RISK MANAGEMENT POLICY

1. INTRODUCTION

1.1 Purpose

Company faces risks from internal and external sources during its day-to-day business operations that create uncertainties over Company's ability to achieve its business goals. Risks are the uncertainties/events/factors that may occur and will impact company's objectives if left unaddressed. The Company considers ongoing risk management to be an integral part of the business operations and understands that the Company's ability to identify and address risks is central to achieving its corporate objectives.

The policy outlines the programs implemented by the Company to ensure appropriate risk management within its systems and culture. In line with the Company's objective of increasing stakeholder value, this policy attempts to identify the key events/risks impacting the business objectives of the Company and attempts to develop risk policies and strategies to ensure timely evaluation, management, monitoring, and reporting of key business risks.

1.2 Applicability

The policy is devised in the context of the present business profile, future growth objectives and new business initiatives that may be necessary to achieve the goals, as well as to maintain the standards followed in line with best industry practices. This policy covers all the events within the Company and events outside the Company which have a bearing on the Company's business.

1.3 Scope

This policy is also formulated in compliance with the provisions of the Companies Act, 2013 (the "Act"), which requires the Company to lay down procedures about risk assessment and risk minimization. The scope of the policy is to establish and implement the Company's risk management program and process and ensure its integration with its business strategy.

2. RISK MANAGEMENT PROGRAM

2.1 Company's risk management program comprises a series of processes, structures, and guidelines that assist the Company to identify, assess, monitor, and manage its business risks, including any material changes to its risk profile.

2.2 The objective of risk management program is as follows:

i. To establish a risk management program of the Company;
ii. To help decision makers of the Company take account of the risks and work towards a solution to manage such risks;
iii. To achieve strategic goals and objectives while ensuring appropriate management of risks;
iv. To continuously improve and strengthen the risk management process through risk testing and assessments.

2.3 The company has clearly defined responsibilities and authority of Management to oversee, manage, develop, and maintain the risk management framework considering the day-to-day needs of the Company.

2.4 Any risk that could have an impact on the Company's business should be identified, assessed and managed in tune with the current operations and practices. As such, due consideration should be given to the following indicative sources of risks:

i. External factors:

-Market-related
-Political and macro-economic environment
-Reputation
-Legal and compliance
-Competition
-Environment and sustainability
-Natural calamity and disaster
-Risks arising out of transactions (Mergers and Acquisitions/Demergers, Restructuring/sale/purchase etc.)

ii. Internal factors:

-Operational

-Contract management

-Project management

-Business disruption and continuity

-Strategic

-Ethical and integrity issues

-Financial management

-Revenue and cost structure

-Corruption or fraud

-Health and Safety

3. RISK MANAGEMENT PROCESS

Risk management is a continuous process. The key components of the Company's risk management process are set out as below:

3.1 Risk Identification

3.2 Risk Assessment

3.3 Risk Evaluation

3.4 Risk Treatment

3.5 Risk Monitoring and Reporting

3.1 Risk identification

Risk identification is a continual process of recognizing and describing risks that might help or prevent the Company in achieving its objectives. A risk library[1] containing an extensive list of risks is to be tracked and monitored to help the Management and Company Personnel to identify and mitigate the possible threats or vulnerabilities which may have an adverse impact on the Company's business. The process of risk identification should include all risks, both external and

[1] Risk library is a repository of all the risks identified across the business operations till date.

internal, whether or not they are under the control of the Company. Risk identification should be carried out on a regular basis, at least annually.

3.2 Risk assessment

Risk assessment is essentially an evaluation of the identified risks on both likelihood (of occurrences) and impact (magnitude/consequence). Risk assessment will necessarily be an exercise in subjective judgment and will draw on the experience and business/industry knowledge of the Management and stakeholders. However, if appropriate, the use of tools like risk scoring/estimation may be preferred.

HODs along with the Compliance Oversight Committee of the Company are responsible for identification, assessment and management of risks and ensuring the implementation of appropriate measures.

Following scale is to be used for determining the likelihood of risk occurrence:

Levels	**Descriptors**
1	Very low or not likely
2	Low or less likely
3	Medium or likely
4	High or most likely
5	Very high

Following scale is to be used for determining the Impact of the risk:

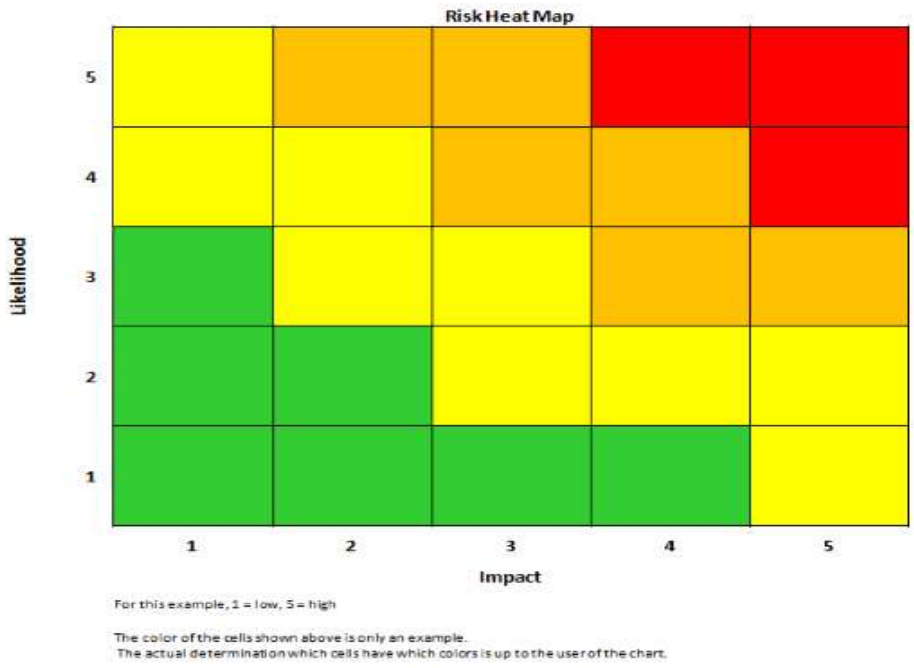
Levels	**Descriptors**
1	Very low
2	Low
3	Medium
4	High

5	Very high

Refer SOP for "Compliance Oversight Committee" for details on the scale for determining likelihood and impact of risk matrix.

