# RISK MANAGEMENT


## PARAMOUNT SPECIALITY FORGINGS LIMITED

www.paramountforge.com
91-22-2373 2656
3, 1, Guru Himmat Building, Dr. Mascarenhas Road Anjirwadi, Mazgaon, Mumbai - 400010, Maharashtra, India

# Risk Management Policy

## Introduction

Risk, as defined by ISO 31000:2009 (Risk Management - Principles and Guidelines), "is the effect of uncertainty on objectives". Enterprise Risk Management (ERM) is an integrated approach to proactively managing risks which affect the achievement of Paramount Speciality Forgings Limited's (herein referred to as "PSFL" or the "Company") vision, mission and objectives. ERM is aimed at protecting and enhancing stakeholder value by establishing a suitable balance between harnessing opportunities and containing risks.\

In the current dynamically changing business environment, PSFL is exposed to a plethora of risks from strategic, regulatory, alliance, operational and financial perspectives. The Board of Directors (Board) is committed to fostering an environment within the Company that enables proactive identification, management, monitoring and reporting of various risks that the Company may need to deal with. The Company-wide ERM initiative by Board would form the basis for ongoing management of risks at PSFL.

## Manage all risk

Manage all types of risk (business, market, operational) across the company
- Manage downside risk (threats) as well as upside risk (opportunities)

## Manage risk systematically

- Manage risks as a portfolio, not separately; optimize risk vs. return; integrate cross-department risks
- Common risk framework across departments aligned to best practices, international standards
- Accountability: every risk has an "owner"
- Standardized risk metrics and reporting
- Align risk management to corporate strategy; risks are clearly linked to affected objectives
- Manage risk at the most appropriate level through an effective risk governance structure Through this document, the Board:
- Mandates its commitment to ERM
- Seeks to embed ERM into the Company's culture by instilling ERM in its processes, people and technology
- Intends to align ERM fundamentals with organizational objectives
- Intends to align ERM performance indicators to organizational performance indicators Through the establishment of an ERM framework, the Board aims to realize the following benefits:
- Enhance proactive risk management
- Facilitate risk based decision making
- Improve governance and accountability
- Enhance credibility with wide range of stakeholders (e.g. Investors, Employees, Government, Regulators, Society, etc.)
- Above all, protect and enhance stakeholder value.

## Terms & Definitions

**Enterprise Risk Management** - Enterprise Risk Management is the systematic approach to managing all risks in an organization, in order to protect and enhance value.

**Risk –** Risk is an uncertain event or condition that may have a positive or negative effect on business goals.

**Challenges –** If the event is certain to happen, or has happened the risk would by definition lead to an issue/challenge. Mostly these challenges/issues are already addressed as part of annual planning processes. A challenge is also a form of obstacle that needs to be overcome to achieve desired business outcome. These are "certain" or on-going events and hence are not to be considered or treated as risks.

**Issue –** An issue is 'a present problem or concern influencing organisational objectives'. In other words, an issue is raised when something has gone or is going wrong and will affect the organization.
- an issue is a problem today

• a risk may become a problem in the future.

**Risk Register –** Compendium of all risks finalized and detailed with risk definition, risk mitigation and risk contingency plans

**Due Diligence of risk –** Deep diving into Class A risks along with RCA & ETA.

**Risk prioritization –** The process of prioritizing risks based on risk scores

**Risk score –** The combined product of risk likelihood & risk impact

**Risk Contingency Plan –** Plan B for risks in case of exigency conditions

**COSO –** Committee of Sponsoring Organisation

**Corporate risks –** Total compendium of risks at corporate level escalated from divisional/ hub/ business unit level.

**Apex Class A Risks -** Top priority risks (Class A) of corporate risks

**Event tree analysis (ETA) –** Analysis techniques for identification of sequence of events or impacts in case of risks play out.

**Root cause analysis (RCA) –** Analysis techniques for identification of plausible causes that may lead to the risk event.

