LMW LIMITED

(formerly known as Lakshmi Machine Works Limited)

RISK MANAGEMENT POLICY

Table of Contents

1. BACKGROUND AND OBJECTIVES

1.1 Preamble

This Risk Management Policy (the “Policy” or “RM Policy”) intends to enable LMW Limited (formerly known as Lakshmi Machine Works Limited) to adopt a well-defined framework to pro-actively manage pertinent enterprise-wide risks to enable sustainable business growth and achievement of objectives.

The Policy lays out the governance structure and the process to identify, assess, respond, monitor and report on key risks actively and effectively. The Policy complements and does not replace any other existing control, compliance and governance programs.

1.2 Legal Framework

This policy is in compliance with the provisions of Section 134(3)(n) of the Companies Act, 2013 and amendments thereof, which requires that the Board annually reports to the shareholders on the development and implementation of Risk Management Policy, including identification of elements of any risk which may threaten the existence of the Company.

Further, in compliance with the SEBI (Listing Obligations & Disclosure Requirements) Regulations, 2015 and amendments thereof, this policy defines the roles and responsibilities of the Risk Management Committee.

1.3 Objectives

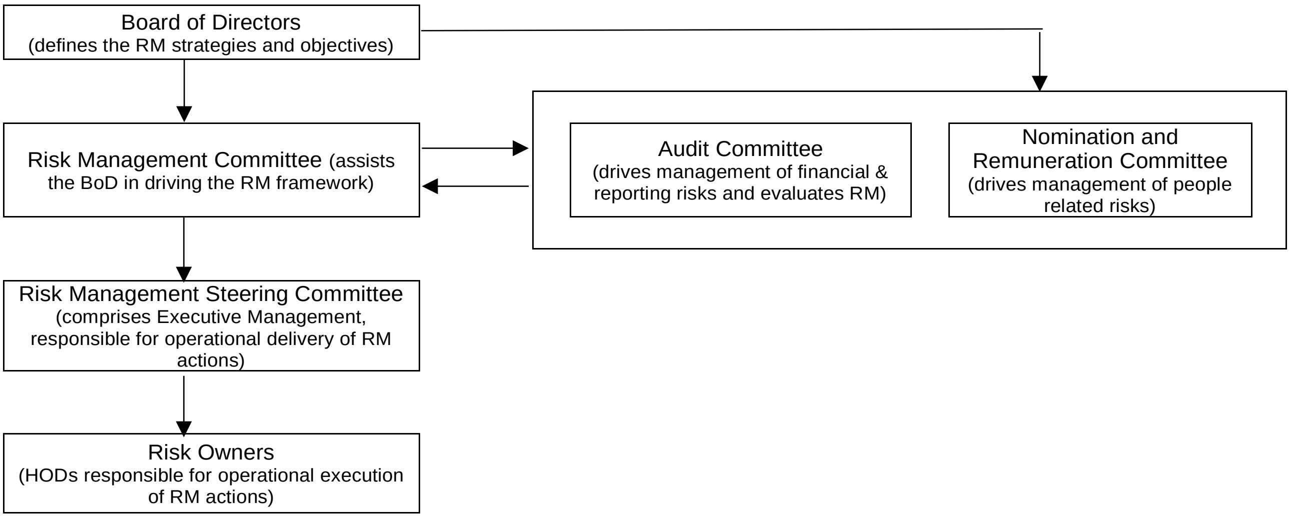
The Risk Management Policy / framework is designed to enable high standards of governance, business conduct and risk management and to achieve the following objectives:

- To enable informed decision making, adequately factoring risks involved
- To promote risk-aware culture
- To safeguard Company’s assets and Stakeholders’ interests
- To aid in achievement of sustainable business growth with financial stability
- To identify, assess and manage current and future material risk exposures
- To establish adequate systems for risk management
- To aid in planning for business continuity
- To enable compliance with appropriate legal and regulatory requirements, wherever applicable

2. RISK MANAGEMENT GOVERNANCE STRUCTURE

To ensure high levels of governance and culture, it is important that the risk management framework is driven by exercising adequate Board oversight, establishing operating structures and defining desired culture. The Company’s RM framework shall be driven by a 4-tier structure comprising the:

- Board of Directors (BoD)
- Risk Management Committee, along with Audit Committee (AC) and Nomination & Remuneration Committee (NRC)
- Risk Management Steering Committee (RMSC)
- Risk Owners



2.1 Board of Directors (BOD)

The BoD defines the RM strategies & objectives, oversees the development, implementation & operation of the RM Policy / framework and sets the culture for effective risk management.

