

Risk Management Policy

**Neuland Laboratories Limited
11th Floor (5th Office Level),
Phoenix IVY Building, Plot No. 573A-III,
Road No. 82, Jubilee Hills, Hyderabad, Telangana – 500033.**

Version Control:

Version	Approved on	Approved by	Reason for change
Version 1.0	29/10/2021	Board of Directors	-
Version 2.0	15/05/2025	Board of Directors	Update of the risk framework for assessing risks

Contents

1. Introduction	3
2. Authority of the Policy	3
3. Responsibility for Risk Management	3
4. Scope of Risk Management	3
5. Risk Management Objectives	3
6. Risk Management Process	4
7. Accountability for execution	7
8. Risk Reporting	7
9. Review and Governance	7
10. Making Improvements	8

1. Introduction

Neuland Laboratories Limited (“Neuland” or “the Company”) is an API (Active Pharmaceutical Ingredients) Company headquartered at Hyderabad, India. Managing risks has always been an integral part of business at Neuland. This Policy aims at formalising a process to deal with risks relevant to the Company, by building on existing management practices, knowledge, and structures, adopting best-practice frameworks, as well as adhering to regulatory expectations.

This Policy outlines Neuland’s risk management process, after suitably considering the applicable regulations as per the laws of India ^{Note 1}, and frameworks pertaining to risk management^{Note2}.

2. Authority of the Policy

This updated Policy applies to Neuland Laboratories Limited and its operational subsidiaries and is applicable effective 15 May 2025.

This Policy shall be under the oversight and advisement of the Risk Management Committee of the Board of Directors (“the Board”). The Board is responsible for risk oversight and approving any changes to this Policy.

This policy may be reviewed every year.

3. Responsibility for Risk Management

Managing risk is a management responsibility. Additionally, management is responsible for tracking and reporting of risks and progress of mitigation plans in line with this Policy.

The Risk Office, currently played by the Strategy Function, shall ensure that the Company’s risk management program is implemented in line with this Policy. The Risk Office may seek guidance from time to time from the CEO or the Risk Committee of the management

4. Scope of Risk Management

As a global player, Neuland is potentially exposed to a multitude of internal and external risks. The Company’s risk management program is designed to identify, prioritise and respond to the key enterprise-wide risks relevant to the Company in the medium-term (up to twenty-four months), as well as key risks that may impact achievement of longer-term objectives.

5. Risk Management Objectives

Neuland’s risk management program operates with the following objectives:

- Better understanding of the Company’s risk profile;
- Contribute to safeguard Company’s value and interest of shareholders;
- Improve compliance with good corporate governance guidelines and practices, as well as laws and regulations;
- Proactively manage risks and drive timely mitigation;
- Optimize cost and efforts needed to manage risks with the impact from risks; and
- Clarify the roles and responsibilities of key stakeholders.

Additionally, in the pursuit of business goals,

- Ensure that the Senior Management is able to make informed business decisions based on risk assessment; and
- Identify sound business opportunities and pursue them without exposing the business to an unacceptable level of risk.

6. Risk Management Process

Neuland's risk management program operates with the following key principles ^{Note 2:}

1. **Governance and Culture:** The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives. The organization establishes operating structures in the pursuit of strategy and business objectives. The organization defines the desired behaviours that characterize the entity's culture in line with risk taking. The organization demonstrates a commitment to the entity's core values. The organization is committed to building human capital in alignment with the strategy and business objectives.
2. **Strategy and Objective setting:** The organization considers potential effects of business context on risk profile. The organization defines risk appetite in the context of creating, preserving, and realizing value. The organization evaluates alternative strategies and potential impact on risk profile. The organization considers risk while establishing the business objectives at various levels that align and support strategy.
3. **Performance:** The organization identifies risks that impacts the performance of strategy and business objectives. The organization assesses the severity of risk. The organization prioritizes risks as a basis for selecting responses to risks. The organization identifies and selects risk responses. The organization develops and evaluates a portfolio view of risk.
4. **Review and revision:** The organization identifies and assesses internal and external changes that may substantially affect strategy and business objectives. The organization reviews entity performance and considers risk. The organization pursues improvement of enterprise risk management.
5. **Information, Communication and Reporting:** The organization leverages the entity's information and technology systems to support enterprise risk management. The organization uses communication channels to support enterprise risk management. The organization reports on risk, culture, and performance at multiple levels and across the entity.