**Risk appetite –** The amount of risk the organization is willing to take in pursuit of its organizational values.

**Business drivers –** Business drivers are the factors/condition that is vital for the continued success and growth of a business

**Objective:**
Standard ERM process so as to provide visibility oversight, control & discipline to drive & thereon improve the organization risk management capabilities in the changing business environment.

## Enterprise Risk Management Policy

**1. Enterprise Risk Management Philosophy**

The Risk Management philosophy of the Company is built based on its vision and strategic goals. The Company upholds its vision:
The Company has developed a dynamic growth strategy and is in the process of implementing robust institution building processes in pursuit of its vision and strategic goals. ERM aims at balancing the two by ensuring that key decisions with regard to strategy and institution building are commensurate with the Company's risk appetite. An enterprise risk management philosophy that is understood by all personnel facilitates employees' ability to recognize and effectively manage risk. The philosophy – the entity's beliefs about risk and how it chooses to conduct its activities and deal with risk – reflects the value the entity seeks from enterprise risk management and influences how enterprise risk management components will be applied.
Management communicates its enterprise risk management philosophy to employees through policy statements and other communications.

**An Integrated Approach**

PSFL has adopted an integrated approach for ERM. This approach to risk management shares a common "risk language", shared tools and techniques and periodic assessments of the total risk profile for the entire organization. This approach is appropriate when risk factors are common across business and functional units, when units are highly interdependent, and when tools and techniques developed in one unit can be readily adapted to others.

PSFL aims to integrate risk management across the organization to support its vision and towards achieving its business objectives. This will be accomplished by:
• Embedding a common risk management framework within the organization
• Proactively identifying future uncertainties and planning for them

- Training employees to consider risks as part of their decision making process

PSFL views ERM as key enabler in achieving its objective of creating and maintaining shareholder value, for successful execution of its strategies and for considering the "risk and reward" principle in the management of all business activities.

In particular, PSFL aims to:

- develop an effective ERM framework that will provide guidance on implementing ERM processes and make it part of its day to day business
- regularly identify significant risks that adversely impact the achievement of objectives and ensure these are appropriately prioritized, reported and managed
- regularly identify potential risk of lost opportunities and minimize adverse effects
- specify roles and responsibilities within ERM framework and include them as performance parameters
- regularly communicate ERM philosophy, principles and policies and procedures at all levels of staff

**Enterprise Risk management (ERM) Definition**

Enterprise risk management deals with risks and opportunities affecting value creation or preservation and is defined as follows:

Enterprise Risk Management (ERM) is a process, effected by the Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect its entity's business objectives, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of PSFL's objectives.

**Enterprise Risk Management framework**

The Enterprise Risk Management framework (ERM framework) refers to a set of components that provide the foundation for designing, implementing, monitoring, reviewing and continually improving risk management throughout the Company. The ERM framework for the Company has been developed keeping in mind the needs of internal and external stakeholders. The Company's ERM framework is based on the 'Risk Management - Principles and Guidelines' developed by the International Organization for Standardization (ISO 31000:2009 - Risk Management Principles and Guidelines).

In addition, several good practices recommended by the Committee of Sponsoring Organizations (COSO) for ERM have also been incorporated to further the Company's endeavor to build world class ERM framework and processes.

**Objectives**

PSFL Enterprise Risk Management ("ERM") Framework provides guidance to implement a consistent, efficient, and economical approach to identify, evaluate and respond to key risks that may impact business objectives.

PSFL's enterprise risk management framework is directed to enable management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value. Broadly, it encompasses:

- Promoting risk awareness throughout the company
- Defining risk appetite
- Identifying and managing multiple and cross-enterprise risks
- Identifying risk management team with clearly defined roles and responsibilities
- Formalizing risk response decisions
- Reducing operational surprises and losses
- Formalizing a process for identifying opportunities arising out of risk situations
- Improving deployment or more efficient use of capital and resources

ERM will help PSFL in managing risks in a proactive manner towards achieving its business objectives, performance & profitability targets and prevent loss of resources. PSFL's ERM is directed to help ensure effective reporting and compliance with laws and regulations, avoid damage to the entity's reputation and its consequences.

