



SHARDA MOTOR INDUSTRIES LIMITED

RISK MANAGEMENT POLICY

[Section 134(3), Section 177(4), Schedule IV [Section 149(8)] of the Companies Act, 2013 and as per Regulation 21 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 read with Section C of Part D of Schedule II]

Document No.	002
Date of First Approval	23 rd June, 2021
Last Amended on	10 th August, 2023
Last Version	1.0
Current Version	2.0
Approved by the Board of Directors	Sd/- Kishan N. Parikh Chairperson on the Board

BACKGROUND

This document lays down the framework of Risk Management at Sharda Motor Industries Limited (hereinafter referred to as the 'Company') and defines the policy for the same. This document shall be under the authority of the Board of Directors of the Company. It seeks to identify risks inherent in any business operations of the Company and lays down the mitigation methods which are periodically reviewed and modified in a manner commensurate with the size and complexity of the business.

OBJECTIVE

The objective of the Risk Management Policy is to lay down procedures and guidelines to assess risk and have mitigation plans in place. It should also provide the Role Mapping for the authorities responsible. The Policy basically sets out the company's approach to risk and should detail the Risk Management process to the staff and concerned representatives.

The policy should ensure sustainable business growth as it gives the mechanism for dealing with the different types of risks that the business could encounter going forward. It gives a structured approach, following which would minimize the impact of the risks. The policy identifies the various risks that could impact the business and its operations and gives a strategy to avoid, reduce, transfer or accept the respective risk.

REGULATORY

Policy is framed as per the regulatory requirements of Section 134(3), Section 177(4), Schedule IV [Section 149(8)] of the Companies Act, 2013 and as per Regulation 21 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 read with Section C of Part D of Schedule II and other applicable provisions, if any (including any statutory modification / re-enactment(s) thereof for the time being in force).

I. RISK GOVERNANCE STRUCTURE AND MANAGEMENT TEAM

1) **Board of Directors** The Board shall be the highest authority to for decision making in respect of Risk Management. The Board shall inter alia: -

- Approve and review the Risk Management Policy

- Define the Company's risk appetite
- Identify and assess internal and external risks in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk that may impact the Company in achieving its strategic objectives or may threaten the existence of the Company
- Define the role and responsibility of the Risk Management Committee and delegate monitoring and reviewing of the risk management plan to the Risk Management Committee and such other functions as it may deem fit; which also shall specifically covers the function related to the Cyber Security.
- Oversee the development and implementation of risk management framework and maintain an adequate monitoring and reporting mechanism.
- Formulate risk management strategy to manage and mitigate the identified risks.
- Give directions to the Audit committee and Risk Management Committee on top priority risks identified and its mitigation plan.

2) Risk Management Committee

The Committee shall be responsible for ensuring that the Company maintains effective risk management and internal control systems and processes, and provides regular reports to the Board of Directors on the effectiveness of the risk management program in identifying and addressing material business risks

"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 Risk management committee shall inter alia -

- Review and approve the risk management policy and associated practices of the company, which shall inter alia 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 Committee.
 - b. Measures for risk mitigation including systems and processes for internal control of identified risks.
 - c. Business continuity plan.
- To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.
- To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.
- To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity.

- To 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.
- Recommend to the Board Policy for hedging Commodity Risk (if any)
- The committee to meet at least twice in a year in such a manner that on a continuous basis not more than one hundred and eighty days shall elapse between any two consecutive meetings.

3) **Senior Management of the Committee (SMG)**

The SMG comprises of core management team of employees including CEO and 2 levels below CEO which heads individual functions in the Company. They will:

- Implement and monitor the principles, actions and requirements of the risk management plan.
- Provide necessary tools and resources to identify, manage and mitigate risks.
- Review risks on half yearly basis- identification of new risks, changes to existing risks, updating risk register etc.
- Report the status of risk items to the Risk Management Committee and Audit Committee on half yearly basis.
- Appraise risk owners' actions taken to manage risk and correction of inappropriate performance Internal compliance and control systems for the implementation of the risk management plan.
- Review and report the status of risks and treatment actions over the Mitigation
- Any new or changed risks shall be identified and escalated, if deemed necessary
- Identify the key risks to be put up in the Risk Management Committee meet.
- Monitor and Supervise the development and implementation of the Risk Management Policy and maintain enterprise-wide view of the key risks and their mitigation measures faced by the organization.

4) **Internal Audit**

Further, the Internal Audit function shall provide assurance on the integrity and robustness of the risk management process.

