
 - Non-realization of money from customers.
 - Increasing interest costs on amounts borrowed for projects, which may get delayed.
 - Non-fulfillment of or breach of any conditions of contracts made with contractors, resulting higher costs or delay the projects thus increasing the overall costs.
 - Imposition of any new or increased taxes or levies on the Company/ industry, by the Government.
 - Discontinuance of any existing finance facilities given by the Banks/ Financial Institutions, which may result in higher cost of borrowed funds to be taken from others.
 - Foreign exchange risks on account of fluctuations in foreign exchange vis-à-vis the rupees, interest rates.
 - Fall in profitability on account of increased cost not matched by prices, and also falling price of the products and services.
 - Fall in liquidity resulting in cash flow problems.
- d. **Human Resource**: There is inherent risk on account of skilled and specialized manpower. They gain experience working with the Company and need continuous motivation and supervision, so that their efforts are best used in the Company. There is a risk of specialized manpower leaving the jobs, joining competitors, sharing confidential information with competitors etc. There is also the risk of them being under-utilized or put in areas where they are misfit.
- e. **Operations**: Risks arising from inadequate controls or failure of controls infrastructure largely having to do with the protection and utilization of existing assets and how they may be leveraged for future growth. Providing comprehensive services of high standard and time management are inherent to successful execution of business.
- f. **Compliance**: For alleged non-compliance/ violation of various laws applicable to the Company, there can be legal liabilities on the Company and the management. This may arise and be fixed on the Directors, individually or collectively, and all the officers who are involved/responsible.

- g. **Information Technology/Cyber Security:** Risk associated with information technology and cyber security like preventing of hacking incidents, losing of sensitive, confidential data etc. New and emerging technologies bring unprecedented threats to internet-connected devices, including vehicles. The loss of sensitive and personal data or a breach in any safeguards aimed at protecting the information related to cyber security could lead to significant legal action combined with the imposition of regulatory and associated fines.
- h. **External:** Risks associated with the environment in which the client operates or external factors beyond the client's control. For example: Competition; Legal and Regulatory; Stakeholder Relations; Geo-political; Economic Conditions / Industry Trends; Hazards; Terrorism, War, Civil Unrest, Government Policies, change(s) in business cycles/ pattern, industry / customer changes, customer demand, customer preference, environmental changes, Merger & Acquisition integration, force majeure affecting business like acts of God, act of Government, act of public enemy, floods, earthquakes, riots, war with enemies, civil commotion, epidemics, cyclone, storm etc., and other external factors beyond the control of Gati.

Some more baskets of risks are Marketing, Business Continuity, Planning, Quality, etc.

14. Risk Appetite

In order to give a uniform guidance to the resources involved in risk management process, one example of Risk Appetite (to be implemented once certain level of maturity achieved), measurement units of severity (impact) and likelihood (probability) and escalation mechanism are given in the table below:

RISK APPETITE					
AUTHORITY / WILLINGNESS TO ACCEPT RISK					
ESCALATION	DEPARTMENT	DEPARTMENT	CEO / FUNCTIONAL HEAD	RISK MANAGEMENT COMMITTEE	FIN. COMMITTEE / BOARD
	1	2	3	4	5
SEVERITY	INSIGNIFICANT	LOW	MODERATE	SIGNIFICANT	CRITICAL
Financial - Budgeted Revenue	1 percent	2 percent	5 percent	10 percent	15 percent
Financial - Budgeted EBIDTA (Margin)	1 percent	2 percent	5 percent	10 percent	15 percent
Financial - Budgeted Asset turnover ratio	1 percent	2 percent	5 percent	10 percent	15 percent
Financial - Prevent Loss of Assets - Dollar value of lost assets	1% of net book value	2 % of net book value	5 percent of net book value	10 percent of net book value	15 percent of net book value
Health & Safety	Minor injury / environmental damage	Serious injury / environmental damage	Multiple injuries / environmental damage	Single fatality / major environmental damage including possibility of prosecution	Multiple fatalities / major environmental damage including prosecution
Regulatory	Warnings, legal notices	Minor penalty	Major penalty	1. Major penalty including prosecution 2. Requirement to incur significant expenditure	Major penalty, legal notices having probability to effect short term / permanent closure of business
Capital Project Execution	Minor delay at intermittent stages which does not change scheduled date of commercial operations.	Minor delay resulting of postponement of scheduled date of commercial operations by 15 days	Minor delay resulting of postponement of scheduled date of commercial operations by 30 days	Delay resulting of postponement of scheduled date of commercial operations upto 6 months	Delay resulting of postponement of scheduled date of commercial operations beyond 6 months
Market share	< 0.50 percent decline	0.50 - 1 percent decline	1 - 2 percent decline	2-3 percent decline	>3 percent decline
Market Reputation	1. Adverse publicity through word of mouth; confined to a small geographical area 2. Negligible number of complaints	1. Adverse publicity in local media and possibility of approaching consumer forums 2. Negligible number of complaints with medium gravity levels	1. Adverse publicity in media and short term loss of customer confidence, cases in consumer forums 2. Higher number of complaints with high gravity levels	1. Short term adverse media publicity and loss of investor / customer confidence 2. Possibility of legal cases and compensations and high complaint numbers	1. Continuous adverse media publicity and long term loss of investor / customer confidence 2. Serious customer complaints and high in number
	REMOTE	UNLIKELY	LIKELY	PROBABLE	HIGHLY PROBABLE
Probability (Likelihood table)	Event may occur in exceptional situations	Event may occur sometime	Event should occur sometime	Event will occur in most circumstances	Event is certain to occur in most circumstances

Risk Management Committee is authorized to approve appropriate criteria to measure risk appetite and escalation mechanism.