In summary, ERM is aimed to act as a process that would help PSFL to manage its risks in a structured manner with an objective to get to where it wants to go and avoid pitfalls and surprises along the way.

## Scope & Applicability of ERM

The ERM framework is applicable to all aspects of PSFL's business. This framework needs to be followed at all its Departments/ locations.

## Key principles of ERM Framework

The guiding principles of PSFL's Risk Management Framework are as follows:

- Risk Management should be a continuous process.
- Risk Management principles should be kept in mind during the strategy and objective setting processes as well as the day-to-day activities and decision-making
- Risks should be understood and prioritized based on the event frequency and impact to one or more objectives
- The same metrics used to measure objectives e.g., revenue, customer satisfaction metrics, are to be preferably leveraged during risk management activities
- Risk response strategies are to be evaluated for those risks deemed to be high or medium priority
- Key risk management information (e.g., key events, results of risk assessments, risk responses) is to be documented in a timely and structured manner
- Policies, procedures and practices should be in synchronization with risks
- A portfolio view of risks is to be reviewed by the Board, Audit Committee, Management Team and Chief Risk Officer on a regular basis

## Components of ERM Framework

**Strategy:** Strategy is critical to the framework and results in:
- Clearly defined business objectives
- Well defined risk appetite (how much risk should be taken to achieve business objectives)
- A risk profile aligned with the business strategy

**Policy:** It defines the guidance and standards to support strategy, consistent with the risk appetite and encompasses the following:
- Well defined roles and accountabilities for management
- Properly documented policies and procedures in line with the business needs and strategy

**Infrastructure:** Risk infrastructure is a set of tools to facilitate the execution of risk management objectives and comprises of:
- Enablers like technology and systems
- A robust information system that helps management in tracking risks
- Appropriate and relevant guidance that helps management to rate risks and prioritize the treatment of risks

**Processes:** Processes are developed to support the risk strategy and infrastructure. Processes are intended to work within the organizational context. Development and implementation of risk processes encompasses the following:
- Procedures that ensure that all risks are considered in a timely manner
- Processes to ensure that all risks are captured, assessed and responded to in a timely manner

**Organization:** Organizational structure is aimed at efficiently executing the strategy by means of leveraging the infrastructure and processes. Establishing an effective risk management organization should result in the following:
- Clearly defined roles and responsibilities
- Appropriate and adequate skills to manage risks
- Effective escalation of critical risk issues within the organization

Implementation of the risk management framework provides a direct link between the business strategy and risk appetite of PSFL and its systems and processes to ensure that those are designed to help PSFL meet its objectives. This framework needs to be reviewed from time to time as the business environment changes.

## Risk Management Concepts

### 1. Risk and Event

**Risk**

Simply stated risk is the possibility that an event will occur and adversely affect the achievement of objectives. Risks can be thought of as threats, uncertainty or lost opportunity.

**Event**
An Event in the context of ERM is defined as an incident or occurrence from internal or external sources that affects achievement of PSFL's objectives. Such "Events" may lead to one or more risks.

**2. Inherent risk vs. residual risk**
Risks need to be assessed to form an appropriate response. Assessment is done first at and Inherent level (quantum of risk at this level is referred as Inherent Risk) and then at a residual level (quantum of risk at this level is referred as Residual Risk).

**Inherent risk**
Inherent risk is defined as the risk to an entity in the absence of any mitigating controls. All business activities in PSFL have risks attached to them, whether these risks are caused by external or internal factors. These risks (in absence of any mitigating controls, as aforesaid) are also referred to as "gross risks".

**Residual risk**
Inherent risks may be controlled by introducing mitigating action points. The remaining likelihood and impact of a particular risk after management has taken action plans by way of instituting controls to alter the risk's likelihood or impact is called as residual risk.

Where PSFL has implemented effective controls to mitigate risks, the quantum of residual risks need to be monitored. Some level of residual risk will always exist, not only because resources are limited, but also because of inherent future uncertainty and limitations inherent in all activities.

