



MAX HEALTHCARE INSTITUTE LIMITED

CIN: L72200MH2001PLC322854

RISK MANAGEMENT POLICY (THE “POLICY”)

Type: Policy	Owner: Board of Directors	Custodian: Chief Financial Officer, Chief People Officer & Head Legal
Effective Date: August 21,2020	Latest Review: June 19, 2020	Communication Plan: Web
Version: 1	Privacy Classification: Open General	Doc. No. Listing Policy / FY 20-21

Contents

1. OVERVIEW	3
2. OBJECTIVE	3
3. APPLICABILITY	3
4. DEFINITIONS.....	3
4.1. RISK	3
4.2. RISK MANAGEMENT	4
4.3. RISK ANALYSIS	4
4.4. RISK EVALUATION	4
4.5. RISK ASSESSMENT	4
4.6. RISK CLASSIFICATION	4
4.7. RISK REVIEW	4
4.8. RISK TOLERANCE OR RISK APPETITE.....	4
5. DOCUMENTATION.....	4
6. ROLES & RESPONSIBILITIES	5
7. RISK MANAGEMENT PROCESS	6
7.1. Risk Identification	7
7.2. Risk Assessment	7
7.3. Risk Classification/Evaluation	8
7.4. Risk Mitigation/Action Plan.....	9
7.5. Risk Review	9
7.6. Risk reporting	10
8. ANNUAL REVIEW	10
9. TRAININGS.....	11
10. AMENDMENT AND CONFLICT	11
11. ANNEXURES.....	12
<i>Annexure I – Risk Register.....</i>	12
<i>Annexure II – Risk Reporting Template</i>	12
<i>Annexure III – Risk Mitigation Plan Report.....</i>	13

OVERVIEW

The Risk Management Policy (**'Policy'**) is intended to enable Max Healthcare Institute Limited (**'MHIL'** or the **'Company'**) to adopt a defined process for managing its risks on an ongoing basis. The purpose of this Policy 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 of directors of the Company (**'Board'**, which term shall include a duly constituted and authorised committee thereof) 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 Board may review and amend this policy from time to time 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.

1. OBJECTIVE

1.1. Risk is an inherent aspect of a dynamic business environment. The Company is committed to high standards of business conduct and comprehensive risk management to:

- Protect the Company's assets;
- Take risk adjusted business decisions;
- Ensure compliance with applicable legal and regulatory requirements; and
- Provide clear and strong basis for informed decision making at all levels of the Company.

1.2. 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 audit and risk management committee of the Company (**'A&RM Committee'**).

1.3. This Policy complements and does not replace other existing compliance programs.

2. APPLICABILITY

This Policy applies to the whole of the Company, its subsidiaries and includes managed hospital and support functions.

3. DEFINITIONS

The Policy is formed around a common understanding of terminology used in this document i.e.:

3.1. RISK

Risk is an adverse event resulting from inadequate or failed internal processes, people and systems, or from external sources. Risk can also be defined as any threat that can potentially prevent the Company from meeting its objectives. It also can be defined as a potential event or action that has a chance of occurring, which may result in a negative

impact on the Company, its subsidiaries and its managed hospital and support functions.

3.2. **RISK MANAGEMENT**

It is defined as the systematic process of identifying, analysing, and responding to anticipated future events that have the potential to generate unwanted effects. It includes the ability to foresee challenges achieving the Company's objectives and attempts to lower the likelihood and impact of their occurrence.

3.3. **RISK ANALYSIS**

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

3.4. **RISK EVALUATION**

It is the process used to determine Risk Management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria, to generate a prioritized list of risk for further monitoring and mitigation.

3.5. **RISK ASSESSMENT**

Risk Assessment is the combined process of Risk Analysis and Risk Evaluation.

3.6. **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.

3.7. **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.

3.8. **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. Refer "Risk Appetite & Tolerance Guidance" for more details.

Any other terms used in this Policy, and not defined herein, shall have the same meaning as assigned to such terms under the Companies Act, 2013 ('**Companies Act**'), the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ('**Listing Regulations**') or any other applicable law.

