Sun Pharmaceutical Industries Limited (SPIL)

Synopsis of Enterprise Risk Management (ERM) Policy

May 2024

Introduction (1/2)

SPIL is a global pharmaceutical company that consistently cares for Life and delivers on its commitments to all stakeholders - patients, regulators, customers, partners, employees, investors, and the community.

Risk Management is integral to SPIL's strategy and the achievement of the Company's long-term and short-term goals. Our success as an organization depends on our ability to identify and leverage the opportunities created by our business and the markets we operate in. To this end, the Company takes an embedded approach to Risk Management, which puts risk and opportunity assessment at the core of the Board's agenda.

The Enterprise Risk Management Policy is framed considering various types of risks faced by the Company, viz. strategic, financial, operational, sectoral, geopolitical, information technology, cyber security, environmental, sustainability, social, governance, third-party, etc., to have a better management and reporting system for such risks and to take appropriate action after assessing such risks on a timely basis.

Regulatory Requirements

The Risk Management Policy of SPIL is framed as per the following regulatory requirements:

1. **The Companies Act, 2013**
   a. Provisions of Section 134 (3) There shall be attached to financial statements laid before a Company in general meeting, a report by its Board of Directors, which shall include — 134(3)(n) a statement indicating the 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.

   b. Section 177(4) (vii) stipulates: 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.

Introduction (2/2)

2. Schedule IV of Companies Act 2013, [Section 149(8)] Code for Independent Directors:

a. Role and functions: The independent directors shall:

- Help bring an independent judgment to bear on the Board's deliberations, especially on strategy, performance, risk management, resources, key appointments and standards of conduct.
- Satisfy themselves with the integrity of financial information and that financial controls and risk management systems are robust and defensible.

3. SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2021: Reference: SEBI/LAD NRO/GN/2021/22 on 5 May 2021

a. The role of the committee shall, among other things, include the following:

- To formulate a detailed risk management policy, which shall include:
  - ✓ A framework for identifying internal and external risks the listed entity faces, including financial, operational, sectoral, sustainability (particularly, ESG-related), information, cyber security risks or any other risk as may be determined by the Committee.
  - ✓ Measures for risk mitigation, including systems and processes for internal control of identified risks.
  - ✓ Business continuity plan.
- To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.
- To monitor and oversee the implementation of the risk management policy, including evaluating the adequacy of risk management systems.
- To periodically review the risk management policy, at least once every two years, including by considering the changing industry dynamics and evolving complexity.

Scope and Objectives (1/1)

Scope:
ERM framework is applicable across SPIL and extends to all its business units, subsidiaries and functions.

Objectives:
This policy describes the organization's risk management processes and sets out management requirements for generating risk management action. It emphasizes SPIL's efforts to remain a competitive and sustainable company, enhancing operational effectiveness and creating wealth for our employees, shareholders and stakeholders. It seeks to identify risks inherent in the Company's business operations and provides guidelines to define, measure, report, control, and mitigate the identified risks.

Enterprise Risk Management at SPIL (1/2)

SPIL has an established Enterprise Risk Management (ERM) Framework and process to ensure the achievement of its strategic objectives.

ERM is an integrated approach to proactively manage risks that
1. affect the achievement of SPIL's vision, mission and objectives;
2. impact brand or reputation;
3. manage uncertainties and vulnerabilities;
4. threats to existence, etc. ERM aims to protect and enhance stakeholder value by balancing harnessing opportunities and surrounding risks.

The organization's ERM framework is based on several good practices recommended by:
1. The Committee of Sponsoring Organizations (COSO) ERM framework;
2. Risk Management Guidelines published by the International Organization for Standardization (ISO 31000:2018);
3. Risk management – Code of practice and guidance for the implementation (British Standard (BS 31100:2011));
4. Governance Risk Compliance Capability Model published by Open Compliance and Ethics Group (OCEG);
5. Risk Management Standard published by the Federation of European Risk Management Associations (FERMA).

