Apollo Hospitals Enterprise Limited

Enterprise Risk Management Policy

Version#	Change Description	Year	Prepared By	Approved by
1.8	Annual review of policy	2025	KBS Manian	RMSC

Table of Contents

1 Introduction 1

2 Enterprise Risk Management Policy 1

2.1 Applicability 2
2.2 Risk Management Objectives 2
2.3 Definitions 2
2.3.1 Risk 2
2.3.2 Risk Management 2
2.3.3 Risk Analysis 2
2.3.4 Risk Assessment 2
2.3.5 Risk Classification 3

3 Risk Management Organization 3

3.1 Risk Management Steering Committee of the Board (RMSC of the Board) 3
3.1.1 Membership 3
3.1.2 Standing invitees to the Risk Management Council Meeting 4
3.1.3 Operation and periodicity of meeting 4
3.2 Risk Council 4
3.2.1 Membership 4
3.2.2 Operation and periodicity of meeting 4
3.2.3 Deliverables 4
3.3 Roles & Responsibilities 5
3.3.1 Review 5
3.3.2 Training 5

4 Key Risk Management Practices 6

4.1 Risk Identification & Assessment 6
4.2 Risk Evaluation, Mitigation & Monitoring 6
4.3 Risk Reporting: 7
4.4 Escalation of risks 7
4.5 Risk Reviews & Reporting Cycle 7

Annexure I: List of risk categories 8

1 Introduction

The Enterprise Risk Management Policy is intended to enable Apollo Hospitals Enterprise Limited ('AHEL' or the 'Company') to adopt a defined process for managing its risks on an ongoing basis.

An important purpose of this document is to implement a structured and comprehensive risk management process, which establishes a common understanding, language and methodology for identifying, assessing, monitoring and reporting risks and which provides management and the Board with the assurance that key risks are being identified and managed.

This policy provides the overall framework for the Risk Management process of the Company. The policies underlined herein define the mechanism by which AHEL will identify measure and monitor its significant risks.

The Board is responsible for establishing and overseeing the establishment, implementation and review of the risk management process. The Board may delegate the responsibility of reviewing the effectiveness of the risk management process.

The Policy is formulated in compliance with Regulation 17(9)(b) of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("the Listing Regulations") and provisions of the Companies Act, 2013 ("the Act"), which requires Companies to lay down procedures about enterprise risk management.

The Policy may be reviewed periodically with the changes in business and market circumstances. All changes to the Policy should be approved by the Board or by the authority as delegated by the Board.

2 Enterprise Risk Management Policy

The Company is committed to high standards of business conduct and good risk management to:

- Provide safe and trusted healthcare;
- Manage uncertainty;
- Encourage multidisciplinary accountability;
- Optimize organizational readiness;
- Protect the company's assets;
- Achieve sustainable growth;
- Take risk adjusted business decisions; and
- Ensure compliance with applicable legal and regulatory requirements.

This policy is intended to ensure that an effective risk management framework is established and implemented within the Company and to provide regular reports on the performance of that framework, including any exceptions, to the Board of Directors of the Company.

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

This Enterprise Risk Management Policy complements and does not replace other existing compliance programs. This document is built taking into consideration various standards and frameworks on risk management such as the Risk Management Standard ISO 31000:2018 and COSO Integrated ERM framework.

2.1 Applicability

This Enterprise Risk Management Policy applies to all hospital units.

2.2 Risk Management Objectives

The main objective of the policy is to ensure sustainable business growth with stability and to promote a pro-active approach in reporting, evaluating and resolving risks associated with the business and ancillary operations. To achieve the key objective, the policy establishes a structured and disciplined approach to Risk Management, to guide decisions on risk related issues.

The objective of Risk Management is to help managers:

- Integrate risk management in the day-to-day management of the business.
- Improve business performance by improving decision making and planning.
- Escalate risk information on timely basis at appropriate levels.
- Promote a more risk aware culture in pursuit of opportunities to benefit the organization.
- Achieve cost savings through better management of internal resources.
- Build safeguards against earnings-related surprises.

2.3 Definitions

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

2.3.1 Risk

Risks are events, the occurrence or non-occurrence of which can result in profits or losses. Risk is a probable event that will have direct or indirect effect on meeting business objectives say due to inadequate or failed internal processes, people, systems or external events.

2.3.2 Risk Management

The systematic process of identifying, analysing, and responding to anticipated future events that have the potential to generate undesired effects.

2.3.3 Risk Analysis

The process of determining how likely the specified events may occur and quantifying the magnitude of their consequences (impact).

2.3.4 Risk Assessment

Risk assessment is the process of estimating the Risk Score using Impact and Likelihood of occurrence of the event.

2.3.5 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. List of risk categories along with their definitions is attached in Annexure-I. This list may be modified in future to add/modify new risk categories that may emerge.