4. **DOCUMENTATION**

4.1. The responsibility for documenting the individual risks has been assigned to the risk owners. Hospital units and functionaries are responsible for performing and

documenting risk assessments and developing appropriate risk management plan.

4.2. The key documents pertaining to risk management process that need to be maintained are:

- a) Risk Register/ Risk library: It contains a list of all identified risks during the periodic review. It is the key document used to communicate the current status of all known risks and is used for management control, reporting and reviews. A template of the Risk Register is set out as **Annexure I**.
- b) Risk Reporting Template: The Risk Reporting Template sets out the format in which the identified risks are forwarded to the concerned CRO (Medical or Non-medical depending upon the nature of the risk) for assessment. A template of the Risk Reporting Template is set out as **Annexure II**.
- c) Risk Profile/Risk Mitigation Plan Report: The Risk Profile or Risk Mitigation Plan Report provides detailed documentation and attributes of risk along with details of actions planned for risk mitigation. A template of the Risk Reporting Template is set out as **Annexure III**.

5. ROLES & RESPONSIBILITIES

The risk management roles and responsibilities will be as follows:

	Definition/Constitutions	Roles & Responsibilities
Board of Directors or "Board"	<ul style="list-style-type: none"> It means the board of directors of the Company. 	<ul style="list-style-type: none"> Approve the risk management policy Defining the roles and responsibilities of the A&RM Committee Delegate monitoring and review of the risk management activities and such other functions as deemed fit to the A&RM Committee <ul style="list-style-type: none"> Include a statement indicating development and implementation of risk management policy in Board's report in accordance with the Companies Act and the rules made thereunder
Audit & Risk Management Committee	<ul style="list-style-type: none"> Constituted with approval of Board Constituted in accordance with the Companies Act and the Listing Regulations. 	<ul style="list-style-type: none"> Carry out responsibilities as assigned by the Board Review and update risk management policy to ensure effective implementation Monitor, review and approve the risk management activities and report there-off for approval of the Board <ul style="list-style-type: none"> Oversee recent developments in the Company and external business environment and periodic updating

		of Company's enterprise risk management program for assessing, monitoring and mitigating the risks
Chief Risk Officers or "CROs"	<ul style="list-style-type: none"> Given the nature of operations, there will be two CROs(Medical Operations & Non-Medical Operations) Appointed by A&RM Committee 	<ul style="list-style-type: none"> To coordinate meetings of A&RM Committee on the subject at least two times in a year. To monitor and report the mitigation plan for the risks identified to A&RM Committee. To propose periodic updates in risk management policy
Risk Owners	<ul style="list-style-type: none"> Nominated by CRO and appointed by the chairman and managing director of the Company ('CMD') during risk identification and assessment process. Entrusted with authority and accountability to manage specific risk(s). 	<ul style="list-style-type: none"> Responsible for identifying initial risks and reassessing risks on a periodic basis Responsible for prepare and update risk register and documenting/implementing mitigation plan in coordination with concerned CRO.

6. RISK MANAGEMENT PROCESS

The risk management is continuous process that is accomplished through-out the life cycle of a Company. Risk management is a shared responsibility. The risk management process model includes the following key activities, performed on a continuous basis:



6.1. Risk Identification

- a) This involves continuous identification of events that may have negative impact on the Company's ability to achieve goals.
- b) Comprehensive risk identification should include all risks whether or not they are under the control of the Company.
- c) Risks can be identified in a number of ways including but not limited to:
 - Structured workshops;
 - Brainstorming sessions;
 - Occurrence of a loss event (internally/externally);
 - Review of documents
- d) Risk owners/function head/unit head must periodically review the risk within their functional areas. Workshops or brainstorming sessions may be conducted amongst the focus groups to identify new risks that may have emerged over a period of time. Any loss event may also trigger risk identification.
- e) Whenever a new unit/ hospital is added to the Company's network, the concerned CROs shall circulate the existing Risk Register to the relevant functionaries. The unit head shall, in consultation with the concerned CROs, assess the applicability of the risks on the unit and also propose additions, if any, to the Risk Register.
- f) Recognizing the kind of risks that Company is/may be exposed to, risks will be classified broadly into the following categories:
 - **Strategic Risk** (e.g. PPP Model, breach of contract, change in policy of the government, *etc.*)
 - **Operational Risk** (e.g. unionization/strike, prevention of sexual harassment, cartelization by insurance companies, shortage of key skills, inadequate infrastructure, *etc.*)
 - **Financial Risk** (e.g. financial frauds and poor control environment, high leverage, mass insurance policy, *etc.*)
 - **Clinical Risk** (e.g. sentinel events, medical negligence, de-accreditation of hospitals, *etc.*)
 - **Legal & Compliance Risk** (e.g. ongoing litigations, non-compliance of critical laws, *etc.*)
 - **Tax & Regulatory Risk** (e.g. withdrawal of income tax exemptions for trust, EWS non-compliance, price regulations, action by local bodies, *etc.*)

