

# Risk Management Policy

# IRCTC

Indian Railway Catering and Tourism Corporation Limited

(Amended w.e.f. 12 Aug, 2021)



## TABLE OF CONTENTS

1	INTRODUCTION .....	2
2	RISK MANAGEMENT VISION STATEMENT .....	3
3	DEFENITIONS .....	4
4	SCOPE AND OBJECTIVES.....	9
5	RISK MANAGEMENT POLICY .....	10
	ELEMENTS OF THE RISK MANAGEMENT PROCESS.....	11
	APPLICABILITY .....	12
	PRINCIPLES .....	12
	PHILOSOPHY.....	12
	STRATEGY .....	13
6	ROLE OF INTERNAL AUDIT .....	14
7	RISK MANAGEMENT DOCUMENTATION .....	15
8	RISK MANAGEMENT GOVERNANCE STRUCTURE.....	17
	RISK MANAGEMENT COMMITTEE (RMC) .....	17
	CHIEF RISK OFFICER (CRO) .....	17
	RISK OWNERS AND RISK COORDINATORS (RO/RC).....	18
	RISK MANAGEMENT ROLES AND RESPONSIBILITIES.....	18
9	RISK APPETITE AND TOLERANCES .....	20
10	RISK MANAGEMENT PROCESS .....	21
	RISK IDENTIFICATION.....	21
	METHODS OF RISK IDENTIFICATION.....	21
	RISK ASSESSMENT.....	22
	RISK CATEGORIES.....	24
	RISK EVALUATION .....	24
	RISK MITIGATION.....	25
	ESCALATION OF RISKS.....	26
	FLOWCHART DEPICTING RISK MANAGEMENT PROCESS.....	28
11	ORGANISATION STRUCTURE.....	29
12	ACTION PLAN.....	29
13	RISK MANAGEMENT INFORMATION SYSTEM (MIS) .....	30
14	APPROVAL OF THE POLICY .....	30
15	REVIEW OF THE POLICY.....	30
16	PUBLICATION OF THE POLICY.....	31



## 1 INTRODUCTION

Ministry of Corporate Affairs, Government of India for the first time accepted the concept of Risk Management and its relevance for the smooth functioning of the Corporate sector in India across all companies including unlisted companies and therefore introduced a specific provision on Risk Management under paragraph (II) (C) of Corporate Governance Voluntary Guidelines, 2009

### **(II) (C) Risk Management**

i) The Board, its Audit Committee and its executive management should collectively identify the risks impacting the company's business and document their process of risk identification, risk minimization, risk optimization as a part of a risk management policy or strategy.

The Companies Act of 2013 is a landmark legislation with comprehensive focus on corporate governance. This Act shall have far reaching consequences on all companies incorporated in India.

As per Section 134 (3) (n) of Companies Act, 2013, there shall be, attached to statements laid before a company in general meeting, a report by its Board of Directors, which shall include a statement indicating development and implementation of a risk management policy for the company including identification therein 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 Companies Act, 2013, Audit Committee of a company shall evaluate the internal financial controls and risk management systems of the Company.

Furthermore, as per clause 7.3.1 of Department of Public Enterprises' Guidelines on Corporate Governance, 2010; the Company shall lay down procedures to inform Board members about the risk assessment and minimization procedures. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework. Procedures will be laid down for internal risk management also.

As per Committee of Sponsoring Organizations of Tread way Commission (COSO)- Enterprise Risk Management is a process affected by an entity's Board of Directors, Management and other personnel, applied in strategy setting, designed to identify potential events that may affect the entity and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.





## 2 RISK MANAGEMENT VISION STATEMENT

1. To adopt risk management practices aligned with the goals and objectives of the organization to ensure that organizational risks are reduced to an acceptable level and the impact of adverse events is minimized.
2. IRCTC considers risk management to be fundamental to good management practice and a significant aspect of corporate governance. Effective management of risk shall provide an essential contribution towards the achievement of IRCTC's strategic and operational objectives and goals.
3. Risk management is an integral part of IRCTC's decision making and routine management, and is incorporated within the strategic and operational planning processes at all levels across IRCTC.
4. Risk assessments is conducted on new ventures and activities, including projects, processes, systems and commercial activities to ensure that these are aligned with IRCTC's objectives and goals.
5. Any risks or opportunities arising from these assessments are identified, analyzed and reported to the appropriate management level.
6. Maintaining a strategic risk register.
7. Commitment to ensure that all staff is provided with adequate guidance and training on the principles of risk management and their responsibilities to implement risk management effectively.
8. To regularly review and monitor the implementation and effectiveness of the risk management process, including the development of an appropriate risk management culture across IRCTC.

### Note:

**Implementation of this policy will only facilitate better management of risk not its elimination. The aim of the policy is not to have risk eliminated completely from the activities of IRCTC, but rather to ensure that every effort is made by IRCTC to manage risk appropriately to maximize potential opportunities and minimise the adverse effects of risk.**



### 3 DEFINITIONS

1. **Risk** - Committee of Sponsoring Organization (COSO) defines 'Risk' as the possibility that an event will occur and adversely affect the achievement of objectives. A business risk is the threat that an event or action will adversely affect an organization's ability to maximize shareholder value and to achieve its business objectives.
2. **Risk Management** - Risk Management is a structured, consistent and continuous process for identification and assessment of risks, undertaking control assessment and continuous monitoring of exposure of the risk. It is a defined and disciplined approach aligning strategy, processes, people, technology and knowledge with the purpose of evaluating and managing the uncertainties the enterprise faces as it creates value. A Risk Management Framework provides direction at all levels of management to enhance and evaluate the effectiveness of an entity's enterprise risk management.
3. **Effect** - Deviation from the expected — positive and/or negative. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Risk is often characterized by reference to potential events and consequences, or a combination of these. It is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
4. **Uncertainty** – It is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.
5. **Risk Management Framework** - Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.  
  
