ORCHID PHARMA LIMITED

RISK MANAGEMENT POLICY

(PURSUANT TO SEBI (LISTING OBLIGATIONS AND DISCLOSURE REQUIREMENTS) REGULATIONS, 2015, AS AMENDED)

(Version 2.1 approved by Board of Directors on January 18, 2025)

BACKGROUND

Orchid Pharma Limited (hereinafter referred to as 'the Company') is engaged in the business of manufacturing & trading of Pharmaceutical products. The business activities of the Company carry various internal and external risks.

The Company's risk management policy provides the framework to manage the risks associated with its activities. It is designed to identify, classify, assess, monitor and manage risk.

'Risk' in literal terms can be defined as the effect of uncertainty on the objectives. Risk is measured in terms of consequences and likelihood. Risks can be internal and external and are inherent in all administrative and business activities. Every member of any organization continuously manages various types of risks. Formal and systematic approaches to managing risks have evolved and they are now regarded as good management practice also called as Risk Management.

'Risk Management' is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of uncertain events or to maximize the realization of opportunities. Risk management also provides a system for the setting of priorities when there are competing demands on limited resources.

Effective risk management requires

- a strategic focus,
- forward thinking and active approaches to management,
- Balance between the cost of managing risk and the anticipated benefits, and
- Contingency planning in the event that critical threats are realized.

LEGAL FRAMEWORK

Risk Management is a key aspect of Corporate Governance Principles and Code of Conduct which aims to improvise the governance practices across the business activities of any organisation. The Companies Act, 2013 and the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 have also incorporated various provisions in relation to Risk Management policy, procedure and practices.

The provisions of Section 134(3)(n) of the Companies Act, 2013 necessitate that the Board's Report should contain a statement indicating 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.

Further, the provisions of Section 177(4) (vii) of the Companies Act, 2013 require that 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 risk management systems. In line with the above requirements, it is therefore, required for the Company to frame and adopt a "Risk Management Policy" (this Policy) of the Company.

OBJECTIVE

The objective of the risk management policy document is to ensure that the company has proper and continuous risk identification and management process. This process will generally involve the following steps:

- To ensure that all the current and future material risk exposures of the Company are identified, assessed, quantified, appropriately mitigated, minimized and managed i.e. to ensure adequate systems for risk management;
- Selecting the appropriate risk management approaches and transferring or avoiding those risks that the business is not willing or competent to manage;
- Implementing controls to manage the remaining risks and
- Monitoring the effectiveness of risk management approaches and controls;

KEY DEFINITIONS

- **"Board of Directors"**- Board of Directors in relation to Company, means the collective body of Directors of the Company (Section 2(10) of the Companies Act, 2013)

- **"Policy"**- means Risk Management Policy.

- **"Inherent Risks"-** refers to impact of a risk considering that the risk responses / controls are either absent or ineffective.

- **"Risk Analysis"-** It is the process of determining how often specified events may occur (likelihood) and the magnitude of their consequences (impact).

- **"Risk Assessment"**– The systematic process of identifying and analysing risks. Risk Assessment consists of a detailed study of threats and vulnerability and resultant exposure to various risks.

- **"Risk Classification**"- Risk elements are classified into various risk categories. Risks are grouped for better management and control. Each risk category is appropriately defined for the purpose of common understanding.

- **"Risk Review"-** A risk review involves re-examination of all risks recorded in the risk register and risk profiles to ensure that the current assessments remain valid. It also aims at assessing the progress of risk treatment action plans.

- **"Risk Management"**– The systematic way of protecting business resources and income against losses so that the objectives of the Company can be achieved without unnecessary interruption.

- **"Residual Risks"-** Residual risk refers to risk remaining after considering existing controls / implementation of a risk treatment plan.

- **"Risk Management Process"**- The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

- **"Risk Tolerance or Risk Appetite"**- It indicates risk taking ability of the Company which will be qualitative in nature. It defines the risk scoring matrix to determine risk level and risk appetite codes indicating the Company's plan from zero tolerance to highest risk appetite level.

APPLICABILITY

This Policy applies to all of the Company's operations.

ENTERPRISE RISK MANAGEMENT FRAMEWORK

The Enterprise Risk Management framework (ERM framework) refers to a set of components that provide the foundation for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization. The ERM framework for the organization has been developed keeping in mind the needs of internal and external stakeholders. The organization's ERM framework is based on the 'Risk Management – Principles and Guidelines' developed by the International organization for Standardization (ISO 31000:2018 – Risk Management Principles and Guidelines). In addition, several good practices recommended by the Committee of Sponsoring Organizations (COSO) for ERM have also been incorporated to further the organization's endeavor to build world class ERM framework and processes.