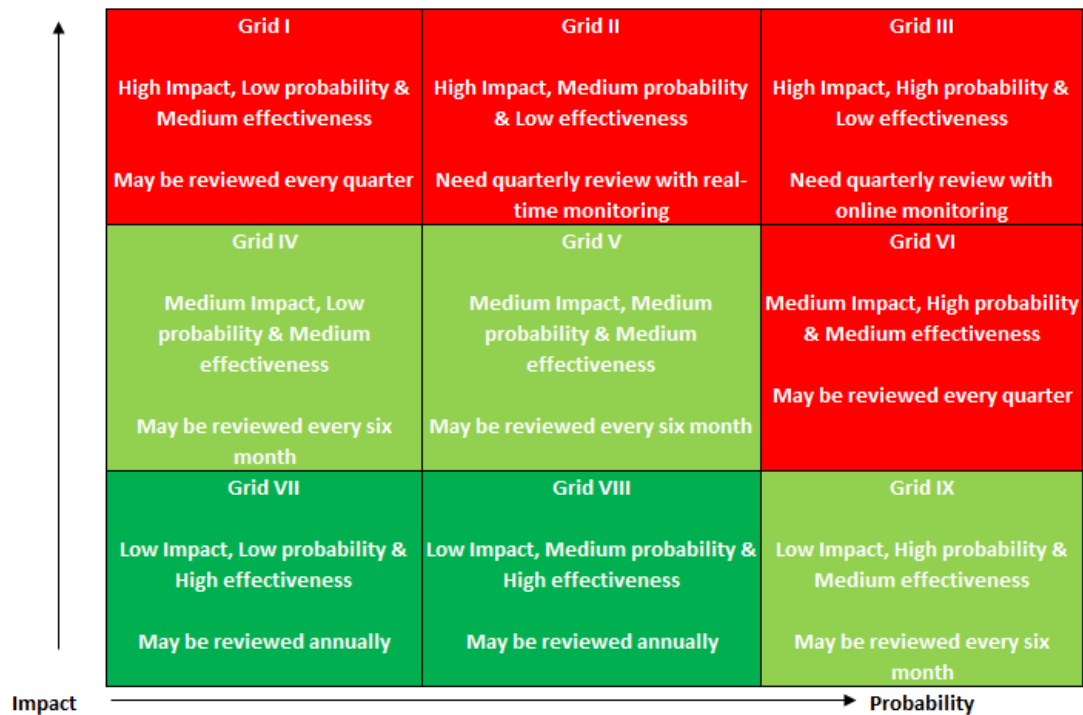
6.2. Risk Assessment

- a) The risks will be assessed on qualitative three-fold criteria. The components are:
 - **Probability** - The likelihood of occurrence of the risk event. It is categorized into "High (Likely), Medium (Possible) and Low (Unlikely or Remote)" for risk classification matrix;

- **Impact** -The magnitude of impact if the risk event occurs. It is categorized into “High (Extreme), Medium (Major or Material) and Low (Minor)” for risk classification matrix; and
 - **Control Effectiveness** - The risk mitigation plans would be subjected to control checks and a subjective rating of mitigation plans. It is categorized into “High (Highly Effective), Medium (Effective) and Low (Ineffective or Highly Ineffective)” for risk classification matrix.
- b) The combination of likelihood of occurrence and the magnitude of impact provides the inherent risk level.
- c) The Risk Owner shall be responsible for assessment of the risks and devising risk mitigation plans and timelines in consultation with the concerned CRO.

