Novartis India Limited

RISK MANAGEMENT POLICY

Table of Contents

RISK MANAGEMENT POLICY

Novartis India Limited

1. Preamble

Novartis India Limited ("**the Company**") is committed to identifying, assessing, monitoring, and mitigating risks that may impact the achievement of its business objectives, operational continuity, and stakeholder value. As a pharmaceutical company operating in a highly regulated industry, the Company recognizes that effective risk management is integral to sound corporate governance, sustainable growth, and compliance with applicable laws.

This Risk Management Policy ("**Policy**") has been formulated pursuant to:

- **Section 134(3)(n) of the Companies Act, 2013** – which mandates disclosure in the Board's Report of a statement indicating the development and implementation of a risk management policy, including identification of elements of risk that may threaten the existence of the Company.
- **Section 177(4) of the Companies Act, 2013** – which requires the Audit Committee to evaluate risk management systems.
- **Regulation 17(9) and Regulation 21 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015** (where applicable).
- **Schedule IV of the Companies Act, 2013** – which casts responsibility on Independent Directors to satisfy themselves on the integrity of risk management systems.

2. Objectives

The objectives of this Policy are to:

1. Establish a structured and disciplined approach to risk management across the Company.
2. Identify, assess, prioritize, and mitigate risks that could affect the Company's strategic, operational, financial, regulatory, and reputational interests.
3. Embed a risk-aware culture across all functions and levels of the Company.
4. Ensure compliance with statutory and regulatory requirements applicable to the pharmaceutical sector.
5. Protect the interests of shareholders, employees, patients, regulators, and other stakeholders.
6. Enable informed decision-making and effective allocation of resources.
7. Detail measures for risk mitigation including systems and processes for internal control of identified risks.
8. Establish a business continuity plan.

3. Scope & Applicability

This Policy applies to all business units, functions, and employees of the Company. To the extent applicable, this Policy shall also extend to the Company's subsidiaries, joint ventures, contractors, and consultants, as may be relevant to the Company's operations from time to time.

4. Definitions

- **Risk** – Any event, action, or inaction that may adversely affect the Company's ability to achieve its objectives or successfully execute its strategies.
- **Risk Management** – A structured process of identifying, assessing, evaluating, mitigating, and monitoring risks.
- **Risk Owner** – The individual/function accountable for managing a specific risk.
- **Board** – The Board of Directors of the Company.
- **Risk Management Committee (RMC or Committee)** – The committee constituted by the Board to oversee risk management.

5. Risk Categories

The Company recognizes the following key categories of risk relevant to the pharmaceutical industry:

5.1 Strategic Risks

- Market competition, generic erosion, pricing pressure
- Mergers, acquisitions, and partnership risks
- Failure of new product launches or pipeline molecules

5.2 Operational Risks

- Supply chain failures
- Quality deviations, batch failures, product recalls
- Dependence on single-source suppliers

5.3 Regulatory & Compliance Risks

- Non-compliance with GMP, USFDA, WHO-GMP, EU-GMP, CDSCO, and other regulatory standards
- Adverse inspection outcomes, warning letters, import alerts
- Pharmacovigilance and product liability risks
- Drug Price Control Order (DPCO) and NPPA-related risks

5.4 Financial Risks

- Foreign exchange volatility
- Credit risk, liquidity risk, interest rate risk
- Working capital and receivables management

5.5 Legal & Intellectual Property Risks

- Patent litigation, infringement claims
- Contractual disputes
- Data integrity and confidentiality breaches

5.6 Information Technology & Cybersecurity Risks

- Data breaches, ransomware, system failures
- Loss of clinical, regulatory, or commercial data
- Compliance with 21 CFR Part 11 and data privacy laws

5.7 Human Resource Risks

- Attrition of key talent in regulatory and quality functions
- Industrial relations and employee safety

5.8 Environmental, Health & Safety (EHS) Risks

- Hazardous waste handling
- Workplace accidents, fire, and chemical hazards
- Climate change and sustainability risks

5.9 Reputational Risks

- Adverse media, social media coverage
- Product quality complaints, recalls

6. Risk Management Framework

The Company adopts the following risk management process:

Step 1: Risk Identification

Risks are identified through internal audits, management reviews, regulatory inspections, employee inputs, industry benchmarking, and external assessments.

Step 2: Risk Assessment

Each risk is assessed based on:

- **Likelihood** (probability of occurrence)
- **Impact** (severity of consequences – financial, operational, regulatory, reputational)

A risk rating matrix (Low / Medium / High / Critical) is used.

Step 3: Risk Mitigation

Appropriate strategies are formulated:

- **Avoid** – Eliminate the activity giving rise to risk
- **Reduce** – Implement controls to lower likelihood/impact
- **Transfer** – Insurance, outsourcing, hedging
- **Accept** – Where risk is within tolerance

Step 4: Risk Monitoring & Reporting

Continuous monitoring through Key Risk Indicators (KRIs), periodic reviews, and reporting to the RMC and Board.