The foundations include the policy, objectives, mandate and commitment to manage risk. The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities. The risk management framework is embedded within the organization's overall strategic and operational policies and practices.
6. **Risk Management Policy** - Statement of the overall intentions and direction of an organization related to risk management
7. **Risk Attitude** - Organization's approach to assess and eventually pursue, retain, take or turn away from risk constitutes its Risk Attitude.
8. **Risk Management Plan** – It's a scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk.






Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

9. **Risk Owner** - Person or entity with the accountability and authority to manage a risk is the Risk Owner
10. **Risk Management Process** - Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.
11. **Establishing the Context** - Defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy
12. **External Context** - External environment in which the organization seeks to achieve its objectives.

External context can include:

- a) the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
  - b) key drivers and trends having impact on the objectives of the organization; and
  - c) relationships with, and perceptions and values of external stakeholders
13. **Internal Context** - Internal environment in which the organization seeks to achieve its objectives, and can include:
    - a) governance, organizational structure, roles and accountabilities;
    - b) policies, objectives, and the strategies that are in place to achieve them;
    - c) the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
    - d) information systems, information flows and decision-making processes (both formal and informal);
    - e) relationships with, and perceptions and values of internal stakeholders;



- f) the organization's culture;
- g) standards, guidelines and models adopted by the organization; and
- h) form and extent of contractual relationships.

**14. Communication and Consultation** - Continuous and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk.

The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management of risk.

Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue.

Consultation is:

- a) a process which impacts on a decision through influence rather than power; and
- b) an input to decision making, not joint decision making.

**15. Stakeholder** - Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity. A decision maker can be a stakeholder.

**16. Risk Assessment** – It's the overall process of risk identification, risk analysis and risk evaluation

**17. Risk Identification** – A process of finding, recognizing and describing risks. Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.

**18. Risk Source** - Element which alone or in combination has the intrinsic potential to give rise to risk. A risk source can be tangible or intangible.

**19. Event** - Occurrence or change of a particular set of circumstances.

- a) An event can be one or more occurrences, and can have several causes. An event can consist of something not happening.
- b) An event can sometimes be referred to as an "incident" or "accident".





- c) An event without consequences can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.
20. **Consequence** - Outcome of an event affecting objectives. An event can lead to a range of consequences.
- a) A consequence can be certain or uncertain and can have positive or negative effects on objectives.
  - b) Consequences can be expressed qualitatively or quantitatively.
  - c) Initial consequences can escalate through knock-on effects.
21. **Likelihood** – it’s the ‘Chance’ of something happening. In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period). In risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability”.
22. **Risk Profile** - It is a description of any set of risks. The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.
23. **Risk Analysis** - It is a process to comprehend the nature of risk and to determine the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment. This includes ‘Risk Estimation’.
24. **Risk Criteria** - Terms of reference against which the significance of a risk is evaluated is Risk Criteria. Risk criteria are based on organizational objectives, and external and internal context. Risk criteria can be derived from standards, laws, policies and other requirements.
25. **Level of Risk** - Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.
26. **Risk Evaluation** - Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists in the decision about risk treatment.
27. **Risk Treatment** - It’s a process to modify risk. Risk treatment can involve:
- a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;





- b) taking or increasing risk in order to pursue an opportunity;
- c) removing the risk source;
- d) changing the likelihood;
- e) changing the consequences;
- f) sharing the risk with another party or parties (including contracts and risk financing); and
- g) retaining the risk by informed decision.

Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”. Risk treatment can create new risks or modify existing risks.

28. **Control** – A measure that is modifying risk. Controls include any process, policy, device, practice, or other actions which modify risk. Controls may not always exert the intended or assumed modifying effect.
29. **Residual Risk** - Risk remaining after risk treatment is Residual Risk. Residual risk can contain unidentified risk. Residual risk can also be known as “retained risk”.
30. **Monitoring** - Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected. Monitoring can be applied to a risk management framework, risk management process risk or control.
31. **Review** - Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. Review can be applied to a risk management framework, risk management process, risk or control.




## 4 SCOPE AND OBJECTIVES

Risk Management is an integral part of good management. The application of sound risk management allows for continual improvement and greater certainty in decision making. The end result is that there is a better chance that Organization objectives are met. Indian Railway Catering and Tourism Corporation Limited (IRCTC), a leading player in the Indian Public Sector, is exposed to number of risks in its ordinary course of business. This is inevitable, as there can be no business activity without the acceptance of risks and associated profit opportunities.

Risk Management Policy has been developed to assist in establishing and maintaining an effective risk management framework for IRCTC. IRCTC operates in a business environment that is characterized by intensifying competition and a greater number of government regulations. Further, increasing speed of business activity and opportunities for expansion and diversification are rapidly changing and expanding the quantum and importance of risks faced by the company. The Risk management framework assists the management in effectively dealing with uncertainty and associated risks & opportunities, thereby enhancing the organization's capacity to build value.

### **Key objectives of the Policy:**

1. To ensure that all the current and future material risk exposures of the company are identified, assessed, quantified, appropriately mitigated and managed;
2. To establish a framework for the company's risk management process and to ensure companywide implementation;
3. To ensure proactive rather than reactive management;
4. To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices;
5. To provide assistance to and improve the quality of decision making throughout the organization;
6. To assure business growth with financial stability.

