Shivalik Bimetal Controls Limited

Risk Management Policy

INTRODUCTION

Risk is an inherent aspect of the dynamic business environment. Risk Management Policy helps organizations to put in place effective frameworks for taking informed decisions about risks. To minimize the adverse consequence of risks on business objectives, the Company has framed this Risk Management Policy. The guidance provides a route map for risk management, bringing together policy and guidance from Board of Directors.

IMPORTANCE OF RISK MANAGEMENT

A certain amount of risk taking is inevitable if the organization is to achieve its objectives. Effective management of risk helps to manage innovation and improve performance by contributing to:

- Increased certainty and fewer surprises,
- Better service delivery,
- More effective management of change,
- More efficient use of resources,
- Better management at all levels through improved decision making,
- Reduced waste and fraud,
- Add better value for money,
- Innovation,
- Management of contingent and maintenance activities.

STATUTORY REQUIREMENT

The Policy is formulated in compliance with Regulation 17(9)(b) of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("the Listing Regulations") and provisions of the Companies Act, 2013 ("the Act"), which requires the Company to lay down procedures about risk assessment and risk minimization.

i. The Board of Directors of the Company shall form a Risk Management Committee (hereinafter referred to as "Committee") who shall periodically review this Policy of the Company so that the Management controls the risk through properly defined network. The Board of Directors may re-constitute the composition of the Committee, as it may deem fit, from time to time.

ii. The responsibility for identification, assessment, management and reporting of risks and opportunities will primarily rest with the Committee. They are best positioned to identify the opportunities and risks they face, evaluate these and manage them on a day to day basis.

The Risk Management Committee shall provide oversight and will report to the Board of Directors who have the sole responsibility for overseeing all risks.

RISK ORGANIZATION STRUCTURE

For successful implementation of risk management framework, it is essential to nominate Chairman of Committee to lead the risk management members. Periodic workshops will be conducted to ensure awareness of the policy and the benefits of following them. This will ensure that risk management is fully embedded in management processes and consistently applied. Senior management involvement will ensure active review and monitoring of risks on a constructive 'no-blame' basis.