- The BoD is assisted by the RMC to drive the RM Policy / framework. The BoD has defined the role and responsibilities of the RMC in the form of an RMC Charter and may delegate monitoring and reviewing of the RM framework to the RMC (along with any other functions as it deems fit, including cyber security).
- The BoD has approved the RM Policy and shall approve any subsequent changes thereof, based on recommendations of the RMC.
- The BoD shall be kept informed by the RMC of the nature and content of the RMC discussions, recommendations and required actions (including status) for key risks. This shall include annual presentations on RM by the RMC, with inputs and support of AC and NRC on management of financial / reporting and people-related risks respectively.
- The BoD shall include a statement in its report to the shareholders on development and implementation of RM Policy, including identification of elements of any risk, which may threaten the existence of the Company.

2.2 Risk Management Committee (RMC)

The RMC was formed by the BoD to assist in developing the RM Policy, guiding implementation, monitoring, and reviewing the effectiveness of RM Policy and practices. The RMC shall guide and oversee the RM process to identify, assess, manage and monitor key enterprise-wide risks, with inputs from AC & NRC and support from RMSC.

Composition of the RMC

The Composition of the RMC shall be in compliance with Regulation 21 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, as amended from time to time.

Meetings of the RMC

- The Risk Management Committee shall meet at least twice in a Financial Year. Also, the meetings of the Risk Management Committee shall be conducted in such a manner that on a continuous basis not more than two hundred and ten days shall elapse between any two consecutive meetings.
- Quorum required for such RMC meetings shall be the higher of two members (or) 1/3rd of RMC members, including at least one member of the Board of Directors in attendance. Participation of the members through video conferencing or other audio-visual means shall be deemed to be adequate for considering quorum.
- Formal decisions shall be made by a simple majority. In case of equality of votes, the Chairperson of the meeting shall have a casting vote.
- The Company Secretary shall act as the Secretary to the RMC for the purpose of convening RMC meeting (in conjunction with RMC Chairperson), circulating the agenda & papers and recording & circulating the meeting minutes.
- RMC may invite any Director, KMP, employee or external experts / professionals to the RMC meetings, as required.
- Agenda of the RMC meetings may include:
  - review of the Company's RM Policy / framework
  - presentations, if any, by RMSC, relevant risk owners or external consultants on identified / prioritized risks, response plans and monitoring mechanisms
  - compilation of key information / recommendations to be presented to the Board (for direction / action) or the Audit Committee (for evaluation of RM system)
  - presentations by domain / sectoral experts on topics relevant to RM
  - any other topics related to RM

Roles and Responsibilities of RMC

- Formulate a detailed RM Policy which shall include:
  - Framework for identification of internal and external risks specifically faced by the Company, including financial, operational, sectoral, environmental, sustainability, governance, information & cyber security risks and any other risk as may be determined by the RMC.
  - Measures for risk mitigation including systems / processes for internal control of identified risks.
  - Business continuity plan.
  - Any other points that the RMC may find relevant to be included in the Policy
- Monitor and oversee implementation of the RM Policy, including evaluating adequacy of RM systems and functioning of the ERM framework. This evaluation shall be done at least once in a year considering the risk portfolio.
- Periodically review the RM Policy (at least once in two years), considering the changing industry dynamics and evolving business complexity.
- Ensure that appropriate methodology, processes and systems for risk management are in place to monitor and evaluate risks associated with the business of the Company, including implementing and overseeing an appropriate Enterprise Risk Management (ERM) Framework.
- Monitor the identified, prioritized and emerging strategic risks across the organization and ensure that they are refreshed at defined intervals.
- Ensure that the Company's risk appetite for the purpose of risk assessment and monitoring is appropriately defined.

