



SAYAJI HOTELS (PUNE) LIMITED

Registered Address: Near, Kala Ghoda Circle, Sayajiganj,
Vadodara, Gujarat- 390020 IN

Email ID: cs@shplpune.com Website: www.shplpune.com

Phone No.: 0265-2363030

Risk Management Policy

(Approved by the Board on 11th August, 2023)

CONTENTS

- 1. Introduction**
- 2. Definition**
- 3. Regulatory requirements**
- 4. Risk Organization Structure**
- 5. Risk Management Framework**
 - 5.1. Risk Identification**
 - 5.2. Risk Measurement**
 - 5.3. Risk Examination**
 - 5.4. Solution Implementation**
 - 5.5. Monitoring results**
- 6. Business Continuity Plan**
- 7. Review and Amendments**
- 8. Disclaimer Clause**

1. INTRODUCTION

Risk is an inherent aspect of the dynamic business environment and managing its potential consequences means anticipating those events that could generate adverse and costly outcomes for the organization, while taking actions to avert and/or diminish the effects of such events. Risk Management Policy helps organizations to put in place effective frameworks for taking informed decisions about risks. To minimize the adverse consequence of risks on business objectives the Company has framed this Risk Management Policy. The guidance provides a route map for risk management, bringing together policy and guidance from Board of Directors.

2. DEFINITIONS

2.1 “Act” means the Companies Act, 2013

2.2 “Audit Committee” means the Audit Committee of the Board constituted by the Board of Directors of the Company in accordance with the provisions of Section 177 of the Act read with Regulation 18 of LODR Regulations, 2015.

2.3 “Board” means the Board of directors of the Company.

2.4 “LODR Regulations, 2015” means Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015

2.5 “Policy” means the Risk Management Policy.

2.6 “the Company” means Sayaji Hotels (Pune) Limited

3. REGULATORY REQUIREMENT

Regulations – 17(9)(b) of LODR Regulations, 2015 requires the Board to frame, implement and monitor the risk management plan for the Company. Also, as per Section 134 (n) of the Act, the board of directors’ report must include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the board may threaten the existence of the Company.

As per Section 177 (4)(vii) of the Act, the Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, inter alia, include evaluation of internal financial controls and risk management systems. Responsibility of the Independent Directors: As per Schedule IV [Part II-(4)] of the Act, Independent directors should satisfy themselves that financial controls and the systems of risk management are robust and defensible.

As per Regulations – 21(5) of LODR Regulations, 2015 the Board of the Company shall constitute a Risk Management Committee if the company falls under the criteria of top 1000 listed entities,

determined on the basis of market capitalization, as at the end of the immediate previous financial year.

4. RISK ORGNAIZATION STRUCTURE

The Board is responsible for ensuring that risks, and also opportunities, are identified on a timely basis and that the Company's objectives and activities are aligned with the risks and opportunities identified by the Board. Where necessary, the Board draws on the expertise of appropriate external consultants to assist in dealing with or mitigating risk.

For successful implementation of risk management framework, it is essential to nominate senior management individuals to lead the risk management teams. Senior management involvement will ensure active review and monitoring of risks on a constructive 'no-blame' basis. The Managing Director, with the assistance of senior management as required, has responsibility for identifying, assessing, treating and monitoring risks and reporting to the Board on risk management. This will ensure that risk management is fully embedded in management processes and consistently applied.

The Board is responsible to assess the adequacy of the Company's internal control systems and that its financial affairs comply with applicable laws and regulations and professional practices.

The Internal control framework of the Company assist the Board in identifying, assessing, monitoring and managing risk. It covers all corporate functions and hotel operating units. Internal controls provide reasonable assurance regarding the effectiveness and efficiency of operations, the adequacy of safeguards for assets, assurance regarding reliability of financial statements, the reliability of financial controls and compliance with applicable laws and regulations.

The internal audit process provides a positive assurance about the internal financial control, it converges process framework, risk and control matrix and a scoring matrix, covering all critical and important functions inter-alia revenue management, hotel operations, purchase, finance, human resources and safety. This ensures that all the transactions are authorized, recorded and reported correctly and assets are safeguarded and protected against loss from unauthorized use or disposition.