6.3. Risk Classification/Evaluation

- a) Risk Analysis is to be conducted using a risk matrix taking the existing controls into consideration. After identification and assessment of risks, the concerned CRO shall classify the risk in 9 (nine) grids based on their ratings.



- b) The objective of risk assessment and risk evaluation is to assist the Company 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
- c) The output of a risk evaluation is a prioritized list of risks for further action.

- A **high-risk category** is indicated when immediate attention is required to ensure that the necessary controls are put in place and/or existing controls are strengthened.
- A **medium-risk category** is indicated when the controls are present but are not effectively used or control are not present. It requires attention in short/medium term. The impact of the risk may be moderate in the short run however may cause a more severe impact in the medium/long run if not adequately addressed.
- A **low risk category** is indicated when there are effective controls in place and functioning effectively to mitigate the risk. It is recommended to review the controls periodically in light of the agreed risk, to ensure that the level of risk does not increase.

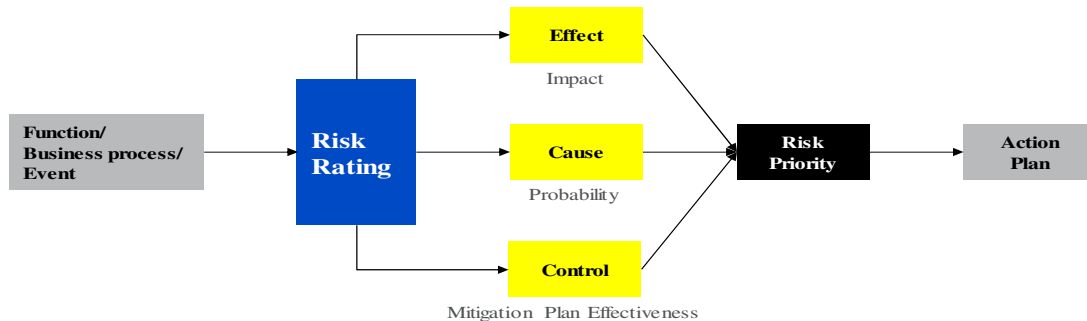
6.4. Risk Mitigation/Action Plan

- a) Risk management involves identifying the range of options for mitigating the risk, assessing those options, preparing risk mitigation plans and implementing them. Mitigation options may include: -
 - Accepting the risk level within established criteria;
 - Transferring the risk to other parties viz. insurance;
 - Avoiding the risk by hedging / adopting safer practices or policies; and
 - Reducing the likelihood of occurrence and/or consequence of a risk event.
- b) For the risk mitigation steps, the cost benefit analysis needs to be evaluated. Action plans supporting the strategy are recorded in a Risk Register along with the timelines for implementation.
- c) Mitigating practices and controls shall include determining policies, procedures, practices and processes in place that will ensure that existing level of risks are brought down to an acceptable level. In many cases significant risk may still exist after mitigation of the risk level through the risk management process. These residual risks will need to be considered appropriately. Some risks can also be transferred by a combination of:
 - Insurance by external agencies; and
 - Self-insurance or internal funding.
- d) The concerned CRO in consultation CMD may form an adjective risk management committee which may assist CROs, A&RM Committee or the chief executive officer of the Company ('**CEO**') in implementation of risk mitigation plans.

6.5. Risk Review

- a) Risks and the effectiveness of control measures need to be monitored to ensure changing circumstances do not alter risk priorities. Factors, which may affect the likelihood and impact of an outcome, may change. Ongoing review is essential to ensure that the management plans remain relevant.