- Participate in major decisions affecting the organization's risk profile and periodically oversee development, implementation and operation of risk responses and provide directions to the RMSC.
- Review Key Risk Indicators (KRI) dashboards and other performance metrics against prioritized risks.
- Ensure adequacy and effectiveness of Business Continuity Plan and Cyber Security framework.
- Review the adequacy of the Company's resources to perform its RM responsibilities and achieves its objectives.
- Keep the BoD informed about the nature and content of its discussions, recommendations and actions to be taken.
- Ensure risk management is integrated into Board Reporting and Annual Reporting mechanism.
- Appointment, removal and terms of remuneration of the Chief Risk Officer (CRO), if any.
- Coordination of activities with Audit Committee and Nomination & Remuneration Committee, where necessary.
- Engage the services of consultants and other external service providers / subject matter experts and require the attendance of any executives in connection with the RMC's role and shall be entitled to interact with the internal auditors wherever it deems fit and shall also require them to make any presentations thereon.
- Periodically review and recommend the expansion of any power or role of the RMC to effectively perform its role.

2.3 Audit Committee (AC) and Nomination and Remuneration Committee (NRC)

- Audit Committee shall be responsible for periodic evaluation of the RM systems and provide insights / recommendations to the RMC. In addition, the AC would oversee management of the financial and reporting risks faced by the Company, relying on the Internal Financial Controls (IFC) and Internal Audit mechanisms in place.
- Nomination & Remuneration Committee shall oversee management of the people-related risks relevant to the Company and provide insights / recommendations to the RMC.

2.4 Risk Management Steering Committee (RMSC)

- Risk Management Steering Committee shall comprise the BU Heads / Presidents, Chief Financial Officer (CFO) and Company Secretary (CS).
- Chairperson of RMSC shall be designated by the Chairman of the Board and such individual shall be an Executive Director or be part of the top management of the Company.
- Under the direction of the RMC, RMSC shall be responsible for operationalizing the RM Policy and framework including:
  - Developing, implementing and operating an effective Enterprise-wide Risk Management (ERM) framework to identify, assess, manage and monitor risks across risk categories.
  - Directing, and overseeing the execution of RM actions by the risk owners / HODs.
  - Keeping the RMC informed of the identified and prioritized risks, risk management actions and results of the risk monitoring mechanisms.

- RMSC shall meet at least twice in a Financial Year, to review the risk monitoring results / dashboards, if any, emerging risks and status of risk response plans and provide directions to the risk owners / HODs. They shall also review the presentations, if any, intended for the upcoming RMC meetings.
- Risk owners / HODs (including one-downs) and any external professional / consultant shall be invited as needed.

2.5 Risk Owners

- Heads of Departments (HODs) shall participate in the enterprise-wide risk identification and assessment exercise. HODs shall be designated as risk owners for the identified / prioritized risks.
- Risk owners shall be responsible for developing, implementing and operating risk response plans against identified / prioritized risks relevant to them. Risk owners shall provide updates on risk response plans and monitor their performance against identified risks (through KRI dashboards, if any) with the RMSC.

2.6 Risk Awareness and Culture

- Since risk is an integral part of every business activity, the Company aims to embed risk management in its business strategy and operations by promoting risk culture and awareness across the organizations.
- The Company has devised and implemented several risk management programs / measures including Enterprise-wide Risk Management (ERM), Internal Financial Controls (IFC), Internal Audit, Code of Conduct, Whistle Blower Policy and various operational / quality policies.
- Periodic awareness sessions and communications / mailers on risk management, domain and sectoral topics shall be organized for the members of the BoD, the Committees, Executive Management and HODs.
- Periodic awareness communications / mailers on relevant risk management, domain and sectoral topics shall be organized for the wider organization.

3. Risk Management Process

Risk management is a process, effected by an entity's Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. The Board of Directors are responsible for overall risk management of the Company, supported by the Risk Management Committee.

The Company has established an Enterprise-wide Risk Management (ERM) framework to identify key risks across categories / functions, assess the criticality of identified risks to prioritize top risks, mitigate / manage the prioritized risks and monitoring the existing & emerging risks.

3.1 Risk Identification

- Risk identification shall be carried out across all business verticals / locations of the Company and covering all key risk areas and categories.