**This Policy applies to all employees of IRCTC and to its every business & functions.**





## 5 RISK MANAGEMENT POLICY

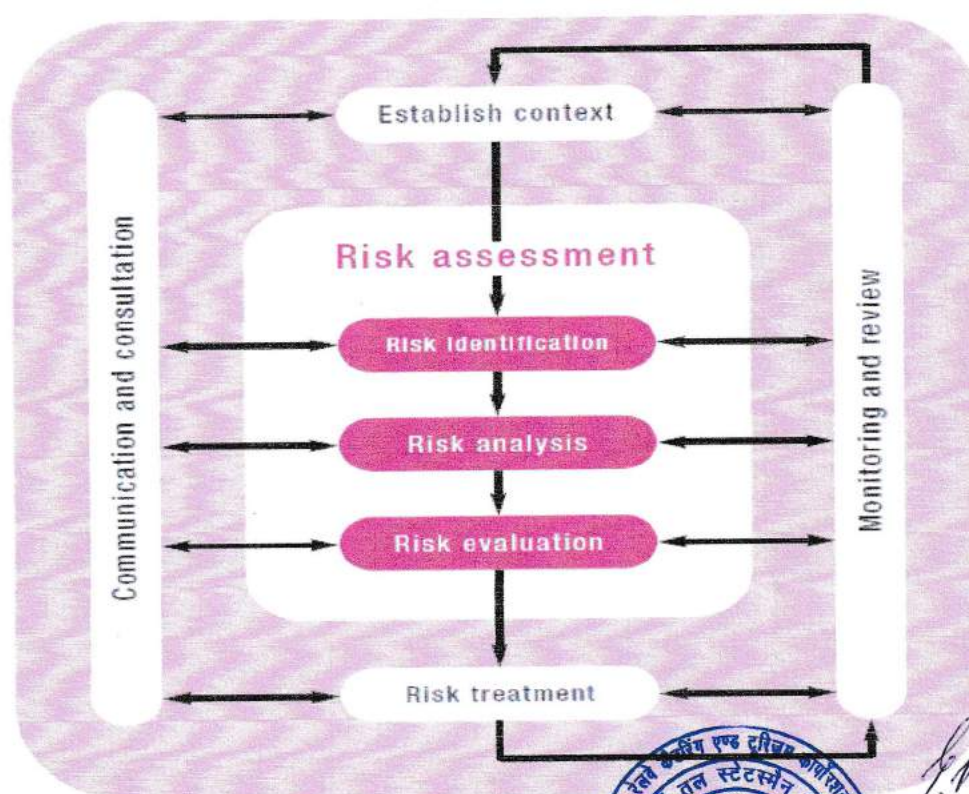
The company is committed to implement a robust risk management process to:

- improve its ability to prevent or timely detect risk event;
- identify, discuss, escalate and provide suggestions to deal with risk issues;
- standardize risk management principles and language across the company;
- improve sharing of risk information;
- provide flexibility for managing upside and downside scenarios;
- to provide a commitment that risk management is a core management capability;
- to control corruption risk

This policy is intended to ensure that an effective risk management framework is established and an appropriate reporting mechanism for the same is embedded within the company. The management 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 policy complements and does not replace other existing compliance programs. It is built on the established principles of sound risk management as detailed in recognized sources such as ISO 31000:2009 and AS/NZS 4360:2004

### **Risk Management Process (based on ISO 31000)**



## 5.1 Elements of the Risk Management Process

The main elements of the Risk Management Process are as follows:

### 1. Communicate and Consult

Communicate and consult with internal and external stakeholders as appropriate to each stage of the risk management process and concerning the process as a whole.

### 2. Monitor and Review

It is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement. Risks and the effectiveness of treatment measures need to be monitored to ensure that the changing circumstances do not alter the priorities. The process followed is as under:

#### a) Establishing the Context

Establishing the external, internal and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined.

#### b) Identifying risks

Identifying where, when, why and how events could prevent, degrade, delay or enhance the achievement of the objectives.

#### c) Analyzing risks

Identifying and evaluating existing controls, determining consequences and likelihood and hence the level of risk. This analysis should consider the range of potential consequences and how these could occur.

#### d) Evaluating risks

This involves comparing the estimated levels of risk against the pre-established criteria and the balance between potential benefits and adverse outcomes. This helps in making decisions related to the extent and nature of treatments required as well as about priorities.

#### e) Treating risks

Developing and implementing specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.



*S. Kumar*



## 5.2 Applicability

Risk is an inherent aspect of all business activities. Sound risk management principles must become part of routine management activity across IRCTC.

This policy is applicable from the date as mentioned on the "Document Control Sheet" and applies to whole of the company and includes all functions, departments, business units.

It shall also apply to any other entities that may be under the control of the management of IRCTC.

## 5.3 Principles

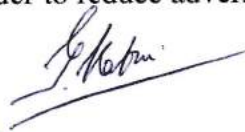
Risk Management is not a onetime event or exercise: rather it is a process which encompasses series of continuous actions that permeate into the activities of the company. Risk management is not an end in itself but rather an absolutely important measure to develop organizational resilience. The risk management principles applicable to the company are as elaborated below:

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

## 5.4 Philosophy

The Company shall follow the Risk management philosophy as under:

1. Drive business growth and competitiveness through strategic and structured risk taking and sustained risk mitigation.
2. To deliver quality service on time by managing the risks encompassing it. The Company cannot eliminate all risks; however, it can systematically identify, analyze, evaluate, address, prioritize treatment & communicate to appropriate levels, the risk that arise in the course of the business and take risk mitigation decisions and execute such decisions with a risk-aware mindset in order to reduce adverse impact of the risk and discourage risk avoidance.

3. Compliance to rules, regulations and procedures can mitigate some critical risk but not all of them and the risk can be managed.

## 5.5 Strategy

The Company recognises that risk is an integral and unavoidable component of business and is committed to managing the risk in a proactive and effective manner. The Company believes that the Risk cannot be eliminated.