In line with the above, the following definitions and risk management process shall apply:

DEFINITIONS

Risk: The possibility that events will occur and affect the achievement of strategy and objectives.

Risk Management: The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value.

Risk Appetite: The maximum amount of risk an entity is willing to absorb in the pursuit of strategy and business objectives.

6.1.Setting up a Risk Prioritisation framework

The Company shall have a documented risk prioritisation framework consistent with the current context and scope. The framework shall define the criteria for determining severity and likelihood of risks, considering the nature and type of risks the organization is exposed to.

While severity and likelihood criteria are established at the beginning of the risk assessment process, they are dynamic and should be continually reviewed and amended, when necessary.

[Reference: A1. Company's Risk Prioritisation criteria, together with a Risk Appetite and response framework]

6.2.Identifying and Assessing risks

Identifying risks:

The Company shall identify new or emerging risks, as well as changes to existing risks that may directly or indirectly impact the achievement of its business objectives.

As an when a new risk is identified, it shall be updated in the risk inventory. Techniques for risk identification are listed in Note 3.

The inventory of risks (and concerns) needs to be periodically reviewed and updated.

The organization may structure the risk inventory by category so that similar risks are grouped together. Additionally, the Company may choose to additionally re-group and evaluate internal and external risks faced by the Company as required by regulations.

Risks in non-routine transactions:

Where the business seeks to undertake a non-routine transaction (such as an acquisition, merger, hiving off or entering a new line of business etc.), the risk identification and assessment process shall be activated as a part of the proposal for undertaking such a transaction.

The risk office shall facilitate setting up of a separate checklist/risk-reward approval process for such non-routine transactions.

[Reference: A2 Company's Risk Universe and Taxonomy of risks and an indicative version of the Company's Enterprise 'Risks and Concerns' Summary]

Assessing risks:

Management determines the relative severity of risks in order to select an appropriate risk response, allocate resources, and support management decision-making and performance.

The risk assessment shall be carried out by applying the risk prioritization framework. Due care must be taken to assess the probability and severity, and relevance of risks (or concerns). Wherever possible, objective or quantitative data such as metrics and historical losses may be considered.

The outcome of risk assessment is recorded, communicated, and confirmed by the Management.

Assessing Substantial Change:

Management practices suitably consider impact of substantial changes to the running of the business. Substantial change could be the introduction of technology, rapid growth, changes in leadership or personnel or changing economic environment.

A systematic review of such substantial changes may be carried out as part of a periodic risk review process by the Risk Office.

6.3.Responding to Risks

For all risks identified, management selects and deploys one or more risk responses. In doing so, management may consider the following factors as key considerations: Business Context, Costs and benefits, Obligations and expectations, Prioritization of risk, Risk appetite, Risk severity.

Risk responses may fall within the following categories:

- Accept: No action is taken to change the severity of the risk. This response is appropriate when the risk to strategy and business objectives is already within risk appetite.
- Avoid: Action is taken to remove the risk. Choosing avoidance suggests that the organization was not able to identify a response that would reduce the risk to an acceptable level of severity.
- Pursue: Action is taken that accepts increased risk to achieve improved performance.
- Reduce: Action is taken to reduce the severity of the risk.
- Transfer: Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk.

Additionally, management may identify contingent plans for high severity and high velocity risks to minimise the impact of significant risk events. Selecting one risk response may introduce new risks that have not been previously identified or may have unintended consequences or also present opportunities that were previously not considered. Such responses must be considered carefully.