5. RISK MANAGEMENT FRAMEWORK

Risk management is a continuous process that is accomplished throughout the life cycle of a Company. It is an organized methodology for continuously identifying and measuring the unknowns; developing mitigation options; selecting, planning, and implementing appropriate risk mitigations; and tracking the implementation to ensure successful risk reduction. Effective risk management depends on risk management planning; early identification and analyses of risks; early implementation of corrective actions; continuous monitoring and reassessment; and communication, documentation, and coordination.

The Company's Risk Management Policy is designed to provide the framework to identify, assess, monitor and manage the risks associated with the Company's business. The Board adopts practices

designed to identify significant areas of business risk and to effectively manage those risks in accordance with the Company's risk profile.

The risks involved in the Company and the specific uncertainties are regularly monitored, the Board of the Company formally reviews such risks at least annually. All proposals reviewed by the Board include a consideration of the issues and risks of the proposal.

The potential exposures associated with running the Company are managed by the Directors and Chief Financial Officer who have significant broad-ranging industry experience, work together as a team and regularly share information on current activities.



Risk management is a shared responsibility. The risk management process of the Company includes the following 5 Steps, performed on a continuous basis:

5.1. Risk Identification

This involves continuous identification of events that may have negative impact on the Company's ability to achieve goals. Processes have been identified by the Company and their key activities have been selected for the purpose of risk assessment. Identification of risks, risk events and their relationship are defined on the basis of related data, previous internal audit reports, past occurrences of such events etc. Risk may be identified based on whether they are internal and external, controllable and non-controllable, inherent and residual.

5.2. Risk Analyzation

Risk analyzation is the process of risk prioritization or profiling. Likelihood and Impact of risk events have been measured for the purpose of analyzing the criticality. In risk management the probability of risk is estimated with available data/ information and appropriate risk treatments are worked out in the following areas:

- **Financial and Operative Risk**

The industry in general has a high operating leverage. At organizational level, cost optimization and cost reduction initiatives are implemented and are closely monitored. We control costs through budgetary mechanism and its review against actual performance with the key objective of aligning them to the financial budgets/model. The focus on these initiatives will further inculcate across the organization the importance of cost reduction and control.

- **Human Risk**

Human Resources (HR) Department will add value to all its Units by ensuring that the right person is assigned to the right job and that they grow and contribute towards organizational excellence. Our growth has been driven by our ability to attract good quality talent and effectively engage them in right jobs.

Risk in matters of human resources is sought to be minimized and contained by following a policy of providing equal opportunity to every employee, inculcate in them a sense of belonging and commitment and also effectively train them in spheres other than their own specialization. Employees are encouraged to make suggestions on innovations, cost saving procedures, free exchange of other positive ideas relating to the industry. It is believed that a satisfied and committed employee will give his best and create an atmosphere that cannot be conducive to risk exposure.

Employee-compensation is always subjected to fair appraisal systems with the participation of the employee and is consistent with job content, peer comparison and individual performance. Packages are inclusive of the proper incentives and take into account welfare measures for the employee and his family. We seek to provide an environment that rewards entrepreneurial initiative and performance.

- **Political Risk**

In addition to economic risks, the Company faces risks from the political environment, is affected by events like political instability, conflict between nations, threat of terrorist activities, etc. which may affect the level of travel and business activity. Risks that are likely to emanate are managed by constant engagement with the Government of the day, reviewing and monitoring the country's industrial, labor and related policies and involvement in representative industry-bodies.

- **Environmental, Social and Governance (ESG) Sustainability Risk**

The definition of Sustainability Risk refers to environmental, social and governance events or condition that, if it occurs, could cause an actual or a potential material negative impact on the value of the investment arising from an adverse sustainability impact.

Environment: Climate change, sustainable use and protection of water and marine resources, transition to a circular economy, waste prevention and recycling, pollution prevention control and protection of healthy ecosystems.

Social: Equality, social cohesion, social integration, and labour relations: and

Governance: Sound management structures, employee relations, remuneration of relevant staff and tax compliance.

Sustainability Risk may impact other risk domains, including Operational Risk, Regulatory Risk and Conduct Risk.

Ensuring Senior Management is collectively responsible for the integration of sustainability risks. The company has skills, knowledge and expertise to manage sustainability risks. We are in a position to identify and assess sustainability Risks and seek to mitigate them, where possible. We comply with the regulatory requirement for managing ESG Risk.

