ALEMBIC PHARMACEUTICALS LIMITED

RISK MANAGEMENT POLICY

Details of Adoption / Amendments to the Policy				
Policy Adoption / Change effective Date	**Clause No.**	**Particulars of the Adoption / Change**	**Board Approval Date**	**Version of Policy**
21/01/2016	-	Adoption of Policy	21/01/2016	Original
26/07/2021	-	Adoption of Revised Policy	26/07/2021	Original
01/02/2023	7	Widened the scope to address Disaster Resilience and Business Continuity Plan	01/02/2023	V-2

This Policy was last reviewed by the Risk Management Committee on 3rd February, 2025.

1. 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 Alembic Pharmaceuticals Limited ('APL' 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.

The Board of Directors of APL (the 'Board') are responsible for developing an ERM framework within the organization that enables proactive identification, management, monitoring and reporting of various risks that the organization may need to deal with.

2. Objective:

The Company considers ongoing risk management to be a core component of the management of the Company and understands that the Company's ability to proactively identify risks and mitigate them is a key to achieve success.

The main objective of this Risk Management Policy ('RM Policy' or 'Policy' as the context may require) is to aid sustainable business growth with stability and to promote a proactive approach in reporting, evaluating and resolving risks associated with the business.

This Policy is formulated in compliance with the provisions of Regulation 17(9) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ('Listing Regulations, 2015') and Companies Act, 2013 (the 'Act'), which requires the Board to lay down procedures about risk assessment and risk minimization and framing, implementing and monitoring the risk management plan. This Policy shall be reviewed once in two years (from the date of the last review) by the Risk Management Committee (the 'Committee') after considering the changing industry dynamics and evolving complexity in order to ensure that management of the Company controls risk through means of a properly defined framework.

3. Applicability:

This Policy is applicable across the Company and extends to all its business units and subsidiaries.

4. Effective Date:

The Board had adopted a risk management policy w.e.f. from 21st January, 2016. Pursuant to the amendments in the SEBI Listing Regulations, 2015 from time to time, this revised Policy is adopted in substitution of erstwhile policy and has come into effect from 26th July, 2021 and further amended as per the details mentioned in the table of amendments provided on the first page.

5. Risk Management Process:

The risk management process should be an integral part of management, be embedded in culture and practices and tailored to the business processes of the organization. The risk management process includes four activities viz. Risk Identification, Risk Assessment, Risk Mitigating and Monitoring & Reporting.

i) Risk Identification

The purpose of risk identification is to identify the events that can have an adverse impact on the achievement of the business objectives. All risks identified may be documented in the form of a risk register. The risk register may incorporate the risk description, category, classification, mitigation plan, responsible function / department and other relevant details.

The management shall assess all areas and functions interfacing the business including operational, sectoral, regulatory, environment, sustainability, governance, financial, information technology and cyber security, for risk identification.

The following risk identification techniques may be deployed to enable focused risk identification:

- Preliminary hazard analysis
- Structured interview / interactions and brainstorming
- Scenario analysis
- Business impact analysis

ii) Risk Assessment

Assessment involves quantification of the impact of risks to determine potential severity and probability of occurrence. Each identified risk shall be assessed on two factors which determine the risk exposure:

a) Impact if the event occurs

b) Likelihood of event occurrence
It is necessary that risks are assessed after taking into account the existing controls, so as to ascertain the current level of risk. Based on the above assessments, each of the risks can be categorized as low, medium and high.

iii) Risk Mitigation

The identified risks may be mitigated by implementing any of the following risk mitigation tools:

a) Risk avoidance: By not performing an activity that could carry risk. While, avoidance may seem the answer to all risks but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed and hence should be applied judiciously.

b) Risk transfer: Mitigation by having another party to accept the risk, either in partial or total, typically by contract or by hedging / insurance.

c) Risk reduction: Employing methods/solutions that reduce the severity of the loss.

d) Risk retention: Accepting the loss when it occurs. Risk retention is a viable strategy for small risks where the cost of insulating against the risk would be greater than the total losses sustained.

iv) Monitoring and reviewing Risks

The Committee shall formulate the process / procedures for effective monitoring and reviewing of the risks including risk prioritization analysis. The Committee shall review the risk register as may be prepared by the management on half yearly basis. The identified risks will be taken up with respective functional head for its mitigation. The Committee may apprise the Board of key risks identified along with its mitigation plan on need basis.