I. RISK MANAGEMENT ORGANISATION STRUCTURE:

Roles & Responsibilities of the above is as follows:

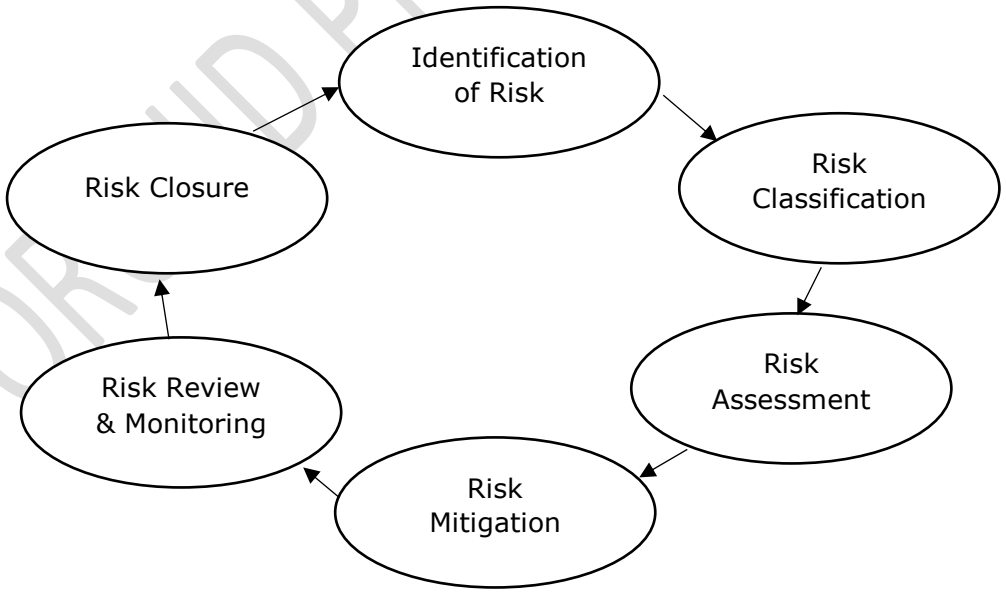
Stakeholder	Summarised Roles & Responsibilities
Board of Directors/	• Review the risk management related inputs basis framework periodically and provide feedback for improvements if any.

Audit Committee	• Evaluate effectiveness of the ERM framework adopted by the management. • Provide necessary guidance to Risk Management Committee for effective monitoring of risks. • Approve the risk management framework and policy for the Company 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	• Formulate a detailed Risk Management Policy that includes: a) A framework to identify the internal and external risks covering financial, operational, sectoral, sustainability, information or cyber security related risks or other risks determined by the Risk Management Committee. b) Measures for risk mitigation including systems and processes for internal control of identified risks c) Business Continuity Plan • Ensure that appropriate methodology, process and systems are in place to monitor and assess the company's business risks • Monitor and oversee the implementation of risk management policy; • evaluate the adequacy of ERM systems • Review the risk management policy at least once in 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 status of treatment plans implemented for prioritized risks. • Provide inputs and support in performing risk management activities in coordination with the Audit Committee. Establish procedures and timelines for various risk management activities ERM Policy.
Core Management Team	• Identify and propose risks, evaluate criticality and formulate steps for mitigation. • Implement Risk Management Plan. • Review progress on mitigation action plan & its effectiveness. • Monitor movement of Key Risk Indicators (KRI) and endeavour to maintain them within the risk appetite. • In case any risk materialises, take appropriate actions as per the policy.
Functional Heads	• Assume primary responsibility for identifying, assessing and managing business, operational and compliance risks within their area of responsibility. • Conduct periodic function meetings/ brainstorming sessions with the below objectives: a) Review updated risk registers for the business unit / function and evaluates need for inclusion of new / emerging risks.

	b) Check status of implementation measures and effectiveness of existing controls. Implement additional measures to reduce risk exposures to an acceptable level. c) Identify reasons for any risks that may have materialized and implement action plans to strengthen the mitigating steps. d) Assist with implementation of procedures for proactive review of risks for projects, transactions, new businesses, etc. e) Review the potential of any risk materializing in the near future which has a major impact for the Company.
Risk Owners	• Take overall responsibility for managing individual risks in line with ERM framework. • Coordinate with the Functional heads in deciding appropriate risk treatment plans for risks assigned. • Identify new or emerging risks and propose treatment plans on an ongoing basis should be within the risk owner's area of operation. • Monitor the progress of risk treatment plans on a monthly basis and review risks on a quarterly basis and provide periodic reports to the Function heads.

