
# Sun Pharmaceutical Industries Limited (SPIL)

## Synopsis of Enterprise Risk Management Policy

May 2022

## 1. Introduction

*Risk, as defined by ISO 31000:2018 (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 Sun Pharmaceutical India Limited (herein referred to as "SPIL") vision, mission and objectives. ERM is aimed at protecting and enhancing stakeholder value by establishing a suitable balance between harnessing opportunities and containing risks.*

SPIL is exposed to a various risk from strategic, regulatory, alliance, operational and financial perspectives. The Board of Directors of SPIL (hereinafter referred to as the 'Board') are responsible for developing an Enterprise Risk Management framework within the organization that enables proactive identification, management, monitoring and reporting of various risks that the organization may need to deal with. This is a requirement as per the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements), 2015. SPIL is also required to have an Enterprise Risk Management (hereafter ERM) framework on account of the following regulatory requirements:

Companies Act 2013 requires that:

- Section 134: The board of directors' report must include a statement indicating development and implementation of a risk management policy for the company including identification of elements of risk, if any, which in the opinion of the board may threaten the existence of the company.

- Section 177: The audit committee shall act in accordance with the terms of reference specified in writing by the board, which shall, inter alia, include evaluation of risk management systems

- Schedule IV: Independent directors should satisfy themselves that systems of risk management are robust and defensible

**Applicability**

ERM framework is applicable across SPIL and extends to all its business units, subsidiaries and functions. This policy underpins our efforts to remain a competitive and sustainable company, enhancing our operational effectiveness and creating wealth for our employees, shareholders and stakeholders. It describes the organization's risk management processes and sets out management requirements in generating risk management action.

While the risk management framework is designed to help the organization meet its objectives, there can be no assurance that risk management activities will mitigate or prevent these, or other, risks from occurring.

The policy will be reviewed at periodic intervals. However, updates may be made earlier if there are any changes in the risk management regulations / standards or as may be deemed appropriate by the management.

## 2. 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 organization. The ERM framework for the organization has been developed keeping in mind the needs of internal and external stakeholders. The organization's ERM framework is based on the 'Risk Management – Principles and Guidelines' developed by the International organization for Standardization (ISO 31000:2018 - 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 organization's endeavor to build world class ERM framework and processes.

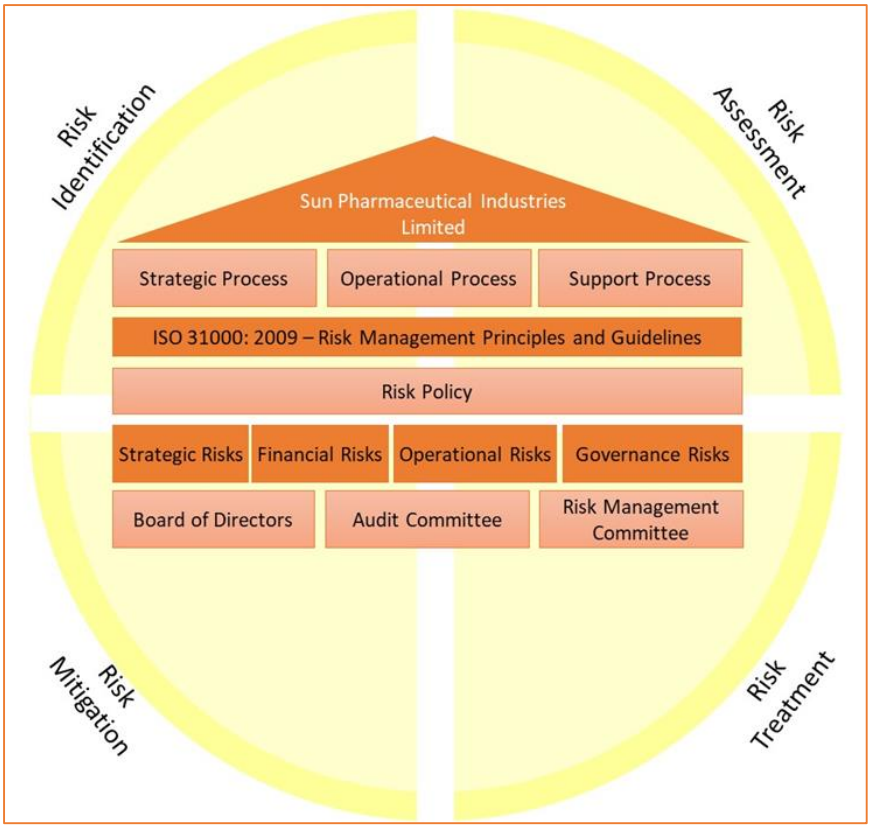


Figure 1.1: ERM framework

## Components of the ERM Framework

The ERM framework at SPIL consists of the following components/phases:

1. **Risk Identification:** Function heads identify internal and external events that may have an adverse impact on the achievement of our Company's objectives. These risks are captured in the form of a risk register with all the relevant information such as risk description, root cause and any existing mitigation plans.

