Mahindra CIE Automotive Limited

Risk Control and Management Policy

Name of the Document	Risk Control and Management Policy
Effective date	21st July, 2021
Approving Authority	Board of Directors
Date of last amendment/ review	21st July, 2021
Current Version	01
Version History	**Please see Annexure**

Contents

RISK MANAGEMENT AND CONTROL POLICY

1. Purpose

The purpose of this document is to define the Risk Management and Control Policy of Mahindra CIE Automotive Limited to establish the general framework for action, as well as the procedures and responsibilities to control and manage the risks that Mahindra CIE Automotive Limited (MCIE / the Company) must face efficiently and effectively.

This Policy is in compliance with SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 and provisions of the Companies Act, 2013 read with applicable rules, including any amendments or statutory re-enactments thereof as may be applicable from time to time which requires the Company to lay down framework for identification of internal and external risks with measures for risk mitigation including systems and processes for internal control of identified risks and a business continuity plan in view of identified risks.

The risk management system of the Company ("RMS") allows it to reasonably ensure that all significant risks, both financial and non-financial risks, are prevented, identified, assessed, subjected to ongoing control and reduced to the defined levels of risk appetite and tolerance and are approved by the risk management committee and ultimately by the Board. MCIE defines the following risk categories: strategic, operational, financial, sectoral, compliance, sustainability (particularly, ESG related risks), information and cyber security.

With a strong and sustained commitment of senior management and the management team, as well as rigorous strategic planning, the Company aims to achieve an environment where it is capable of working with risks in a controlled manner, managing them actively and thereby, take advantage of new opportunities.

The principles on which it is based are fundamentally:

- ✓ To promote a constructive vision of the concept of risk.
- ✓ Commitment and competence of participants.
- ✓ To use a common language.
- ✓ Transparent communication throughout the organization.

MCIE employees with RMS-related responsibilities will have the material and human resources necessary to perform their functions. Through this Policy, MCIE defines the guidelines to follow to identify and maintain the risks within the tolerance limits approved at any given time by the Board.

The procedures developed by this Policy must be consistent with the principles and guidelines established here that are aimed at:

- ✓ Contributing to achieving the strategic objectives of the Company.
- ✓ Introducing maximum guarantees in relation to the protection of corporate interests and therefore, all shareholders and other stakeholders.
- ✓ Protecting the reputation of MCIE.
- ✓ Safeguarding the business stability and financial solidity of MCIE in a sustainable manner.
- ✓ Contributing to complying with the regulations.
- ✓ Facilitating the performance of transactions under the conditions of security and quality undertaken.

In accordance with the foregoing, this Policy is based on the following basic principles:

- ✓ Promoting an approach to risk management that ranges from defining the strategy and risk appetite to incorporating the aforementioned variables into operational decisions.

- ✓ segregating and assigning responsibilities to the risk-taking areas and those in charge of its analysis, control and supervision, as well as seeking to guarantee the use of the most effective instruments to hedge risks.

- ✓ Reporting transparently on the risks of the Company and the functioning of the control systems through the approved channels of communication.

- ✓ Ensuring compliance with the corporate governance rules and ensuring that the aforementioned rules are updated in accordance with international best practices in relation to the matter, acting at all times in accordance with the Company's corporate governance regulations.

