ENTERPRISE RISK MANAGEMENT POLICY

- Adopted by the Board of the Company on 12th May 2022

About Foseco India Limited

Foseco India Limited (referred as “The Company”) is a listed public Company incorporated on 22 March, 1958. The Company operates factories in Sanaswadi, Pune, and Pondicherry, India. The Company manufactures industrial chemicals for companies with steel milling and foundry operations. The Company operates through metallurgical products and services segment. The Company's product technology includes coating, metal filtration, feeding systems, flow control, metal treatment, binders and crucibles.

Foseco India Limited is the Foundry Technologies Division of Vesuvius plc, a Company that offers products, such as feeding aids, filtration, ferrous and non-ferrous metal treatment, binders, coatings, molten metal transfer and moulding materials. The Company's product technology includes coating, metal filtration, feeding systems, flow control, metal treatment, binders and crucibles.

- **Vision of the Company**- The Company’s vision is to become:
  - The preferred partner to the foundry industry providing the greatest value.
  - A highly respected industry leader with which all stakeholders are proud to be associated.
- **Business Strategy**- The Company’s business strategy is to improve its customer’s business performance:
  - By being the partner providing the greatest value.
  - Achieved through a solution partnering and value selling approach delivering improved foundry processes and casting quality.
  - Based upon world-class proprietary technology, foundry process and product application expertise and excellence in quality and customer service.
- **Foseco Values**

The Group has adopted values that guide the Company in its ability to grow and significantly improve its results. The Company conducts an extensive strategic review of its activities. Following this review, ambitious goals are set for its growth and improvement of its profitability.

To help each one of the employees make the right decisions and bring them together – the following set of values and behaviours have been built: CORE – Courage, Ownership, Respect and Energy. These values convey the mindset and attitudes which is expected from each of the employees to actively demonstrate every day. The Management firmly believes that these CORE values will enable the Company to strengthen its leadership position in the business.

Index

I. Introduction:

Internal and external factors affect the organization regardless of size, industry and influence that make it uncertain whether and when they will accomplish their business objectives. The effect of such uncertainty on an organization's objectives is “RISK”. Risk is an integral part of the dynamic business environment.

As per COSO, Risk Management

Enterprise 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.

Foseco India Limited recognizes that risk management is a vital driver of effective Corporate Governance, and views it as a constant process. The Company is devoted to confirming the adequacy of its risk management systems and that risks and opportunities are adequately and appropriately addressed on time.

Enterprise Risk Management policy (ERM Policy) has been formalised in response to regulations of Companies Act, 2013 and SEBI (LODR) Regulations, 2015. Among other requirements as per SEBI LODR amendments the Company has to:

- Review the existing risk management framework and policy
- Constitute a Risk Management Committee and define specific roles, responsibilities and power of the RMC
- Develop a framework for identification and assessment of internal and external risks faced by the organisation, including financial, operational, sectoral, sustainability (particularly Health, safety & Environment (HSE) related risks), information, cybersecurity risks and any other risk determined by the Risk Management Committee (RMC).
- Define measures for arriving at appropriate risk responses, including systems/processes for internal control of identified risks
- Integrate the risk management framework with the business continuity plan*, (BCP) and crisis management
- Conduct RMC meetings at least twice in a year within a period of 180 days between any two consecutive meetings etc.

**Business Continuity- “The capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident”.*

Business Continuity Planning – "The process of creating systems of prevention and recovery to deal with potential threats to a Company".

A BCP is a set of contingencies to minimize potential harm to businesses during adverse scenarios. Therefore, BCP is a subset of risk management. BCP's are written ahead of time and can also include precautions to be put in place. Usually created with the input of key staff as well as stakeholders. Business continuity Planning enhances value creation objectives and protection objectives of the organization. Whereas the ERM, design framework to identify risk and mitigation plan for the risks. For effective execution, the merging of ERM and BCM programs is required.

II. Objectives

The prime objective of risk management is to ensure that the risks facing the business are appropriately managed by:

- Protecting stakeholder's value by minimizing the threat and maximizing the opportunities.
- Minimizing the adverse consequence of risks on business objectives and provide a direction for risk management by bringing together the policy and guidance from the Board of Directors, Audit Committee, Risk Management Committee and all other stakeholders.
- Ensuring the risk responses for assessed risks are in line with the organizational risk appetite and tied in with the business continuity plans, disaster recovery plans and crisis management processes wherever applicable.

