EIH ASSOCIATED HOTELS LIMITED

RISK MANAGEMENT POLICY

1. Introduction

1.1. The Board of Directors (the "Board") of EIH Associated Hotels Limited (the "Company") has adopted the following policy and procedures with regard to Risk Management Framework of the Company.

1.2. This revised policy is in effect from 1st August 2022.

2. Definitions

2.1 **Risk**

Risks are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organisation's business objectives. The exposure to the consequences of uncertainty constitutes a risk.

2.2 **Risk Management**

Risk Management Process can be defined as 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 unfortunate events or to minimize the realization of opportunities.

2.3 **Risk Register**

A prioritized risk register to be maintained at all times, highlighting the key risks for the unit/division where the impact is rated as very high (5).

2.4 **Chief Risk Officer**

A Chief Risk Officer is a person appointed by the company as required under regulation 24(1) read with Sr. No. C, Part D of Schedule II of the listing regulations and is subject to review by the Risk Management Committee.

2.5 **Risk Database**

The risks have been classified based on considered inputs from the Business Units and Corporate Functions. The risk database is a repository of all risks facing the Company categorized as High, Medium or Low based on the impact and likelihood ratings.

2.6 **Trigger Events**

Events or conditions that could lead to the risk.

2.7 **Impact**

The degree of consequences to the organization should the event occur.

2.8 **Likelihood**

The likelihood of the event occurring expressed as an indicative annual frequency.

2.9 **Consequence**

Potential resulting events that could be affected by the key group risk.

2.10 **Risk Source**

Element which alone or in combination has the intrinsic potential to give rise to risk.

2.11 **Risk Rating**

The relative rating determined from the risk score derived from qualitative analysis of impact and likelihood. Categorized as High, Medium or Low.

2.12 **Risk Management Committee**

Risk Management Committee is the Board nominated committee comprising of a mix of Board members and senior executives of the Company. The committee members consist of two Independent Directors, Managing Director, Chief Financial Officer and CFO of EIH Limited. The Company Secretary of the Company is the Secretary of the Committee.

2.13 **Meetings of the Risk Management Committee**

The Risk Management Committee shall meet at least twice in a year and the meetings are conducted in such a manner that on a continuous basis not more than 180 days shall elapse between any two consecutive meetings.

2.14 **Quorum for the meeting of Risk Management Committee**

The quorum for the meeting of the Risk Management Committee shall be either two members or one third of the members of the committee, whichever higher, including at least one member of the Board of Directors in attendance.

2.15 **Functional Risk Management Sub-Committee (FRMS-C)**

Functional Risk Management sub-committee is a sub-committee of Risk Management comprising of Mr. Vikram Oberoi, Managing Director as Chairperson and one Independent Director.

3. The Policy

3.1 **Purpose of the Policy**

i) The policy forms part of the Company's Internal control and Governance arrangements;

ii) The policy explains the Company's approach to risk management, documents the roles and responsibilities of the Board/ Risk Management Committee/Functional Risk Management sub-committee/ Chief Risk Officer/ Risk owners etc.;

iii) It also outlines the key aspects of the risk management process & identifies the reporting procedures.

iv) This policy shall operate in conjunction with other business and operating /administrative practice

3.2 **Policy Statement**

The Company is committed to develop an integrated Risk Management Framework:

i) To achieve the strategic objective while ensuring appropriate management of risks;

ii) To ensure protection of stake holders value;

iii) To provide clear & strong basis for informed decision making at all levels of the organization;

iv) To strive towards strengthening the Risk Management System through continuous learning and improvement.

Every employee of the company is recognized as having role in risk management for identification of risk to treatment and shall be invited and encouraged to participate in the process.

There will be a Functional Risk Management Sub-Committee to determine Key Risks, communicate Policy, objectives, procedures & guidelines and to direct & monitor implementation, practice and performance throughout the Company.

The RMC and the Board shall review the policy & procedures periodically but at least once in two years.