2. **Risk Assessment:** Risks identified are assessed/ rated on likelihood and impact based on the risk appetite defined for SPIL by senior management members. Based on the risk rating, top risks for the organization are prioritized for developing the risk mitigation plan.

3. **Risk Treatment:** Mitigation plans are developed by respective risk owners for risks owned by them. Well defined action plans are agreed upon with timelines for implementation. Mitigation plans are discussed with the senior management to seek buy-in and approval

4. **Risk Monitoring:** Management defines a periodic process for reviewing risks and their mitigation plans. It also defines the Risk Management roles and responsibilities across the organization. The Risk management committee reviews the status against the action plans agreed with the risk owners. Periodically an update is provided to the Board and Audit committee on the risks.

Similarly, there is a defined process to ensure that new risks are escalated appropriately and existing risks are reviewed periodically considering the change in the business environment. In case of adverse events, management shall apprise all relevant stakeholders of the same. Based on the materiality of the event, management may also share updates with the Board. In any case, every six months, the Board shall be apprised of any new risks that may have emerged during the period

**Accountability**

Individual Functional heads are responsible for managing risks owned by them. They are responsible to identify and implement risk mitigation plans in line with leading industry practices/trends or as adopted / agreed by senior management to bring those risks within tolerable limits. Select risk management teams are listed below along with the areas of risk for which they may have responsibility.

## 3. Risk Management organization structure

The Risk Management Organization structure (RMO) defines the roles and responsibilities of key internal stakeholders for developing, implementing and maintain the ERM initiative on an ongoing basis. The RMO aligns individuals, teams and functions with the intent of establishing responsibility and accountability with regard to:

1. Monitoring effective implementation of the ERM framework
2. Update the ERM framework and its components on an ongoing basis based on business needs
3. Embedding ERM into the organization's culture

The overall structure and roles for the ERM framework is summarized below:

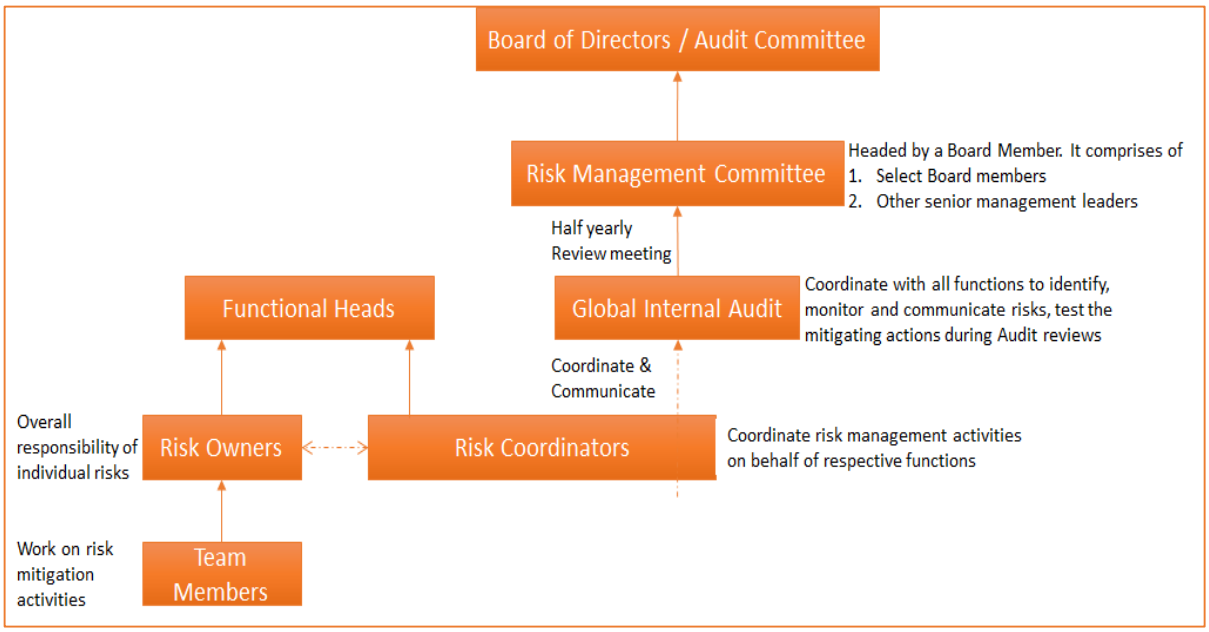


Figure 1.2: Risk Management Organization Structure

## 4. Roles and Responsibilities of key stakeholders

Summarized roles and responsibilities of key stakeholders are enumerated below.