6. Oversight and management:

i) Board of Directors

The Board is responsible for reviewing and ratifying the risk management structure, processes and procedures which are developed and implemented by the Committee in consultation with senior management. The Committee may also refer particular issues to the Board for final consideration and direction.

ii) Audit Committee

The Audit Committee shall review the risk management framework including risk management related procedures and risk level parameters that govern the risk management activity within the Company and make suggestions for enhancing or modifying the framework. The Audit Committee may provide necessary support to the Committee in performing their activities.

iii) Risk Management Committee

The day to day oversight and management of the Company's risk management program has been conferred upon the Committee. The Committee is responsible for ensuring that the Company maintains effective risk management and internal control systems and processes, and provides reports to the Board on the effectiveness of the risk management program in identifying and addressing material business risks.

iv) Senior Management

The Company's senior management shall design and implement risk management and internal control systems identifying material risks for the Company and taking necessary measures. Senior management shall implement the action plans developed to address material business risks across the Company and each of the business units.

Senior management should regularly monitor and evaluate the effectiveness of the action plans and the performance of employees in implementing the action plans, as appropriate. In addition, senior management should promote and monitor the culture of risk management within the Company and compliance with the internal risk control systems and processes by employees. Senior management should report to the Risk Management Committee regarding the status and effectiveness of the risk management program.

7. Disaster Resilience and Business Continuity Plan ('BCP'):

The Company is committed to safeguard the interests of all its stakeholders in the event of a disaster or disruption that may affect the business operations. The Company shall strive to build robust systems and processes to minimize damages in an event of a disaster, quick recovery, and normalization of operations.

A business continuity management ('BCM') framework prepares an organization to continue operations amidst the potential myriad business

disruptions and aims to build high-level resilience across the organization. The BCP focuses on the survival and health of the business entity through an emergency situation.

i) The Company under the oversight of the Committee would consider adopting the following process for ensuring a robust Business Continuity Planning Process:
   a) Inclusion of potential natural and man-made disasters into risk register;
   b) Business Impact Analysis of identified disasters;
   c) Develop preparedness and mitigation strategies for rescue, recovery, and resumption;
   d) Develop plans for various matters including relocation, human resource management, establishing back-up IT servers at a secondary location, IT disaster recovery, manual workarounds, etc.;
   e) Testing & Exercises / Drills;
   f) Update BCP to incorporate lessons learned from testing and exercises;
   g) Continuously monitor emerging threats and potential disasters;
   h) Engagement with relevant stakeholders including government authorities, and local communities for building capacity on disaster resilience; and
   i) Build coherence with National Disaster Management Policy/Plans.

ii) The Risk Management Committee shall from time to time:
   a) Assess how the Company functions, including determining critical operations and its requirements, identifying survival and recovery operations and procedures for succession of management;
   b) Identify alternate sources for key materials, suppliers, resources, and other business requirements;
   c) Create a continuity of operations plan and review it annually;
   d) Define crisis management procedures including back-up management and set individual / functional responsibilities;
   e) Plan for robust communication channels amongst employees, local communities, relevant third parties, and other relevant stakeholders to ensure timely communication and appropriate coordination; and
   f) Delegate responsibility of ensuring disaster resilience and business continuity to appropriate official/management committee.

iii) Disaster resilience preparedness shall include:
   a) Emergency evacuation plans;
   b) Emergency medical assistance;
   c) Building infrastructure and other safeguards to minimize impacts; and

d) Coordination with nearby industries and communities on above-mention aspects.

In the event of disaster, the Company endeavours to resume business and operations to an acceptable level within a reasonable time.

BCP will be reviewed and maintained on regular basis to incorporate any changes to environment, people, process and technology. The Committee shall oversee the functioning of BCP.

8. General:

The Board of the Company has adopted this Policy at their meeting after obtaining recommendations from the Committee. The details of the original adoption and subsequent amendments, if any, are mentioned in the table provided at the beginning of the Policy.

Any term(s) not defined in the Policy shall have the same meaning as assigned to such term(s) in the Act and / or the SEBI Listing Regulations, 2015 or any other applicable laws or regulations.

9. Review:

The Committee shall review this Policy, at least once in two years or such other intervals as may be prescribed under SEBI Listing Regulations, 2015 from time to time and make suggestions for any change to the Board of Directors.

10. Amendment:

The Board and persons duly authorized by it, shall have the power to severally amend any of the provisions of this Policy, substitute any of the provisions with a new provision or replace this Policy entirely with a new Policy.

Any amendments in the policy undertaken by the authorized persons shall be informed to the Committee and the Board of Directors in their ensuing meetings.

*****