However, it can be:

1. Reduced, by having good internal controls;
2. Retained,
  - a) If the cost of mitigation is more than the cost of risk itself, or
  - b) In anticipation of higher profits by taking on more risk
  - c) Transferred to another party who is willing to take risk; and;
  - d) Avoided, based on sound reasoning, by not undertaking risky businesses/activities.





## 6 ROLE OF INTERNAL AUDIT

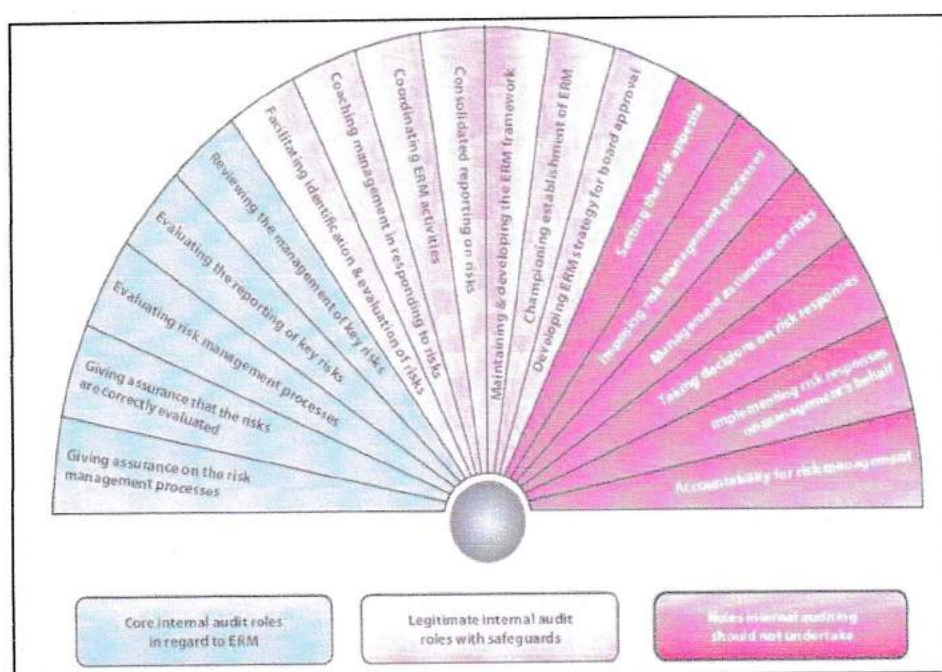
Internal auditing professional standards require the function to evaluate the effectiveness of the organization's Risk management activities.

The Company recognizes the synergy and inter-dependence between the internal audit function and the risk management program and wishes to draw up a plan which will ensure that-

- Internal audit plans are drawn up based on outcomes of risk assessment program
- Internal audit function provides effective, independent and objective evaluation of risk management process at regular intervals.
- Risk management program receives constant inputs on controls evaluation from the internal audit function

The IIA (Institute of Internal Auditors Inc., USA) Position Paper titled The Role of Internal Auditing in Enterprise-wide Risk Management provides an illustration that presents a range of risk management activities and indicates which roles an effective professional internal audit activity should and, equally importantly, should not undertake.

The five areas on the left of the “fan” represent core internal audit roles for risk management. The paper states that “They form part of the wider objective of giving assurance on risk management. An internal audit activity complying with the International Standards for the Professional Practice of Internal Auditing can and should perform at least some of these activities.”



## 7 RISK MANAGEMENT DOCUMENTATION

Appropriate documentation at each stage of the risk management process should be followed. This framework provides a guide to documentation standards and how they are to be implemented. The documentation will serve the following purpose:

- a) provide evidence or a systematic approach to risk identification and analysis
- b) provide a record of risks to support the development of a database of the company's risks
- c) provide risk mitigation plans for approval and subsequent implementation
- d) provide accountability for managing the risks identified
- e) facilitate continuous monitoring and review
- f) provide an audit trail, and
- g) share and communicate risk management information across the company.

The responsibility for documenting individual risks specific to business functions would be assigned to the Risk Management Committee. The designated Chief Risk Officer ('CRO') would be responsible for ensuring that the required documentation required at the corporate level has been developed and maintained up to date. The Risk Coordinators (RC) at the functional level would be responsible for ensuring that the required documentation required at the functional level has been developed and maintained up to date.

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

### 1. Risk Management Policy

The Policy provides the overall framework for risk management process of the company. Further amendments may be initiated / approved by the Risk Management Committee (RMC) and ratified by the Board.

### 2. Risk Register

Risk register is a consolidated list of all risks that have been identified during the periodical review. It is the key document used to communicate the current status of all known risks and is used for management reviews, control and reporting. The consolidated risk register is owned by the RMC and maintained by the CRO. The functional level risk registers are owned by the respective Risk Management Committee (RMC) and maintained by the Risk Coordinators at unit level.





### 3. Risk Management Meeting Proceedings

The RMC meeting template is used to document the minutes of meetings. The template aids in capturing and documenting the key discussion points and decisions taken during the meetings.

### 4. Risk Profile

Risk profile helps the management and the Board to effectively monitor the management of the risk faced by the company. It provides detailed description of the risk and related information required for proposing and documenting mitigation plan to reduce the risk exposure.



## 8 RISK MANAGEMENT GOVERNANCE STRUCTURE

The Board has the responsibility of determining the strategic direction of the organization and creating the context for risk management. There need to be arrangements in place to achieve continuous improvement in performance.

### 8.1 Risk Management Committee (RMC)

The RMC is the committee formed at the functional level in the risk management governance structure, comprising of key decision makers within the respective function/unit. It is responsible for adopting and implementing the risk management framework at their respective function/unit. RMC is a Board level committee.

#### **Composition:**

The Risk Management Committee shall have minimum three members with majority of them being members of the board of directors, including one independent director.

