Enterprise Risk Management - Framework

SONA COMSTAR

Contents

1 Background

2 Approach

- 2.1 Governance and Culture
- 2.2 Strategy and Objective Setting
- 2.3 Risk Performance

3 ERM Improvement

Background

Enterprise Risk Management. ERM is an on-going process, involving the Company's Board of Directors, senior management and other personnel. It is a systematic approach to setting the best course of action to manage uncertainty by identifying, analyzing, measuring, responding to, monitoring and communicating risk issues and events that may have an adverse impact on the Company successfully achieving its business objectives.

Enterprise Risk Management (ERM) enhances financial health, sustenance and growth of a business and creates value for stakeholders. The Board of Directors have approved the ERM policy. The ERM Framework has been developed in order to elaborate upon the risk management philosophy captured in the ERM Policy and defines the mode of capturing, monitoring and mitigating the enterprise risks.

This document outlines the details of the ERM principles, standards, and objectives along with the associated procedures to be followed by all concerned stakeholders. The Enterprise Risk Management framework has been designed and developed in alignment with the regulatory requirements and leading Enterprise Risk Management standards and guidelines – COSO ERM 2017.

o Scope

This framework covers ERM aspects of all Business Units and Plants of Sona BLW Precision Forgings Limited. It includes detailed processes for implementation and adherence with the ERM Policy and is applicable to Board of Directors, Management, employees, contractors, business partners, or individuals directly/indirectly associated with the Company.

Background

o Purpose

The purpose of this framework is to provide visibility, oversight, control and discipline to drive and improve the Company's risk management capabilities in a dynamic business environment.

The fundamental objective of ERM is to ensure that the risks are identified and managed in a prioritized, consistent, effective and efficient manner at all levels within the Company.

In order to realize its ERM objectives, the Company aims to:

- Develop an enterprise-wide integrated risk management framework for implementation and adherence of ERM policy
- Develop guidance on risk identification, assessment and risk response/mitigation plans
- Create a risk register for all identified risks
- Define risk tolerance limits and risk appetite
- Develop a risk monitoring structure to provide visibility of risk management capabilities to the concerned stakeholders
- Set up process to periodically report risk exposures to appropriate risk authorities including management and Board of Directors.
- Enable compliance with appropriate regulations, wherever applicable

o Administration

Any revision(s) to the framework will be incorporated after endorsement by the Executive Board followed by the approval of the Risk Management Committee.

Enterprise Risk Management Approach

The Enterprise Risk Management process adopted by Sona is aligned with internationally recognized "COSO ERM Framework 2017 - Enterprise Risk Management Integrating with Strategy and Performance"

The five components of the COSO ERM Framework as applicable to Sona are described below:

- Governance and Culture;
- Strategy and Objective Setting;
- Risk Performance (Risk Identification, Risk Assessment, Risk Prioritization, Risk Response);
- Risk Review and Revision and
- Information, Communication and Reporting.