This document places the framework of Enterprise Risk Management at Foseco India Limited. Risk Management within Foseco India Limited is the accountability of the Company's people, and the proactive identification of risks will be actively encouraged and supported.

III. Importance of Risk Management

Risk management empowers a business with the required tools so that it can adequately identify and deal with potential risks. Only once a risk has been identified, management can start working on its mitigation. In addition, risk management offers a business with a basis upon which it can undertake sound decision-making.

Effective risk management plays a key role in any Company's pursuit of financial stability and superior performance by contributing including:

- Organizational Growth

- Maintaining Corporate Governance and public disclosure
- Continuing to enhance our industry expertise
- More effective management of change
- More efficient use of resources
- Improved decision making
- Reduced waste and fraud
- Further develop Culture of Innovation
- Management of contingent and maintenance activities etc.

IV. Regulatory Background

A brief overview of certain key provisions in relation to risk management under the said acts have been provided below:

i. **Companies Act 2013-** There are specific requirements for Risk Management that a Company needs to comply with. In addition, the Board of Directors and Audit Committee have been vested with specific responsibilities in assessing the robustness of risk management policy, process and systems.

- **Responsibility of the Board:** Section 134(3) (n) states that the Directors' Report should include: a statement indicating development and implementation of a **Risk Management Policy** for the Company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company.

- **Responsibility of the Audit Committee:** As per Section 177 (4), Every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, inter alia, include evaluation of internal financial controls and risk management systems

- **Responsibility of the Independent Directors:** As per Schedule IV [Part II-(4)] of the Act, Independent Directors should satisfy themselves that financial controls and the systems of risk management are robust and defensible.

ii. **SEBI (LODR) Regulations, 2015**- The Securities and Exchange Board of India (SEBI), has included Risk Management as part of the Securities & Exchange Board of India. (Listing Obligations and Disclosure Requirements) Regulations 2015 (LODR) requirement.

- **Regulation 17** - Disclosures to the Board are to be made by the listed entity on whether the risk assessment and its minimization procedures are in place.

- **Regulation 21 – Risk Management Committee:** It requires that Top 1,000 listed companies should have a Risk Management Committee

V. Key Terms

- **Audit Committee:** A sub-group of a Company's board of directors responsible for the oversight of the financial reporting and disclosure process.

- **Board of Directors / Board:** A collective body representing shareholders and jointly supervise the activities of an organization.

- **Company:** Means Foseco India Limited

- **Consequence:** Potential resulting events that could be affected by the key group risk.

- **ERM Policy:** Enterprise Risk Management Policy.

- **Inherent risk:** The risk to an entity in the absence of any mitigating controls. These risks (in absence of any mitigating controls, as aforesaid) are also referred to as "Gross risks"

- **Impact:** The degree of consequences to the organization should the event occur.

- **Likelihood:** The likelihood of the event occurring is expressed as an indicative annual frequency.

- **Risk:** The possibility of an event occurring that will have an impact on the achievement of objectives. Risk implies future uncertainty about deviation from expected earnings or expected outcome**.**

- **Residual Risk:** Residual Risk is the risk we will continue to face even if the mitigation plan works.

- **Risk Register:** A risk register is a document used as a risk management tool and to fulfill regulatory compliance acting as a repository for all risks identified the likelihood and consequences of a risk occurring and also includes additional information about each risk, e.g., nature of the risk, type and owner, mitigation measure

- **Risk Source:** Element which alone or in combination has the intrinsic potential to give rise to risk.

- **Risk Rating:** The relative rating is determined from the risk score derived from qualitative analysis of impact and likelihood. Categorized as High, Medium or Low.

- **Risk Score:** The combined product of risk likelihood, risk consequence and risk velocity

- **Risk Prioritization:** The process of prioritizing risks based on risk scores

- **Risk Appetite:** Risk appetite defines the nature and degree of risk that an organization will take and the risks that it will avoid in pursuit of its objectives. In other words, the Company will take risks that do not result in the breach of its appetite.

- **Risk Velocity:** It is how fast an exposure can impact an organisation. It is the time that passes between the occurrence of an event and the point at which the organisation first feels its effects.