| Stakeholder | Summarized Roles and Responsibilities |
|---|---|
| Board of Directors / Audit Committee | • Review the risk management related inputs basis framework periodically and provide feedback for improvements if any<br>• Evaluate effectiveness of the ERM framework adopted by the management<br>• Provide necessary guidance to Risk Management Committee for effective monitoring of risks<br>• Approve the risk management framework and policy for SPIL in coordination with the Risk Management Committee<br>• Provide overall oversight and direction to the risk management process including inputs and oversight on key strategic risks |
| Risk Management Committee (RMC) | • Formulate a detailed Risk Management Policy that includes<br>• A framework to identify the internal and external risks covering financial, operational, sectoral, sustainability, information or cyber security related risks or other risks determined by the Risk Management Committee<br>• Measures for risk mitigation including systems and processes for internal control of identified risks<br>• Business Continuity Plan<br>• Ensure that appropriate methodology, process and systems are in place to monitor and assess the company's business risks<br>• Monitor and oversee the implementation of risk management policy; evaluate the adequacy of ERM systems<br>• Review the risk management policy at least once in two years, including by considering the changing industry dynamics and evolving complexity<br>• Keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken<br>• Review status of treatment plans implemented for prioritized risks.<br>• Provide inputs and support in performing risk management activities in coordination with the Audit Committee. Establish procedures and timelines for various risk management activities |

| Stakeholder | Summarized Roles and Responsibilities |
|---|---|
| Global Internal Audit | • Maintain the risk register for all functions, business units, subsidiaries and countries<br>• Review the risk registers to ensure adequacy of risk management<br>• Monitor the trends and factors impacting the risk profile of the organization, communicate the information internally and document updates to risk register.<br>• Work closely with respective risk coordinators and risk owners as well as function heads to ensure action items against each risk area are in place.<br>• Facilitate implementation of the ERM framework (in liaison with the risk coordinators) within the organization and its underlying business units, subsidiaries and functions.<br>• Track progress of implementation of risk treatment plans for significant risks<br>• Co-ordinate in preparation and submission of risk reports to the Risk Management Committee and Audit Committee. Highlight any differences of opinion<br>• Share feedback from Audit Committee and Risk Management Committee to the relevant function heads, risk owners and coordinators<br>• Align the Audit plan with the risk register<br>• Validate the effectiveness of mitigation plans |
| Function Heads | • Assume primary responsibility for identifying, assessing and managing business, operational and compliance risks within their area of responsibility.<br>• Conduct periodic function meetings/ brainstorming sessions with the below objectives:<br>a. Review updated risk registers for the business unit / function and evaluates need for inclusion of new / emerging risks<br>b. Check status of implementation measures and effectiveness of existing controls. Implement additional measures to reduce risk exposures to an acceptable level<br>c. Identify reasons for any risks that may have materialized and implement action plans to strengthen the mitigating steps<br>d. Assist with implementation of procedures for proactive review of risks for projects, transactions, new businesses, etc.<br>e. Review the potential of any risk materializing in the near future which has a major impact for the Company |
| Risk coordinator | • Coordinate risk management activities<br>• Facilitate and support respective functions in collaboration with the ERM team in identifying, assessing, evaluating, prioritizing, monitoring and reporting of risks |

| Stakeholder | Summarized Roles and Responsibilities |
|---|---|
| Risk Owners | • Take overall responsibility for managing individual risks in line with ERM framework.<br>• Coordinate with the Function heads in deciding appropriate risk treatment plans for risks assigned<br>• Identify new or emerging risks and propose treatment plans on an ongoing basis should be within the risk owner's area of operation<br>• Monitor the progress of risk treatment plans on a monthly basis and review risks on a quarterly basis and provide periodic reports to the Function heads. |
| Team members | • Work closely with the risk owner and risk coordinator in taking steps to mitigate / reduce the risk |

## 5. Risk Appetite

**Risk appetite** is the amount of risk that the organization is willing to pursue or retain in pursuit of its objectives. In other words, the organization will take risks which do not result in the breach of its appetite. The risk appetite statements are articulated under three key parameters

Financial parameters which provide the threshold in terms of

1. Impact on targeted annual sales
2. Impact on annual budgeted profit (EBITDA)

**Other qualitative/reputational parameters** have been articulated that set out the appetite with regard to

1. Environment, Health and Safety
2. Business disruption
3. Legal and Regulatory matters
4. 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 organization.