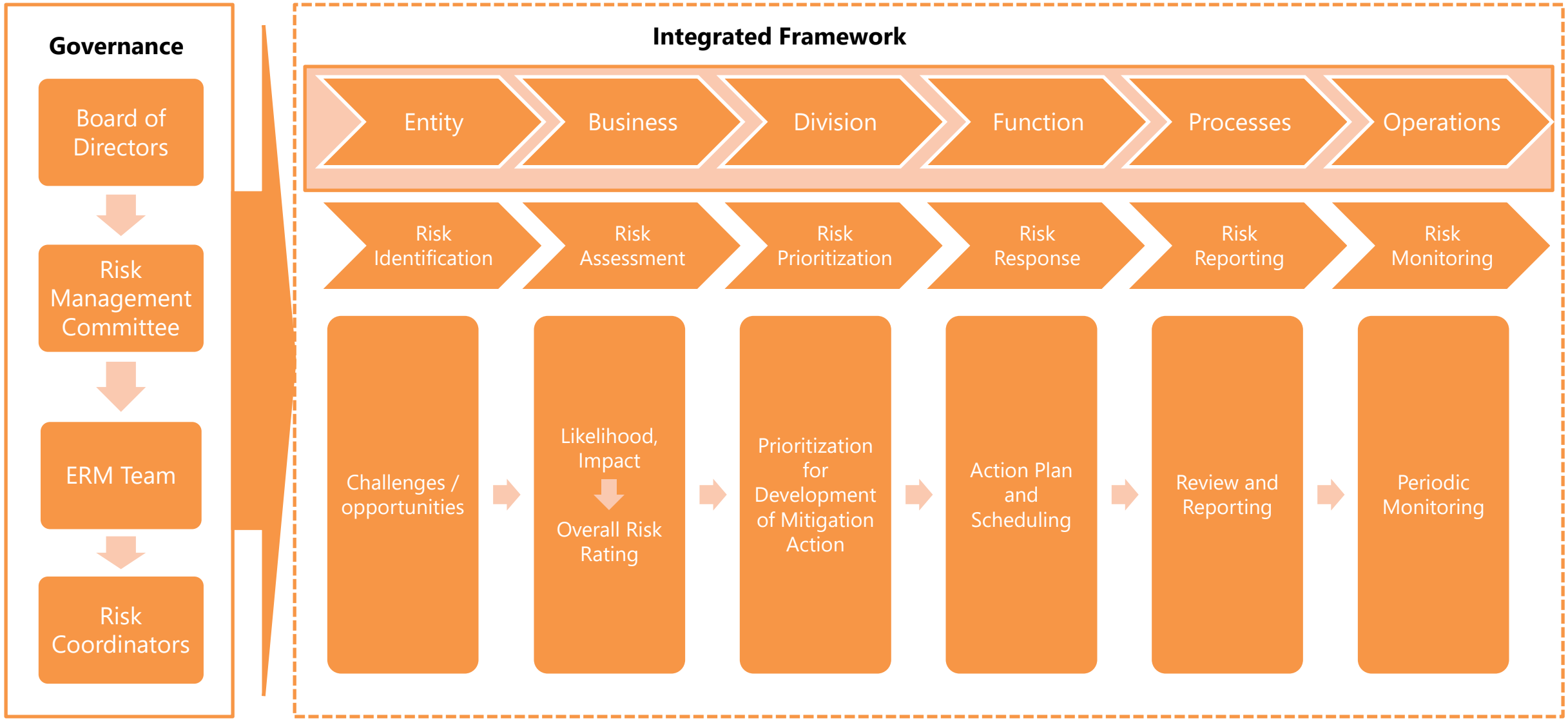
Risk Management is a continuous process that is accomplished throughout the life cycle of a Company. SPIL ERM framework helps identify potential events that may affect the enterprise, manage the associated risks and opportunities, and provide reasonable assurance that our Company's objectives will be achieved. It is an organized methodology for continuously identifying and measuring the unknowns, developing mitigation options, selecting, planning, and implementing appropriate risk mitigations/optimizations, and tracking the implementation to ensure successful risk optimization.

Enterprise Risk Management at SPIL (2/2)

In order to fulfil the objectives of this policy and lay a strong foundation for the development of an integrated risk management framework, the policy outlines the following guiding principles of risk management:

1. We acknowledge that all activities involve risk and that not all risks can or should be transferred.
2. We acknowledge that no risk management system can address every risk; the goal is to ensure that prioritized risks are managed within acceptable levels.
3. Since many risks can impact our reputation, all risks must be evaluated in terms of potential impact.
4. Risk issues will be identified, analyzed and ranked consistently. Standard systems and methodologies will be used.
5. The risk mitigation measures adopted by the company shall be effective in the long term and, to the extent possible, embedded in the company's business processes.
6. Risk tolerance levels will be regularly reviewed and decided upon based on changes in the company’s strategy.