Sustainability Risks are taken into account when establishing, implementing and maintaining effective reporting within the company and with third parties.

We have relevant components in relation to the Sustainability Risk including policies, procedures to align company's risk appetite. We set clear goals and targets and expand our monitoring capabilities to ensure we are continuously improving our overall sustainability performance.

- **Economic cycle/Sectorial Risk**

The hospitality industry is prone to impacts due to fluctuations in the economy caused by changes in global and domestic economies, changes in local market conditions, excess hotel room supply, reduced international or local demand for hotel rooms and associated services, competition in the industry, government policies and regulations, fluctuations in interest rates and foreign exchange rates and other social factors. Since demand for hotels is affected by world economic growth, a global recession could also lead to a downturn in the hotel industry.

- **Legal and compliance Risk**

Legal risk exposes to legal action. We focus on evaluating the risks involved in a contract, ascertaining

our responsibilities under the applicable law of the contract, restricting our liabilities under the contract, and covering the risks involved, so that adherence to all contractual commitments can be ensured.

We encourage our employees to place full reliance on professional guidance and opinion and discuss impact of all laws and regulations to ensure company's total compliance. Advisories and suggestions from professional agencies and industry bodies, chambers of commerce etc. are carefully studied and acted upon where relevant.

Changing laws, regulations and standards relating to accounting, corporate governance and public disclosure can create uncertainty for companies. These new or changed laws, regulations and standards may lack specificity and are subject to varying interpretations. Their application in practice may evolve over time, as new guidance is provided by regulatory and governing bodies. This could result in continuing uncertainty regarding compliance matters and higher costs of compliance as a result of ongoing revisions to such corporate governance standards. We strive to place robust process with the help of consultants to mitigate and minimize such compliance risk.

- **Risk related to Cyber Security**

Cyber security has been a big concern for the hospitality business, we are more focused on preventing data and identify theft. We collect a lot of information from our guests to insure them against damages and to fuel their own rewards programs. This makes them popular targets among cyber criminals and hackers, as a single breach could result in hundreds or even thousands of pieces of guests' personal information (names, addresses, social security numbers, etc.) and payment details being compromised. Because of this, we need to make sure that data is protected against fraudsters.

A security breach has huge ramifications. At the very least, the company is required to contact other guests (past and present) and inform them that their data may have been compromised – this alone can be costly and may also lead to brand damage. If stolen data is used by fraudsters, the company may face liability claims for failure to protect data and maintain reasonable safeguards.

Being in hospitality, the Company use digital systems to automate tasks and manage data of guests, we identify potential cyber security related risks and works on mitigation of the same to bring solution to the table.

5.3. Risk Examination

Risk examination is to be conducted using a risk matrix for likelihood and Out-turns, taking the existing controls into consideration. Risk events assessed as "high" criticality may go into risk mitigation planning and implementation; low and medium critical risk to be tracked and monitored on a watch list.

The Risk Reporting Matrix below is used to determine the level of risks identified. A risk reporting

matrix is matched with specific likelihood ratings and Out-turns ratings to a risk grade of low (yellow), medium (orange) and high (red).

S. No.	Out-turns	Likelihood			
		1	2	3	4
		Rare	Unlikely	Likely	Almost certain
4	High				
3	Medium				
2	Low				
1	Insignificant				

The likelihood of occurrence of risk is rated based on number of past incidences in the industry, previous year audit observations, future trends or research available.

Risk Score = Out-turns * Likelihood	
11-16	High
6-10	Medium
0-5	Low

5.4. Solution Implementation

Risk mitigation options are considered in determining the suitable risk treatment strategy. For the risk mitigation steps, the cost benefit analysis needs to be evaluated. Action plans supporting the strategy are implemented by the board as per the risk score. Implementation of action plan consist of first getting up to carry out the plan and then actually implementing the various steps of the plan.

Our adequate organizational structure and set of procedures in place, the various elements of plan get successfully implemented. The Basic elements of mitigation measures are flexible to be the most efficient and includes:

- Risk reduction actions
- Contingency management
- Recovery

The Board delegates responsibility for various elements of the plan to those who are in the best position to complete them and follow up with them to ensure that the task given actually gets completed.