II. RISK MANAGEMENT PROCESS:

Risk Management is a continuous process that is accomplished throughout the life cycle of the organisation. Effective Risk Management covers risk management planning, early identification and analysis of risks, implementation of corrective actions, continuous monitoring & reassessment, and communication, documentation and coordination.



1. **Risk Identification:**
   The framework identifies internal and external risks faced by the Company including financial, operational, sectoral, sustainability (ESG related), information and cyber security risks. Strategic and operating risks are captured in risk register.

   Risk Identification techniques are elaborated below:

Sources	Description
Internal Audit Reports	Internal audit observations are evaluated to identify if any of those could pose a risk and mapped to the risk management framework wherever required
Peer Companies	Risks identified by the company and their mitigation measures are benchmarked with the risks and mitigation measures reported by peer entities in their Annual Reports to identify blind spots, if any and appropriate action taken to map them into the risk management framework wherever required
Whistle Blower Mechanism	Learnings from investigations into whistle blower complaints also help to identify process gaps and risks
Brainstorming	Perceived risks for a business are identified by key members of business teams through a brainstorming discussion every two years which acts as a platform to identify risks and opportunities
SWOT Analysis	During the preparation of the strategic plan, leadership team carries out a SWOT analysis and the weaknesses and threats identified during the said processes serve as inputs for risk identification
Scenario Analysis	Unprecedented or Unexpected events that have the potential to majorly impact the company's operations are evaluated by the Risk Management Committee on an annual basis

2. **Risk Classification:** The Following are the major risks identified for the Company:

Risk Categories	Description
Regulatory Risks	Pharmaceutical industry is a highly regulated segment, covering entire spectrum of activities like, product development and approval, approval of manufacturing facilities, price controls, etc. Hence, the regulatory risk is one of the significant risks identified by the management, namely: Changes in laws, regulations, litigation, governmental investigations, sanctions, etc. may result in potential business disruptions; Non-compliance of Insider trading regulations and frauds by employees can impact the reputation of the company; infringement of intellectual property rights of other pharmaceutical companies has the risk of restricting Company's revenue and/or impacting profitability
Competition Risks	Being a global pharmaceutical player, selling branded generic and generic formulations across the globe, competition and price pressures are common risk in all markets. Counterfeit pharmaceutical products can

	erode consumer trust and pose safety risks, impacting market share. Competitors may poach key talent, including researchers and executives, impacting innovation and company performance
Supply Chain Disruption Risks	With the recent experience of Covid-19 pandemic, management has identified supply chain disruption as a major risk. This includes procurement, manufacturing & delivery of final products. Company procures its raw material, packing material and other services both from within the country and outside the country. Disruption in supply chain can impact production plan as well as prices of critical materials, thereby impacting the market deliveries and costs.
Cyber Security including Data Security Risks	The company faces the risk of unauthorized access, disclosure, modification or destruction of its data both from internal as well as external sources. Cyber threats and Data security breach can result in increased internal and external security threats, leading to business disruption, reputational damages and litigations. Phishing attacks can target employees to gain unauthorised access to sensitive data.
Economic & Political Environment Risks	Company's operations span across different countries across the globe having diverse political and economic environment. Any adverse change in this may impact Company's business with that country adversely, like, Risk of political instability leading to policy uncertainty, tariff/ trade wars, economic sanctions, leading to weakening of Global economy.
Environmental, Social & Governance (ESG) Risks	ESG has gained lot of importance in recent past. Company is complying with all the regulations, but there are risks relating to this area in case of any slippage in the prescribed norms with respect to emission controls, waste management and hazardous materials handling in the form of injuries, deaths, closure of units, penalties, fines, etc. There can also be risk of reputation among customers, investors, communities, etc.
Financial & Reporting Risks	Changing laws, regulations and standards relating to accounting create uncertainty for the Company. Their application in practice may evolve over time, as new guidance is provided by regulatory and governing bodies which could result in continuing uncertainty regarding compliance matters.
IP (Intellectual property) Risks	The Company endeavours to protect its intellectual property, which is a crucial part of Company's growth. Sale of spurious drugs/products is a critical risk to the business.

