Piramal Pharma Limited

Risk Management Policy Document

Version 1.0: 30th August 2022

DOCUMENT CONTROL SHEET

Document Name : **Risk Management Policy**

Issued By : **Chief Risk Officer**

Authorized By : **The Board of Directors**

Management Sign-off		
(Chief Risk Officer)	**Date:**	**Signature:**

Version History

Version	Date	Prepared by	Changes and Reasons for change
1.0	30-Aug-2022		

Table of Contents

1. Introduction

The significance of risk management is inexorably linked to entrepreneurial activities, and these are inseparably tied up with opportunities and risks. Within the framework of external requirements (such as regulations) and the circumstances specific to each company resulting from its business activity, a company's success is influenced by its recognition of opportunities and risks and the way in which it sets about proactively dealing with them. Effective risk management provides a platform to the organization to grow and thrive successfully in all its business endeavors.

Risk management framework comprising of the risk management process and underlined policies are intended to enable Piramal Pharma Limited ('PPL or 'the Company') to adopt a defined process for managing the risks faced by PPL and its subsidiaries on an on-going basis. An important purpose of the framework is to implement a structured and comprehensive risk management system, which establishes a common understanding, language and methodology for identifying, assessing, responding, monitoring and reporting risks which provides management and the PPL Board of Directors ('the Board') with the assurance that key risks are being properly identified and effectively managed.

The Board shall discharge its responsibility of risk oversight by ensuring the implementation and review of the risk management system within the organization. Board may delegate to any other person or committee the task of independently assessing and evaluating the effectiveness of the risk management system.

This document would be shared with executive management of PPL, its subsidiaries and business divisions for better understanding and implementation of the risk management process.

2. Risk Management Policy

The Company is committed to implement a risk management framework to:

- Improve its ability to prevent or timely detect risk event;
- Identify, discuss, escalate and provide suggestions to deal with critical risk issues;
- Standardize risk management principles and language across the Company;
- Improve sharing of risk information; and
- Provide flexibility for managing upside and downside scenarios.

This policy is intended to ensure that an effective risk management framework is established and an appropriate reporting mechanism for the same is embedded within the Company.

The management should periodically assess the impact of changes in external and internal environment on the pertinence of this policy. If the Board deems fit, it may approve necessary changes to this policy to align it with the prevailing business circumstances.

This policy complements and does not replace other existing policies.

2.1 Applicability

This policy is applicable from the date as mentioned on the "Document Control Sheet" and applies to whole of the PPL and includes all corporate functions and divisions and subsidiaries.

2.2 Risk Management Principles

Risk Management is not a onetime event or exercise; rather it is a process that encompasses series of continuous actions that permeate into the activities of the Company. The risk management principles applicable to the Company are as elaborated below:

- All risk management activity will be aligned to corporate aims, objectives and organizational priorities set by the Company;
- Risk Management in the Company shall be proactive and reasoned (dynamic, iterative and responsive to change);
- Risk Management shall be systematic and structured to address uncertainty and shall be an integral part of decision making; and
- Managers and staff at all levels, directly or indirectly, will have a responsibility to identify, evaluate and manage and / or report risks.

2.3 Definitions

This Risk Management policy is formed around a common understanding of terminology used in this document.

Risk

Risk is the potential for loss or harm – or the diminished opportunity for gain – that can adversely affect the achievement of an organization's objectives.

Risk may be a direct or indirect effect on an organization resulting from inadequate or failed internal processes, people and systems or from external events.

Risk Management

The systematic process of identifying, analysing and responding to risk events that have the potential to generate adverse effect on the achievement of organizational objectives.

Gross / Inherent Risk

Gross / Inherent risk refers to impact of a risk considering that the risk responses / controls are either absent or ineffective.

Residual Risk

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

Risk Statement

Risk statement is the description of the risk event(s) along with the likely effect/ impact on the organizational objectives.

Contributing Factors

Contributing factors are the possible proximate causes, which jointly or severally accentuate the chances of the occurrence of a risk event or increase the level of impact of the risk on the organization.