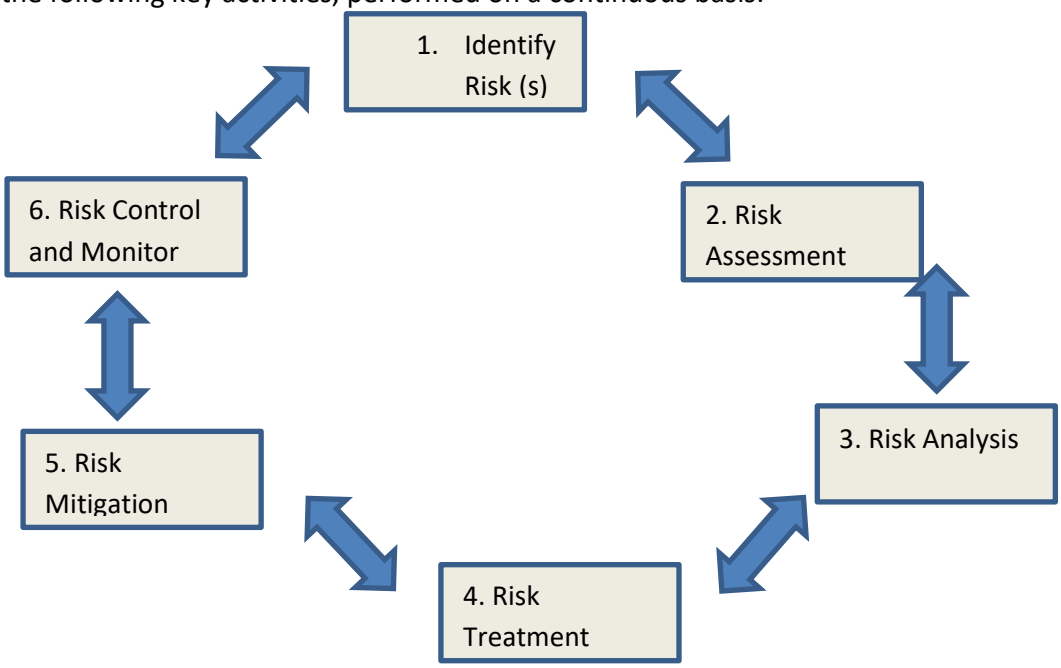
RISK MANAGEMENT FRAMEWORK

PROCESS

Risk management is a continuous process that is accomplished throughout the life cycle of a Company. It is an organized methodology for continuously identifying and measuring the unknowns; developing mitigation options; selecting, planning, and implementing appropriate risk mitigations; and tracking the implementation to ensure successful risk reduction. Effective risk management depends on risk management planning; early identification and analyses of risks; early implementation of corrective actions; continuous monitoring and reassessment; and communication, documentation, and coordination.

STEPS IN RISK MANAGEMENT

Risk management is a shared responsibility. The risk management process model includes the following key activities, performed on a continuous basis:



***Last reviewed and amended on February 12, 2025**

1. **Risk Identification:**

This involves continuous identification of events that may have negative impact on the Company's ability to achieve goals. Processes have been identified by the Company for the purpose of risk assessment. Identification of risks, risk events and their relationship are defined on the basis of discussion with the Department Heads.

2. **Risk Classification:**

The risk can be classified as follows: Firstly, the risk can be identified as being internal or external, secondly subject matter wise the risk can be classified as:

I. Operational risks

Operational Risks/Business risk relates to the day to day business activities carried out within an organisation, arising from structure, systems, people, products or processes. The Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Broadly, there are risk associated to manufacturing and trading operation.

II. Financial risks:

Financial risk is the possibility of losing money on an investment or business venture. For eg. Claims from debtors due to quality and other issues, Export obligation etc.

III. Sectorial risks

IV. Sustainability risks (particularly, environment, safety and governance related risks):
Environmental, social and governance (ESG) are three central factors in measuring the sustainability and ethical impact of a company. ESG factors, though non-financial, have a material impact on the long-term risk and return of investments. Responsible investors evaluate companies using ESG criteria as a framework to screen investments or to assess risks in investment decision-making

V. Information, Cyber security risks

Information (Data) and Cyber security risk is the probability of exposure or loss resulting from a cyberattack or and data breach on the organization. Organizations are becoming more vulnerable to cyber threats due to the increasing reliance on computers, networks, programs, social media and data globally.

VI. Other Risks
Natural calamities, Global or regional climate change or natural calamities, Any outbreak of health epidemics

3. Risk Assessment:

Risk assessment is the process of risk prioritization or profiling. Likelihood and Impact of risk events have been assessed for the purpose of analyzing the criticality. The potential Impact may include:

- ✓ Financial loss;
- ✓ Non-compliance to regulations and applicable laws leading to imprisonment, fines, penalties etc.
- ✓ Health, Safety and Environment related incidences;
- ✓ Business interruptions / closure;
- ✓ Loss of values, ethics and reputation.

Risk may be evaluated based on whether they are internal and external, controllable and non-controllable, inherent and residual.

4. Risk Analysis:

Risk analysis involves:

- consideration of the causes and sources of risk
- the trigger events that would lead to the occurrence of the risks
- the positive and negative consequences of the risk
- the likelihood that those consequences can occur

Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

4. Risk Treatment - Mitigation:

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are tolerable;
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

Based on the Risk level, the company should formulate its Risk Management Strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances.

5. Control and Monitoring Mechanism:

Risk management uses the output of a risk assessment and implements counter measures to reduce the risks identified to an acceptable level. This policy provides a foundation for the development of an effective risk register, containing both the definitions and the guidance necessary for the process of assessing and mitigating risks identified within functions and associated processes.

In circumstances where the accepted risk of a particular course of action cannot be adequately mitigated, such risk shall form part of consolidated risk register along with the business justification and their status shall be continuously monitored and periodically presented to Risk Management Committee and Audit Committee.

RISK REPORTING

- **RISK TO BE REPORTED TO AUDIT COMMITTEE**

While the Company will be monitoring, evaluating and responding to risks. 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 significant impact or where there is limited ability for mitigation by the Company. These risks are identified and assessed based on the Company's expertise, judgement and knowledge.