15. Risk Likelihood Measurement

Each risk statement will be assessed on following scale:

Likelihood measurement unit	Description	Numeric Value
Very unlikely	Selecting 1 means that you believe the event is "Very Unlikely" with a probability of occurrence lower than 20%	1
Unlikely	Selecting 2 means you believe the event is "Unlikely" with a probability of occurrence between 21% and 40%	2
Somewhat Likely	Selecting 3 means you believe the event is "Somewhat Likely" with a probability of occurrence between 41% and 60%	3
Likely	Selecting 4 means you believe the event is "Likely" with a probability of occurrence between 61% and 80%	4
Very Likely	Selecting 5 means you believe the event is "Very Likely" with a probability of occurrence greater than 81%	5

16. Risk Impact Measurement

Each risk statement will be assessed on following scale:

Impact measurement unit	Description	Numerical Value
Insignificant	Impact is insignificant	1
Low	A low impact event on the organizational objectives	2
Moderate	Event will have impact on organizational objectives.	3
Significant	Impact is high and can affect organizational objectives.	4
Critical	Impact is extremely high and can severely affect organizational objectives.	5

17. Risk Categories

Each risk statement will be assessed for severity (impact) and likelihood on the scale of measurement mentioned in Risk Appetite. Based on the score the risks will be classified in to three categories such as Critical (High), Cautionary (Medium), and Acceptable (Low). Any score of 16 and above (maximum score 25) will be treated as **Critical**, Score of 9 and above however below 16 will be **Cautionary** and any score below 9 will be treated as **Acceptable**.

ANNEXURE-1 TERMS OF REFERENCE

Name of the Committee	Risk Management Committee
Statutory / Non Statutory	Statutory
Role	<p>(1) To formulate a detailed risk management policy which shall include:</p> <p>(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 Committee.</p> <p>(b) Measures for risk mitigation including systems and processes for internal control of identified risks.</p> <p>(c) Business continuity plan.</p> <p>(2) To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;</p> <p>(3) To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;</p> <p>(4) To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;</p> <p>(5) To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken;</p>

	<p>(6) The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.</p> <p>The Risk Management Committee shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the board of directors.</p>
<p>Constitution</p>	<p>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.</p> <p>Following shall be permanent invitees:</p> <p>Chief Financial Officer Chief Information Officer Chief Assurance & Risk Executive</p> <p>The Board of Directors may re-constitute the composition of the Risk Management Committee, as it may deem fit, from time to time.</p>
<p>Term of Reference</p>	<ul style="list-style-type: none"> - Frame, Monitor and Implement the Risk Management Plan and Policy of the Company and review the Company’s risk governance structure, risk assessment and risk management practices and guidelines, procedures for risk assessment and risk management; - Adopting polices, systems for maintaining information/cyber security of the Company from preventing of global hacking incidents, losing of sensitive, confidential data etc; - Identify, Review and Monitor risks of each business vertical and functions of the Company including strategic, financial, operational, currency, work place environment, safety & information security, regulatory and reputational risk periodically; - Continually obtaining reasonable assurance from management heads of each business vertical that all known and emerging risks have been identified and mitigated or managed; - Framing guidelines, policies and processes for monitoring and mitigating risks; - Setting strategic plans and objectives for risk management and risk minimization;

	<ul style="list-style-type: none"> - Overseeing the risk management process, controls, fraud risk assessment, risk tolerance, capital liquidity and funding; - Review compliance with risk policies, monitor breach/trigger trips of risk tolerance limits and direct action; - Development and deployment of risk mitigation plans to reduce the vulnerability to the prioritized risks and provide oversight of risk across organisation; - Maintain, Update and Review Risk Registers from time to time; - Delegate authorities from time to time to the Committee Members, Executives, Authorized persons to implement the decisions of the Committee and execution of necessary documents; - To achieve sustainable business growth, protect the Company’s assets, safeguard Members investment, ensure compliance with applicable laws and regulations and avoid major surprises of risks; - To obtain advice and assistance from internal or external legal, accounting or other advisors; - Periodically reporting to the Board; - Performing such other functions as may be necessary or directed by the Board.
Chairperson	The Chairperson of the Committee shall be a member of the Board of Directors.
Secretary	The Company Secretary shall act as the Secretary to the Committee.
Frequency, Attendance & Quorum	<p>The Committee shall meet as frequently as it deems necessary but at least twice in a year.</p> <p>Members of the Company’s executive and senior management shall attend the meetings by invitation, in accordance with items on the agenda.</p> <p>The quorum for a meeting of the 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.</p>
Reporting	The Chairperson of the Committee shall update the Board and recommend the action plans.

ANNEXURE – 2 FORMAT OF RISK REGISTER

RISK REGISTER					
Sl.No	Contributing factors	Risk owners	Likelihood Rating	Impact Rating	Combined Score