3.3 **Objectives of the Policy**

The prime objective of this Risk Management Policy and Procedure is to ensure sustainable business growth with stability and establish a structured and intelligent approach to Risk Management. This would include the process for development and periodic review of the unit-wise Risk Registers and Databases in order to guide decisions on business risk issues. This would promote a proactive approach in analysis, reporting and mitigation of key risks associated with the business in order to ensure a sustainable business growth.

The specific objectives of the Risk Management Policy are:

1. To establish a risk intelligence framework for the organization;
2. To establish ownership throughout the Organization and embed risk management as in integral part of the business rather than a stand-alone system;
3. To help the decision makers of the organization explicitly take account of uncertainty, the nature of that uncertainty, and work towards a solution to address it;
4. To ensure that all the current and expected risk exposures of the organization are identified, qualitatively and quantitatively evaluated, analyzed and appropriately

managed;

5. To enable compliance with the relevant legal and regulatory requirements and international norms;
6. To assure demonstrable achievement of objectives and improvement of financial stability of the organization.

3.4 **Scope and extent of application**

The policy guidelines are devised in the context of the present business profile, future growth objectives and new business endeavors/services that may be necessary to achieve the goals and the emerging global standards and best practices amongst the comparable organizations. This policy covers all the events with in the company and events outside the company which have a bearing on the company's business.

4. Legal Framework

4.1 In accordance with Regulation 21 of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("Listing Regulations"), the Board of Directors shall define the role and responsibility of the Risk Management Committee ("RMC") and may delegate monitoring and reviewing of the risk management plan to the RMC and such function as it may deem fit, such function shall specifically cover cyber security.

4.2 The role and responsibilities of the RMC shall, *inter alia*, mandatorily include, to formulate a detailed risk management policy which shall include:

1. A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly ESG related risks), information, cyber security risks or any other risk as may be determined by the RMC;
2. Measures for risk mitigation including systems and processes for internal control of identified risks;
3. Business continuity plan.

4.3 In accordance with the above, the RMC has formulated the following policy and procedure for effective management of Company's risks.

5. Risk Management Framework

5.1 **Role and function of RMC**

Besides the mandatory role and responsibility as enumerated in Para C, Part D of Schedule-II of the listing regulations, the RMC shall have the following:

i) Overall responsibility of reviewing with management the Company's risk appetite strategy relating to key risks, including credit risk, liquidity and funding risk, market risk, product risk and reputational risk, all short term and long term risks that significantly affect the operation of the Company as well as the guidelines, policies and processes for monitoring and mitigating such risks;

ii) Reviewing that the company has a structured risk governance framework which includes risk assessment and risk management practices and the guidelines, policies and processes for risk assessment and risk management.

iii) Annual review and approval of Risk Management Framework of the Company;

iv) Periodic review of the risk management processes and practices of the Company and ensure that appropriate measures are taken to achieve prudent balance between risk and reward in both ongoing and new business activities;

v) Evaluation of significant risk exposures of the Company and assessment of management's actions to mitigate the exposures in a timely manner;