Governance and Culture

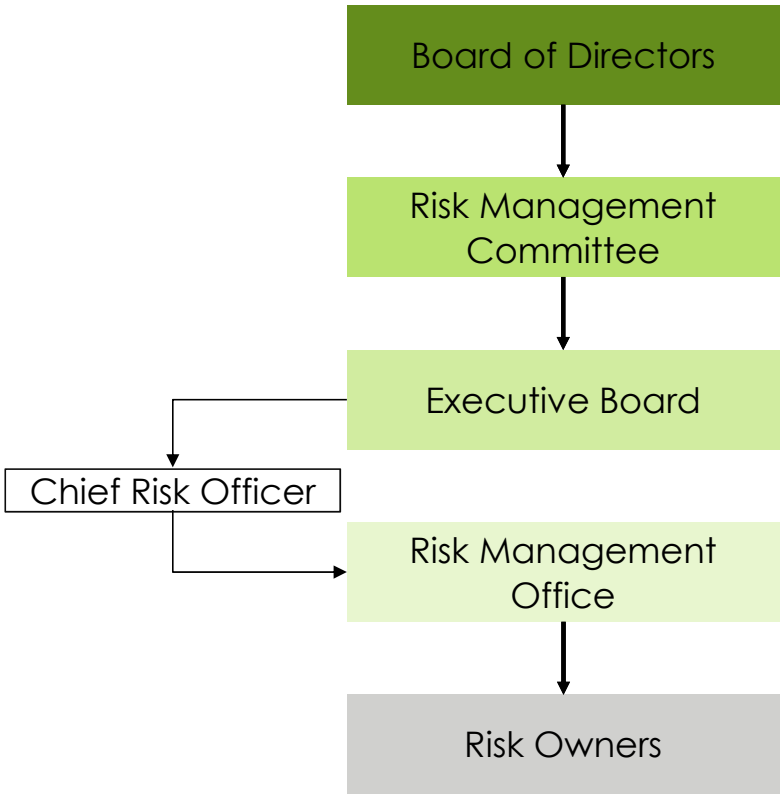
The Company has adopted the "three pillars" ERM Governance Structure. The roles and responsibilities will be:

- **First Pillar (Risk Governance and Oversight):** The Board of Directors plays a critical role in overseeing the deployment of risk management process throughout the Company. They set the tone and culture towards effective risk management by defining risk appetite, business objectives and strategy setting. The Board of Directors, through the Risk Management Committee (RMC) oversees the establishment and implementation of an effective risk management process across the Company. Risk Management Committee reviews the effectiveness of ERM on a semi-annual basis and update the Board of Directors on the same.

- **Second Pillar (Risk Infrastructure and Management):** The Executive Board consisting of the Managing Director, Group Chief Financial Officer, Chief Technology Officer, CEO – Driveline and CEO-Motor drives the ERM framework throughout Sona. In implementing the risk framework in the Company as well as reporting on the status of risk to the Board, the Executive Board is supported in its role by the Risk Management Office led by the Chief Risk Officer.

- **Third Pillar (Risk Ownership):** The third pillar consists of Risk Owners. The Risk Owners are responsible for ongoing identification of risks and development of the respective response plans for their functions. These risks and mitigation plans are captured in a risk register.

Governance and Culture



As updated by RMC

Bi-annual

1st Pillar: Risk Governance and Oversight

- Board of Directors is responsible for Risk Management oversight
- The Risk Management Committee (RMC) is responsible for semi-annual review and will apprise the Board on risk management matters

Quarterly

Quarterly

2nd Pillar: Risk Infrastructure and Management

- The Executive Board includes risk management matters in its agenda on a quarterly basis.
- The Chief Risk Officer (CRO) acts as the coordinator to collate and presents risk management matters to the Executive Board every quarter and presents key enterprise risks approved by the Executive Board to the Risk Management Committee every six months.
- The Risk Management Office (RMO) constitutes 1-2 members for administrative and operational activities to support the CRO in ERM process and reporting requirements.

Ongoing

3rd Pillar: Risk Ownership

- The Business Unit and Corporate Function Risk Owners have the primary responsibility for identifying risks, developing response plans and monitoring risks for their BU/functions/processes.

Strategy and Objective Setting

The Executive Board is involved in identifying the risks to strategy and risk of strategy as part of the Annual Business Planning exercise. The role of ERM in strategy and objective setting is to add perspective to the strengths and weaknesses of a strategy as conditions change.

The Executive Board also performs risk assessment of any strategic business initiative to identify impact of risk to the plan and develop mitigation strategies for the same.

Risk Appetite: The aggregate level of risk the Company is prepared to accept while pursuing its business strategies.