#### **Operation and Periodicity of Meeting:**

The designated Risk Coordinator coordinates activities relating to the RMC. The RMC shall meet at least twice in a year or more frequently if required for urgent matters. Reports of RMC activities (agendas, decisions) and minutes of meetings (including attendance) will be maintained for each meeting by the Risk Coordinator as identified by individual RMCs.

The functional heads and other senior personnel may be invited to participate in the committee meetings as required.

#### **Quorum for the meeting of RMC**

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

#### **Time gap between two meetings of RMC**

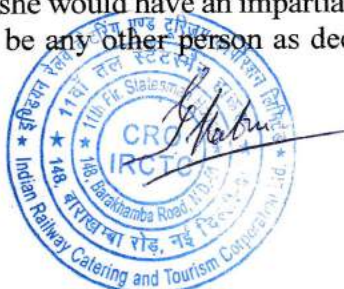
The meetings of the Risk Management Committee shall be conducted on a continuous basis and not more than one hundred and eighty days should elapse between any two consecutive meetings

### 8.2 Chief Risk Officer (CRO)

The CRO would be a member of the RMC and be responsible as coordinator for risk management activity for the entire company. The CRO would liaise with the Risk Coordinators to coordinate flow of information between them and the RMC.

The CRO would be responsible to ensure that meetings of the RMC are held quarterly or as required to review the risks identified, to appraise the RMC and Board of Directors about the status of the risk management at the company.

The Chief Risk Officer (CRO) for the company should be the officer taking care of Internal Audit at IRCTC, as being the officer of the board, he/she would have an impartial view about the risks being identified. However, CRO may also be any other person as decided by the Board.





### 8.3 Risk Owners and Risk Coordinators (RO/RC)

Risk Owners are individuals who understand the risk better and can contribute in mitigation of the same. The Risk-Owners own, and therefore are deemed accountable for the effective management of risks assigned to them. Each risk will have one Risk Owner. The Risk Owners shall put in coordinated efforts to discuss the risks in detail, identify gaps in existing controls and thereby propose risk mitigation plans for the assigned risk. Risk Owner is also responsible to implement the approved mitigation plan and periodically review the implementation status of mitigation plans.

The Risk Coordinators would be the member of the respective RMCs and be responsible as coordinator for risk management activities for their respective functions. The Risk Coordinator would liaise with the risk Owners to coordinate the flow of information between them and the RMC. The Risk Coordinator would be responsible to ensure that meetings of the RMC are held quarterly or as required, to review the risks identified and necessary attendance and minutes of meetings are maintained. The Risk Coordinator would be responsible to appraise the RMC chairperson and the CRO about the status or the risk management at their respective RMC.

Risk Owners and Risk Coordinator will be nominated by the respective RMC Head.

### 8.4 Risk Management Roles and Responsibilities

<b>Board of Directors</b>	<ul style="list-style-type: none"> <li>○ Approve Risk Management Policy</li> <li>○ Review and approve risk management process and provide inputs/directions to the executive management</li> <li>○ Set Risk Appetite for the Company</li> </ul>
<b>Audit Committee</b>	<ul style="list-style-type: none"> <li>○ Lead the Risk management initiative within the company</li> <li>○ Set standards for risk documentation and monitoring</li> <li>○ Recommend training programs for staff with specific risk management responsibilities</li> <li>○ Review and approve the risk management report including selection of critical risks to be put before the Board</li> </ul>
<b>Risk Management Committee (RMC)</b>	<p>The role and responsibilities of the Risk Management Committee shall mandatorily include the performance of functions specified in Part D of Schedule II, which is prescribed hereunder:</p> <ol style="list-style-type: none"> <li>1) Formulate a detailed Risk Management Policy which shall include:             <ol style="list-style-type: none"> <li>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 Committee.</li> <li>b) Measures for risk mitigation including systems and processes for internal control of identified risks.</li> <li>c) Business continuity plan.</li> </ol> </li> <li>2) Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;</li> <li>3) Monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;</li> <li>4) To conduct periodic review the Risk Management Policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;</li> </ol>

	<ol style="list-style-type: none"> <li>5) Keep board of directors informed about the nature and content of its discussions, recommendations and actions to be taken;</li> <li>6) Conduct review of appointment, removal and terms of remuneration of the Chief Risk Officer (if any). RMC shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the board of directors.</li> <li>7) RMC shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if considered necessary</li> <li>8) Quarterly review of function wise risk registers.</li> <li>9) Review Risk Profile document on Risk-mitigation plan and its implementation status</li> <li>10) Provide updates and seek approval from RMC on Risk Management.</li> </ol>
<b>Chief Risk Officer (CRO)</b>	<ul style="list-style-type: none"> <li>o Implementing the risk management initiatives across the entire company/organization.</li> <li>o Liaise with the Risk Coordinators to coordinate the flow of information and escalation of key risk issues/concerns between the RMC and Risk Coordinators</li> <li>o Ensure that meetings of the RMC are held regularly</li> <li>o Prepare and maintain relevant documentation for the company and present it to the Board of Directors of the Company.</li> </ul>
<b>Risk Owners (RO)</b>	<ul style="list-style-type: none"> <li>o Ensure preparation of suitable risk mitigation plan keeping in mind the current controls mechanism in place, proposed mitigation measures and organizational priorities</li> <li>o Ensure that the risk profiles are filled and key risks are escalated to the respective RMC for their approval of proposed mitigation plan</li> <li>o Ensure that the approved plans are implemented within the target timeframes and reported regularly.</li> </ul>
<b>Risk Coordinators</b>	<ul style="list-style-type: none"> <li>o Assist in complying with risk management policy adopted by the company</li> <li>o Responsible for identifying and escalating risks to the next level</li> <li>o Exercise reasonable care to prevent loss, to maximize opportunity and to ensure that all the operations, reputation and assets are not adversely affected</li> <li>o Liaise with Risk Owners to coordinate flow of information and escalation of key risk issues / concerns between RMC and Risk owners</li> <li>o Ensure that meetings of the RMC are held regularly</li> <li>o Prepare and maintain relevant documentation for the RMC and submit the same to CRO</li> </ul>
<b>Internal Audit</b>	<ul style="list-style-type: none"> <li>o Develop a risk-based internal audit program</li> <li>o Audit the risk processes across the organization</li> <li>o Receive and provide assurance on the management of risk</li> <li>o Develop a Report on the efficiency and effectiveness of internal controls</li> </ul>





