ASAL

AUTOMOTIVE STAMPINGS AND ASSEMBLIES LIMITED

RISK MANAGEMENT POLICY

INTRODUCTION:

Automotive Stampings and Assemblies Limited (the Company) is exposed to inherent uncertainties owing to the sectors in which it operates. A key factor for a Company's capacity to create sustainable value is the risks that the Company is willing to take (at strategic and operational levels) and its ability to manage them effectively. This Risk Management Policy aims to detail the objectives and principles of Enterprise Risk Management at Automotive Stampings and Assemblies Limited along with an overview of the process and related roles and responsibilities. The policy is a formal acknowledgement of the commitment of the Company to Enterprise Risk Management (ERM).

The Risk Management Policy provides the Framework/ Structure under which Risks shall be Identified, Prioritized, Rated, Mitigated and Reported to the Board.

COMPANY'S POLICY STATEMENT:

The Company is committed to adopt a proactive approach to risk management which is based on the following underlying principles:

- The Company endeavors to create a culture of informed decision-making at all levels of the organization.
- The Company strives to anticipate and take preventive action to manage or mitigate risks and deal with the residual risk.
- The Company will develop, implement, review and monitor a uniform risk management policy, framework and plan across all business units, functions and locations.
- The Company will develop and deploy relevant capability building measures for concerned employees and relevant stakeholders to ensure effective risk management.
- All employees of the Company take responsibility for the effective management of risks in all aspects of the business.

RISK MANAGEMENT FRAMEWORK, GUIDELINES AND PRINCIPLES:

The Risk Management Framework is in line with Tata AutoComp Group's framework laying down the Systems and Procedures to be followed to Identify, Prioritize and Control the Risks within Risk Appetite and best practices with the focus to keep the process relevant to the dynamic business environment and keep it pragmatic and simple from an implementation perspective.

The process may be reviewed periodically along with the business planning exercise or at any point of time on account of significant changes in internal business conduct or external business environment.

ERM GOVERNANCE FRAMEWORK:

The risk management process is supported by the Risk Management Governance Structure as summarized below:

A. The Board of Directors shall exercise an overview of risk management functions performed by the Management. The Board shall delegate the responsibility of monitoring, reviewing and deploying Risk Management Plan to the Risk Management Committee. The Board may periodically review the performance of the Risk Management Committee. The Board shall be responsible to define the risk appetite of the Company.

B. The Committee shall review the Risk Management Practices and actions deployed by the Management in respect of identification, assessment, monitoring, mitigation, and reporting of key risks to the achievement of business objectives. The Committee shall be entrusted with the following roles:

- To formulate, review and amend the Risk Management Policy;
- 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 shall also be subject to review by the Risk Management Committee.

C. The Risk Management Committee shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, under the guidance of Board of Directors.

D. 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 and in case of a listed entity having outstanding SR equity shares, at least two thirds of the Risk Management Committee shall comprise independent directors.

E. The Chairperson of the Risk management committee shall be a member of the board of directors and senior executives of the listed entity may be members of the committee.

F. The Risk Management Committee shall meet at least twice in a year.

G. The quorum for a meeting of the Risk Management 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.

H. The meetings of the Risk Management Committee shall be conducted in such a manner that on a continuous basis not more than one hundred and eighty (180) days shall elapse between any two consecutive meetings.

I. The board of directors shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit

J. The Risk Management Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

ALIGNMENT OF RISK AND AUDIT COMMITTEE OVERSIGHT:

The Audit Committee oversees the financial reporting process of the Company and the Risk Management Committee (the "Committee") overseas the governance of risk through formal processes. In doing so, the Committee considers the risk policy and plan, determines the Company's risk appetite and risk tolerance, ensure that risk assessments are performed at regular intervals, and ensures that the Company has and maintains an effective on-going risk assessment process, consisting of risk identification, risk quantification and risk evaluation.