- Risk identification shall be performed through internal ideation (such as workshops, brainstorming sessions and inputs from operational reviews), research, inputs from external domain / sectoral experts and any loss event.
- HODs / risk owners shall have the primary responsibility to identify pertinent risks for the Company, with directions / inputs from the RMSC.
- Risk register (in a pre-defined format) shall be used to compile the identified risks across functions / areas. The risk register shall be reviewed, updated and refreshed periodically.
- Key risk areas / business functions for coverage shall include Business Planning / Strategy, Marketing & Sales, Spares & Services, Quality, R&D, Engineering, Manufacturing, Energy & Safety, Supply Chain Management, Finance, Information Technology, Human Resources & Industrial Relations, Projects, General Administration, Legal & Compliance and Secretarial.
- Key categories of risks for coverage shall include Strategic / Business, Operational, Financial & Reporting, Sectoral, Sustainability (Environmental, Social & Governance / ESG), Technology, Cyber security, Regulatory and Third-party.

3.2 Risk Assessment

- Criticality of the risks identified across the organization shall be assessed and top / prioritized risks shall be identified based on the risk ratings. This would enable focused approach to risk mitigation / management and monitoring at Management and Committee / Board levels. Such risk assessment should be done periodically to review the relevance of the top / prioritized risks.
- Criticality shall be assessed based on two parameters - Likelihood (probability of risk event occurring) and Impact (consequence of risk occurrence). Based on the Company’s risk appetite, risk assessment guidelines shall be developed for both parameters for assessment under the scales below:

Scale	Likelihood
5	Almost Certain
4	Probable
3	Possible
2	Remote
1	Improbable

Scale	Impact
5	Severe
4	Major
3	Moderate
2	Minor
1	Negligible

- The HODs shall have the primarily responsibility to assess the identified risks, with directions / inputs from the RMSC. Using risk assessment form and referring to risk assessment guidelines, the HODs and RMSC shall assess each identified risk on the two parameters.
- Criticality score for each risk for each respondent shall be the product of the Likelihood Score and the Impact Score.
- The risk assessment template (in a pre-defined format) shall be used to compile the criticality responses for each identified risk from various respondents.
- The risk assessment template (in a pre-defined format) shall be used to statistically compute the weighted average criticality scores for each identified risk, assigning 40% weightage to designated risk owners (HODs responsible for the concerned risk area), 40% weightage to designated risk customers (HODs responsible for the functions impacted by the risk) and 20% weightage to other respondents. Based on such weighted average criticality score, the risks are classified into three zones as per the below heat map:

- Risks with score of 15 & above shall be in the 'red' zone, are considered to have "high" criticality and require active monitoring of risk response and resultant impact. These shall be reviewed by RMSC at least twice in a Financial Year and by RMC as and when they meet.
- Risks with score between 8 & 12 shall be in the 'yellow' zone, are considered to have "medium" criticality and need periodic monitoring of risk response. These shall be reviewed by RMSC twice in a Financial Year and by RMC on annual basis.
- Risks with score below 8 shall be in the 'green' zone, are considered to have "low" criticality and may need annual review of risk response by RMSC.

Risk Assessment Zone

Likelihood \ Impact	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

High
Needs active monitoring

Medium
Needs bi-annual review

Low
Needs annual monitoring

Criticality = Likelihood x Impact

- ➢ The risk registers (in a pre-defined format) shall be updated with the weighted average criticality scores, rankings and zone.
- ➢ RMC shall direct and review the risk assessment approach and outcomes periodically.
- ➢ Risk assessment exercise shall be refreshed once in two years to re-visit the prioritized risks.

3.3 Risk Response

- ➢ For the prioritized risks in 'red' zone, root cause analysis shall be performed, existing risk responses shall be evaluated (including process and status) and additional / alternate risk responses shall be identified, by the designated risk owners / HODs considering the Company's risk response strategy and with the directions / inputs from RMSC.
- ➢ The Company may adopt any of the following strategies to respond to a prioritized risk:
  - Risk Acceptance / Retention - Accept and tolerate the risk.
  - Risk Exploitation - Take measures to ensure that the opportunity will be realized.
  - Risk Avoidance / Termination - Take measures which would result in elimination of the risk.
  - Risk Reduction / Mitigation - Take measures which would result in reduction of likelihood or impact of the risk event.
  - Risk Transfer - Transfer some aspects of the risk to a third-party.
- ➢ Risk response plan (in a pre-defined format) shall be prepared for each prioritized risk, including the existing measures, additional / alternate measures, responsibility, timelines and status. In addition, Key Risk Indicators (KRIs) / performance metrics shall be defined for each prioritized risk, including the relationship with the identified risk, tolerance levels (guided by the Company's risk appetite), source of information, format, timing, frequency and responsibility.