Head of Departments will place Risk Register to the Audit Committee and Risk Management Committee. However, Risk Committee can present all the identified risk to the Audit Committee as per the need.

- **PROCESS OF RISK REPORTING**

The Risk Identification Form (RIF) 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, Department Heads of respective department will notify to Risk Management Committee by submitting the RIF.

RIF will be reviewed by Committee for evaluation. After review of the RIF and in consultation with Audit Committee, Risk Management Committee will determine whether the risk contained in this report warrants inclusion in the risk register.

- **RISK REPORTING OF ADVERSE EVENTS**

All adverse events must be recorded in Event Recording Register. Details will be captured as per format specified.

The adverse event reporting form (Risk alert Form) should be completed as soon as possible after the event, within one working day, unless there are exceptional reasons for delay, for example the event was identified retrospectively following a complaint or claim. All adverse events, as may be decided as significant by Department Heads in consultation

with risk member should be reported, even if some time has passed since the event occurred. The final decision of an adverse event to be reportable or not lies with the Department Heads.

It is imperative that person(s) reporting the adverse event reports the fact. There is no place for any opinion or assumptions. It is important that details are accurate and factual for any future review.

BOARD'S RESPONSIBILITY STATEMENT

Board of Directors shall 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.

The Board of Directors of the Company and the Audit Committee shall periodically review and evaluate the risk management system of the Company, so that the Management controls the risks through risk management framework.

The Chief Financial Officer (CFO) shall provide quarterly a statement to the Board in writing, that the Company's financial reports present a true and fair view, in all material aspects, of the Company's financial condition and operational results and are in accordance with relevant accounting standards; and that this statement is established on a sound system of risk management and internal compliance and control which implements the policies adopted by the Board.

The Company has a control processes in place to help ensure that the information presented to senior management and the Board is both accurate and timely. The control processes include, among other things:

- Annual audit and interim review by the Company's external auditor;
- Planned review by internal auditors reviewing the effectiveness of internal processes, procedures and controls;
- Monthly review of financial performance compared to budget and forecast.

INTERNAL AUDIT (IA)

The Audit Committee and CFO is responsible for approving the appointment of the internal auditor and approving the annual internal audit plan.

Internal Audit function is independent of the external auditor and to ensure its independence, has direct access to the CFO and audit committee.

Any deviations from the Company's policies identified through internal audits are reported to responsible management for action and to the Audit Committee for information or further action.

POLICY REVIEW

This policy shall be reviewed periodically, at least once in two years, including by considering the changing industry dynamics and evolving complexity to ensure effectiveness and that 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.

***Last reviewed and amended on February 12, 2025**

APPENDICES

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 below format will allow review by senior management.

Risk Identification				Risk Assessment							

***Last reviewed and amended on February 12, 2025**

Event Recording Register

Sr.No	Date of occurrence of event	Nature of event	Weather the event already identified in Risk Register, If Yes		Risk Treatment Mitigation (Terminate, Treat, Transfer, Accept	Action taken to mitigate or reduce the risk	Actual Impact on the Company	Date of reporting of risk, if any
			Risk Reference No.	Mitigation Plan				

***Last reviewed and amended on February 12, 2025**

SHIVALIK

Risk Identification Form

Risk Identification Form

REVIEW DATE

Assessment No.

Brief Outline of Activity or work		Assessor	
Location		Reviewed by	

Risk Identified	Who Might be at risk	Existing Controls	Likelihood	Severity	Residual Risk	Additional Control Measures Required	Date Actioned	Estimated Residual Risk

*Last reviewed and amended on February 12, 2025

Risk Alert Form

Risk Alert ……(Subject)……

To:

Cc:

Company Name (abbreviation)	Reporter (Head of Department)

Date of Occurrence	
Event Occurred / which may occur	
The sequence of Event (briefly)	
Content of Violating Act	
Law supporting Violating act	
Influence / Penalty (including worst scenario)	

***Last reviewed and amended on February 12, 2025**