- **Risk Response:** Risk response consists of determining the appropriate action to manage risks categorized within the levels defined by the Company.

VI. Scope & Applicability of ERM

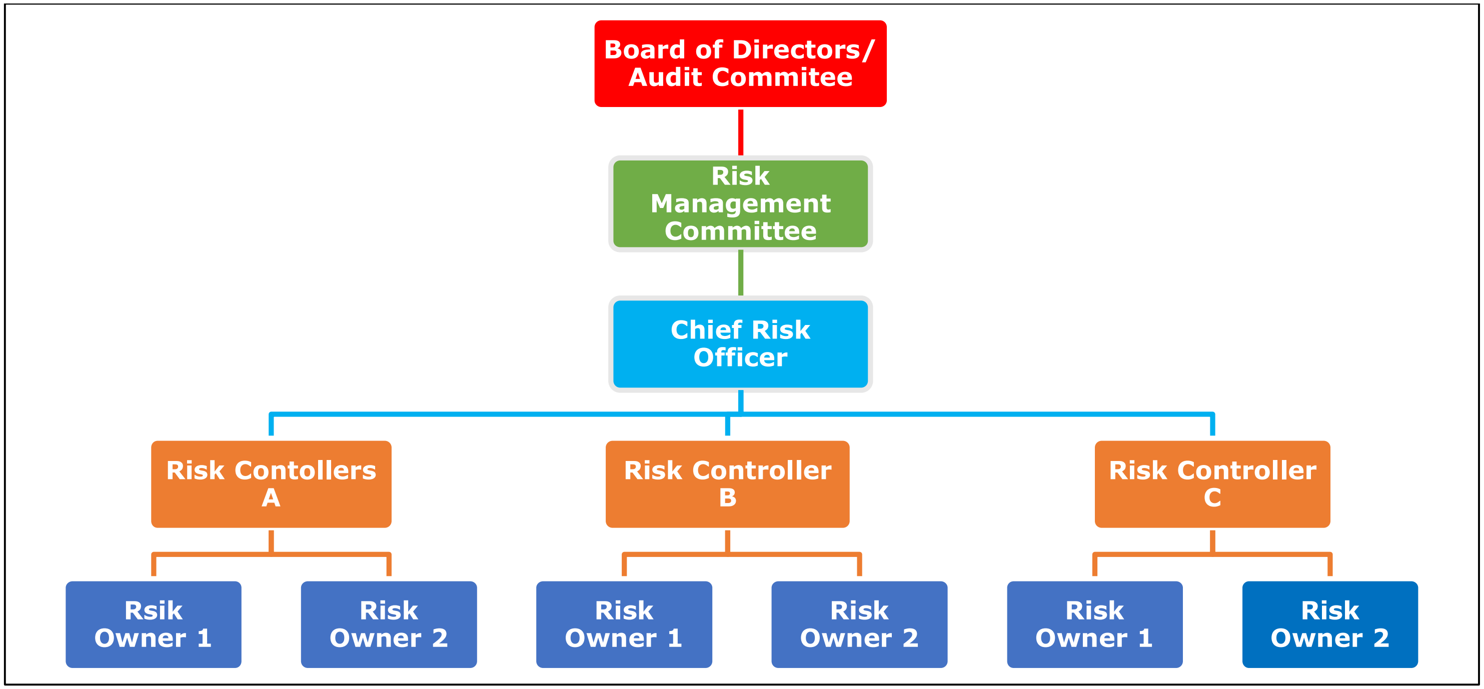
The ERM framework applies to all aspects of Foseco India Limited. This framework needs to be followed at all its departments/ locations.

VII. Risk Organization Structure

Risk management provides a balance between taking risks and reducing them. Effective risk management may add value to any organization. For effective implementation of the risk management framework, it is important to nominate senior management individuals to lead the risk management teams.

A well-defined organizational structure offers a clear path for risk assessment procedures. Before risk assessment teams can initiate to work, each member of the team must have sufficient operating knowledge of the Company or its organizational structure. The organizational structure will help team members to understand that who is responsible for each area of operation being evaluated.

The risk management structure will define the responsibility of the Company's personnel. Senior management participation will ensure active review and monitoring of risks.