**3. Business Risk vs. Operational Risk**
**Business risk**
Business risk is the risk that results from your decisions about the products and services you offer. When you decide to develop and market a particular product, there's a risk that the product won't work as well as you hoped or that your marketing campaign will fail. Other business risks include changes in the cost of raw materials or shipping and managing technological developments that affect sales or manufacturing.

**Operational Risk**
Operational risks exist in the way your company tries to carry out your decisions. Operational risk rises from your company's internal decision-making and practices. Even if your business idea is sound and you have a solid customer base, an operational risk can sink your business

## Benefits of Risk Management

Risk management is an important aspect of any business, as risks are an integral part of business. Risk management helps organizations manage risk to be within their risk appetite. Effective RM provides reasonable assurance regarding the achievement of the key organizational objectives in four broad categories: Strategic, Operations, Financial and Compliance. If an organisation has an effective Risk Management system, it helps in the following ways:

- **Link growth, risk and returns** - Risk management enhances the capacity to identify events and assess risks and set risk tolerances consistent with growth and return objectives;
- **Rationalise resources** - Deploy resources more effectively, thereby reducing overall capital requirements and improving capital allocations;
- **Exploit opportunities** - Identify and take advantage of positive events quickly and efficiently;
- **Reduce operational surprises and losses** - Recognise potential adverse events, assess risks and establish responses, thereby reducing surprises and related costs or losses;
- **Report with greater confidence** - Prepare internal and external information that is reliable, timely and relevant; and
- **Satisfy legal and regulatory requirements** - Ensure compliance with legal and regulatory requirements and identify risks of non-compliance.

## Limitations of Risk Management

Effective ERM, no matter how well designed and operated, does not guarantee achievement of all of an entity's objectives. Achievement of objectives is affected by limitations inherent in all management processes, which include:

- Human judgment in decision making, which can be faulty and that breakdowns can occur because of such human failures
- Controls can be circumvented by the collusion of two or more individuals
- Management's ability to override the risk management decisions
- Decisions on responding to risk and establishing controls depend on their related costs and benefits.

## ERM Process & Framework

ERM follows the 5 step process which covers process steps and components as per COSO. The structured approach is equally compatible with ISO 31000. The framework comprises of policies, processes, tools reports and the governance structure to help the enterprise manage all the material risk and facilitate linkages between strategy risk and capital requirements.

**Purpose**:
- Management sets the strategic and derived operational objectives for the organisation
- Without clear objectives there is no clear direction for Risk Management
- The risks that have to be mitigated are the risks that influence or threaten (the achievement of) the (strategic) objectives of the organisation
- Each component in the framework has to act on all objectives in order to be successful

**Process:**
Risks may arise from factors that are external to the organization. Further, in an attempt to pursue objectives, the organization might make internal changes that could result in exposure to risks. An effective ERM process takes cognizance of both external and internal context in which the Company operates. This entails understanding the external environment and internal objectives of the Company/ Departments as relevant in order to ensure that risks identified are in context of the same.

**Consideration of external context**
The following are indicative factors that need to be considered/ understood from an external context perspective:

- New/ changes in policies or regulations that may affect the business decisions at a Sector/ Company level
- Competitive landscape and position taken by competitors
- Supplier Company, partners, alliances
- Political scenario at the state and centre in India as well as the scenario in the countries where PSFL has business interests (E.g. Europe)
- Economic condition in the states/ countries of operation
- Social factors that may affect the decisions pertaining to a project
- Technological changes applicable to each business

External context in which the Company operates may be determined using the following techniques:
- Porter's five forces
- PESTLE analysis
- SWOT analysis

**Consideration of internal context**
The following need to be considered/ understood from an internal context perspective:

- Strategy and objectives of the Company/ Department/ Corporate Services
- Inherent strengths and weaknesses/ vulnerabilities of the Company/ Departments.
- Organization structure and expected roles & responsibilities
- Values & beliefs
- Profile of people (qualification/ experience and its relevance to their role)
- Incentive mechanisms and how it is expected to drive behaviours
- Systems and processes
- Supervision and monitoring mechanisms

**Objective Setting**
At PSFL, business/ corporate objectives are set by the top management. The operating management prepares Functional/ Processes level objectives that are aligned with overall corporate objectives. Every setting of objectives is an essential precondition before management can identify and assess risks with

respect to them and take necessary actions to respond to those risks.
PSFL's objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity.