3. Risk Assessment:

The risks can be assessed on two-fold criteria. The two components of risk assessment are:

a) The likelihood of occurrence of the risk event, and

b) The magnitude of impact if the risk event occurs.

The magnitude of impact of an event (should it occur), and the likelihood of the event and its associated consequences, are assessed in the context of the existing controls.

In determining what constitutes a given level of risk the following scale may be used for likelihood:

Levels	**Descriptors**
5	Very High Likelihood
4	High Likelihood
3	Moderate Likelihood
2	Low Likelihood
1	Very Low Likelihood

In determining what constitutes a given level of risk the following scale may be used for impact:

Levels	**Descriptors**
5	Very High Impact
4	High Impact
3	Moderate Impact
2	Low Impact
1	Very Low Impact

For each risk, the average score for likelihood and impact should be multiplied to arrive at a combined score. In case the rating of risks is done by a group, average of the group's score should be determined. The average is to be determined for each component of risk assessment viz., Likelihood and Impact. The simple average for each component of each risk should be calculated.

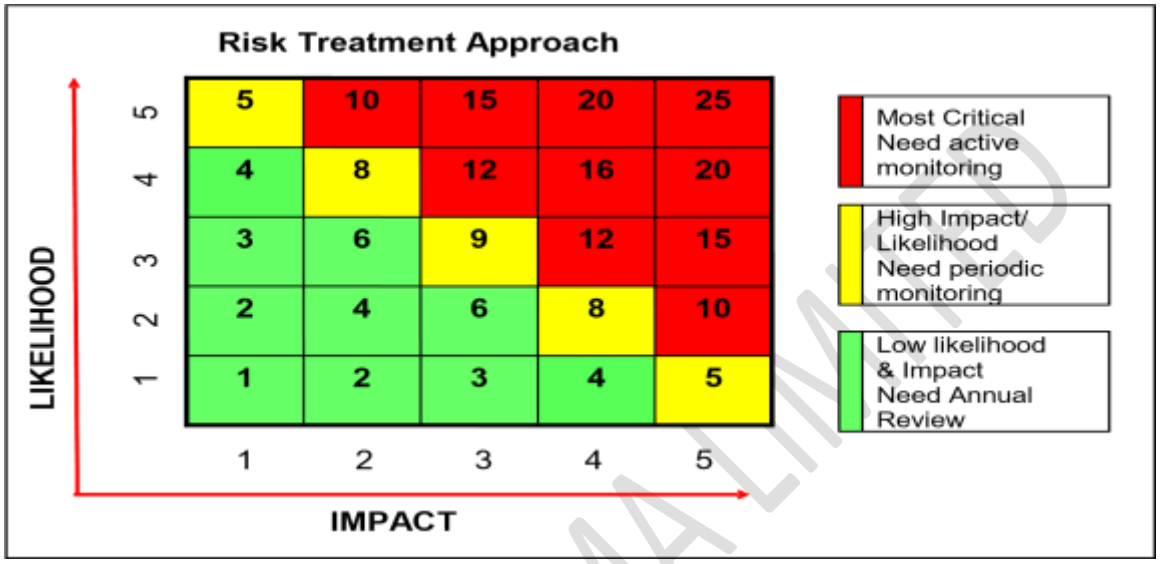
Example of calculation of group score:

	Likelihood (A)	**Likelihood (B)**
Participant 1	2	5
Participant 2	3	5
Participant 3	4	5
Total	**9**	**15**
Group Score i.e. Simple Average (Total / No. of Participants)	**3**	**5**
Combined Score (Group Score A*Group Score B)	**15**	

The risk would be classified into one of the three zones based on the combined score.

- Risks that score within a red zone are considered "Critical / High / Unacceptable" and require immediate action plans to deal with the risk. (Average score 12 and above)

- Risks that score within the yellow zone are considered "Cautionary / Medium" where action steps to develop or enhance existing controls is also needed. (Average score in the range of 6 and less than 12)
- Risks that score within the green zone are considered "Acceptable / Low". (Average score less than 6).



4. **Risk Mitigation:** Mitigation plans are developed by respective risk owners for risks owned by them. Well defined action plans are agreed upon with timelines for implementation. Mitigation plans are discussed with the senior management to seek buy-in and approval.

The following techniques can be used while treating and mitigating the risks:

(a) Risk avoidance:

Exiting the activities giving rise to risk. Risk avoidance may involve exiting a product line, declining expansion to a new geographical market etc. This option may be taken in cases where the exposure of risk is very high as compared to the expected benefits/ returns in continuing those activities.