Particulars	Risk Management Committee (RMC)	Chief Risk Officer (CRO)	Risk Controller (RC)	Risk Owners (RO)
Constitution	• Constituted with approval of Board • There shall be minimum of 3 members- 1. Member of Board of Director 2. Member of Board of Director 3. An Independent Director, 4. Any other member as decided by the Company	Managing Director	• Respective Functional Heads will be Risk Controllers for their respective Unit.	• Risk Owners shall be nominated by the Risk Controllers • Each of the departments shall be represented by a Risk Owner. List of departments: 1. Production, 2. Maintenance, 3. Marketing, 4. Purchase, 5. Inventory, 6. Information Technology, 7. Accounts and Tax, 8. Treasury, 9. Logistics, 10. Indirect Tax/GST, 11. Any additional Department
Roles, Responsibilities and Power	• Frame a comprehensive Risk Management policy • Ensure that appropriate processes and systems are in place to monitor and assess	• CRO to review the risk register submitted by RC and prepare a consolidated risk register based on analysis. • CRO is required to prepare quarterly a report for the	• Evaluate and guide the RO for risk response plan prepared • Perform Risk analysis, and identify the Risk treatment and Control mechanism	• The Risk Owner is responsible to identify future risks and evaluate the criticality of the risk. • The Risk Owner will be responsible for the

Particulars	Risk Management Committee (RMC)	Chief Risk Officer (CRO)	Risk Controller (RC)	Risk Owners (RO)
	risks associated with the Company. • Monitor implementation of the risk management policy, and assessment of the competence of risk management systems. • Review the policy periodically, at least once a year, considering the complexity, dynamic changes in the industry. • Inform the board of directors about RMC discussions on risk management i.e., recommendations and the actions to be taken. • Appointment, removal and terms of remuneration of Chief Risk Officer (CRO) to be reviewed. • To seek information from any employee, obtain outside legal or other professional advice and	Risk Management Committee • Update to the Audit Committee on a periodically on all key risks and work under the direction of RMC (Risk Management Committee). • Providing the overall leadership, vision and direction for entity level risk • Ensuring adherence to control mitigation plan and timelines and reporting to RMC and AC on the efficiency of Risk Management Framework (RMF). • Initiating and coordinating actions for the effective working of the RMF.	• Update Risk Register (refer to Appendix B) and communicate to CRO for approval. • Initiate review meeting at least once every Quarter for reporting of any new risk identified/ status of the corrective action plan.	formulation of risk response of their respective areas. • Risk Owner shall present the new risks identified along with the proposed mitigation plan in the Risk template Form (refer to Appendix A) to Risk Controller for their approval.

Particulars	Risk Management Committee (RMC)	Chief Risk Officer (CRO)	Risk Controller (RC)	Risk Owners (RO)
	secure attendance of outsiders with relevant expertise if it considers necessary. • Obtain at the Company's expense, outside legal or professional advice on any matters within its terms of reference when the Committee reasonably believes it necessary to do so.			
Responsible To	Board of Directors/ Audit Committee	Risk Management Committee	Chief Risk Officer	Risk Controller

VIII. Risk Management Process

1. Risk Identification - *Analysis of risk occurrence*

Risk universe analysis involves consideration of the sources of risk, their consequences and the likelihood of their occurrence. The existing systems, control measures and procedures to control risk are identified and their effectiveness is assessed. The impact and likelihood of an event and its associated consequences are assessed in the context of the existing controls.

Risk Identification involves identifying all risks that affect the organization's objectives. The initial step of risk identification is to recognize uncertainties and causes of interruption to the operation due to internal as well as external factors. There are several techniques to identify risks like:

a) Safety audit – Engaging safety and environment agencies to conduct the specific audits
b) Threat analysis – Assessing potential losses arising out of the business environment.
c) Event analysis – Assessing the potential events taking place in the business environment.
d) Hazard study – Assessing the potential hazards associated with the business operations.
e) Internal Audit – Engaging auditors to access the internal controls & identify potential risk areas

Analysis of all the risks thus identified shall be carried out by the Chief Risk Officer through the participation of the vertical/functional heads (Risk Controllers) and a preliminary report thus finalized shall be placed before the Risk and Audit Committee.

To identify an organization's exposure to uncertainty, risks may be primarily classified as follows:

Based on Type -

Internal Risks: Internal risks arise from the events taking place within the business enterprise. Such risks arise during the ordinary course of a business.