7. Governance Structure

7.1 Board of Directors

The Board of Directors shall have overall responsibility and oversight for the risk management framework of the Company. The Board shall:

- Define the role and responsibility of the Committee and may delegate monitoring and reviewing of the risk management plan to the Committee and such other functions as it may deem fit and such function shall specifically cover cyber security.
- Approve the Risk Management Policy and any amendments thereto.
- Review the effectiveness of the risk management systems at least once a year.
- Ensure that risk management is integrated with the Company's strategic planning and decision-making process.
- In compliance with Section 134(3)(n) of the Companies Act, 2013, identify and evaluate, at least once in each financial year, elements of risk which, in the opinion of the Board, may threaten the existence of the Company, and disclose the same in the Board's Report along with the steps taken or proposed to be taken for their mitigation.
- In accordance with Regulation 17(9) of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, lay down procedures to inform all Board members about risk assessment and minimization procedures.

The RMC, in coordination with the Company Secretary, shall ensure that a risk update, including a summary of the Risk Register, key risk indicators, and material developments, is circulated to all Board members at least on a quarterly basis or as and when a material risk event occurs, whichever is earlier.

7.2 Risk Management Committee (RMC)

A. Composition

The Risk Management Committee shall be constituted by the Board in accordance with Regulation 21(2) of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015. The composition of the RMC shall be as follows:

- The Committee shall comprise at least three members, of which at least two-thirds shall be members of the Board of Directors.
- At least one Independent Director shall be a member of the Committee.
- The Chairperson of the Committee shall be a member of the Board of Directors. Senior executives of the listed entity may be members of the Committee.
- The Board may invite senior executives such as the Chief Financial Officer, Head of Internal Audit, or other functional heads to attend meetings of the Committee as invitees, as it may deem appropriate.

B. Meetings

- The RMC shall meet at least twice in a financial year, with a gap of not more than two hundred and ten days between two consecutive meetings.
- The quorum for the meetings of the RMC shall be either two members or one third of the members of the committee, whichever is higher, including at least one member of the board of directors in attendance.

C. Responsibilities

The role of the RMC, *inter alia*, includes:

- Reviewing the Policy at least once every two years, including by considering the changing industry dynamics and evolving complexity;
- Ensuring that appropriate methodology, processes and systems are in place to monitor and evaluate the risks associated with the business of the Company;
- Monitoring and overseeing the implementation of the Policy, including evaluation of adequacy of risk management systems;
- Reviewing the appointment, removal and terms of remuneration of the chief risk officer (if any);
- Keeping the Board informed about the nature and content of the discussions, recommendations and actions to be taken by the Committee; and
- Coordinating with other committees of the Board in instances where there is any overlap of the activities of the Committee with such other committees of the Board.

- Reviewing and assessing the principal risks facing the Company, including strategic, operational, financial, regulatory, cybersecurity, and reputational risks, and ensuring that appropriate mitigation plans are in place.
- Reviewing cybersecurity risks and other emerging risks on a periodic basis, as required under Regulation 21(3A) of the SEBI LODR Regulations, 2015.
- Reviewing the Risk Register and Key Risk Indicators on a quarterly basis and reporting material findings to the Board.
- Carrying out such other functions as may be delegated by the Board from time to time or as prescribed under applicable law.

The Risk Management Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, in each case, as approved by the Board.

7.3 Audit Committee

- Evaluates the adequacy and effectiveness of risk management systems as per Section 177(4).
- Reviews internal financial controls and risk-related disclosures.

7.4 Managing Director / CEO

- Overall accountability for implementation of the Policy.
- Ensures resources are allocated for effective risk management.

7.5 Chief Risk Officer (CRO) / Risk Coordinator

- Drives the day-to-day risk management process.
- Maintains the Risk Register.
- Reports to the RMC.

7.6 Functional Heads / Risk Owners

- Identify and manage risks within their function.
- Implement mitigation plans and report status.

7.7 Independent Directors

- Satisfy themselves regarding the integrity and robustness of risk management systems as per Schedule IV of the Companies Act, 2013.

8. Risk Register and Business Continuity Plan

8.1 A comprehensive Risk Register shall be maintained documenting:

- Identified risks
- Risk description and category
- Risk owner
- Likelihood and impact rating
- Existing controls
- Mitigation actions and timelines
- Residual risk and status

8.2 The Committee shall create a business continuity plan ("**BCP**") to support business process recovery in the event of a disruption or crisis, and to ensure that personnel and assets are protected and are able to function quickly in the event of natural or man-made disasters.

The BCP shall set out:

- The manner in which risk(s) affect the operations of the Company and/or its subsidiaries;
- Safeguards and procedures to mitigate the risks;
- Testing procedures/strategies to ensure effective implementation of mitigants; and
- Review of processes from time to time to make sure that risk mitigation measures are updated.

9. Reporting and Disclosure

- Material risks shall be reported to the RMC, Audit Committee, and Board.
- A statement on the development and implementation of the risk management policy shall be included in the Board's Report as required under Section 134(3)(n).
- Risk-related disclosures shall be made in the Annual Report, Business Responsibility and Sustainability Report (BRSR), and other statutory filings.

10. Review of Policy

This Policy shall be reviewed by the Risk Management Committee at least once every 2 years, or earlier in case of:

- Significant regulatory changes
- Major business changes (M&A, new geographies, new products)

- Material risk events

Any amendments to this Policy, as recommended by the Risk Management Committee, shall be placed before the Board of Directors for approval.

In the event of any conflict between the terms of this Policy and applicable law, the provisions of applicable law shall prevail.

11. Policy Dissemination

This Policy shall be communicated to all relevant employees and made available on the Company's intranet and website www.nilpharma.co.in (where applicable).