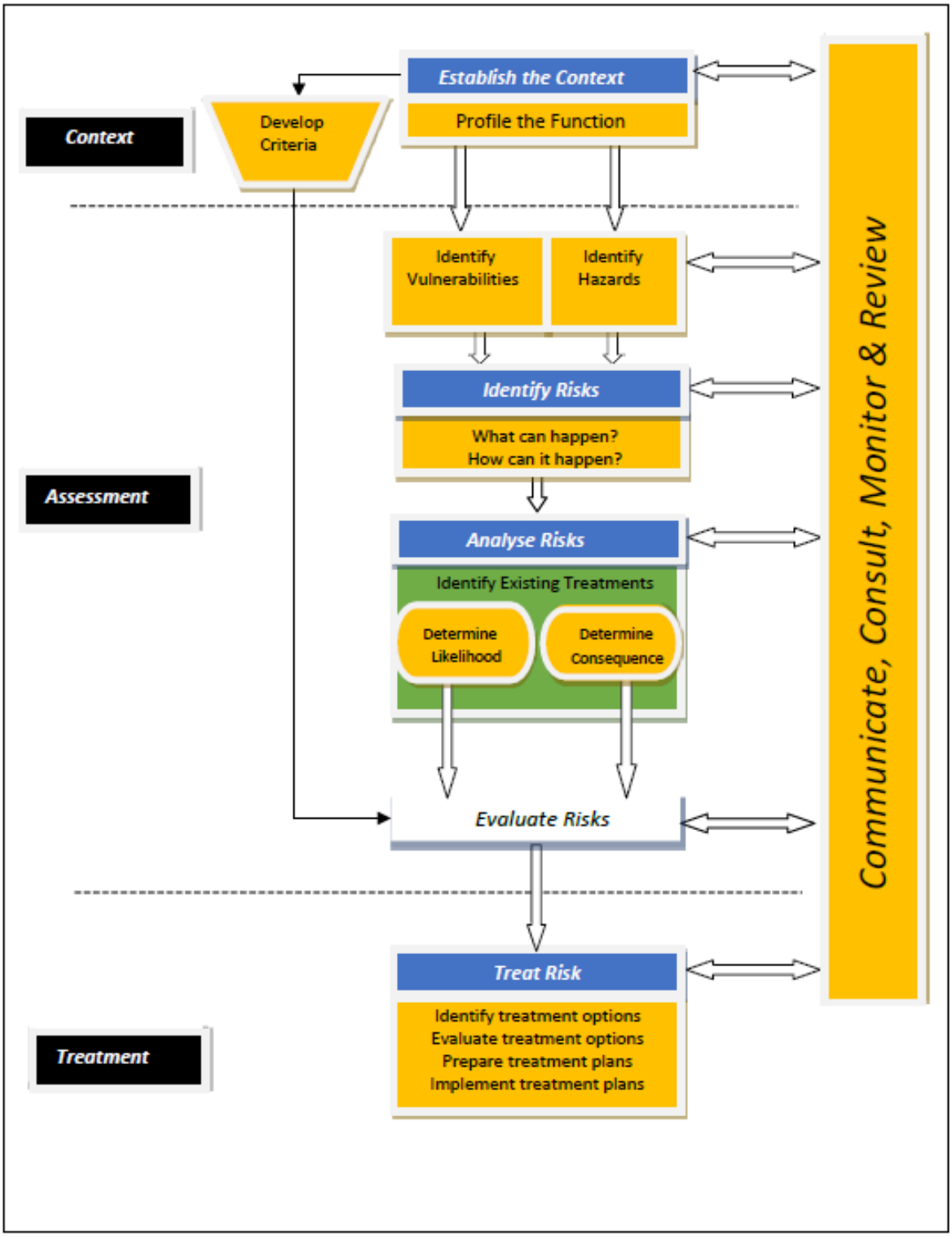
vi) Reporting to the Board its evaluations, actions and recommendations.

5.2 Enterprise Risk Management Framework

The Enterprise Risk Management Framework is a group wide framework aimed at identifying and addressing the risk priorities across the organization. The framework deals with the identification, analysis and treatment of potential and materialized risk. The Risk Management model for each function is as follows:

- Establishing the context;
- Risk Assessment (identification, analysis and evaluation);
- Risk Treatment (mitigation plan);
- Monitoring, review and reporting;
- Communication and consultation

Risk Management Model for each Function



5.2.1 Establishing the Context

Articulate the objectives and define the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process**.**

Establishing the External Context

Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.