Risk Assessment

The process of determining the possibility of occurrence of the risk event (Likelihood) and the magnitude of their consequences (Impact) on the organization, used to determine risk management priorities.

Risk Category

Risks are classified into various categories for better management and control. Each risk category is appropriately defined for the purpose of common understanding. An illustrative list of risk category along with their definitions is attached as **Annexure I**. This list may be modified in future to add / modify new risk categories that may emerge.

2.4 Documentation

Appropriate documentation at each stage of the risk management process should be followed. This framework provides a guide to documentation standards and how they are to be implemented. The designated risk coordinator would be responsible for ensuring that the required documentation has been developed and maintained up to date.

The key documents pertaining to the risk management process that need to be maintained by the Company are:

- Risk Management Policy
  The risk management policy provides overall framework for risk management process of the Company. Further amendments will be initiated / approved and ratified by the Board.

- Risk Register:
  Risk register is a consolidated list of all risks that have been identified during the periodical review. It is the key document used to communicate the current repository of all identified risks and is used for management reviews, control and reporting. A template of the risk register is given in **Annexure II**.

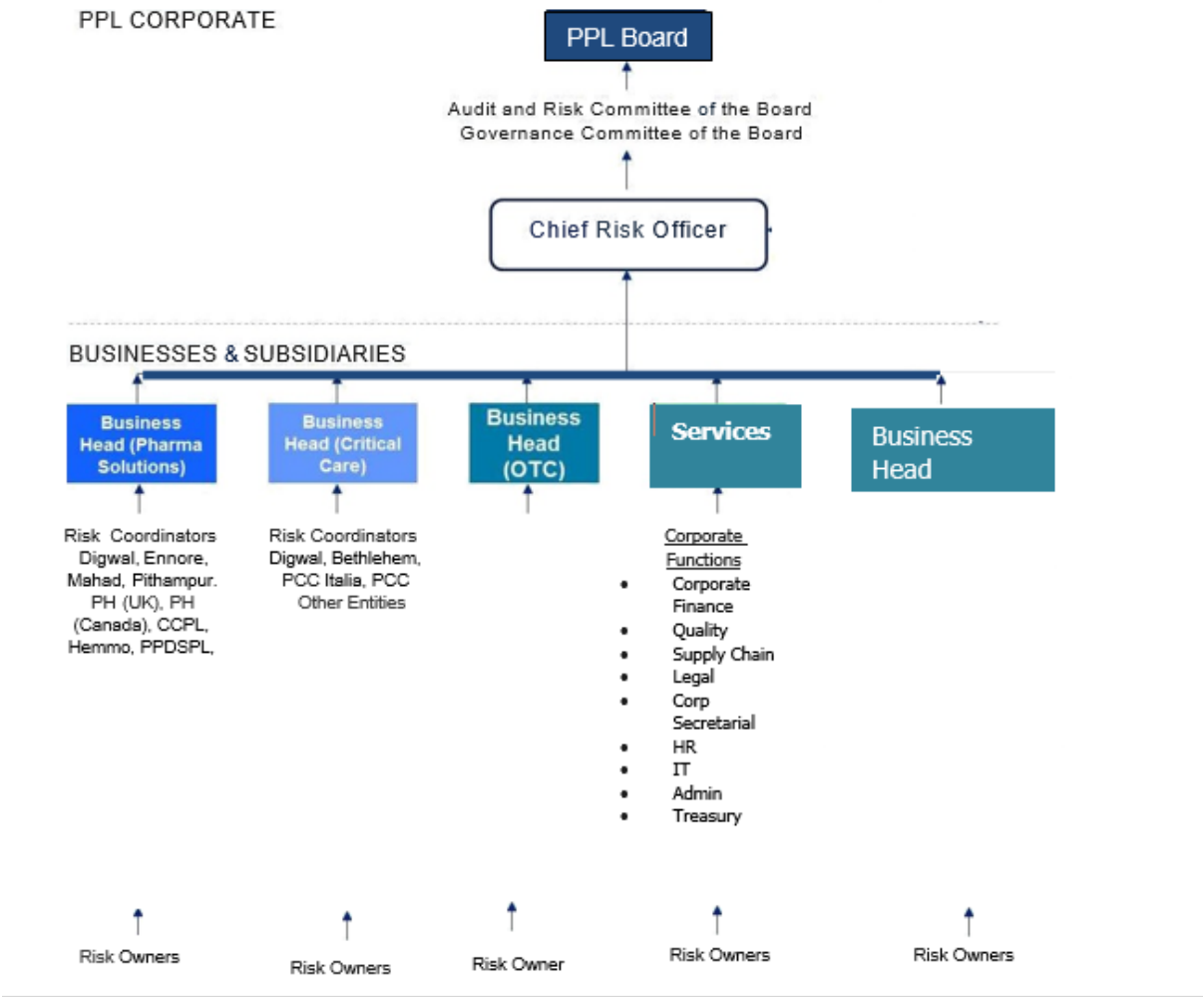
- Risk Profile:
  The purpose of the risk profile is to ensure ownership and accountability of the risks. This also helps the management and Board to effectively monitor the status of the