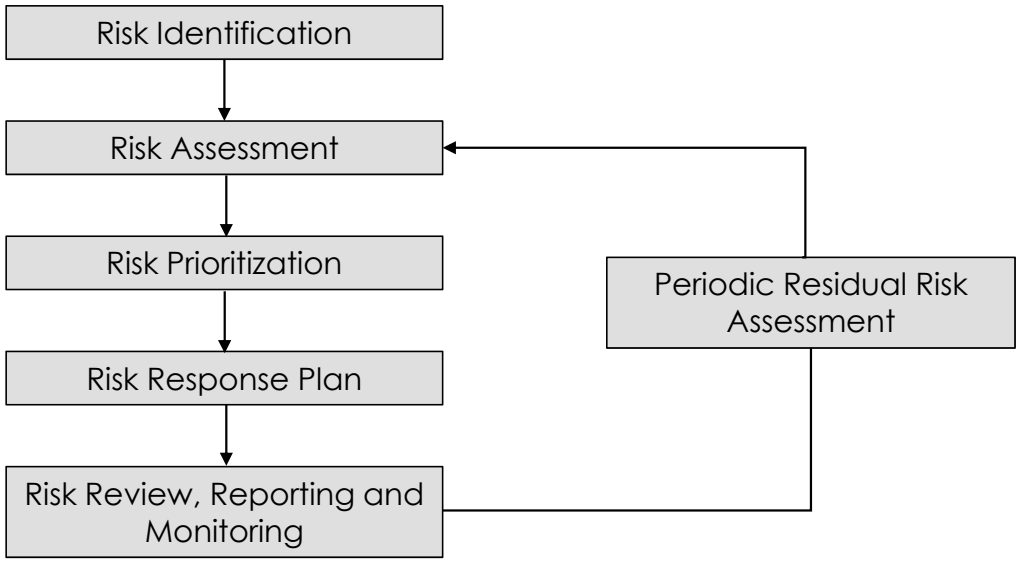
The Enterprise Risk Appetite will be agreed between the Board of Directors and the Management. At the Board level, risk appetite helps to drive strategic risk decisions. At the management level, risk appetite translates into a set of procedures to ensure that risk receives adequate attention when making tactical decisions. At the operational level, risk appetite dictates constraints for routine activities. Board of Directors will approve, review and refresh the Risk Appetite on an annual basis. Risk appetite is developed based on the following components:

- **Existing risk profile**: The current level and distribution of risks across the Company, across various risk categories.
- **Risk Capacity**: Maximum amount of risk the Company can assume in pursuit of its business objectives. It's a combination of financial strength, ability to raise capital, operational capability, and risk management practices
- **Risk Philosophy**: The Company's willingness to accept risk in its business operations, from strategic planning and implementation to its day-to-day activities
- **Strategy and Objectives**: The Company's long-term plans and business objectives.

Risk Performance

The Company has established a five-step process (as per COSO framework) to identify and assess risks that may affect the ability of the business to achieve its strategy and business objectives

This process is as shown below:



Risk Performance

Risk Identification

This step involves identification of sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on events that stakeholders perceive might enhance, prevent, degrade, accelerate or delay the achievement of business objectives. Risks can be identified using various methodologies i.e., Risk Workshops, Interviews, Surveys and External Study.

Inherent Risk - risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact

Residual Risk - remaining level of risk following the development and implementation of the entity's response.

Risk identification is an ongoing process. Each department/function will collate their risks in the risk register. Each identified risk will be assigned to a risk owner.

Risk Performance

The Company has identified the following Risk Categories:

- **Strategic –** Risk associated with the competitive positioning of the business and our ability to respond in a timely manner to changes in the competitive landscape. This includes risks to the value of the Company brand.
- **Financial -** Risk of loss resulting from participating in credit and financial markets. This includes the risk of loss from refinancing issues and changes in financial market variables that impact the revenue, expenditure, EBITDA and also valuation of assets and liabilities.
- **Operational** - Risk of loss resulting from various operations of the Company, inadequate or failed internal processes, people and systems or from external events. This includes disruptions caused by a failure to identify, measure and mitigate risks at key third-party organizations
- **Regulatory** - Risk from non-compliance of various statutory, regulatory, legal provisions and contractual obligations, perceived or actual conflicts of interest leading to penalties, litigation etc. This includes adherence to internal policies and industry standards.