The external context can include, but is not limited to:

- The social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- Key drivers and trends having impact on the objectives of the organization; and
- Relationships with, perceptions and values of external stakeholders

Establishing the Internal Context

The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way risks will be managed. This can include, but is not limited to:

- Governance, organizational structure, roles and accountabilities;
- Policies, objectives, and the strategies that are in place to achieve them;
- Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- The relationships with and perceptions and values of internal stakeholders; the organization's culture;
- Information systems, information flows and decision making processes (both formal and informal);
- Standards, guidelines and models adopted by the organizati

5.2.2 Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risk Identification

Risks are about events that, when triggered, cause problems. Hence, risk identification can start with the source of problems, or with the problem itself. This stage involves identification of sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

Risk Analysis

Risk analysis involves:

- consideration of the causes and sources of risk;
- the trigger events that would lead to the occurrence of the risks;
- the positive and negative consequences of the risk;
- the likelihood that those consequences can occur

Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties, other than the organization, that benefit from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

[Refer Appendix I for details of the risk criteria definitions required for analyzing risk impact and likelihood]

5.2.3 Risk Treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are tolerable;
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

Based on the Risk level, the company should formulate its Risk Management Strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Following framework shall be used for risk treatment:

1. **Avoidance (eliminate, withdraw from or not become involved)**
   As the name suggests, risk avoidance implies not to start or continue with the activity that gives rise to the risk.

2. **Reduction (optimize - mitigate)**
   Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied.

3. **Sharing (transfer - outsource or insure)**
   Sharing, with another party, the burden of loss or the benefit of gain, from a risk.

4. **Retention (accept and budget)**
   Involves accepting the loss, or benefit of gain, from a risk when it occurs. Risk retention is a viable strategy for risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

5.2.4 Monitoring and review

In order to ensure that risk management is effective and continues to support organizational performance, processes shall be established to:

- Measure risk management performance against the key risk indicators, which are periodically reviewed for appropriateness;
- Periodically measure progress against, and deviation from, the risk management plan;
- Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;
- Report on risk, progress with the risk management plan and how well the risk management policy is being followed;
- Periodically review the effectiveness of the risk management framework;
- Structured scientific and analytical tools may be used for this purpose.

5.2.5 Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

5.3 Risk Reporting

Reporting is an integral part of any process and critical from a monitoring perspective. Results of risk assessment need to be reported to all relevant stake holders for review, inputs and monitoring.

A. The **Risk Owners** would be required to prepare unit level risk evaluation reports on a quarterly and annual basis.

Quarterly Risk Register Review Report

The Risk Owners shall review the Risk Registers and identify any emerging/new risk and the existing control to mitigate that risk. They must ensure robustness of design and operating effectiveness of existing mitigating controls. If required, re-rate (existing risks)/rate (emerging risks) and prepare, implement action plan for risk treatment in situations where the existing controls are inadequate.

The Quarterly Risk Register Review Report shall include:

- Risk rate movements, if any, along with reasons for changes in the impact and/or likelihood ratings;

- New key risks identified, if any, along with risk criteria ratings and mitigation plans;
- Status of the implementation of mitigation plans and reasons for any delays or non-implementation;

The Risk owner will be responsible for preparing and consolidating the report and the report will be shared with the Chief Risk Officer by 10th day following the quarter end.

Post the review and re-rating of the risks in Risk Register, if the impact is rated below 5 (Very High) for a risk existing in Risk Register, **the same risk shall move to Risk Database**.

Annual Risk Database Review Report

The Risk Owners shall review the respective Risk Database annually and evaluate if any changes are requisite to the impact and likelihood assigned to the risks and, re-rate the risks if applicable as per the guidelines and ensure effectiveness of design and operating effectiveness of existing mitigating controls.

The Annual Risk Database Review Report shall include:

- Risk rate movements, if any, along with reasons for changes in the impact and/or likelihood ratings;
- New key risks identified, if any, along with risk criteria ratings and mitigation plans;
- Status of the implementation of mitigation plans and reasons for any delays or non-implementation;

The Risk Owner will be responsible for preparing and consolidating the report and the report will be shared with the Chief Risk Officer by 45th day of the end of Financial Year.