action plans taken and changes in the rating of the risks over a period of time. Risk profile provides detailed description of the risk, existing controls and action plans / controls for risk treatment. A template of risk profile is given in **Annexure III**.

[Space left blank intentionally]

3. Risk Management Structure

The risk management organization has been developed keeping in mind the existing organization structure of PPL to ensure smooth functioning of the risk management process.



[Space left blank intentionally]

3.1 Chief Risk Officer

The Chief Risk Officer ('CRO') would be responsible as the single point of contact / coordinator for risk management activity for the entire Company. He would liaise with the Heads of Plant/Division/Subsidiary across PPL to coordinate flow of information between them and the Board. The CRO would be responsible to collate risk reports from various Plants/Divisions/Subsidiaries and prepare the consolidated risk report for PPL and present it to the PPL Board and Management.

3.2 Risk Coordinator

The Risk Coordinator would be responsible for coordinating risk management activities of the respective Plant/Division/Subsidiary. He would liaise with the Risk Owners within the Plant/Division/Subsidiary to coordinate flow of information between them and the Head of the Plant/Division/Subsidiary and the Head of respective Businesses.

3.3 Risk Owners

Risk owners are individuals who understand the particular risk better and can contribute in mitigation of the same. Each risk will have one risk owner. Risk owners shall put in coordinated efforts to discuss the risks in detail, identify gaps in existing controls and thereby propose risk mitigation plans for the assigned risk. Risk owner is also responsible to implement the approved mitigation plan and periodically review the implementation status of mitigation plans.

The respective Business Head will nominate risk owners.

3.4 Roles & Responsibilities

The risk management roles and responsibilities will be as follows:

Roles	Responsibilities
Board of Directors	• Approve risk management policy • Review and approve risk management process and provide inputs/ directions to the executive management
Sustainability and Risk Management Committee	• Provide oversight to the risk management process • Review risk reports • Provide inputs/ directions to the executive management
Chief Risk Officer	• Review of risk management framework and related activities of PPL businesses and subsidiaries • Coordinate timely execution of risk management process across PPL • Advise PPL businesses and subsidiaries on risk management related matters • Improve awareness around risk management across PPL
Business Head	• Lead the risk management initiative for the Plant/Division/Business Segment • Report to the Sustainability and Risk Management Committee through

Roles	Responsibilities
	the CRO on matters related to risk management • Review and approve the risk management reports for the Plant/Division/Business Segment
Risk Coordinator	• Implement risk management initiatives across the Plant/Division/Business Segment/Subsidiary • Liaise with the Risk Owners to coordinate flow of information and escalation of key risk issues/concerns to the Head of the Plant/Division/Business Segment/Subsidiary • Prepare and maintain relevant risk documentation for the Plant/Division/Business Segment/Subsidiary • Improve awareness around risk management across the Plant/Division/Business Segment/Subsidiary
Risk Owners (RO)	• Prepare suitable risk mitigation plan • Ensure risk profile document(s) is/are filled and updated periodically • Ensure approved plans are implemented within the target timeframe and reported regularly