2. Scope of application

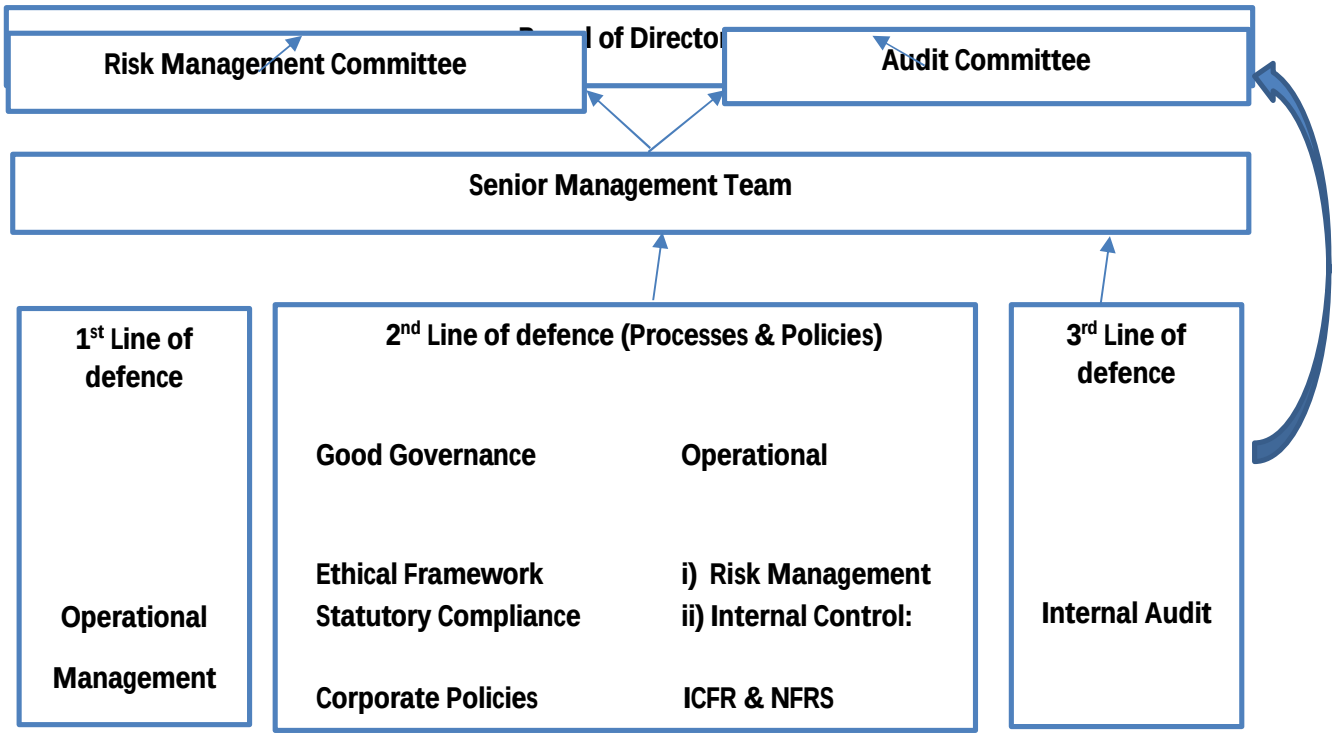
This policy provides a framework for identification of internal and external risks and measures for risk mitigation including systems and processes for internal control of identified risks. Framework is applicable to all of its operations, covering all the risks regarding financial and non-financial reporting that affect or may affect MCIE, whether they arise from its environment or from its activities.

3. Responsibilities

MCIE Board members, the Risk Management Committee, Senior Management team and all employees are responsible for implementing this policy within their scope of management and to coordinate their responses to the risks with the other managers and departments affected, wherever applicable.

The various roles involved in the RMS may be grouped into three lines of defense against the risks that threaten fulfilment of the strategic, operational, financial, ESG objectives.

As shown in the accompanying chart, in RMS the three lines of defense are supervised by the Board:



ICFR: Internal Control over Financial Reporting
NFRS: Non-Financial Reporting Statement

GDPR: General Data Protection Regulation
ESG: Environment, Social & Governance

In this context, the roles and responsibilities of each member of the organization involved in the RMS arethe following:

Body	Responsibilities
Board of Directors	✓ The Board of Directors is ultimately responsible for the existence and operation of the RMS including framing, implementing and monitoring the risk management plan. ✓ Monitoring and reviewing of the RMS through the activities carried out by the Audit Committee and the Risk Management Committee.
Audit Committee	✓ Evaluation of the RMS of MCIE. ✓ Informing the Board of the results of the assessments carried out and the schedule assigned to the measures proposed for the weaknesses detected.
Risk Management Committee	✓ Formulating a detailed risk management policy and periodically reviewing the same. ✓ Designing and monitoring the implementation of the RMS and periodically evaluating the adequacy of RMS. ✓ Defining the methodology, procedures and criteria for identifying, assessing, classifying, approving and responding to risks. ✓ Reviewing and approving the Risk Map. ✓ Reviewing and approving the plans and actions proposed that maybe considered necessary to handle the risks identified. ✓ Monitor and evaluate the implementation of action plan. ✓ Defining, establishing and/or modifying the risk appetite that will be shared with theBoard for its approval. ✓ Periodically reporting to the Audit Committee regarding general operations of RMS. ✓ Periodically reporting to the Board regarding the evolution of the risks, action plan as well as the general operation of the RMS.
Senior Management and Management Team	✓ Responsible for implementation and operation of the RMS. ✓ Implementing and spreading a culture focused on risk at the Company. ✓ Identifying, assessing, classifying and responding to risks. ✓ Responsible for preparing the Risk Map and presenting the same to the Risk Management Committee. ✓ Preparing the action plans, placing the same before Risk Management Committee for approval and ensuring implementation of the same. ✓ Periodically reporting to the Risk Management Committee regarding the evolution of the risks and the action plan. ✓ Assessing the efficacy of the RMS and periodically reporting to the Audit Committee and Risk Management Committee the weaknesses detected and the schedule established for implementing measures to correct them.
Employees	✓ Responsible for identifying risks that threaten fulfilment of objectives and communicating them to the head of department. ✓ Collaborating with the head of department in the assessment and classification of the risk, aswell as proposing action plans to address the risks identified and collaborate on the execution thereof.

RMS segregation of duties matrix:

	Board of Directors	Audit Committee	Risk Management Committee	Senior Management and Management Team	Internal Audit	Employees
Identification of risks			X	X		X
Risk assessment			X	X		
Risk management				X		
Risk monitoring	X		X		X	
Update			X	X		
Breaches				X	X	X
Evaluation of RMS	X	X	X			

4.1. Description of the process

The Company defines risk as any event, caused either by internal or external factors, that hinders or impedes the achievement of its strategic and operational objectives.

The RMS adopted by the Company is comprehensive and takes into account all the significant risks of any nature to which it may be exposed and in particular, those that may affect fulfilment of the Business Plan or effects continuity of business.

4.2. Identification of risks

The risk identification process consists of searching for events (associated with internal and external factors) that may affect the objectives of MCIE including the Strategic Plan, Annual Budget as well as Sustainability. This involves providing an overview of each material risk, making an assessment of the risk level and preparing action plans to address and manage the risk.

It is important to understand the external factors to ensure that stakeholders' objectives and concerns are taken into account. The external context may include, but is not limited to:

a) The social, cultural, political, legal, financial, technological, economic, natural and competitiveenvironment at the international, national, regional or local level.
b) The factors and trends that have an impact on the organization's objectives.
c) Stakeholder relations.

Internal factors are those on which the organization may have an influence and, consequently, manage the risk. The risk management process must be

consistent with the culture, processes, structure and strategy of the organization.

The risk categories defined are the following:

- **Strategic:** risks that affect the high-level objectives directly related to the Strategic Plan.
- **Operational**: risks that affect the objectives related to the effective and efficient use of resources.
- **Financial**: risks that affect the financial objectives and resources, including compliance on reporting.
- **Compliance**: risk of management or employees breaching external and internal regulations or applicable laws.
- **Sustainability**: risks that affect environmental, social, health, safety, ethical and corporate governance matters.
- **Cyber security**: risks that affects the data privacy, data security and the security of the IT infrastructure of the Company.

4.3. Risk assessment

With the goal of defining homogeneous criteria for assessing risks, assessment scales have been defined: probability of occurrence and impact, where the impact is measured in three categories: economic, organizational and reputational. These scales serve to locate each risk and the Risk Map, the main tool for assessing risks.