3 Risk Management Organization

The organization structure for risk management is depicted through the diagram below. Detailed notes on roles and responsibilities of each level follow.

3.1 Risk Management Steering Committee of the Board (RMSC of the Board)

3.1.1 Membership

The Risk Management Steering Committee shall consist of majority of members from the Board of Directors of the company and senior executives of the company. The chairperson of the committee shall be a member of the Board of Directors.
The composition of the Risk Management Steering Committee needs to be proposed and approved by the Board of Directors. Other invitees may be called to join specific Risk Management Steering Committee meetings, if required. Standing members of the RMSC will consist of:
Standing members of the RMSC will consist of:

- Ms. Suneeta Reddy, Managing Director
- Ms. Preetha Reddy, Exec Vice Chairperson
- Ms. V. Kavitha Dutt, Independent Director

- Dr. Madhu Sasidhar, President and CEO - Hospitals Division
- Dr. Rohini Sridhar, Chief of Medical Services

3.1.2 Standing invitees to the Risk Management Council Meeting

- Krishnan Akhileswaran, GCFO
- KBS Manian, GCRO and Head - IA
- Deepa Seshadri, Sr. VP
- Functional Heads

3.1.3 Operation and periodicity of meeting

Ms. Suneeta Reddy, MD will chair the RMSC of the Board. Company Secretary will be responsible as the Secretary to the RMSC of the Board. The RMSC shall meet on a quarterly basis or as required for urgent matters. Reports of RMSC's activities (agendas, decisions) and meetings (including attendance) will be maintained for each meeting by the Secretary to RMSC.

The CRO Office would coordinate information flow between the RMSC and Risk Council. The Company Secretary would be responsible to ensure that meetings of the RMSC are held quarterly as required, for the purpose of risk management.

3.2 Risk Council

3.2.1 Membership

Standing membership of the Risk Council (RC) will consist of:

- Dr. Madhu Sasidhar, President and CEO - Hospitals Division
- Krishnan Akhileswaran, Chief Financial Officer
- KBS Manian, GCRO and Head – IA
- Functional Heads

The Risk Council may nominate additional members as may be required from time to time.

3.2.2 Operation and periodicity of meeting

The Risk Council shall meet on a quarterly basis or more frequently if required for urgent matters. Reports of Risk Council's activities (agendas, decisions) and minutes of meetings (including attendance) will be maintained for each meeting by the Secretary to RMSC

3.2.3 Deliverables

At a minimum, the Risk Leaders will ensure:

- Quarterly review of risks
- Quarterly update to Risk Register including mitigation plans

3.3 Roles & Responsibilities

The risk management roles and responsibilities will be as follows:

Level	Key roles and responsibilities
Board of Directors	• Corporate governance oversight of risk management performed by the Executive Management. • Review the performance of Risk Management Steering Committee.
Risk Management Steering Committee	• Fulfill responsibilities as assigned by the Board. • Approve Enterprise Risk Management Policy. • Evaluate risk profile against risk appetite. • Provide ERM governance oversight.
Risk Council	• Oversee recent developments in the company and external environment and provide inputs on company's enterprise risk management. • Provide inputs on risk tolerance and targets. • Support risk management culture across the organization.
ERM Office (Led by the Chief Risk Officer)	• Provide ERM subject matter expertise. • Design & facilitate ERM framework & process. • Develop and provide risk status reports for the Executive Team and board. • Develop and deliver risk training. • Facilitate quarterly risk status reports to RMSC. • Facilitate quarterly risk evaluation meetings on a staggered basis. involving Risk Owners/Champions and Regional Risk Leaders.
Risk Champions (Unit Level)	• Coordinate the risk management activities for respective hospital / business unit / Corporate Function. • Provide update on risk management activities to the Chief Risk Officer. • Ensuring that ERM objectives are effectively met within the respective hospital / business unit / Corporate Function.
Risk Owners (Functional Heads in each Unit)	• Identify risks, update and reassess risks on a periodic basis. • Recommend mitigation plan. • Manage the risk by implementing approved mitigation plans. • Escalate risks to Chief Risk Officer.

3.3.1 Review

This document shall be reviewed annually or as and when there is a relevant amendment in the SEBI (LODR) Regulations, 2015 to ensure it meets the requirements of legislation and the needs of the company.

3.3.2 Training

The relevant risk owners shall be responsible for training the units and functional departments on risk management framework and required initiatives as and when required.

The main agenda of the training will be:

- Definition of risk;
- Risk management framework and its context;
- Key definitions;
- Role of Risk Owners and expectation from unit/functional management; and
- Contribution of units/ functions in identifying new risks.