[Space left blank intentionally]

A summary chart displaying the activities to be followed periodically is given below:

Roles	Periodicity of Meeting	Activities	
		Half-Yearly	*Yearly*
Risk Owner	-	• Review and update risk profiles and report to risk coordinator	-
Risk Coordinator	-	• Review risk profiles and report to the Head of Plant/Division/ Business Segment /Subsidiary • Update risk register and risk profile documents and report to the Plant/Division/ Business Segment/ Subsidiary and the CRO	-
Business Head	-	• Review of consolidated risk register, risk profile documents and top risk	-
CRO	-	• Review of consolidated risk register and risk profile documents	• Develop a ERM implementation status report and present it to the Board
Sustainability and Risk Management Committee	Half -Yearly	• Review of top risks	• Review the progress of ERM implementation
Board of Directors	Half-Yearly	-	• Review the progress of ERM implementation

[Space left blank intentionally]

4. Risk Management Process

4.1 Risk Identification

Risk identification is a process of identifying risks for assessment, evaluation and determination of appropriate action plans. Identification should include all risks that would have an impact on the achievement of organisational objectives. The Company may use following tools and methodologies to identify new risks that may have emerged or risks that would have changed over a period of time:

- Structured workshops;
- Brainstorming sessions;
- Interviews by risk coordinator;
- Review of loss events; and
- Review of documents (such as strategy documents, business reports, etc.).

All identified risks should be updated in a risk register. Risk register should be periodically reviewed to ensure pertinence of the risks listed. Risks that would have ceased should also be closed appropriately. The risk coordinators should ensure that the risk registers are reviewed and updated on a half-yearly basis.

4.2 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

Levels	Descriptors
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:

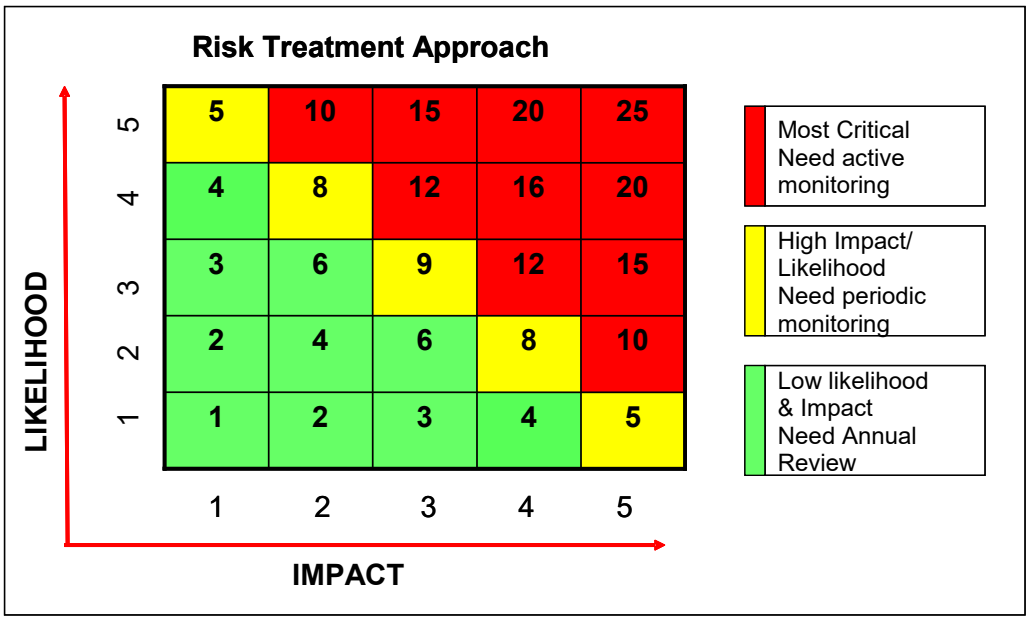
Rating of Risk

	Likelihood (A)	**Impact (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).