When assessing risk, the speed of occurrence is also considered. This is defined as the time that elapses from the materialization of the risk until it directly or indirectly affects the objectives of MCIE.

In addition to defining the assessment scales for each risk, the following aspects will be defined:

a) Source of the risk.
b) Identification of the areas of impact of the risk, i.e., define, in the event of occurrence, in whatway it would affect the Company.
c) Identification of the parties responsible for managing risks.

The risk assessment process is the responsibility of senior management and the management team who will have to assess the risks identified in the periods established.

Once the assessments are obtained, they will be consolidated to obtain the Risk Map. The consolidation of the risks will take into account the specific weight of the assessments of each one of the parties responsible and of each geographic

area for each type of risk so that it provides a vision of MCIE and enables them to be prioritized and enhance the risk profiling.

4.4. Risk management

Once the risks have been identified, assessed and consolidated, the action plans to reach the risklevel accepted by the organization must be determined.

The actions or responses to the risk that the organization may adopt are the following:

- ✓ **Mitigation:** actions aimed at reducing the impact or the probability of occurrence of the risk to a level acceptable to the organization by determining suitable risk treatment strategy.
- ✓ **Acceptance:** no actions taken in relation to the risk in question. The consequences of the risk and their probability of occurrence are accepted.
- ✓ **Sharing:** actions aimed at sharing a portion of the risk with third parties, for example, througharranging insurance, outsourcing processes, etc.
- ✓ **Avoidance:** suspending the activity that gives rise to the risk so that it ceases to exist.

For each one of the risks identified, in particular for the critical risks, the manager of the risk will periodically monitor them and analyze their possible materialization through appropriate quantitative or qualitative indicators. If an indicator exceeds the established tolerance, the risk manager will be in charge of identifying the causes and proposing an action plan or response.

The senior management is responsible for the process of reviewing the responses to the risks and afterwards it will present it to the Risk Management and Audit Committee.

4.5. Risk monitoring

To ensure that the responses to the risks agreed are viable and efficient, the senior management will perform an assessment each year with the following objectives:

- ✓ To ensure that the risks are being managed in the manner approved by senior management and the management team.
- ✓ To evaluate whether the agreed-upon responses are efficient and to implement action plans if necessary.
- ✓ To determine whether the risk catalogue anticipates and reflects changes in the business circumstances and new economic conditions.
- ✓ Additionally, the senior management must identify whether any risk has materialized and wherever applicable, the measures implemented to

mitigate it.

The following reporting levels will exist to facilitate risk monitoring:

a) **Internal reporting:** The Risk Map Report, which will include the Risk Map and the risk catalogue of MCIE, and a graphic representation of the main risks by geographic area and type of risk, including the high-level control activities implemented for the top risks, as well as the action plans established to mitigate them.

b) **External reporting:** This is comprised of the information on risk management to be included inthe Non-Financial Information Statement and in the Annual Report, in which the main risks to which MCIE is exposed and theactions established in relation to the main risks identified are detailed.

4.6. Business Continuity

Each manufacturing unit of the Company has a disaster management plan which inter alia ensures compliance with applicable laws and aims to protect the assets and people of the Company and ensures continuity of its key business processes after a disaster i.e. an unexpected business interruption caused by natural or man-made events.

4.7. Updating and monitoring

The business risks change over time and, therefore, give rise to changes in the RMS. In the connection, risks that were critical may lose relevance, while others may gain importance.

To maintain an effective and up-to-date RMS, the risk management committee updates the Risk Map annually following the process described above.

4.8. Breach

Any employee that has evidence or suspects irregular behavior or behavior that could lead to the materialization of a risk must immediately inform MCIE through the whistle-blowing channel available on the corporate website.

Version History

Version	Date of amendment/review	Change & Reason for change, if any
Version 1	21st July, 2021	In accordance with the requirement of the Companies Act, 2013 and SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, the Company has reviewed its Risk management framework and have formulated this Policy in accordance with the amendments made in the Listing Regulations.