Enterprise Risk Management (ERM) Integrated Framework (1/1)



Enterprise Risk Management Process (1/2)

Risk Identification and Categorization at SPIL

Risk Management is a continuous process accomplished throughout the organization's life cycle. Effective Risk Management covers risk management planning, early identification and analyses of risks, implementation of corrective actions, continuous monitoring and reassessment, communication, documentation and coordination.

Enterprise Risk Management Process (2/2)

Risk Identification:
This step involves understanding and listing the potential threats that may affect the realization of the organization's objectives.

Function heads identify internal and external events that may harm the achievement of the Company's objectives. It also focuses on identifying new emerging risks and additional risks/concerns that may arise while implementing the action plan for existing risks. These risks are captured as a risk register with all the relevant information, such as risk description, root cause, existing mitigation plans, etc.

Risk Assessment and Prioritization:
Risks identified are assessed/rated on likelihood and impact based on the risk appetite defined for SPIL by senior management members. The process of identifying the likelihood and impact of risk events is both a quantitative and qualitative process of analysis. Based on the risk rating, the organization's top risks are prioritized for developing the risk mitigation plan.

Risk Response:

Respective function heads develop mitigation plans for risks they own. Well-defined action plans are agreed upon, along with timelines for implementation. Mitigation plans are discussed with the senior management to seek buy-in and approval. The activity or situation posing a risk may be reduced, accepted, shared, transferred, or avoided depending on the facts and circumstances.

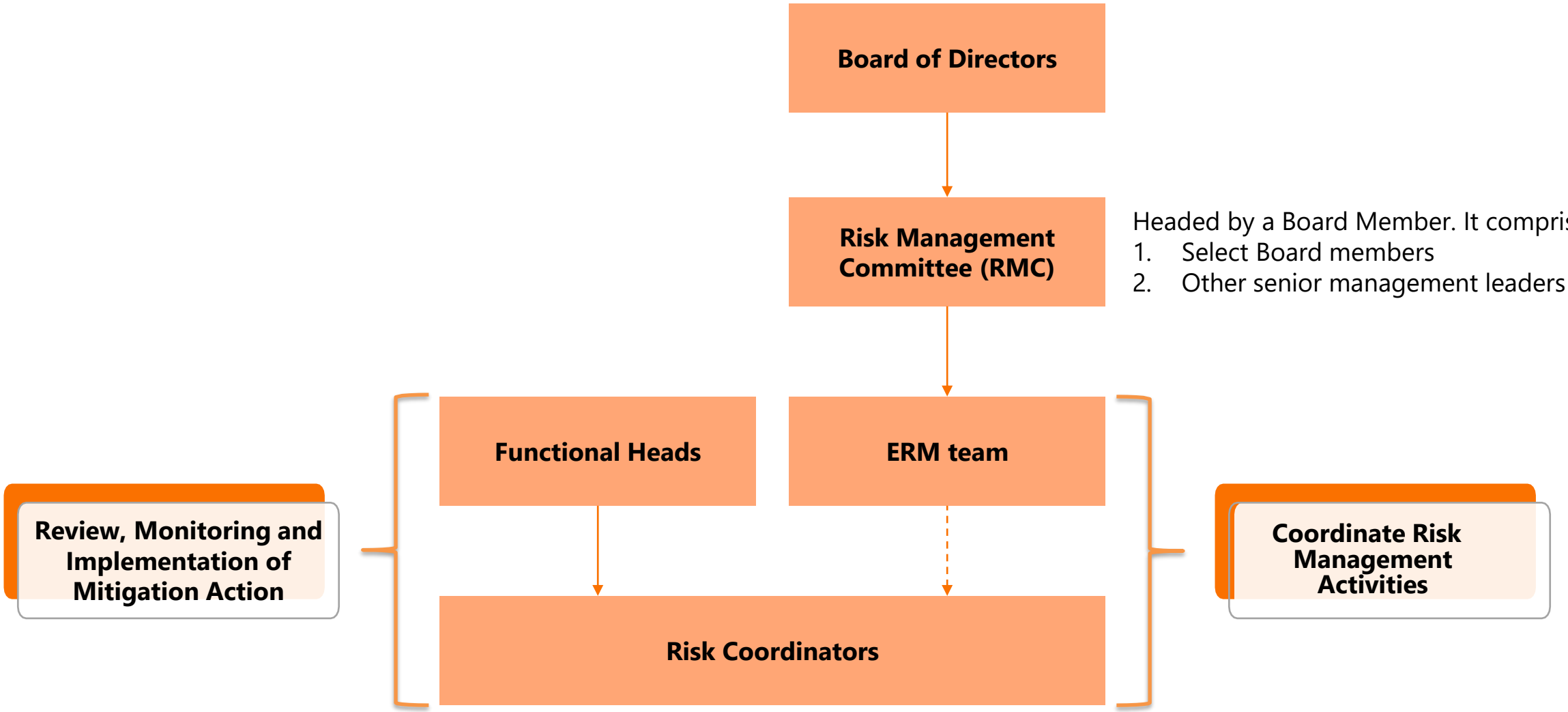
Risk Reporting:

The ERM team and respective risk coordinators/functional heads review all risks. Key risks are periodically reported to the Senior Management/Risk Management Committee.

Risk Monitoring

Management has defined a periodic process for reviewing risks and their mitigation plans. The Risk Management Committee periodically reviews the status of the action plans for key risks, as agreed upon with the risk coordinators/function heads.

Risk Management Governance Structure (1/1)



Headed by a Board Member. It comprises of

1. Select Board members
2. Other senior management leaders

Roles and Responsibilities of Key Stakeholders (1/3)

Department / Committee	Summarized Roles and Responsibilities
Board of Directors	• Review the risk management-related inputs based on the framework periodically and provide feedback for any improvements. • Evaluate the effectiveness of the management's adoption of the ERM framework. • Provide necessary guidance to the Risk Management Committee for effective monitoring of risks. • Approve the Risk Management Framework and Policy for SPIL in coordination with the Risk Management Committee. • 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: ✓ Framework for identifying internal and external risks specifically faced by the listed entity, including financial, operational, sectorial, sustainability (particularly, ESG-related risks), information, cyber security risks or any other risk as may be determined by the Risk Committee. ✓ Measures for risk mitigation, including systems and processes for internal control of identified risks. ✓ Business continuity plan. • Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the company's business. • Monitor and oversee the implementation of risk management policy, including evaluating the adequacy of risk management systems. • Periodically review the risk management policy at least once every two years, including by considering the changing industry dynamics and evolving complexity. • Keep the board of directors informed about the nature and content of its discussions, recommendations, and actions to be taken. • Review the status and adequacy of mitigation plans implemented for prioritised risks. • Provide inputs and support in performing risk management activities. Establish procedures and timelines for various risk management activities.

Roles and Responsibilities of Key Stakeholders (2/3)

Department / Committee	Summarized Roles and Responsibilities
ERM Team	• Maintain the risk register for all business units/support functions. • Ensure adequacy of the risk management process. • Facilitate implementation of the ERM framework (in liaison with the risk coordinators) within the organization and its underlying business units. • Work closely with respective risk coordinators to ensure action items against each risk area are in place. • Track the progress of implementation of risk treatment plans for significant risks. • Coordinate the preparation and submission of risk reports to the Risk Management Committee. • Share the Risk Management Committee feedback with the relevant function heads and coordinators.

Function Heads	• Assume primary responsibility for identifying, assessing and managing risks within their area of responsibility.
	• Conduct periodic function meetings/ brainstorming sessions with the below objectives:
	  • Monitor the trends and factors related to the respective business unit/support function impacting the company's risk profile, communicate the information internally and coordinate the updates to the risk register.
	  • Review of updated risk registers for the respective business unit/support function and evaluation of the need to include new/emerging risks.
	  • Check the status of implementation measures and the effectiveness of existing controls. Implement additional measures to reduce risk exposures to an acceptable level.
	  • Identify reasons for any risks that may have materialized and implement action plans to strengthen the mitigating steps.
	  • Assist with implementing procedures for proactively reviewing risks for projects, transactions, new businesses, etc.
	  • Review the potential risk to the respective business unit/support function materializing shortly, which has a major impact on the Company.

Roles and Responsibilities of Key Stakeholders (3/3)

Department / Committee	Summarized Roles and Responsibilities
Risk coordinator	• Coordinate risk management activities. • Review the risk registers to ensure the adequacy of risk coverage within the respective business unit/support function. • Facilitate and support respective business unit/support function in collaboration with the ERM team in identifying, assessing, evaluating, prioritizing, monitoring and reporting risks. • Work closely with respective business units/support functions to ensure action items against each risk area are in place. • Review the current status of the risk, track the progress of the action plan and periodically submit it to the ERM team.