**Categorization of Objectives**
PSFL's business objectives can be categorized into following:
- **Strategic –** relating to high-level goals, aligned with and supporting the entity's vision.
- **Operations** – relating to effectiveness and efficiency of the entity's operations, including performance and profitability goals.
- **Reporting –** relating to the effectiveness of the entity's reporting. They include internal and external reporting and may involve financial or non-financial information.
- **Compliance –** relating to the entity's compliance with applicable laws and regulations.

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

Risk appetite, established by management with oversight of the Board of Directors, is a guidepost in strategy setting. Risk appetite can be expressed as the acceptable balance of growth, risk, and return, or as risk adjusted shareholder value-added measures. Risk appetite can be expressed in quantitative or qualitative terms.
The risk appetite statements are generally articulated under following key parameters
**Financial parameters** which provide the threshold in terms of
- Impact on annual budgeted revenue
- Impact on annual budgeted profit
- Impact on project Internal Rate of Return (variation from cost of capital)
- Impact on project NPV (variation from projected cash flows)
- Impact on budgeted costs/ cost to completion in case of projects in construction stage

**Other qualitative parameters** have been articulated that set out the appetite with regard to-
- Environment, Health and Safety
- Business disruption/ project delays
- Legal issues
- Position with the regulator
- Reputation parameters with respect to specific stakeholders o Investors, analysts, lenders and rating agencies
- Key customers
- Key vendors/ alliance partners
- Employees o Media/ general public

Risk appetite shall form an integral part of the risk management framework to demonstrate common understanding of the same, and to consistently measure risks across the Company.

## Alignment of Objectives with risk appetite

There is a relationship between an entity's risk appetite and its strategy. ERM, applied in strategy setting, helps management select a strategy consistent with its risk appetite. If the risk associated with a strategy is inconsistent with the entity's risk appetite, the strategy should be revised. Higher the risk appetite, more aggressive can be the strategy.

Management addresses the following questions while considering its risk appetite in setting strategies to achieve objectives:
- What risks will PSFL accept and what risks will it not accept?
- Is PSFL comfortable with the amount of risk accepted, or to be accepted, by each of its Business Functions/ Processes or line of products?
- What levels of risk is PSFL prepared to accept on new initiatives in order to achieve the company-wide desired return on investment?

## Risk Identification

**Purpose:**

- Identify which events are potentially of influence on (the achievement of) the strategy and objectives.
- This step involves current as well as future events
- ERM recognises two types of events: internal and external -
- Internal events such as a strike, lack of quality checks or fraud control, etc.
- External events such as an earthquake, crash of the stock market, etc.

**Process:**
Risk identification is the mechanism of identifying exposure to uncertainty across the Company. This involves assessment of the external environment within which the Company operates, as well as the internal context of the Company/ Departments.

As part of risk identification, a comprehensive list of risks is generated based on events (historical and anticipated) which may prevent, degrade, accelerate or delay the achievement of business objectives. It shall also include risks associated with not identifying/ evaluating opportunities pursuant to the organization's strategic, project or business objectives, otherwise being pursued by competing organizations.

The risk causes, source, events, situations or circumstances which could have a material impact on the business objectives of the Company shall also be identified during this phase.

Risks for each Department and overall Company shall be documented in individual risk registers. The ownership of these risk registers shall lie with individual Departments; however the ERM function shall assist in creating and updating the registers.

Risks once identified shall not be deleted. In case a risk becomes irrelevant, the status of the risk shall be updated to reflect the same.

Monitoring of existing risks and identification of new events on an ongoing basis is important to ensure that the inventory of events is kept current and updated. As the business environment changes over time, it is critical to have processes in place to continuously monitor and review the completeness and accuracy of the event inventory. Event identification may be carried out as and when new objectives are identified, during independent risk reviews, such as Internal Audit, Management brainstorming sessions etc.