(b) Risk reduction:

Developing mitigation plan to reduce risk exposure. Mitigation plans need to be developed and implemented for reducing the risk exposure.

(c) Risk retention:

Risk retention is a viable strategy for small risks where the cost of insuring would be greater over time than the total losses sustained. No action is taken to mitigate the risk or reduce the likelihood or impact. This option may be taken in cases where the cost of reducing the exposure is very high as compared to the benefit accrued from reducing the risk exposure.

(d) Risk transfer:

Means transfer of risk to another party by entering into a contract, e.g. insurance cover, hedging instruments etc. Depending on the risk assessment, severity and probability of occurrence, company may adopt one or more of the methods to minimize or mitigate the risk and includes purchasing insurance products, engaging in hedging transactions, or outsourcing an activity

Mitigation plan for each risk shall be documented in the risk profile template provided in Action Taken Report (ATR). The profile contains details of the risk, its contributing factors, risk scores, controls documentation, and specific and practical mitigation plans that will ensure that existing level of risks is brought down to an acceptable level. Mitigation plans need to be time bound and responsibility driven to facilitate future status monitoring. For risks considered to be "acceptable" risk profile will be developed with mitigation plan as accepted and no further actions required.

5. Risk Review & Monitoring:

Ongoing review is essential to ensure that the management plans remain relevant. Factors, which may affect the likelihood and impact of an outcome, may change, as may the factors, which affect the suitability or cost of the various treatment options.

Risk review aims at assessing the progress of risk treatment action plans. It also ensures that the current assessments remain valid. The risk register should be reviewed, assessed and updated on a half-yearly basis.

As the risk exposure of any business may undergo change from time to time due to continuous changing environment, the risk management process will be updated on a regular basis. The following process will be followed:

- **On an immediate basis**
  Escalation of risks which have substantial impact to the business and meet determined escalation tolerance levels to the Risk Cell.
- **Quarterly**

a) Respective functional/department heads will review the status Of risks and treatment actions with key staff in their respective areas.
b) Any new or changed risks will be identified and escalated, if deemed necessary.
c) Respective functional/department heads will report to the Risk Management Committee.
d) Risk Management Commitee shall compile the reports received from all the functional/department heads and will submit a comprehensive report to the Risk Management Committee.
e) Particular emphasis is to be given to risks with high ratings and their corrective actions.

- **Annually**

a) The Risk Management Committee will report its collective findings annually.
b) The Risk Management Plan will be subjected to annual audit by the Internal Auditor.

Everyone in the organization is responsible for the effective management of risk. All staff is responsible for identifying potential risks. Management is responsible for developing risk mitigation plans and implementing of risk reduction strategies. The risk management process will be integrated with other planning processes and management activities.

6. Closure of Risks

A risk issue identified and documented shall not be deleted from risk registers and shall be closed after the approval of the Chairman of the Risk Management Committee and Managing Director of the Company, due to any one of the following reasons:

- Risk mitigated: The risk is mitigated to the desired extent.
- Risk not relevant: The risk is not relevant/applicable due to change in external business environment.

Reporting / Risk Management Information System

Risk Information is needed at all levels of the organisation to identify, assess and respond to future occurrences of risk events. Pertinent information from both internal and external sources must be captured and shared in a form and timeframe that equips personnel to react quickly and efficiently. Effective communication would also involve the exchange of relevant data with external parties, such as customers, vendors, regulators and shareholders. Further, both historical and current data needs to be collected. Historical data tracks actual performance against target, identifies trends, correlate results and forecasts performance. Historical data also provides early warning signals concerning potential risk-related events. Current data gives management a real time view of risks inherent in a process, function or unit. This will enable the company to alter its activities as needed in keeping with its risk appetite.

The Company needs to start preparing 'Risk Registers' as an immediate measure. The Risk Registers will be maintained at the level of each functional head for capturing comprehensively all risks in their respective functions. Each risk will be identified, categorized and assessed using the methodology as specified in this policy or in accordance with the established norms in the industry.

The Company ensures that the Audit committee and the Board are adequately informed of significant risk management issues and the actions undertaken to manage risks on a regular basis.

Review

This Policy shall be periodically reviewed, at least once in two years, or as and when it deems necessary under the amendments in accordance to the provisions of the Companies Act 2013 and the SEBI Listing Regulations to ensure it meets the requirements of legislation and the needs of organization.

Amendment

This Policy can be amended at any time by the Board of Directors of the Company.