[Reference: A3. Company's Risk Register template that provides the Analysis and Treatment of Risks]

6.4.Developing a portfolio view of relevant Risks

Having a fully integrated portfolio view of risks vis-à-vis overall entity strategy and business objectives, would enable not only the continuous identification and mitigation of risks but would enable identification of opportunities vis-à-vis business objectives.

Risks are considered relevant if they have a significant bearing on the achievement of the Company's business objectives, can create a significant downside in the medium term and can be objectively measured or quantified.

Focusing on the most relevant risks to Business objectives helps boards and management focus greater attention on the achievement of strategy.

7. Accountability for execution

Line management at all levels should take accountability for risk identification, risk management, business decisions that involve risks.

Suitable Responsibility, Accountability, Consult or/and Inform (RACI) matrix may be operational at a risk transaction level to clarify the roles, responsibilities and accountabilities of various stakeholders.

8. Risk Reporting

The risk management process and its implementation should be documented and reported, with due consideration applied to their use, information sensitivity, internal and external context. Risk reporting may include any or all the following:

- Portfolio view of risk(s)
- Profile view of risk(s)
- Analysis of root causes
- Sensitivity analysis
- Analysis of new, emerging, and changing risks
- Key performance indicators and measures
- Trend analysis
- Disclosure of incidents, breaches, and losses
- Tracking enterprise risk management plans and initiatives

The company may automate all or a substantial portion of its risk management process to in order to benefit from the efficiencies, speed and scale of managing information.

9. Review and Governance

By Management:

Company management shall develop suitable oversight, governance and reporting mechanisms to provide independent assurance on the overall effectiveness and efficiency of the risk management program and process.

Relevant members of the management may form a Risk Committee to periodically review progress of risks, guide the Risk Office, and help in evaluating and approving decisions and initiatives involving risk.

The Risk Office would setup and operationalise such Management Committee reviews.

By Risk & Sustainability Committee of the Board:

The board periodically engages in conversations with management to determine whether enterprise risk management is suitably designed to enhance value. In addition to reviewing periodic risk management updates from Company management, it also oversees a formal annual presentation by the Executive Management to the Board on the Risk Management activities at the Company. The Risk & Sustainability Committee may operate with a separate Charter that may define the scope and mechanisms of such reviews.

[Reference: A4. Company's ERM Organisation structure]

10. Making Improvements

Neuland shall continually improve suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated.

In addition to committing to make the necessary resources available, there should be a periodic review and improvement of the risk management policy and framework in response to an event or change in circumstances.

Relevant members of the management may form a Risk Committee to periodically review progress of risks, guide the Risk Office, and help in evaluating and approving decisions and initiatives involving risk.

Notes

Note 1

Sec 134 Companies Act 2013 - requires every Company's Director to confirm the Company's Risk management policy and framework.

SEBI (LODR, May 2021) requires Top 1000 Companies by market capitalization a mandatory set-up of Risk Management Committee (RMC) and to specifically cover risk areas including ESG & BCP. Accordingly, it is proposed that the role of the RMC shall inter alia- include the following:

- 1) To formulate a detailed risk management policy which shall include:
A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), 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;
- 2) To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;
- 3) To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;
- 4) To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;
- 5) To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken; and
- 6) The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.

Note 2

The Company proposes to adopt, in a phased manner, the COSO 2017 framework for its Enterprise Risk Management (ERM) process. The COSO ERM framework describes 20 principles alongside five components. While many of the principles are implicitly operational, it is likely that some of the principles may take a bit longer to become explicit.

Note 3

Depending on the degree of uncertainty, several Risk Identification techniques are possible to be used, ranging from low complexity and low on resources to high on complexity and resources and capability. A few of them indicated in the COSO ERM 2017 guideline are given below:

- Industry analysis, external reports (Cognitive Computing);
- Data tracking: Tracking past events that help predict future occurrences;
- Interviews and Workshops: Key performance indicators and other risk metrics; and
- Process analysis.

Additionally, the Company may use techniques that are prevalent in their manufacturing, quality, safety, or business continuity processes such as FMEA, HAZOP or Business Impact Analysis.

- End of Policy-