Risk Performance

Risk Assessment

Risks identified in the previous step are assessed on the basis of the Risk Rating criteria.

Risk Rating: This framework sets up the criteria to rate risks in order to prioritize them. The assessment involves analyzing and evaluating the probable **likelihood, impact** and **velocity** of risk occurrence.

Likelihood of occurrence of the risk: The likelihood of an event is expressed as the probability and frequency of the risk event materializing based on the judgement of the risk owner. The likelihood scales are as defined below:

Likelihood of occurrence	Past occurrence	Future occurrence	Probability	Rating
Almost certain	Similar instances have commonly occurred in the past year	Will be almost a routine feature within the immediate next year	Probability ranges as approved by RMC	5
Likely	Similar instances have occurred several times in the past years	May arise several times within the immediate next year		4
Possible	There have been a one or two similar instances in the past year	May arise once or twice within the immediate next year		3
Unlikely	There have been one or two similar instances in the last 2 to 5 years	May occur once or twice in the next few years		2
Rare	Similar instances have never occurred in the past or occurred once or twice in more than 5 years	Highly unlikely to occur in the next few years		1

Risk Performance

Impact of a risk on the stated objectives and goals: This is the degree of consequence to the organization should the risk event occur. The guidance for assigning the risk impact score is as below :

Likely impact	Financial Impact	Likely brand/reputational impact	Regulatory impact	Rating
Extreme	Impact thresholds as approved by RMC	Extreme adverse public exposure / brand image in the long term (over a year) leading to deterioration in the credit rating.	Loss of business license or conditions imposed by the regulator impairing Company's operations in the long term (over a year). Criminal offence on Director or Manager. Substantial penalty.	5
Major		Negative public exposure / brand image in the long term (over a year) leading to deterioration in the credit rating	Loss of business license or conditions imposed by the regulator impairing the Company's operations for about a year; Sizeable penalty.	4
Moderate		Negative public exposure/ brand image with short term (less than a year) Impact	Conditions imposed on business license by the regulator for a short period (less than a year); Civil offence on Director or Manager; Moderate Penalty	3
Minor		Minor Incident reported in media without any negative public exposure.	Civil offence by employee; Warning by the regulator; Minor Penalty	2
Insignificant		Minor and segmented business partner concerns / incidents, but not reported in media	Caution letters from the regulator; Nominal penalty	1

Risk Performance

Risk Velocity: Risk velocity or speed of onset refers to the time it takes for a risk event to manifest itself. It is the time that passes between the occurrence of an event and the point at which the Company first feels its effects.

Following the risk event, the period for the impact to unfold is called **Time to Impact** (**TTI**). Risks with high-velocity TTI should have a rapid response to address the consequence of the impact. These are mostly reactive controls called contingency plans or "Plan B". A high-velocity TTI risk may indicate the need to have a well-thought-out crisis management plan in place to reduce the consequence of such a risk event.

Rating	Definition
3 (High)	Rapid onset, little or no warning, instantaneous from event to impact
2 (Moderate)	Moderate onset occurs in a matter of few weeks to several months from event to impact
1 (Low)	Slow onset, occurs over a year or more from event to impact

Risk Performance

Risk Prioritization

In order to identify the key risks to focus on, it's important to prioritize the risks, which is based on the **Risk Score.**

Risk Score = (Risk Impact x Risk Likelihood) + Risk Velocity

The maximum rating of all parameters will be considered as risk impact for risk prioritization score.