External Risks: External risks arise due to the events triggered in the environment outside the business organization.

Based on Control -

Controllable Risks: Controllable risks are those risks where the management can implement measures either to prevent those risks or minimize their impact.

Uncontrollable Risks: Uncontrollable risks are those risks which the management may not be able to anticipate effectively and will need to resort to detective measures or procedures post the risks have occurred to minimize their impact.

Further, risks can be segregated into these major types: -

Types of Risk	Examples
i. Strategic	• Reduction in business vitality (due to change in business strategy, customer spending patterns, product discovery & development, changing technology, etc.). • Business Continuity Risk • Disaster Recovery Risk

Types of Risk	Examples
	• Pandemic Risk • Currency Risk
ii. Reputational	• Brand Equity • Reputational Risk
iii. Customer	• Competition Risk • Satisfaction risk- dissatisfaction amongst the customer due to lack of attention, focus, etc. • Enquiry Monitoring Risk
iv. Supply Chain	• Absence of supply chain strategy • Ineffective cost comparison • Vendor evaluation
v. Technology	• Technology Upgradation Risk • Substitute Technology Risk • Information Security • Cyber Security Risk • Social Media Management Risk

vi. Compliance	• Health, Safety & Environment
	• Violation of laws or regulations governing areas such as
	  • Environmental
	  • Employee health & safety.
	  • Selling and promotion of our products.
	  • Protection of personal data in accordance with global data protection requirements.
	  • Local tax and statutory laws

vii. Entity Level	• Management Oversight • Board Oversight

Types of Risk	Examples
viii. Financial Reporting	• Funding & cash flow • Mandatory Reporting
ix. People	• Succession Planning (to fill key business leadership positions in the Company) • Key Personnel Risk • Organizational Structure Risk (undefined organizational structure/ job positions/ hierarchy/ lines of communication leading to inadequate authority & responsibility/ unsatisfied employees in the organization)

2. Identification of Risk Owners - *Accountability*

Risk Owner is the representative from respective business operation who is accountable to identify future risks and evaluate the risk criticality.

The respective Risk Controller will identify Risk Owners for their operation areas. Assigning an owner for these risks is important for a few reason-
One, a designated risk owner ensures someone in the organization is accountable for the risk. If there is not one person or a group charged with managing a risk, then by default, the entire organization will own the risk, and therefore it is highly likely the risk will fall through the crack. In terms of control ownership, this should lie with whichever department is responsible for the performance of the control. Where a control has multiple owners, each owner must clearly understand what part of the control they are responsible for, otherwise responsibility will be lost between the cracks.

Having a risk owner is an important step toward ensuring that a response plan is developed and acted upon in a timely manner.

The CRO may discuss the identified risk with the Risk controller for further analysis of related data, previous internal audit reports, past occurrences of such events, etc.

3. Setting of acceptable levels of risk - *Defining Risk Weights/ Risk Appetite*

Acceptable levels of risk mean the amount of risk an organization is willing to take in pursuit of objectives it deems have value. Setting acceptable level of risk is the process of defining tolerable limits to accept on occurrence of particular risk.

Risk appetite can also be described as an organization's risk capacity, or the maximum amount of residual risk it will accept after controls and other measures have been put in place. Risk appetite, an integral component of enterprise risk management, can be influenced by a wide variety of factors, including the following:

- Culture of an organization;
- Industry an organization is in;
- Competitors;
- Types of initiatives pursued; and
- Current industry position and/or financial strength.

4. Risk Assessment - *Evaluating risk against acceptable level*

Risk Assessment involves comparing the level of risk found during the analysis process against the pre-defined risk weights to assess their potential severity of loss and probability of occurrence. Risk weights of High / Medium / Low can be assigned based on parameters for each operating activity.

The output of the risk assessment is a prioritized list of risks for further action. If the resulting risks fall into the low or acceptable risk categories they may be accepted with minimal further treatment. Low and accepted risks should be monitored and periodically reviewed to ensure they remain acceptable.

- **Likelihood of Risk Occurrence (P) to be done based on the below matrix-**

Score	Likelihood	Description
1	Remote	Event may only occur in exceptional circumstances.
2	Possible	Event could occur at some point of time.
3	Occasional	Event could occur occasionally.
4	Frequent	Event could occur at continuously/frequently
5	Constant	Event is expected to occur in most circumstances.