[Space left blank intentionally]



4.3 Risk Treatment / Action Plan

Risk treatment involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them. Treatment options may include:

- *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.
- *Acceptance* – 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.
- *Reduction* – Developing mitigation plan to reduce risk exposure. Mitigation plans need to be developed and implemented for reducing the risk exposure.
- *Transferring* – 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 **Annexure III**. 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.

4.5 Risk Reviews

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.

The risk owners should review the risks owned by them on a half-yearly basis to ensure that ratings remain pertinent and to monitor the status of action plans. The risk coordinator should review the risk register, risk profiles for critical risks and status of action plans on a half-yearly basis.

4.6 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 Business Head and –the CRO, 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

5. Reporting

A report comprising of top critical risk areas (including mitigation plans) duly approved by the Business Head and CRO, shall be placed before the Sustainability and Risk Management Committee on a half-yearly basis. The format of such a report may be as suggested by the Sustainability and Risk Management Committee. On a half-yearly basis, the Board would review the progress of risk management implementation (including areas such as training requirements, process improvisation etc.).

Enterprise Risk Management Framework

Piramal Follows the COSO model for Enterprise Risk Assessment. COSO model defines internal control as "a process effected by an entity's board of directors, management and other personnel designed to provide reasonable assurance of the achievement of objectives in the following categories:

- Operational Effectiveness and Efficiency
- Financial Reporting Reliability
- Applicable Laws and Regulations Compliance

In an effective internal control system, the following five components work to support the achievement of an entity's mission, strategies and related business objectives:

1. *Control Environment*

- Exercise integrity and ethical values.
- Make a commitment to competence.
- Use the board of directors and audit committee.
- Facilitate management's philosophy and operating style.
- Create organizational structure.
- Issue assignment of authority and responsibility.
- Utilize human resources policies and procedures.

2. *Risk Assessment*

- Create companywide objectives.
- Incorporate process-level objectives.
- Perform risk identification and analysis.

- Manage change.

3. *Control Activities*

- Follow policies and procedures.
- Improve security (application and network).
- Conduct application change management.
- Plan business continuity/backups.
- Perform outsourcing.

4. *Information and Communication*

- Measure quality of information.
- Measure effectiveness of communication.