- b) On a periodical basis, the concerned CRO shall be responsible for running a survey across the organisation for assessment and review of risks. Mitigated risks shall be excluded from the survey and new risks included in the Risk Register shall be added to the survey. The respondents shall include all the units and functionaries (including those added during the relevant period).
- c) The concerned CRO shall collate all the responses and rate all the risks on the basis of impact, probability and control effectiveness, as filled up by the respondents to the survey. Further, he/ she will calculate the residual risk as per the formula below:



- Risk Rating = I*P*E
- Impact, Probability & Effectiveness are measured on a scale of 1-4

6.6. Risk reporting

- a) Risk mitigation plan report will be used to highlight emerging risk or add new risk to the Risk Register. It is responsibility of Risk Owners and concerned CROs to prepare and present the consolidated risk mitigation plan report to A&RM Committee on half yearly basis. It consists the following information:
 - New risks added to the Risk Register;
 - Progress of implementation of the risk mitigation plans and reasons for delay/ non-implementation of risk mitigation plans;
 - Status of trainings to units/hospitals and functionaries.
- b) The concerned CRO shall take actions on gaps in execution of risk mitigation plans and any other action required by the A&RM Committee from time to time.

7. ANNUAL REVIEW

- 7.1. On bi-annual basis, the A&RM Committee shall carry out assessment and adherence to the risk management process and its effectiveness in managing risks.
- 7.2. The report on the assessment of risk management process shall be discussed with the concerned CROs, Risk Owners and the CEO/CMD before being presented to the A&RM Committee.

8. TRAININGS

8.1. The concerned CRO and the Risk Owners shall be responsible for training the units and functional departments on risk management framework and required initiatives.

8.2. The main agenda of the trainings will be

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

9. AMENDMENT AND CONFLICT

Any subsequent amendment/modification in the applicable laws shall automatically apply to this policy. The Board has the right to amend or modify this policy in whole or in part, at any time without assigning any reason, whatsoever. In the event of conflict between this policy and any applicable laws, applicable laws shall prevail.

10. ANNEXURES

Annexure I – Risk Register

List of identified risks

Sr. no.	Risk description	Function	Risk category

Risk description –

Function		Risk category	
Risk owner		Impact category	
Probability		Risk rating	
Severity of impact			
Control effectiveness			

Mitigation plan

S. No.	Activity	Closure Date

Annexure II – Risk Reporting Template

Unit			
Function		Risk category	
Probability	Likely/ Possible/ Unlikely/ Remote	Impact category	Financial/ Brand/ Legal/ Regulatory/ People
Severity of impact	Extreme/ Major/ Material/ Minor	Control/ mitigation plan effectiveness (if assessed)	Highly Effective/ Effective/ Ineffective/ Highly Ineffective

Contributing Event/s or Occurrence/s or Threat/s

S. No.	Event/Occurrence/Threat	Company/Dept. Objective affected
1.		
2.		

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

Probability of Occurrence	%age
Likely	76-100%
Possible	41-75%
Unlikely	11-40%
Remote	0-10%

In determining what constitutes a given level of risk the following scale is to be used for Impact:

Impact	Net Profit	Cost	Quality
Extreme	41-100%	51-100%	Unacceptable Quality
Major	26-40%	31-50%	Quality reduction require top management approval
Material	6-25%	11-30%	Quality reduction require Unit head approval
Minor	0-5%	0-10%	Barely noticeable

In determining what constitutes a given level of risk the following scale is to be used for Control Effectiveness:

Control Effectiveness	Rating
Highly Effective	4
Effective	3
In-effective	2
Highly In-Effective	1

Annexure III – Risk Mitigation Plan Report

Unit & Function		Risk ID No.	
Risk Owner		Risk Category	
Probability* (P)	Likely/ Possible/ Unlikely/ Remote	Impact Category	Financial/ Brand/ Legal/ Regulatory/ People
Severity of Impact* (I)	Extreme/ Major/ Material/ Minor	Control/Mitigation Plan Effectiveness (As first assessed) (C)	Highly Effective/ Effective/ Ineffective/ Highly Ineffective
Residual Risk Exposure (PxIx C)	First assessed = Current =	Control/Mitigation Plan Effectiveness (Current) (C)	Highly Effective/ Effective/ Ineffective/ Highly Ineffective

Mitigation Plan/s – Progress					
S. No.	Control/Activity	Original Closure Date	Completed On	Reasons for delay (if not completed)	Revised Closure Date

* As first assessed