It shall be performed by each employee during the course of his work and particularly at the time of any significant decision, initiation of new Bid/Opportunity, during project planning and execution and periodically during the life of every operating asset. While the ERM department shall assist in risk identification, it is the responsibility of each Department to identify risks.

Risk identification involves identifying potential sources/ root cause of risk events. The purpose of identifying potential root causes is to give direction to risk intervention measures. The fact that one risk might have multiple root causes also needs to be considered. As a part of the risk identification process, it is also important to understand which of the business drivers are impacted by the materialization of a risk or any of its root causes.

**Risk categorization**
In order to facilitate an objective assessment of identified risks, these are categorized in terms of nature of impact on the objectives. The ERM program would cover the following four main types of risks: • Strategic risks: Risks that impact the strategic objectives of the division or Company

- Financial risks
- Credit Risks
- Market Risks
- Operational risks
- Supply Chain & Operations Risks
- IT and Security
- HS&E
- HRM
- Regulatory & Compliance Risks

Depending on their nature of activities, each Department in PSFL would be involved in assessing and mitigating one or more types of above risks.

There is a possibility that one element may primarily belong to one business objective and at the same time may also be mapped to an extent to another objective to some extent. This overlap depends on the facts and circumstances of each case. The process owner may decide to categorise such event to the best possible fit, which enables most effective risk management.

## Risk Assessment and Evaluation

**Risk assessment**

Risk assessment refers to the process followed to comprehend the nature of risk and determine the level of risk. Risk assessment is intended to provide inputs for risk evaluation.

Risk assessment provides a standard and consistent process for PSFL and its Business Units / Functions to consider the extent to which potential events might have an impact on achievement of its objectives. It provides PSFL management with a portfolio view of risks, i.e. a "risk profile".

During this process, events with a potential of impacting objectives are assessed and included in the overall risk profile of the respective Business Functions/ Departments. Risk profiles of the various Departments are combined to form a portfolio view of risk at the Corporate level.

Risk analysis refers to the process followed to comprehend the nature of risk and determine the level of risk. Risk analysis is intended to provide inputs for risk evaluation.

Risk analysis shall be performed for each risk identified. The onus of risk analysis is with the risk identifier, who may choose to consult with the ERM department for this purpose. Based on the results of the analysis, appropriate action shall be taken (risk escalation and risk treatment).

**Techniques of risk analysis**

Risk analysis involves consideration of-

- Risk velocity – How quickly is the risk likely to manifest itself
- Likelihood of risk events – How frequently the event / risk is likely to occur
- Impact of risk – Quantum of the effect of the event / risk

**Consolidate risks**

Each Department shall arrive at a number of top risks for their respective entities. These top risks shall then be prioritized at the Department level. Similarly, top risks for all Department shall be consolidated and prioritized to arrive at a portfolio of top risks for the Company.

In order to visually depict the prioritization, a "heat map" (graphical representation of impact and likelihood) maybe used based on the risk analysis (i.e. Likelihood * Impact) wherein each risk will be plotted on the "heat map" based on its relative likelihood and impact. The placement of the risks on the

"heat map" will indicate the risk zone (High/ Medium/ Low) for each of the respective risks. The heat map shall also form the basis of escalation as and when new risks are identified.

**Risk evaluation**

Risk evaluation is the process to determine whether the risk and/ or its magnitude is acceptable or tolerable.

The intent of risk evaluation is to:

- Enable escalation to the appropriate level of Management as per risk measurement criteria
- Prioritize for treatment implementation

Risk evaluation helps ensure appropriate resource allocation for the purpose of risk treatment and channeling of Management attention towards risks of significant concern.