4 Key Risk Management Practices

4.1 Risk Identification & Assessment

Periodic assessment to identify significant risks for the Company and prioritizing the risks for action. Mechanisms for identification and prioritization of risks include risk survey, business risk environment scanning and focused discussions in Risk Council and RMSC meetings. Risk survey of executives across units, functions and subsidiaries is conducted before the annual strategy exercise. Risk register and internal audit findings also provide pointers for risk identification.

Risks will be assessed on qualitative 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 combination of likelihood of occurrence and the magnitude of impact provides the inherent risk level. The likelihood and impact should be rated over a period of 12 to 18 months.

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. Impact and likelihood may be determined using a combination of quantitative and qualitative criteria (Risk Assessment Criteria) approved by the RMSC.

4.2 Risk Evaluation, Mitigation & Monitoring

Impact and likelihood are combined to produce a level of risk. Based on the level, the risks are evaluated and classified into suitable categories as below:

Risk Score Range	Criticality	Treatment
21-25	Critical	Needs Active Monitoring and corrective action
16-20	High	Needs Active Monitoring
11-15	Medium	Needs Quarterly Monitoring
6-10	Low	Needs Annual Review
1-5	Negligible	Needs Annual Review

The objective of risk assessment and risk evaluation is to assist the organization in prioritizing risk to ensure that appropriate attention is given to risks based on their criticality and that company resources are effectively utilized in managing these risks.

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

- Terminate: Avoiding the risk by hedging / adopting safer practices or policies;
- Transfer: Transferring the risk to other parties viz. insurance;
- Treat: Reducing the likelihood of occurrence and/or consequence of a risk event; and
- Tolerate: Accepting the risk level within established criteria.

For top risks, dashboards are created that track external and internal indicators relevant for risks, to indicate the risk level. The trend line assessment of top risks, analysis of exposure and potential impact are carried out. Mitigation plans are finalized, owners are identified, and progress of mitigation actions are monitored and reviewed.

4.3 Risk Reporting

Top risks report outlining the risk level, trend line, exposure, potential impact and status of mitigation actions is discussed in Risk Council and RMSC on a periodic basis. In addition, risk update is provided to the Board. Entity level risks are reported to and discussed at appropriate levels of the organization.

4.4 Escalation of risks

It is critical to institute an effective system of escalation which ensures that specific issues are promptly communicated and followed up appropriately. Every employee of the Company has the responsibility of identifying and escalating the risks to appropriate levels within the organization.

4.5 Risk Reviews & Reporting Cycle

Risks and the effectiveness of control measures need to be monitored to ensure changing circumstances do not alter risk priorities. Few risks remain static. 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.

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. Review also aims at assessing the progress of risk treatment action plans. Risk reviews should form part of agenda for every RMSC meeting. The risk register should be reviewed, assessed and updated on a periodic basis.

The frequency of review and reporting of the risk management process is given below:

Activities	Frequency
Updating Risk register	As and when risks are identified and assessed, at least once in a quarter
Risk Management Reporting	Quarterly

Annexure I: List of risk categories

Sr. No.	Risk Categories	Definitions
1	Service Excellence	Risks associated with adequate infrastructure to support patient services, patient satisfaction and care for IP, OP and International Patients
2	Health & Safety	Risks associated with environment pollution, safety of resources and employees' health and security at health care establishments
3	Nursing Operations	Risks relating to the adequacy of policies and procedures relating to nursing operations and maintain continuous care.
4	Facilities & Equipment	Risks associated with inadequacy or failure of facilities and equipment for delivery of care.
5	Human Resource	Risks associated with culture, organisational structure, communication, recruitment, performance management, remuneration, learning & development, retention, Occupational Health & Safety and industrial relations, including supporting systems, processes and procedures.
6	Information Technology	The risk that systems are inadequately managed or controlled, data integrity, reliability may not be ensured, inadequate vendor performance and monitoring, system or network architecture not supporting medium or long term business initiatives and strategy, capacity planning not being reviewed on a regular basis resulting in processing failures, risks of data or systems migration or interfaces.
7	Marketing/Business Development	Risks associated with customer sources, competition, brand management & brand licensing and reputation of the company.
8	Finance	Risks relating to liquidity /treasury operations, relationship management with lenders, receivables management, inadequacy of controls, lack of adequate monitoring leading to higher risks of frauds, etc.
9	Billing and Collection	Risks relating to Cash Management, billing and claims processing, customer credit risks, etc.
10	Legal and Compliance	Risk relating to non-compliance with legislations including direct & indirect tax law provisions, adequacy of financial reporting & disclosures, regulations, internal policies and procedures
11	Corporate Governance	The risks associated with board and board procedures including risk oversight, internal controls, etc.
12	Corporate/External communication	Risks associated with appropriateness/adequacy of external communication & PR
13	Market/Environmental impact assessment	Risks associated with changing consumer/business trends/technological shifts affecting all aspects of business and adequacy of assessment of such risks

[End of Document]