Chemistry of Success at Work

Enterprise Risk Management (ERM) Policy

Meghmani Organics Limited

Registered & Corporate office

1st to 3rd Floor, Meghmani House
B/H.Safal Profitaire, Corporate Road,
Prahlad Nagar, Ahmedabad 380015
Phone : +91-79-7176 1000
Website : http://www.meghmani.com
Email : helpdesk@meghmani.com
CIN : L24299GJ2019PLC110321

Enterprise Risk Management (ERM) Policy

1. Purpose

The purpose of this Enterprise Risk Management (ERM) Policy is to establish a framework for identifying, assessing, managing, and monitoring risks across Meghmani Organics Limited (MOL). Purpose of this policy is to align and improve current risk management practices with ISO 31000 (Risk Management), ISO 22301 (Business Continuity), as well as the guidelines prescribed by the Securities and Exchange Board of India (SEBI) for listed companies in India.

2. Scope

This policy applies to all business processes of enterprise, operations, departments, and sites under MOL. It covers all categories of risk, including but not limited to strategic, operational, financial, compliance, ESG / sustainability, cybersecurity, and business continuity risks.

3. Objectives

- Establish a unified approach to risk management across the organization.
- Protect organizational assets, reputation, and business continuity by proactively managing risks.
- Enhance decision-making by embedding risk considerations into planning and performance management.
- Ensure compliance with statutory, regulatory, and industry-specific requirements, including SEBI's risk management framework for listed companies.
- Provide a structured approach for assessing, managing, and monitoring risks, ensuring alignment with ISO standards and best practices.

4. Risk Management Principles

Risk management at MOL will be based on the following principles:

1. **Integration into Organizational Processes**: Risk management will be integrated into all organizational processes, including strategy development, project management, operational decision-making, and business planning.
2. **A Structured Approach**: A risk management framework will be followed, incorporating identification, assessment, treatment, and monitoring of risks in line with ISO 31000 and ISO 31010 guidelines.
3. **Holistic Risk View**: Risks will be considered from a holistic perspective, including both internal and external factors, and the interaction between different types of risks will be recognized.
4. **Proportionality**: Risk responses will be proportional to the potential impact of the risk, ensuring that resources are applied efficiently to address risks of higher significance.
5. **Continuous Improvement**: The risk management process will be reviewed regularly and refined based on new insights, lessons learned, and changes in the business environment.

6. **Compliance and Regulatory Alignment**: The organization will adhere to all relevant laws, regulations, and standards, including SEBI's guidelines for risk management, as well as ISO standards to ensure that risks related to environmental, safety, cybersecurity, and financial concerns are effectively managed.

5. Risk Management Process

The ERM process will follow a structured approach aligned with ISO 31000, incorporating the following steps:

1. **Risk Identification**: Systematic identification of risks that could impact the organization's objectives, including strategic, operational, environmental, and regulatory risks.
2. **Risk Assessment**: Evaluation of identified risks to determine their potential impact and likelihood, considering both existing controls and possible risk events. This will be done using risk assessment methodologies such as HAZOP, HIRA, and QRA.
3. **Risk Mitigation or Treatment**: Developing strategies to mitigate, transfer, accept, or avoid risks. This may include process improvements, contingency planning, insurance, and strengthening controls.
4. **Monitoring and Review**: Ongoing monitoring and review of the effectiveness of risk treatments and the emergence of new risks. Regular risk audits and reviews will ensure continuous improvement of the risk management framework.
5. **Communication and Reporting**: Clear communication of risks and risk management activities across all levels of the organization. Risk reports will be escalated to the leadership team and communicated to relevant stakeholders. Regular risk assessment reports to the Risk Management Committee and CMD. Quarterly updates to the Board of Directors on key enterprise risks. Transparent communication with stakeholders regarding ESG and sustainability risks
6. **Business Continuity Planning**: Disaster recovery measures for critical business functions.

6. Roles and Responsibilities

- **Board of Directors**: Ensure that the organization has an effective risk management framework in place and that risk management activities are integrated into strategic decision-making. This includes compliance with SEBI's risk management guidelines for listed companies.
- **Executive Management**: Provide leadership and support for the implementation of risk management across the organization and ensure that risk management is integrated into organizational processes.
- **Risk Management Committee**: Oversee the ERM process, ensuring that risk management is aligned with organizational objectives and provide guidance on risk-related decisions.
- **Site and Department Heads**: Implement risk management practices at the site and department levels, ensuring that risk management processes are followed in all operations.
- **Risk Management Team**: Facilitate the identification, assessment, and management of risks at the enterprise level. Support sites in developing and implementing site-specific risk management plans.

7. **Governance** Structure

- **Board of Directors & Independent Directors**: Ultimate oversight of ERM, ensuring alignment with strategic objectives and regulatory compliance.
- **Chairman & Managing Director (CMD)**: Accountable for enterprise-wide risk management implementation and performance.
- **Risk Management Committee (RMC)**: Monitors risk management activities, approves policies, and reviews key risks periodically.
- **Chief Executive Officer (CEO) & Business Process Heads**: Responsible for integrating risk management into business functions.
- **Functional Heads (EHS, HR, Procurement, Finance, IT, etc.)**: Ensure compliance with risk controls and implementation of mitigation strategies.
- **All Employees & Contractors**: Adhere to risk management policies and report potential risks.

8. **Risk** Categories:

Indicative (not exhaustive list) of risk categories shall be considered for risk management,

- **Strategic Risks**: Market fluctuations (Market Risk), geopolitical instability, and ESG non-compliance.
- **Operational Risks**: Chemical process safety, regulatory compliance (GPCB, DISH, PESO), and catastrophic failures.
- **Financial Risks**: **Credit Risk,** Liquidity Risk, Interest Rate Risk Foreign exchange volatility, supply chain disruptions, and pricing instability.
- **Regulatory Risks**: Compliance Risk, Changes in environmental permits and government regulations.
- **Business Continuity Risks**: Disruptions in utilities, transportation failures, and labour strikes.
- **Cybersecurity Risks**: Data breaches, hacking, and IT system failures.
- **Ethical Risks**: Corruption, fraud, bribery, and governance issues.
- **Business Operation Risk**: Raw material process, fall in competitive prices, on-availability of materials, obsolescence of technology, reputation risk etc.

9. **Policy Review and Updates**

This policy will be reviewed at least once every three years or as required based on major regulatory changes, market conditions, or internal risk assessments.
This Enterprise Risk Management Policy serves as the apex document for all sub-policies related to risk management at the site level. It ensures a consistent and unified approach to risk management across MOL, while also aligning with SEBI's risk management guidelines for listed entities.

10. **Reference:**

In addition to ISO 31000, other supporting standards referred area as ISO 31010, ISO 22301, ISO 27001, ISO 27005, ISO 14001 and ISO 45001.

Note: The above Policy was adopted by BOD in their meeting held on 10 May, 2025.

****