Risk evaluation will involve risk prioritization for Department and the Company. Risk evaluation shall be done individually and collectively by Risk Management team / Steering Committee at various levels.

a) **Risk escalation**

A critical element of ERM is an effective system of escalation which ensures that specific issues are promptly communicated to relevant authorities. In the context of the Company, escalation may stem from one or more of the following:

- Identification of new risks at Department/ Company level
- Change in impact/ likelihood of identified risks causing a change in the risk evaluation • Unforeseen contingencies

It is to be noted that at each level of escalation, the risk shall be reassessed so that only the key risks are filtered upwards on a timely basis.

b) **Risk prioritization**

The ranking of risks in terms of net potential effect provides Management with some perspective of priorities. This should assist in the allocation of capital and resources in the business. Although the scales of quantification will produce an automated ranking of risks, Management may choose to raise the rank of certain risks for other reasons. This may be justified because of non-financial influences such as media implications, social responsibilities or regulatory pressures. The ranking of risks should be shaped by strategic and business objectives. The prioritized risks must be compared with the risk appetite and all risks falling beyond the acceptable appetite must be short listed for risk treatment.

## Risk Treatment

Risk treatment involves selecting one or more options for managing risks, and implementing such action plans. This phase of the ERM process is intended to:

- Understand existing controls/ mitigation mechanisms in place for managing risks
- Generate a new risk treatment plan
- Assess the effectiveness of such treatment plans

Risk mitigation relates to the policies, procedures, processes and other actionable steps implemented to address the risks associated with specified future events. Response to a risk has to be considered in light of costs to be incurred and consequent benefits (typically measured in terms of as estimate of the quantum of reduction in risk exposure).

Business risks are normal for any organization and as much as it is for PSFL. It is not the intent in all cases to minimize, avoid or eliminate all risks that are identified. However, it is the intent that all PSFL Business Units/ Functions/ Processes understand the significant events that may impact business objectives and the associated risks. This is achieved by establishing a standard and consistent process for developing an acceptable risk response.

Steps for risk treatment:

- Evaluate the strategic mitigations in place for key risks
- Evaluate control requirements
- Verify and evaluate the controls currently in place for key risks
- Identify and evaluate the post event measures in place for risk
- Review the financial risk protection measures in place to respond to the consequences of risk events
- Take decisions on the acceptability of identified risks and controls
- Document action plans for risk mitigation
- Use the outputs of risk assessments for budgeting and capital allocation processes

## Risk Monitor, Review and Report

Risk monitoring shall be conducted by each Department on a monthly basis, for identified risks, in order to track the status of treatment plans and consequently update changes to risk profiles.

Risk reviews shall be conducted to enable continuity of the ERM process. Risk reviews entail the reassessment of all risks recorded in the Company, Department level risk registers along with new/ emerging risks to ensure concurrence and relevance of risks and their treatment. Risk reviews will be carried out at a minimum on a quarterly basis.

The ERM function shall assist the monitoring and review process at the Department/ Company level. The ERM function shall ensure that results of the monitoring process depicted in the form of risk reports are reported internally and externally, as appropriate.

## Managing materialized risks

In the event of a particular risk materializing, it is necessary to have in place a crisis/ incident management plan for timely and effective management of such events. The incident management plan is a set of well-coordinated actions aimed at preparing and responding to unpredictable events with adverse consequences. The intention of this plan is to preserve the confidence of internal and external stakeholders in the Company's risk readiness for potentially adverse events. The Company recognizes the need for and shall design such a plan that will detail:

- The situations for which action plans shall be invoked
- The manner in which such plans shall be actioned
- The individuals/ departments involved in such planning and execution.

## Document management

The ERM framework is owned by the Chief Risk Officer. Changes to the document need to be processed through the owner, and require the consensus of the Board for ratification.

The framework shall be reviewed annually to ensure that the intent of the same and its covenants are relevant to the Company and its entities.

The ERM department shall ensure that updates to the framework are communicated across the organization, and shall also be responsible for promoting risk awareness across the Company. The ERM function may use tools, workshops, newsletters, formal training sessions, and undertake other initiatives as deemed required for this purpose.

## Record retention

For the purpose of ensuring traceability of ERM activities, documentation shall be maintained in physical or electronic form and retained as defined by the Company's Corporate Record Retention Standards.

Records, both physical and electronic, at an Enterprise level shall be maintained by the ERM function on behalf of the Board of Directors.

However, those at the business and Sector levels shall be maintained by Department representatives designated for this purpose.

## Effective Date:

This Policy shall be effective from **November 1, 2023**.