Post review and re-rating of risk in Risk Database, if the impact is rated as Very High (5), **the same risk shall move to Risk Register**.

[Refer Appendix II for all the reporting formats]

B. The Chief Risk Officer would be required to prepare on a quarterly basis a report for the FRMS-C detailing the following:

- List of applicable risks for the business, highlighting the new risks identified, if any and the action taken w.r.t the existing and new risks;
- Prioritized list of risks highlighting the Key strategic and operational risks facing the Company;
- Root causes and mitigation plans for the Key Risk
- Status of effectiveness of implementation of mitigation plans for the Key Risks identified till date

C. The FRMS-C would be required to submit report to the RMC on a quarterly basis the following:

- An overview of the risk management process in place;
- Key observations on the status of risk management activities in the quarter, including any new risks identified and action taken w.r.t these risks;
- Status of effectiveness of implementation of the mitigation plan for key risks.

[Refer Appendix II for all the reporting formats]

5.4 Risk Management Activity Calendar

Activity	**Timelines**
Risk Register Review report to be submitted by risk owners to the Chief Risk Officer	Quarterly. By 10th day following the quarter end
Risk Database review report to be submitted by risk owners	Annual By 45th day following the financial year end
FRMC-S meeting to review the Corporate key risks/ reports from units	Quarterly
Review by Risk Management Committee	Bi- Annually
Board Meeting	Annually

APPENDIX I

KEY RISKS AND CONTROLS

Risk #	Outcome/ Risks	Control Summary	Significant Measurement Criteria
[R01 RC]	Revenue Contraction	Inadequate Increase in- New Business; existing business/investments	Monitoring targets as per statutory documents: Revenue from existing businesses; Operationalizing ongoing/ new projects; New Contract signings and openings
[R02 LR]	Low or Negative Returns	Decrease in Return on Equity (RoE)	Monitoring Target RoE
[R03 IG]	Inadequate Growth	Loss of market share within competition set	Monitoring, as per STR target in strategy document
[R04 DF]	Deterioration of Financial Health	-Decline in EBIDTA/PAT/Free Cash Flow; Net Debt higher than tolerance limit	Monitoring, as per strategy document
[R05 BI]	Business Interruption	BCP-DRP; Force majeure events; Socio political events.	Implemented BCP-DRP; Adherence to SOPs/ Government Guidelines; Adequacy of Insurance Coverage.
[R06 IE]	Impact on environment	Sustainable energy initiatives and landscape; Waste reduction, recycling and reuse; Architectural parameters	Monitoring energy efficient/ carbon footprint; Implementation of alternate energy sources; Effective waste management including e- waste.
[R07 IR]	Impact on Reputation	Media Management Guest Feedback	Monitoring guest feedback and media; REVPAR leadership; Awards and accolades

[R08 SHS]	Safety, health and security	Safety and Security; Health Risk	Monitoring number of incidents; Adherence to SOPs, government guidelines.
[R09 CR]	Cyber Risk	Cyber Attacks; Legal Non- Compliance; Data protection.	Platform protection and preventive maintenance; Access and DLP Management; Independent system monitoring and audits, SOC; Continuous training and SOP Compliance.
[R10 IC]	Inadequate Compliance	Statutory and Legal Provisions	Monitoring statutory and legal compliances; Effective response mechanism.
[R11 F]	Fraud	Internal Financial Controls; ITG Controls; Insider Trading	Effective DoA, SoD and automated controls; Risk based internal audit.
[R12 TM]	Talent Management	Retention of top talent and management of attrition	HR Policy

APPENDIX II

REPORTING FORMATS AND TEMPLATES

A. Quarterly Risk Register Review Report To be sent to the Chief Risk Officer

Function	Risk Description	Risk Register Ref	Trigger Events	Risk Rating	Proposed Risk Mitigation Plan	Status of implement ation of Risk Mitigation Plan	Action Plan based on Key Risk Indicators