5.5. Monitoring results

Risk management uses the output of a risk assessment and implements counter measures to reduce the risks identified to an acceptable level. This policy provides a foundation for a robust plan for the process

of assessing and mitigating risks identified within functions and associated processes.

In circumstances where the accepted risk of a particular course of action cannot be adequately mitigated, such risk shall form part of strict reviewing and their status shall be continuously monitored.

6. BUSINESS CONTINUITY PLAN

6.1 Introduction

Business Continuity Plan (“BCP”) identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

A BCP is closely linked with disaster and emergency management, risk assessment, health and safety directives and various regulations. It should provide greater structure and consistency in the public response to emergencies.

6.2 Purpose of this Business Continuity Plan

BCP is designed to help the Company recover from a disruption in service. Specifically, this plan provides policy and guidance to ensure that the Company can respond effectively to a disruption and restore essential services to the public as quickly as possible.

6.3 Objectives of BCP

The objectives of this business continuity plan are to:

- Identify advanced arrangements and procedures that will enable the company to respond quickly to an emergency event and ensure continuous performance of critical business functions.
- Reduce employee injury or loss of life and minimize damage and losses.
- Protect essential facilities, equipment, vital records, and other assets.
- Reduce and mitigate disruptions to business operations.
- Identify managers and other staff who might need to be relocated depending upon the emergency.
- Identify teams which would need to respond to a crisis and describe specific responsibilities.
- Facilitate effective decision-making to ensure that company’s operations are restored in a timely manner.
- Provide support to employees and their families during an event so that employees know that the safety of their families has been addressed, and that employees will therefore be available to

work and help restore company function.

- Identify alternative courses of action to minimize and/or mitigate the effects of the crisis and shorten the company's response time.
- Quantify the impact of any kind of emergency in terms of money, time, services, and work force.
- Recover quickly from an emergency and resume full service to the public in a timely manner.

6.4 Direction and Control

During a disaster/disruption, it is imperative to have a clear chain of command and delegation of authority. The Board is responsible for drafting and finalizing the Company's BCP. This includes developing a project work plan outlining the steps necessary to draft the plan and ensuring that each step is completed. Further the Board will finalize the questions to be asked as part of the Business Impact Analysis (BIA) process.

Each head of department will fill out a BIA questionnaire and will also assign staff within his/her own unit to answer BIA questions, as necessary. The Board will meet periodically to review project progress, will revise work plan as necessary, and will edit and approve the final plan.

The Board further is responsible for responding in the event of a disaster. This includes assessing potential damage to the Company facility(ies). This also includes taking lead responsibility for ensuring that the company can function effectively during a crisis and can resume business operations as quickly as possible.

The Board or any officer, delegated by Board for the same, may order activation of the Company's BCP.

6.5 BCP Activation procedure

This procedure involves following steps which are given here below:

6.5.1 Identification of Potential Disaster Status

Criteria for determining whether a particular emergency situation requires that emergency actions be taken or the BCP be enacted include:

- Is there an actual or potential threat to human safety?
- Is there likely to be a need to involve emergency services?
- Is there an actual or potential serious threat to buildings or equipment?
- Is there an actual or potential loss of IT/network?
- Is there an actual or potential loss of workforce?

Destructive events and emergencies - Any event that prevents the normal operations of the hotel, whether due to an event whether its natural or manmade.

Following is the inclusive list of events, any of which could have a cataclysmic effect on the company and determine the probability of each one affecting our business by applying the above-mentioned questionnaire:

- Transport accidents
- Key staff illness
- Terrorist strikes and bombings
- Fire, Fuel crises and Sabotage
- Vandalism and theft (including data theft)
- Civil disorder and industrial action
- Flooding or Earthquakes
- Computer and power outages, gas leaks and utility problems
- Epidemic and pandemic scale illnesses (SARS, flu, bird flu, foot & mouth)
- Drought
- Oil spills and man-made disasters
- Disasters affecting suppliers and customers
- Hurricanes, Cyclones, Tornados, wind storms and typhoons

6.5.2 Warning Conditions

a. With warning:

It is expected that in some cases, the Company will receive a warning at least a few hours prior to an event. This will normally enable the plan to be enacted with an orderly notification and evacuation of staff.

b. Without warning:

The ability to execute this plan following an event with little or no warning will depend on the severity of the emergency and the number of company's personnel who have been affected by the event.