## 9 RISK APPETITE AND TOLERANCES

It is important that the Board sets rules for risk taking in respect of all types of risk, and some organisations have produced a risk appetite statement that is applicable to all classes of risk. It is fairly easy to confirm that it has no appetite for causing injury and ill health. In practice, however, this may need to be developed into a set of targets for health and safety performance.

There is a danger that risk appetite statements fail to be dynamic, and they can constrain behaviour and rapid response. At Board level, risk appetite is a driver of strategic risk decisions. At executive level, risk appetite translates into a set of procedures to ensure that risk receives adequate attention when making tactical decisions. At operational level, risk appetite dictates operational constraints for routine activities.

IRCTC encounters risk every day as it pursues its objectives. In conducting appropriate oversight, the Management and the Board of the company are responsible for describing how much risk is acceptable in pursuing these objectives. To fully embed Risk Management in IRCTC, the Management must know how much risk is acceptable as it considers ways of accomplishing objectives, both for the organization and for their individual operations (division, department etc.)

Defining a risk appetite statement starts with analysing the long-term and short-term goals of the company. The company should be able to identify its strategic and tactical objectives. Based on the strategic and tactical objectives a broad - level statement depicting the overall risk appetite of the organization shall be defined. In addition, risk tolerance levels for the following broad organizational objectives shall also be defined:

- Strategic - high-level goals, aligned with and supporting its mission
- Operational - effective and efficient use of its resources
- Reporting - reliability of reporting
- Compliance - compliance with applicable laws and regulations

The Board shall be responsible for defining the risk appetite statement for the company. The Risk Management Steering Committee shall be responsible for reviewing the risk appetite of the company on a yearly basis and revising the same based on changes in internal/ external business environment and stakeholder expectations.

Any changes to risk appetite need to be approved by the Board.



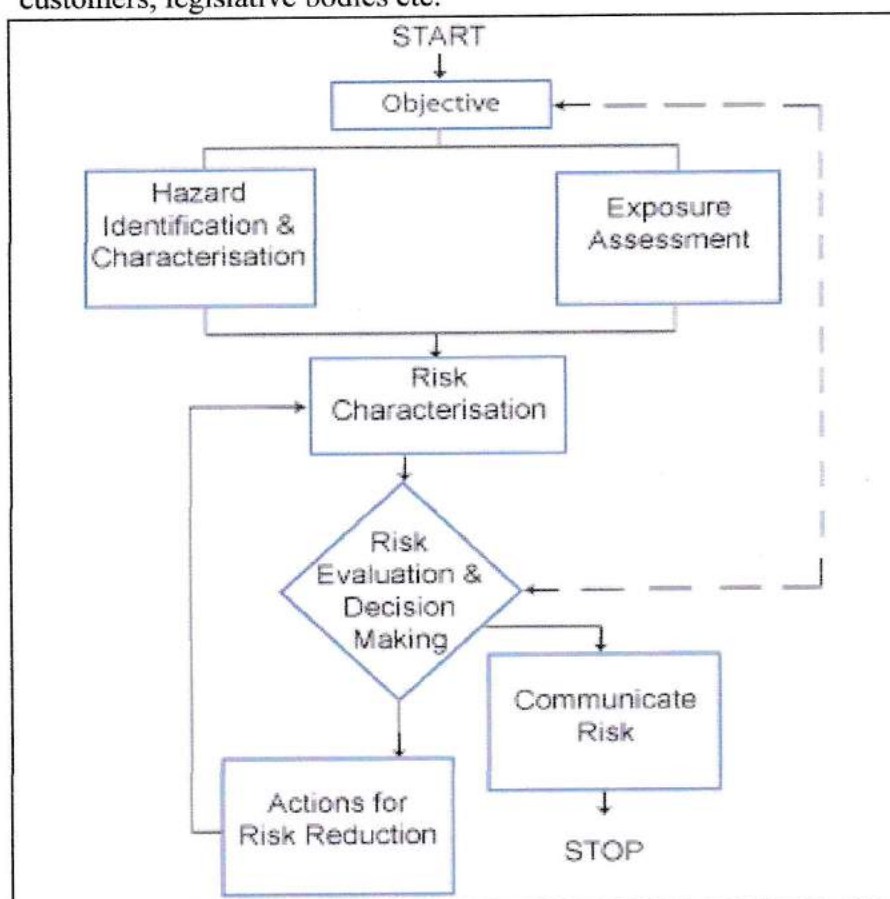
## 10 RISK MANAGEMENT PROCESS

### 10.1 Risk Identification

Risk Identification is a process of identifying risks for assessment, evaluation and determination of appropriate mitigation plans. A systematic process of comprehensive risk identification is the foundation on which edifice of risk management is built.

The first step in the management of risk is to identify the potential risks. Risks are about events which when triggered cause problems. Hence, risk identification can start with the source of problems or with the problem itself.