- **Measurement Yardstick for Risk Consequence (C) –**

Level	Description	Ranking Criteria
1	Negligible	• Less than £50k impact on revenue. • No impact on market share. • No impact on reputation.
2	Minor	• £50k to £100k impact on revenue. • Consequences can be absorbed under normal operating conditions. • Potential impact on market share. • Potential impact on reputation.
3	Moderate	• £100k to £200k impact on revenue. • There is some impact on market share. • There is some impact on reputation.
4	High	• £200k to £300k impact on revenue. • Market share will be affected in the short term. • Reputation is affected in the short term.
5	Significant	• £300k to £500k impact on revenue. • Serious diminution in reputation. • Sustained loss of market share.
6	Major	• More than £500k impact on revenue. • Major diminution in reputation. • Major loss of market share.

- **Frequency of Risk Velocity (V) to be done based on the below matrix:**

Score	Velocity	Description
1	Very low	Impact may be felt over a period of 10 years and above
2	Low	Impact may be felt over a period of 5-10 years
3	Medium	Impact may be felt over a period of 2-5 years
4	High	Impact may be felt over a period of 1-2 years
5	Very High	Impact may be felt multiple times during the year

- **Risk Impact Assessment Matrix (P*C*V)**

A risk reporting matrix is matched with specific likelihood ratings, impact ratings and velocity ratings to a risk grade. The risk reporting matrix is typically used to determine the level of risk identified-

Risk Range	Risk Category
01 to 20	Low Risk
21 to 60	Medium Risk
61 to 150	High Risk

5. Risk Response and Risk Control - Mitigation/ Treatment - *Identification and implementation of controls*

Post completion of analysis and risk prioritization, the next step is to take action to reduce the risks identified to an acceptable level. Every risk needs to removed or contained.

Risk response involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them. Options include avoiding the risk, reducing the likelihood of the occurrence, transferring the risk, and retaining the risk.

There are four strategies for treating risk

- **Avoid the risk-** Exit activities that bring on the risk.
- **Reduce the risk-** Take steps to reduce the likelihood of a negative event occurring by implementation of adequate mitigation controls

- **Share the risk-** Transference of risk by obtaining insurances, by transferring liability by incorporation of reciprocal clauses in contractual obligations etc.
- **Accept the risk-** Simply live with the risk, acknowledging that if the threat occurs the organization will have to bear the consequences.

Once all reasonable potential solutions are listed, the one that is most likely to achieve desired outcomes needs to be selected based on the cost-benefit analysis and also needs to ensure that does not result in the breach of its Risk Appetite. Action plans supporting the strategy are recorded in a risk register along with the timelines for implementation. A formal process needs to be defined to implement the solution logically and consistently across the organization.

6. Risk Monitoring Mechanism - *Monitoring of residual risks and the effectiveness of controls*

Any strategy will not ensure the complete elimination of risk; therefore, it is always required to have a close watch on all risk factors. The step of monitoring mechanism contents a close watch. Under this stage, the risk needs to be continuously monitored to make the mitigation process more effective.

It also includes determining whether the initiatives are effective and whether changes or updates are required. Sometimes, it may also require starting over with a new process if the implemented strategy is not effective.

7. Risk Reporting - *Reviewing and reporting on the Risk Management process at appropriate intervals.*

The Risk Template Form (RTF) (Refer Appendix A) will be used to highlight emerging risks or add new risks to the risk register throughout the year. On an ongoing basis, when a new or emerging risk is identified, Risk owners of the respective department will notify to Risk Controller by submitting the RTF.

RTF will be reviewed by the concerned Risk Controller. Post-approval of RTF by the Risk Controller, a consolidated risk register will be mailed to Chief Risk Officer for review. After review, Chief Risk Officer will determine whether the risk contained in this report warrants inclusion in the consolidated Risk Register (Appendix B). Risk included in the Risk Register in the quarter will be reported to Risk Management Committee (RMC) in the Bi-Annually meeting.

A. Risk to be reported to Risk Management Committee

The Chief Risk Officer should report all the Risks (i.e., High, Medium, and Low) to the Risk Management Committee Bi-Annually. The complete Risk Register containing all open risks and newly added risks needs to be submitted to the Risk Management Committee for their review and analysis.