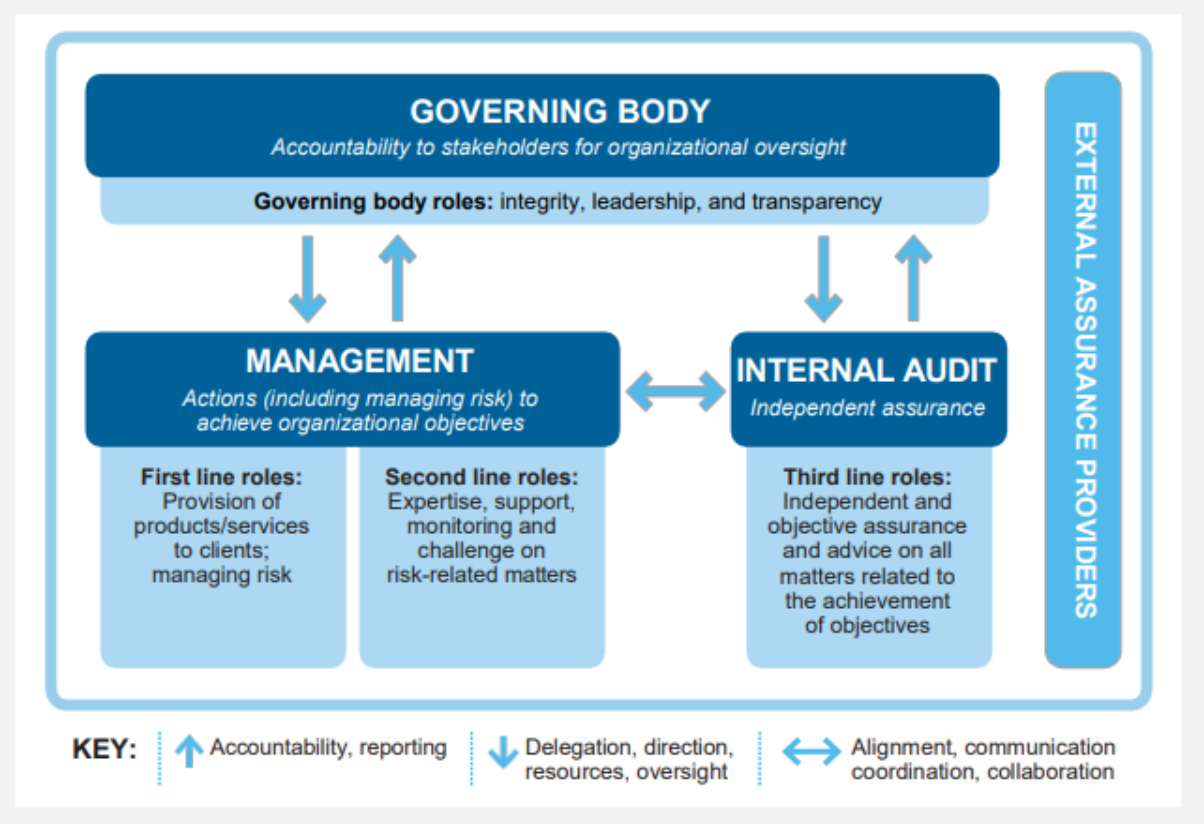
5. *Monitoring*

- Perform ongoing monitoring.
- Conduct separate evaluations.
- Report deficiencies.

These components work to establish the foundation for sound internal control within the company through directed leadership, shared values and a culture that emphasizes accountability for control. The various risks facing the company are identified and assessed routinely at all levels and within all functions in the organization. Control activities and other mechanisms are proactively designed to address and mitigate the significant risks. Information critical to identifying risks and meeting business objectives is communicated through established channels across the company. The entire system of internal control is monitored continuously, and problems are addressed timely.

Piramal has three lines of Defense for Risk Management

The Three Lines of Defense are:



The three lines of defense model provides guidance for effective risk management and governance. Each of the three lines plays a distinct role with the University's control environment.

First Line of Defense – Management

The first line of defense lies with the business and process owners. Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. This consists of identifying and assessing controls and mitigating risks. Additionally, business and process owners guide the development and implementation of internal policies and procedures and ensure activities are consistent with University goals and objectives. Mid-level managers may design and implement detailed procedures that serve as controls and supervise execution of those procedures by their employees.

Second Line of Defense – Risk Management and Compliance

The second line supports management to help ensure risk and controls are effectively managed. Management establishes various risk management and compliance functions to help build and/or monitor the first line-of-defense controls. Typical functions in this second line of defense include: "A risk management function (and/or committee) that facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization.

A compliance function to monitor various specific risks such as noncompliance with applicable laws and regulations. In this capacity, the separate function reports directly to senior management.

A controllership function that monitors financial risks and financial reporting issues." Management establishes these functions to ensure the first line of defense is properly designed, in place, and operating as intended. The second line of defense serves an important purpose but because of their management function, they cannot be completely independent.

Third Line of Defense – Internal Audit

The third line of defense provides assurance to senior management and the board that the first and second lines' efforts are consistent with expectations. The main difference between this third line of defense and the first two lines is its high level of organizational independence and objectivity. Internal Audit may not direct or implement processes, but they can provide advice and recommendations regarding processes. Additionally, Internal Audit may support enterprise risk management but may not implement or perform risk management other than inside of its own function. Internal auditors accomplish their objectives by bringing a systematic approach to evaluating and improving the effectiveness of risk management, control, and governance processes.

Statutory Auditors

External auditors are responsible for expressing an opinion on the fairness (accuracy within a degree of materiality) of the financial statements in conformity with certain accounting standards. Additionally, external auditors may provide assurance to the Board of Trustees regarding institutional compliance requirements.