To align the functions of both the Committees and to drive efficiency and effectiveness in the overall Enterprise Risk Management Framework, there would be adequate and optimum composition and overlapping in membership of the Audit Committee and the Risk Management Committee, as deemed appropriate by the Board to ensure seamless integration among both Committees.

RISK ASSESSMENT PROCESS

The objective of risk assessment is to systematically evaluate identified risks to determine their likelihood, impact, and priority for treatment.

Step 1: Risk Identification

Risks shall be identified across all organisational functions, projects, and activities. Identification will be carried out using a combination of methods, including but not limited to Audit Findings, Customer inputs, Gemba walks, Operations data, Cross Functional Risk Workshops, Change management etc.

Step 2: Determine Likelihood and Impact

Each risk will be assessed using the organisation's approved Risk Matrix, which defines:

- Likelihood: the probability that the risk will occur.
- Impact: the severity of the consequences if the risk occurs.

Step 3: Calculate Risk Score
Risk Score = Likelihood × Impact

The risk score determines the risk's priority level (Low, Medium, High, or Critical).

Step 4: Evaluate Control Effectiveness

Existing risk controls shall be assessed to determine their adequacy and effectiveness. This evaluation shall consider:

- Design effectiveness of controls
- Operating effectiveness and consistency of application
- Coverage of the identified risk scenarios

Based on this assessment, the residual risk (risk remaining after considering existing controls) shall be determined and documented. Where residual risk exceeds the Organisation's defined risk appetite or tolerance levels, further risk treatment actions shall be required.

RISK REGISTER

The Company to maintain a Risk Register. The Risk Register to provide a structured and centralized repository for identifying, categorizing, assessing, monitoring, and reporting key risks that may affect the organization's objectives, operations, assets or stakeholders.

IMPLEMENTATION OF RISK MANAGEMENT PLAN:

i. Management:

Management will be responsible for operationalizing the risk management framework and implementation of the Risk Management Plan as follows:

- The ERM framework for identification of risks shall be implemented by Top management. It shall be ensured that all internal as well as external risks are covered for purpose of such identification including the specific coverage of Geo-political risks, financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security and such other risks as may be determined by the Committee.

- The Risk Identification framework shall mandatorily include area of cyber security.

- The measures taken for risk mitigation including systems and processes for internal control of identified risks shall be taken by the Management which shall be laid for review before the Committee.
- Management will further support the Risk Management Committee by providing necessary inputs on the economy, industry and the Company.

- The business continuity plan:

  - Address threats to the continuity of its business arising out of uncertainties

- Make systematic efforts to minimize their impact on the organization, customers, employees, and other stakeholders
- Create and maintain business impact analysis
- Develop business recovery strategies and plans to mitigate major incident/disruption, to reduce the impact and likelihood
- Make business continuity planning a constituent part of all new business requirements
- Conduct periodic audits and exercises to check, validate and improve the robustness of the Policy and to provide confidence that people are aware of their roles, and the policy meets its objectives.

ii. Division/ Profit Centre/ Common Functional Level Risk Management:

Each Division/Profit centre/ function should strive to support the Management pursue its objectives by providing necessary Division/Profit centre/ function specific inputs.

iii. Chief Risk Officer:

The Company will have Chief Risk Officer (CRO) for overseeing the deployment of the Enterprise Risk Management framework and procedures. The primary role of CRO will be to ensure that the Company achieves its objectives of timely anticipation of risks and opportunities, and a cohesive and consistent response through the active involvement of process owners in reviewing risks, timely meetings, and comprehensive discussions at respective units, effective escalation and regular monitoring of risks. The CRO will lead an ERM team and regularly report to the RMC on the progress of the implementation of ERM and the various risks faced by the Company.

REVIEW OF THE POLICY

This policy will be reviewed and reassessed by the Risk Management Committee as and when required and appropriate recommendations shall be made to the Board to update this policy based on changes that may be brought about due to any regulatory amendments or otherwise.