- RMC shall direct and review the risk response strategies and plans periodically.

3.4 Risk Monitoring and Reporting

- **Monitoring of Status of Risk Responses:** Status of identified mitigation responses for prioritized risks shall be presented by the risk owners to the RMSC atleast twice in a Financial Year and by the RMSC to RMC as and when the Committee meets. During such reviews, adequacy of the risk responses and need for additional / alternate response plans shall be also assessed.
- **Monitoring of Key Risk Indicators (KRI)**
  - Data for each KRI shall be compiled and dashboards / reports of performance shall be prepared as per defined frequency by risk owners. Based on performance against defined targets / tolerance levels, the status of KRIs shall be marked as 'Green', 'Yellow' or 'Red' for attention / action.
  - Risk owners shall present the KRI dashboards to the RMSC atleast twice in a Financial Year. Remediation / response plans shall be identified and implemented by the risk owners, with the direction / input from RMSC.
  - RMSC and RMC shall present the KRI dashboards (along with remediation / response plans) to the RMC and the Board respectively.
- **Identification of emerging Risks:**
  - Beyond the risks identified through the ERM exercise, it is important to monitor the changing eco-system to identify emerging risks relevant to the Company.
  - Such emerging risks may be identified by Directors, Executive Management, HODs, employees, customers, vendors, external consultants / experts and any other components in the ecosystem.
  - Under the direction of the RMC, the RMSC shall implement a mechanism / process to receive and compile inputs on emerging risks from various sources on an ongoing basis.
  - The RMSC shall monitor and assess potential emerging risks being received and highlight the relevant emerging risks to the concerned risk owners / HODs and in turn to the RMSC for assessment. After such assessment by HODs and RMSC, pertinent emerging risks shall be presented to the RMC along with proposed response plans.
  - The HODs shall include the relevant risks in the risk register.
- **Review by RMSC:** As explained above in Section 2.4, RMSC shall meet atleast twice in Financial Year to review the risk monitoring results / dashboards, emerging risks and status of risk response plans and provide directions to the risk owners / HODs.
- **Review by RMC:** As explained above in Section 2.2, RMC shall meet to review the risk monitoring results / dashboards, emerging risks and status of risk response plans and provide directions to RMSC.
- **Annual Review by Board:** RMC shall report to the Board on annual and need basis on the prioritized risks, related response plans and their KRIs (along with its recommendations for actions), to also aid the Board to include a statement in its report to the shareholders on development and implementation of risk management.
- **Evaluation by AC:** Audit Committee shall periodically evaluate the adequacy and effectiveness of the risk management framework in place, through review of risk management reports and actions.

- **Integration with Internal Audit:**
  - RMC may provide recommendations to the Audit Committee for coverage of certain risk areas / prioritized risks as part of the Internal Audit plan. RMC may also interact with the internal auditors wherever it deems fit and require them to make any presentations thereon.
  - Audit Committee may also mandate internal auditors to perform a review of adequacy and / or effectiveness of the risk management framework, to aid the AC's evaluation of the RM framework.

4. BUSINESS CONTINUITY PLANNING

- Business Continuity Plans (BCP) and Disaster Recovery (DR) are designed, implemented and operated to enable to the organization to have a rapid response to address the consequence of high impact and high velocity risks, with respect to information technology.
- Documented BCP and DR framework shall be reviewed by the RMC and approved by the Board, including any amendments thereof.
- Reports on operation of BCP and DR framework, including periodic mock drills and testing, shall be presented by the RMSC to the RMC on annual basis.

5. AMENDMENTS TO THE POLICY

The Risk Management Policy may be amended to remove ambiguities, enhance clarity or comply with applicable regulations. Any changes to the Risk Management Policy should be reviewed and approved by the RMC and the Board of Directors.

In case of any amendment, clarification, circular, notification etc. issued by a competent authority, which is not consistent with the provisions laid down under this Policy, the provisions of such amendment, clarification, circular, notification, etc. shall prevail and this policy shall stand amended accordingly, without any further action, on and from the date on which such amendment, clarification, circular, notification comes into effect.

Policy amended as on 24.01.2025