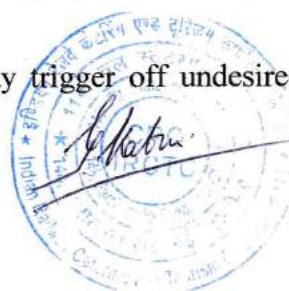
1. Source Analysis: These may be internal or external to the system e.g. internal could be the employees of IRCTC and external could be the stakeholders.
2. Problem Analysis: These are the risks related to identified threats e.g. threat of losing money or threat of accident etc. The threat may exist with various entities such as customers, legislative bodies etc.



### 10.2 Methods of Risk Identification

**Objective based Risk Identification:** This involves identifying events which may endanger achieving an objective either partly or completely.

**Scenario based Risk Identification:** Any event that may trigger off undesired scenarios is identified as a risk.





**Taxonomy based Risk Identification:** Based on Taxonomy (breakdown of possible risk sources) and identification of best practices a questionnaire is compiled whose answers reveal risks.

**Common Risk Checking:** In several sectors lists with known risks are available. The check list can be used to assess the risk in a particular situation.

**Risk Mapping:** This is a combination of the above methods. A matrix is created under which the impact/consequences of different risks on various factors are charted.

The company may use following tools to identify new risks that may have emerged or risks that would have changed over a period of time:

- Structured workshops
- Brainstorming sessions
- Interviews by CRO and or the Risk coordinators
- Review of losses /events
- Review of documents.

All identified risks shall be updated in a risk register. Risk registers shall be quarterly reviewed and updated by the respective Risk Management Committees to ensure pertinence of the risks listed. Risks that would have ceased shall also be doused appropriately. The CRO and Risk Coordinators shall ensure that the risk registers are reviewed and updated quarterly.

### 10.3 Risk Assessment

Risk assessment will be required as part of the decision-making processes intended to exploit business opportunities. One way of ensuring that risk is part of business decision- making is to ensure that a risk assessment is attached to all strategy papers presented to the Board. Likewise, risk assessment of all proposed projects should be undertaken and further risk assessments should be undertaken throughout the project.

Finally, risk assessments are also required in relation to routine operations. The risks shall be assessed on qualitative two-fold criteria. The two components of risk assessment are:

1. The likelihood of occurrence of the risk event and
2. The magnitude of impact if the event occurs.

The risks shall be assessed according to the risk assessment criteria defined in table below

The combination or likelihood or occurrence and the magnitude of impact provide the risk level. The magnitude of impact of an event (shall it occur) and the likelihood of the event and its associated consequences, are assessed in the context of the existing controls. In determining what constitutes a given level of risk the following scale is to be used for likelihood and impact.





## Risk Likelihood Descriptors

Rating	Description	Likelihood of Occurrence
1	Rare	Highly unlikely, but it may occur in exceptional circumstances. It could happen, but probably never will.
2	Unlikely	Not expected, but there's a slight possibility it may occur at some time.
3	Possible	The event might occur at some time as there is a history of casual occurrence at IRCTC &/or Similar Institutions.
4	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence at IRCTC &/or similar institutions.
5	Almost Certain	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence at IRCTC &/or similar institutions.

## Risk Consequence Descriptors

Rating	Description	Financial Impact	Customers, Employee, Health & Safety	Business Interruption	Reputation & Image	Corporate Objectives
1	Insignificant	Minimal financial loss; Less than 0.25% of Turnover	No or only minor personal injury; First Aid needed but no days lost	Negligible; Critical systems unavailable for less than one hour	Negligible impact	Resolved in day-to-day management
2	Minor	Financial loss in between 0.25%-0.5% of Turnover	Minor injury; Medical treatment & some days lost	Inconvenient; Critical systems unavailable for several hours	Adverse local media coverage only	Minor impact
3	Moderate	Financial loss in between 0.5%-1.0% of Turnover	Injury; Possible hospitalisation & numerous days lost	Client dissatisfaction; Critical systems unavailable for less than 1 day	Adverse national media coverage	Significant impact
4	Major	Financial loss in between 1.0%-2.0% of Turnover	Single death &/or long-term illness or multiple serious injuries	Critical systems unavailable for 1 day or a series of prolonged outages	Adverse and extended national media coverage	Major impact
5	Catastrophic	Financial loss in between 2.0%-5.0% of Turnover	Fatality(ies) or permanent disability or ill-health	Critical systems unavailable for more than a day (at a crucial time)	International Media Coverage & Demand for high level inquiry	Disastrous impact

**Note:** Any risk with an impact probability of more than 5% of Turnover shall also be categorized as “Catastrophic”, however the “Risk Response” shall be decided only by the Board of Directors.





Impact	Risk Management Actions		
Significant	Considerable management required	Must manage and monitor risks	Extensive management essential
Moderate	Risks may be worth accepting with monitoring	Management effort worthwhile	Management effort required
Minor	Accept risks	Accept, but monitor risks	Manage and monitor risks
	Low	Medium	High
	Likelihood		

#### 10.4 Risk Categories

Before we can plan for management of risk, we need to identify different types of risks faced by the entity and the severity of those risks. Proper identification of risks in an enterprise is itself a major task, as it is those risks on which the organization will focus.

As the risk environment is so varied and complex, it is useful to group potential events in to risk categories. By aggregating events horizontally across an organization and vertically within operational units, management develops an understanding of the inter-relationship between events, gaining enhanced information as a basis for risk assessment.

#### 10.5 Risk Evaluation

For each risk the average score for likelihood and impact shall be multiplied to arrive at a combined SCORE. In case the rating of risks is done by a group, average of the group's score shall be determined. The average is to be determined for each component of risk assessment viz. Likelihood and Impact. The simple average for each component of each risk shall be calculated.