[Space left blank intentionally]

Annexure I: Illustrative list of Risk Categories

Sr. No.	Risk Categories / Baskets	Definitions
1.	Strategy	Risks associated with strategy development, strategic alliances, business planning, business model, growth, reputation, competition, innovation and performance targets.
2.	Concentration	Risks due to limited number of products, customers, suppliers, or markets. It could expose the organization to an imbalance of revenue streams between product lines and markets as well as uncertainties around sustained revenue growth.
3.	Marketing	Risks associated with managing new and existing customers, customer service, pricing, marketing and feasibility of new business opportunities.
4.	Human Resource (HR)	Risks associated with culture, organizational structure, communication, recruitment, performance management, remuneration, learning & development, retention, including supporting systems, processes, and procedures.
5.	Operations	Risks associated with operational planning and scheduling. Also includes risks associated with inadequate or failed internal processes, people and systems, or from failure of infrastructure largely having to do with the performance, protection and utilization of existing assets.
6.	Planning	Risks associated with planning, budgeting and management reporting. It also includes risk associated with a lack of defined policies, processes, procedures or delegations of authority.
7.	Information Technology (IT)/ Information Security	IT risk include issues like IT strategy, architecture, infrastructure, networks, support systems, interfaces, data reliability, access controls disaster recovery., data loss, fraud, system outages, breach of confidentiality, legal/regulatory violations, as well data integrity. Risk associated with the organization's ability to design, develop, test and implement a strategy to mobilize critical staff during a business interruption, as well as recover infrastructure and data.
8.	Finance	Financial risks include risks associated with capital structuring, capital allocation, financial management, taxation and preparation of financial statements.
9.	Compliance	Risk relating to noncompliance with legislation, regulations, supervision, internal policies and procedures.

Sr. No.	Risk Categories / Baskets	Definitions
10.	Legal & Regulatory	Failure of infrastructure processes, systems, and resources to support legal and regulatory requirements.
11.	Procurement	Risks associated with procurement process, outsourcing and vendor relationships
12.	External Factors	Risks associated with external factors like political, economic /markets, social, technological, legal and regulatory, fraud, and environmental conditions pose threat to the organization.
13.	Reporting	Risk associated with collection of data from internal and external sources and relate to quality and integrity of the data Risk associated with timely and accurate disclosure of data / information like annual reports, MIS to internal and external stakeholders
14.	Governance	Risks associated with the structure, policies, procedures and authorities in which the key directions and decisions of the organization are overseen

This list may be modified in future to add / modify new risk categories that may emerge.

[Space left blank intentionally]

Annexure II: Template for Risk Register

Risk ID	Entity	Risk Category	Risk Statement	Contributing Factors	Existing Controls	Impact Score	Likelihood Score	Overall Rating	Risk Owner	Mitigation Plans

[Space left blank intentionally]

Annexure III: Template for Risk Profile

<table>
<tr><th colspan="4">BACKGROUND</th></tr>
<tr><td>Risk Ref No:</td><td colspan="3"></td></tr>
<tr><td>Risk Category:</td><td colspan="3"></td></tr>
<tr><td>Risk Statement:</td><td colspan="3"></td></tr>
<tr><td>Risk Owner</td><td colspan="3"></td></tr>
<tr><td>Date of validation:</td><td colspan="3"></td></tr>
<tr><td>Date of next review:</td><td colspan="3"></td></tr>
<tr><td colspan="4">Contributing Factors:
•</td></tr>
<tr><td colspan="4">Description of existing controls:
•</td></tr>
<tr><th colspan="4">RISK ASSESSMENT SUMMARY</th></tr>
<tr><td rowspan="3">Overall Risk Criticality</td><td rowspan="3">Critical/ Cautionary/ Acceptable</td><td>Impact Rating (A)</td><td></td></tr>
<tr><td>Likelihood Rating (B)</td><td></td></tr>
<tr><td>Overall Risk Rating (A*B)</td><td></td></tr>
<tr><th colspan="4">RISK MITIGATION PLAN</th></tr>
<tr><td colspan="4">Proposed Risk Mitigation Plans:</td></tr>
</table>

Sr. No	Description	Resource requirements including budgeted amount	Target date	Approving authority	Status as on