Non-Duty Hours: Although the Corporate office and Hotel buildings may be rendered inoperable, it is likely that the majority of the staff could be alerted and deployed to the alternate site.

Duty Hours: If possible, this plan will be activated and the pre-designated available staff will be deployed.

6.5.3 Communication Plan

6.5.3.1 Board Communications

During a crisis situation, communication with all affected parties – from staff to customers– is vital. The information provided to all audiences must be accurate and timely. The Company is responsible for issuing information to:

- Help prevent loss of life and property

- Warn and inform people in danger about the threat, and tell them what they can do to reduce their risk
- Improve appropriate public response to future emergencies and disasters through education.

The estimate of the timing to return to normal working operations will be announced by the board with care and considering all aspects of the crisis.

6.5.3.2 Staff Communications

- If a staff member learns of a potential crisis situation, the staff person should immediately contact his/her department head or authorized official of the company.
- If the building structure is in question, staff should not enter the building.

Once a crisis has occurred, the Board shall communicate with all parties.

6.5.3.3 Customer Communications

The Board or authorized official of the board will develop an official statement for customers. Depending upon the type and severity of the event, the statement may be issued in the following ways:

- Through local media
- Scheduled customers may be called or e-mailed
- Notice may be posted at the affected facility(ies)

A brief message shall be issued explaining the crisis and directing callers to the Company's web site for additional information and updates.

6.5.3.4 Management and Staff Communications

The Board or authorized official of the board will develop an official statement for managers and staff. If the event happens during work hours, and depending upon the severity of the event:

- Staff may be sent home
- Staff may be asked to assist in implementing work-around procedures

If the event happens after work hours, or becomes a multi-day event, staff will be contacted through:

- Employee call tree which involves all department heads, Human resources manager and other designated executives.
- A call-in number for information about which types of employee positions are to report to work.
- Information posted to company's web site.

6.5.3.5 Suppliers Communications

The Board shall designate a person to contact with suppliers during the business recovery phase. Designated person will use emergency procurement procedures and receive authorization for emergency purchases from the Board or authorized official of the board.

6.5.3.6 Other Third Parties Communications

The Board or authorized official of the board shall be primarily responsible for all contact with other third parties. If appropriate, after consulting with the Board of director, the authorized official will provide information to other staff to assist in responding to these requests for information.

6.5.4 Recovery Plan

The BCP formed shall ensure continuity of operations in any of the following situations:

- The facility is either temporarily or permanently unavailable.
- The facility is disabled by power loss.
- The facility is disabled by loss of computer function
- Any other situation which disturbs the continuity of operations of the Company.

6.5.4 Recovery Procedure

The recovery procedure will depend largely upon how quickly access to computers can be restored. If remote computer access is functional, pre-identified staff will be asked to work remotely until the corporate office is again available.

When computer systems are available, remote work will continue until the Corporate office is again available.

The recovery procedure also depends upon the length of time the power is anticipated to be out. Being a Hotel Company, our major staff has to be physically present for working, in case the crisis stress for major staff to absent from the Hotel unit, we will use the call tree to let employees know not to report to work until further notice unless they will be reporting to a remote worksite that is unaffected by the outage.

The recovery procedure consists of working with IT to restore normal systems. After an emergency declaration we may purchase if necessary, to expedite recovery.

The recovery procedure depends upon the length of time the computer system is anticipated to be out. If we anticipate restoration in two days or less, we will complete those processes that do not require the affected computer systems.

7. REVIEW AND AMENDMENTS

This Policy shall be reviewed and amended annually to ensure it meets the requirements of legislation and the needs of Organization. The Board of Directors will be the approving authority for the company's overall Risk Management System. The Board will, therefore, monitor the compliance and approve the Risk Management Policy and any amendments thereto from time to time.

8. DISCLAIMER CLAUSE

The Management Cautions Stakeholders that the risks outlined above are not exhaustive and are for information purposes only. Management is not an expert in assessment of risk factors, risk mitigation measures and management's perception of risks. Stakeholders are therefore requested to exercise their own judgment in assessing various risks associated with the Company.

***** End *****