Signature Risk Owner

B. Annual Risk Database Review Report To be sent to the Chief Risk officer

Function	Risk Description	Risk Database Ref	Risk Rating	Proposed Risk Mitigation Plan	Status of implementation of Risk Mitigation Plan	Changes to risk ratings or scenario	Comments, if any

Signature Risk Owner

C. **Risk Movement Report**

To be filled up by the risk owner and submitted to the Chief Risk Officer in case there are any

Risk Movement	**Risk Description**	**Risk Register Ref**	**Movement caused by Change in**	**Reason for change**	**Proposed Risk Mitigation Plan**
From To			**Impact Likelihood**		

Signature Risk Owner

D. Quarterly Key Risk Report

Presented to the Functional sub- committee on Risk Management by the Chief Risk Officer
Quarter Ending:

Function	**Risk Description**	**Risk Category**	**Risk Rating**	**Proposed risk mitigation plan**	**Status of implementation of Risk Mitigation Plan**	**Changes to risk ratings or risk scenario**	**Action plan based on the KRIs monitoring**

Number of Key Risks as per the previous review: Number of Key Risks as per the current review:

Chief Risk Officer

****

Amendments/ Revision

1. *The Risk Management Policy of the Company was originally framed in the year 2017 when the Company voluntarily adopted Risk Management Policy, procedures and frame work;*
2. *The Policy was revised in the year 2019 to comply with the amendments made in regulation 21 of the listing regulations making it mandatory for constitution of a Risk Management Committee in which Board members also formed part of the committee for Top 500 listed entities based on Market Capitalization under which company was covered;*
3. *The Policy was again revised in the year 2021 to incorporate the amendments made in regulation 21 of the listing regulations including addition of Part D in Schedule II in the listing regulations mandating the role and functions of the Risk Management Committee.*
4. *The Policy has been further revised and intended to be put into effect from 1st August, 2022 in incorporate changes in the risk environment and mitigation measures, where necessary*

GLOSSARY

TABLE 1.1 – LIKELIHOOD SCALE AND CRITERIA

Ratings Descriptor	Description
5. Almost Certain	The adverse consequences are expected to occur in most circumstances; and/or high level of recorded incidents; and/or strong anecdotal evidence; and/or a strong likelihood the event will recur; and/ or great opportunity, reason, or means to occur; may occur once every year or more. (or once up to every year)
4. Likely	The adverse consequences will probably occur in most circumstances; and/or regular recorded incidents and strong anecdotal evidence; and/or considerable opportunity, reason or means to occur; may occur once every one to five year
3. Possible	The adverse consequences might occur at some time; and/or few, infrequent, random recorded incidents or little anecdotal evidence; and/or very few incidents in associated or comparable organizations, facilities or communities; and/or some opportunity, reason or means to occur; may occur once every 5 to 20 years
2. Unlikely	The adverse consequences are not expected to occur; and/or no recorded incidents or anecdotal evidence; and/or no recent incidents in associated organizations, facilities or communities; and/or little opportunity, reason or means to occur; may occur once every 20 to 50 years
1. Rare	The adverse consequences may occur only in exceptional circumstances; may occur once every 50 or more years.

TABLE 1.2: CONSEQUENCE SCALE AND CRITERIA

Consequence Descriptor	Description
A. Catastrophic	Risk arising from extraordinary and improbable events which, due to their magnitude, involve a great deal of damage
B. Major	A major risk is defined by its low frequency and its gravity, generally involving a large number of people and/or organizational resources, causing severe damage, often going beyond society's response capacity
C. Moderate	An event that, if it occurred, would cause moderate cost and possible disruptions, but important requirements would still be met
D. Minor	An event that, if it occurred, would cause only a small cost and minor to negligible disruptions, but by and large all requirements would still be achieved
E. Insignificant	Risks that lead to outcomes having little or no importance; trifling. almost or relatively meaningless