II. **RISK IDENTIFICATION**

Risk identification consists of a detailed study of threats on the business based on vulnerability and resultant exposure to various risks. Some of the major risks are identified as below:-

- **Strategic Risk** - risks from competing firms, social trends, capital availability and business mix

- **Business Risk** - risks specific to the industry (industry, market, technology advancements, etc), counterparty risks (risks to supplier, client, and other JV partners, their suppliers, clients and business), and risks from resources (sourcing decisions, capital expenditure utilization, etc)
- **Operations Risk** - risks such as Customer Satisfaction, product failure, integrity, and reputational risk.
- **Societal Risk** - risks from environmental interactions of the Business (carbon emissions, water and energy depletion, hazardous waste disposal, etc), society (impact of projects on communities), and natural disasters
- **Risk from Regulatory/political Environment** - risks that arise from adverse developments in the regulatory scenario, and the political environment in all the countries involved in the functioning of the business
- **Asset Risk**- Risk of loss resulting from depreciation, under-utilisation or loss of control over physical assets of company
- **Competition Risk** – Risks pertaining to the external competitors of the company such as entry of new competitors.
- **Compliance Risk** - Risk of loss resulting from legal and regulatory factors, such as strict privacy legislation, compliance laws, and intellectual property enforcement.
- **Contract Risk** – Risks pertaining to the contracts signed with client and sub-contractors.
- **Sustainability/ESG Risk** – Risks having footsteps on the environment, weather, pollution or risks arising due to changes in environment
- **Financial Risk** - All risks which have a financial implication such as adverse movements in foreign exchange rates, capital expenditure, change in value caused by the fact that the timing and/or the amount of expenses incurred differs from those expected etc.
- **Foreign environment risk** - The risk arising due to exposure to foreign laws, regulation and socio-political environment.
- **Litigation Risk** - Risk of loss arising out of litigations against or litigation initiated by the company
- **Market Risk** – Risks pertaining to external market factors such as demand uncertainty, price volatility etc
- **Human Resource Management Risk**- Risks (like attrition) that are part of the personnel related processes of the company such as recruitment, skill sets and performance measurement
- **Process Risk/ Execution Risk** – The risk arising due to lack of adequate process or inadequate execution of defined processes/
- **Project Risk** – Risks which impacts the execution of any project resulting in time and cost overrun.

- **Reporting Risk** - Risk of inadequate internal or external reporting due to wrong financial as well as non-financial information in the reports
- **Goodwill Risk** – Risks having implications on the brand and reputation of the company.
- **Technology Risk** – Risks originating from usage and deployment of technology in the organisation in its operations and management such as product obsolescence because of technology gap.
- **Cyber Security Risk** – cyber security risk is the probability of exposure or loss resulting from a cyber-attack or data breach on your organization

III. RISK ASSESSMENT & EVALUATION

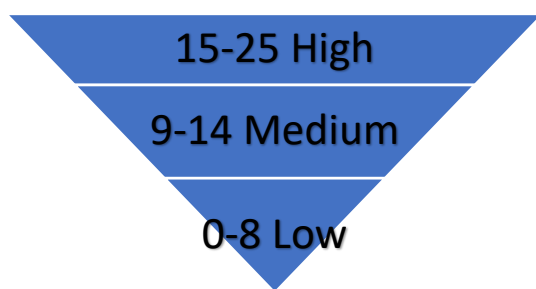
The Risk Assessment and Evaluation process can be considered to be qualitative or quantitative in nature. It should take into account two contributing factors – the probability of occurrence of the event and the impact of such an occurrence.

Risk assessment and evaluation also includes the categorization of each type of risk categorized into high risk, medium risk, and low risk based on the analysis done on these risks.

Risk Assessment Matrix

Probability	Rating	Impact				
Almost Certain	5	Low	Medium	High	High	High
Likely	4	Low	Low	Medium	High	High
Possible	3	Low	Low	Medium	Medium	High
Unlikely	2	Low	Low	Low	Low	Medium
Remote	1	Low	Low	Low	Low	Low
↑ Probability		1	2	3	4	5
→ Consequences		Insignificant	Minor	Moderate	Major	Catastrophic

Risk Score



IV. **Risk Mitigation Strategy**

There are four common strategies for treating risk. There is no single “best” response strategy, and each risk must be considered on its own merits. Some risks may require a combination of strategies and multiple responses, whereas others may need only one strategy with a single response.