B. Risks to be reported to Audit Committee

Only significant risks (or those that could become significant) need to be reported to the Audit Committee and Board. Significant risks include those risks that have a high likelihood or significant impact (i.e., having Highlighted in Red) or where there is limited ability for mitigation by the Company. These risks are identified and assessed based on the Company's expertise, judgment and knowledge. However, Chief Risk Officer can present all the identified risks to the Audit Committee as per the need.

C. Risks to be reported to Board of Directors

The significant risks (i.e., Highlighted in red) should be presented to the Board. The risks for which the action plan has not been identified or mitigation plan has not been completed within defined timelines needs to be reported to the Board.

IX. Appendices

1. APPENDIX -A: Risk Template Form

<table>
<tr><th rowspan="2">S N</th><th rowspan="2">Risk Category</th><th rowspan="2">Risk Heading</th><th rowspan="2">Industry /Company</th><th rowspan="2">Risk Description</th><th rowspan="2">Risk Velocity</th><th rowspan="2">Risk Appetite</th><th rowspan="2">Risk Owner</th><th colspan="5">Inherent Risk Score</th></tr>
<tr><th>Consequence</th><th>Probability</th><th>Velocity</th><th>Score</th><th>Grade</th></tr>
<tr><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4"></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><th colspan="5">Residual Risk Score</th></tr>
<tr><th>Consequence</th><th>Probability</th><th>Velocity</th><th>Score</th><th>Grade</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><th colspan="8">Type of Risk
(Internal/ External)</th><th colspan="5">Nature of Risk
(Controllable/ Uncontrollable)</th></tr>
<tr><td colspan="8"></td><td colspan="5"></td></tr>
<tr><th colspan="6">Management Mitigation Plan</th><td colspan="7"></td></tr>
<tr><th colspan="6">Action Plan</th><td colspan="7"></td></tr>
</table>

2. APPENDIX -B: Risk Register Template

The Management has established a template for each section to develop their Risk Register. The template could be viewed as a single sheet, which shows the following fields (or headings). Completion of the Risk Register in the below format will allow review by Senior Management.

The Risk Registers needs to cover the following columns:

- Risk SN
- Risk Categorization- *Business Continuity Management, Human Assets, Market, Information Technology, etc.*
- Industry/Company Specific
- Risk Heading- *Currency Risk, Vendor Concentration Risk, Maintenance Risk, Sub-contractor Dependency Risk, etc*.
- Risk Description
- Risk Owner
- Types of Risk- *Controllable/ uncontrollable*
- Nature of Risk- Internal / External
- Inherent Risk- Probability (P) & Consequences (C), Velocity (V)Product of P & C & V
- Management Mitigating controls
- Residual Risk- Probability (P) & Consequences (C), Velocity (V) Product of P & C & V
- Risk Appetite
- Risk Grading

SN	Risk Category	Industry/Company	Risk Heading	Risk Description	Risk Owner	Types of Risk	Nature of Risk	Inherent Score					Management Mitigating controls	Residual Score					Risk Appetite
						Controllable/ Uncontrollable	Internal / External	P	C	V	P*C*v	Risk Grading		P	C	V	P*C*V	Risk Grading	

3. APPENDIX -C: Risk Management Activity Calendar

Activity	Timelines
Risk Template form to be submitted by Risk Owner to Risk Controller	Event-based/ Monthly
Risk Register Review report to be submitted by Risk Controller to the Chief Risk Officer	Quarterly By the 10th day following the quarter-end
Entity Level Risk Analysis to be reviewed by Chief Risk Officer	Quarterly
Review by Risk Management Committee- Meeting to be held as per timelines with the quorum shall be either two members or one - third of the committee members, whichever is higher, including at least one member of the board of directors in attendance minimum	Bi-Annually (Not more than 180 days shall elapse between any two consecutive meetings)
Audit Committee meeting	Annually

4. APPENDIX -D: Document Change History and Revision Control

This policy should be reviewed periodically to ensure effectiveness and its continued application and relevance to the business. Feedback on the implementation and the effectiveness of the policy will be obtained from the risk reporting process, internal audits and other available information.

Date Approved: 12th May 2022 Effective Date: 12th May 2022
Last Reviewed: Next Review:

Version	Sections Revised	Description of Revisions	Changed By	Approved By	Date

Authorized by:
The Board of Directors of
Foseco India Limited