3.3 Risk evaluation

Risk evaluation is an activity where the average score from likelihood and impact should be multiplied to arrive at a final risk score. Average scores for each criterion can be obtained by involving multiple members or forming a group as part of the risk evaluation process. The objective of risk evaluation is to prioritize risks and to plan appropriate measures that will lead to a focused approach and optimal utilization of the Company resources in managing these risks.



Classification of risk level is based on final score obtained from the risk evaluation process. Below are the risk levels assigned (to be populated on the risk heat map shown above):

1. RED (Critical/High): Requires immediate actions and will be monitored regularly until the risk is either mitigated or brought to acceptable levels through effective controls/mitigation plans.

2. YELLOW (Medium/Cautionary): Considered as moderate and requires action plans or steps to improve existing controls.
3. GREEN (Low): Considered as acceptable, however needs to be monitored on periodic basis to ensure that risk level remains consistent.

3.4 Risk treatment

The purpose of risk treatment is to select and implement options for addressing risks. Risk will primarily be treated and managed by the concerned HOD. Hence the manager of the risk is responsible for escalating such identified risk to the concerned HOD, who shall further record, treat and inform the Management on a timely basis, so that the encountered risks can be appropriately treated and managed. For this, the Company follows a progressive level of escalation right up to the Management and further to the Hold Co Board.

The Company will select the most appropriate treatment option based on consideration of risk appetite and costs and efforts of implementation vis-a-vis benefits derived. While identifying treatment options, the Company should consider the values and perceptions of all stakeholders. It should also be noted that risk treatment itself can introduce new risks and/or result in change in profile of existing linked risks and that may require a review of treatment measures.

The treatment options may include:

- those controls already in place such as specific strategies, management reporting, legislative frameworks, or industry standards; and
- the actions agreed which will manage and/or mitigate the impacts or the likelihood of the risk materialising, such stakeholder engagement plans; training opportunities; or new technology solutions.

Risk action plans should include the actions identified and captured at specific risk working groups and other such meetings, to ensure transparency and tracking. Risk action plans may include:

• Transferring or outsourcing risks for which the Company does not have the necessary expertise;

- Formulating action plans to prevent/control exposure from known/predictable sources of risk;
- Developing strategic plans to counter potential risks which may have entity-wide/strategic impact;
- Constant monitoring and assessment of exposure – especially for the external environment;
- Building appropriate controls in business operations; and
- Avoiding an alternative that may expose the Company to undesirable levels of perceived/actual risk.

The Hold Co Board or the Management may also require the HODs/functional owners and/or Compliance Officer to periodically report on the status of the risk management exercise.

3.5 Risk monitoring and reporting

Once a risk action plan is put in place for risk management, the overall responsibility of preparing the risk report at departmental level lies with the respective HODs. The report should be reviewed and approved by the Compliance Oversight Committee.

Specified Key Performance Indicators (KPIs) may be assigned for tracking progress of the undertaken risk action plan and further the manager of risk may be made accountable for the implementation of agreed risk mitigation measures within a defined timeline. Refer SOP for "Compliance Oversight Committee" for details on frequency of reporting and monitoring of classified risks.

4. COMPLIANCE OVERSIGHT COMMITTEE

The overall responsibility of risk management primarily rests with the concerned HODs, since they are in the best position to identify the risks that may be encountered on a day-to-day basis, as well as to advise on the basis of the process outlined in the policy.

The Company has a committee, namely, the Compliance Oversight Committee, which is constituted with the responsibility of overseeing and reviewing risk management across the Company. The terms of reference of the Compliance Oversight Committee are as follows:

- review of strategic risks;
- review of operational risks;
- review of financial and reporting risks;
- review of compliance risks;
- review and discuss the Company's risk philosophy and the quantum of risk on a broad level that the Company, as an organization, is willing to accept in pursuit of stakeholder value;
- review the extent to which management has established effective enterprise risk management at the Company;
- inquire about existing risk management processes and review the effectiveness of those processes in identifying, assessing, and managing the Company's most significant enterprise-wide risk exposures;
- review the Company's portfolio of risk and ensure its alignment with its risk appetite by reviewing the integration of strategic and operational initiatives with enterprise-wide risk exposures; and
- review periodically key risk indicators and management response thereto.

Compliance Oversight Committee shall periodically review this policy, at least on an annual basis, so that the Management undertakes the risk management through the framework defined in the policy and related SOPs.

5. REVIEW OF THIS POLICY

This policy shall be subject to review, if necessary. Any change/amendment to this policy shall be approved by the Compliance Oversight Committee.

6. VIOLATION OF THIS POLICY

Any Company Personnel found to have violated this policy shall be subjected to disciplinary action in line with the Code of Conduct and Ethics Policy and Consequences and Disciplinary Action Matrix (CADAM) of the Company.