- **Risk Avoidance/ Termination:** This involves doing things differently and thus removing the risk (i.e. divestments). This is particularly important in terms of project risk, market risk or customer risk but often wishful thinking in terms of the strategic risks.
- **Risk Reduction/ Mitigation:** Reduce or Treat the risk. This is the most widely used approach. The purpose of treating a risk is to continue with the activity which gives rise to the risk but to bring the risk to an acceptable level by taking action to control it in some way through either:
 - Containment actions (lessen the likelihood or consequences and applied before the risk materializes) or;
 - Contingent actions (put into action after the risk has happened, i.e. reducing the impact. Must be pre-planned)

If the risk treatment mechanism selected is risk mitigation or risk reduction for an identified risk then the next step shall be to review and revise existing controls to mitigate the risks falling beyond the risk appetite and also identify new and improved controls. New control activities are designed in addition to existing controls post assessment of risk exposure at current level to ensure that the risks are within the accepted risk appetite. Control activities are categorized into Preventive or Detective on the basis of their nature and timing:

- Preventive controls – focus on preventing an error or irregularity.
- Detective controls – focus on identifying when an error or irregularity has occurred. It also focuses on recovering from, repairing the damage from, or minimizing the cost of an error or irregularity.

The controls identified for each risk event shall be evaluated to assess their effectiveness in mitigating the risks falling beyond the risk appetite. Implement Controls It is the responsibility of the CRC to ensure that the risk mitigation plan for each function is in place and is reviewed regularly.

- **Risk Acceptance/ Retention:** Accept and tolerate the risk. Risk Management doesn’t necessarily mean risk reduction and there could be certain risks within the organization that it might be willing to accept and continue with its operational activities. The organization shall tolerate such risks that are considered to be acceptable, for example:
 - a risk that cannot be mitigated cost effectively;
 - a risk that opens up greater benefits than loss
 - unavoidable risks

It's the role of SMP or KMP or such other designated Official(s) of the Company to decide to tolerate a risk, and when such a decision is taken, the rationale behind it shall be fully documented. In addition, the risk shall continue to be monitored and contingency plans shall be in place in the event of the risk occurring.

- **Risk Transfer:** Transfer some aspects of the risk to a third party. Examples of risk transfer include insurance and hedging. This option is particularly good for mitigating financial risks or risks to assets.
 - a) The following aspects shall be considered for the transfer of identified risks to the transferring party:
 - Internal processes of the organization for managing and mitigating the identified risks.
 - Cost benefit of transferring the risk to the third party.
 - b) Insurance can be used as one of the instruments for transferring risk.

V. Risk Monitoring & Review

The vertical/functional teams shall review progress on the actions agreed to mitigate the risk and make an assessment of the current level of risk including:

- Establishing whether actions have been completed or are on target for completion.
- Report the status of implementation of mitigation plans to the Risk Management Committee. Any monitoring and review process shall also determine whether:
 - The measures adopted resulted in what was intended.
 - The procedures adopted and information gathered for undertaking the assessment was appropriate.
 - The acceptability of each identified risk and their mitigation plan shall be assessed and risks shall then be ranked to identify key risks for the organization.
 - Proposed actions to eliminate, reduce or manage each material risk shall be considered and agreed.
 - Responsibilities for the mitigation measures for key risks management of each risk shall be assigned to appropriate department/regional heads.

VI. Business Continuity Plan

Business continuity plan refers to maintaining business functions or quickly resuming them in the event of a major disruption, whether caused by a fire, flood or any other act of God. A business continuity plan outlines procedures and instructions an organization must follow in the face of such disasters; it covers business processes, assets, human resources, business partners and more. Such

plan is generally conceived in advance after taking inputs from the board, the Committee, audit committee and independent directors of the Company.

The Company shall delineate business continuity processes and disaster management plans, for unforeseen exigencies and keeping the organization constituents, prepared to appropriately and adequately deal with all kind of risks associated with such circumstances or under eventuality of such happenings and thus making it an important part of Company's risk management system.

VII. Review and Disclosures

The Policy shall be reviewed by the Committee periodically, but at least once in 2 (two) years or earlier if required by a change in circumstances, including by considering the changing industry dynamics and evolving complexity. The same shall be amended and approved by the board of Directors as and when required under applicable laws.

In accordance with Section 134(3)(n) of the Companies Act, 2013, a disclosure shall be made in the Board Report of the Company, indicating development and implementation of the Policy for the Company including identification therein of elements of risk, which in the opinion of the board may threaten the existence of the Company. Further, appropriate disclosures as required to be made under the provisions of the Listing Regulations shall also be complied with.

The Policy shall also be disclosed on the website of the Company, i.e., <https://www.shardamotor.com/investor-relations/policies/>.

If case of any inconsistency between this Policy and the Indian regulations, the requirements of the Indian regulations shall prevail.

In case of any amendment(s), clarification(s), circular(s) etc. issued by the relevant authorities including SEBI, not being consistent with the provisions laid down under this Policy, then such amendment(s), clarification(s), circular(s) etc. shall prevail upon the provisions hereunder and this Policy shall stand amended accordingly from the effective date as laid down under such amendment(s), clarification(s), circular(s) etc.