		I M P A C T				
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
L I K L I H O O D	**Almost Certain (5)**	5	10	15	20	25
	Likely (4)	4	8	12	16	20
	Possible (3)	3	6	9	12	15
	Unlikely (2)	2	4	6	8	10
	Rare (1)	1	2	3	4	5

Risk Performance

Risk Prioritization

Combining Risk Velocity with Risk Prioritization

The risk prioritization matrix is a two-dimensional matrix displaying Risk Impact and Likelihood. Impact assessment takes place for risks based on all impact parameters and the highest rating amongst the impact parameters will be considered for the final rating. A risk with Very High Impact (5) and High Velocity (3) has a potential of creating a crisis. Hence, often Risk Prioritization Matrix is integrated with Risk Velocity.

Risks are prioritized basis the following criteria.

Risk Rating	Criteria
High	Risk score >= 15 and <=28
Medium	Risk score >9 and <15
Low	Risk score <=9

Risk Performance

Risk Response

Risk Response involves identifying the most appropriate strategies to manage or mitigate the risks to an acceptable level (risk appetite - as set by the Company's management). This risk appetite will be revised annually and approved by the Board of Directors and RMC.

Risk mitigation and contingency plans for the risks must be formulated by the risk owners. The different action items of the mitigation plan however may be delegated by the owner as he/she may deem necessary.

Mitigation planning is classified into four main types:

- **Terminate:** If risk is too high, avoid activities related to the risk causes. E.g., Exit the line of business, stop operations, invest in safety or risk reduction measures even if it is costly.
- **Treat:** risk mitigation measures are applied, and attempts are made to reduce the likelihood of occurrence or the impact of the occurred risk events and have clear accountabilities and roles defined
- **Tolerate:** Accept the risk and proceed with related activities, perform regular monitoring of the risk exposure, if risk exceeds acceptance threshold, then take appropriate action
- **Transfer:** The strategy involves shifting risk to another party, e.g., contracting or utilizing third-party contracts, Purchase insurance policies (limited, full)

Risk Performance

Risk Response

A. Develop Contingency Plans

Develop contingency plans for risks with high velocity/ high impact rating to enable rapid response to address the consequence of such risks, in case they materialize. Risk register helps in identifying risks where contingency plans need to be developed.

B. Documentation of Risk Response/Mitigation plan

Once the response option has been identified, a risk response plan will be developed and documented against the respective risk. Response/mitigation plans will be documented along with the risk information in the risk register. A risk mitigation plan will identify responsibilities for action, timelines implementation, budget and resource requirements, performance measures and review process where appropriate. This documented risk response/mitigation plan will be monitored on a quarterly basis to verify its effectiveness.

Implement agreed Risk Response

Once budgetary and resource approvals are authorized, mitigation plans will be implemented by the risk owners and will also be overseeing its progress.

Risk Performance

Risk Review

In order to ensure that risk management is effective the Company has set up a risk reporting, monitoring and review process. Risk reviews ensure evaluation of risks at predetermined frequencies to track the dynamics of the internal and external environment continuously. Risk review process will include the following action steps:

- Risk Owners will review the implementation status of risk response strategies and their defined action plans for their functions and will update the risk register
- Risk owners will re-assess risks as per the following frequency:

Risk Level	Frequency of Reassessment
High	Quarterly
Medium	Bi-annually
Low	Annually

Risk Performance

Information, communication & reporting

To ensure accountability for implementing risk management process, the Company has set up a communication and reporting mechanism for ERM process.

Results of risk assessment will be reported to all relevant stakeholders for review, inputs and monitoring.

The following steps will be followed for communication and reporting process:

- Once a quarter, the Risk Management Office will consolidate the risks received from all the functions
- A brief summary of the risk profile setting out the most significant risks faced by the Company will be prepared. For each risk, the report shall
    a. describe the risk under appropriate category with the assigned risk score;
    b. show the key activities and controls to mitigate/manage the risk;

ERM Improvement

ERM Improvement

- The Executive Board would plan to undertake initiatives for strengthening and improvement of ERM deployment across the Company. The same must be communicated to the Risk Management Committee.
- Regular review of risks by the risk owners and Executive Board help to improve the efficacy of risk controls.

References

This framework should be read in conjunction with the Risk Management policy of the Company.

Thank you