	Likelihood (A)	Impact (B)
Participant 1	2	5
Participant 2	3	5
Participant 3	4	5
Average	3	5
Combined Risk Score	3*5=15	



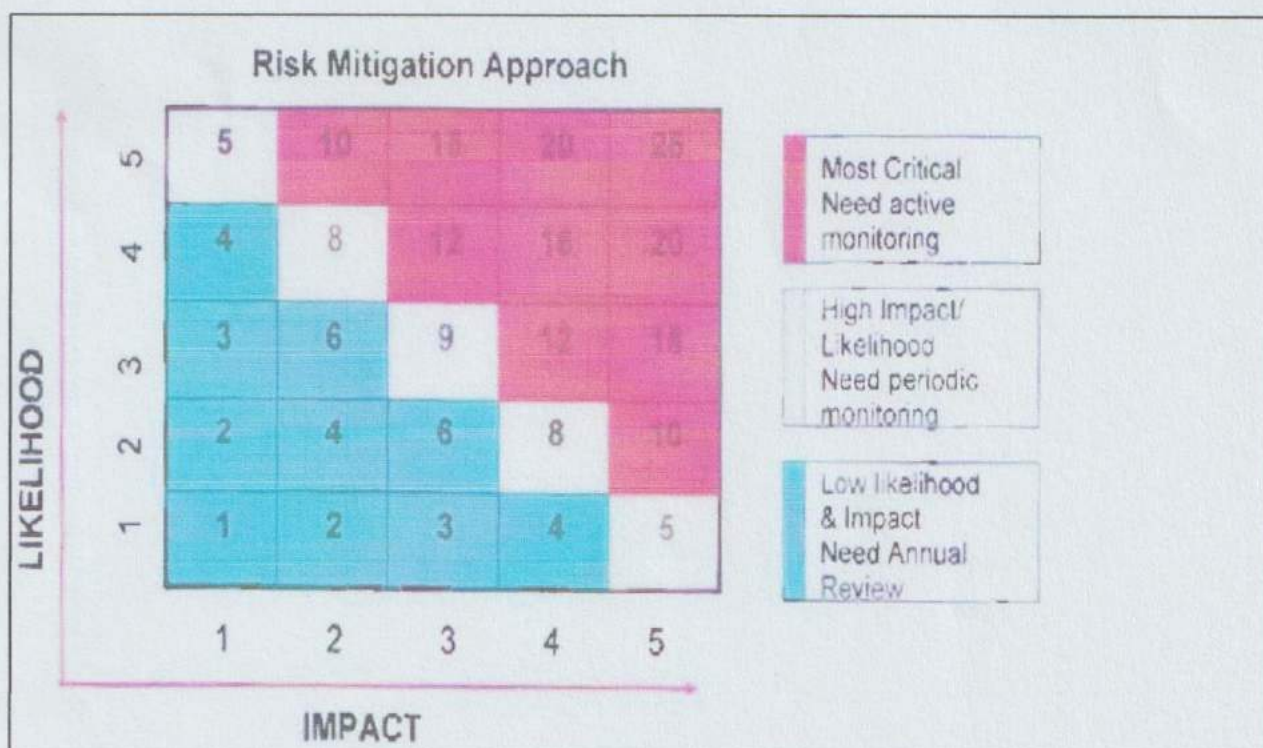


The risk would be classified into one of the three zones based on the combined score,

Risks that score within a red zone are considered "Critical, High & Unacceptable" and require immediate mitigation plans to deal with the risk. (Average score 12 and above)

Risks that score within the yellow zone are considered "Cautionary / Medium" where action steps to develop or enhance existing controls is also needed. (Average score in the range of (6 and less than 12)

Risks that score within the green zone are considered "Acceptable / Low". (Average score less than 6).

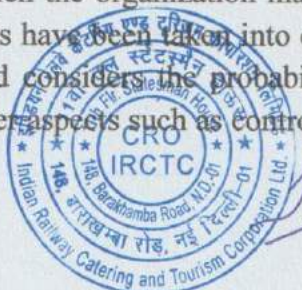


The output of a risk evaluation is a prioritized list of risks for further action.

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.

## 10.6 Risk Mitigation

The risk mitigation plan adopted by the company would also depend on the vulnerability factor. Vulnerability is the extent to which the organization may be exposed in relation to various risk factors after existing controls have been taken into consideration. Vulnerability differs from the likelihood as likelihood considers the probability of an event occurring, whereas Vulnerability also considers other aspects such as control effectiveness and level of





preparedness to deal with risks.

Risk mitigation involves identifying the range of options for mitigating risk, assessing those options, preparing risk mitigation plans and implementing them.

Mitigation options may include:

- a. **Avoidance:** Exiting the activities giving rise to risk, Risk avoidance may involve exiting a product line, declining expansion to a new geographical market or selling a division. This option may be taken in cases where the exposure of risk is very high as compared to the expected benefits/returns in continuing those activities.
- b. **Acceptance:** No action is taken to mitigate the risk or reduce the likelihood or impact. This option may be taken in cases where the cost of reducing the exposure is very high as compared to the benefit accrued from reducing the risk exposure.
- c. **Reduction:** Developing mitigation plan to reduce risk exposure. Mitigation plans need to be developed and implemented for reducing the risk exposure.
- d. **Transferring:** Includes purchasing insurance products, engaging in hedging transactions or outsourcing an activity.

Mitigation plan for each risk shall be documented, and shall contain details of the risk, its contributing factors, risk scores, controls documentation along with specific and practical mitigation plans. Mitigation plans need to be time bound and responsibility driven to facilitate future status monitoring. Mitigating practices and controls shall include determining procedures and processes in place and additional resource allocation that will ensure that existing level of risks is brought down to an acceptable level. In many cases significant risk may still exist after mitigation of the risk level through the risk mitigation process.

For risks considered to be "acceptable", risk profile will be developed with mitigation plan as accepted and no further actions required.

## 10.7 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 company.

After the risk is identified, upward escalation of the same will be as below:

1. Risk Management Committee head to select risks to be escalated which primarily will be of following types:



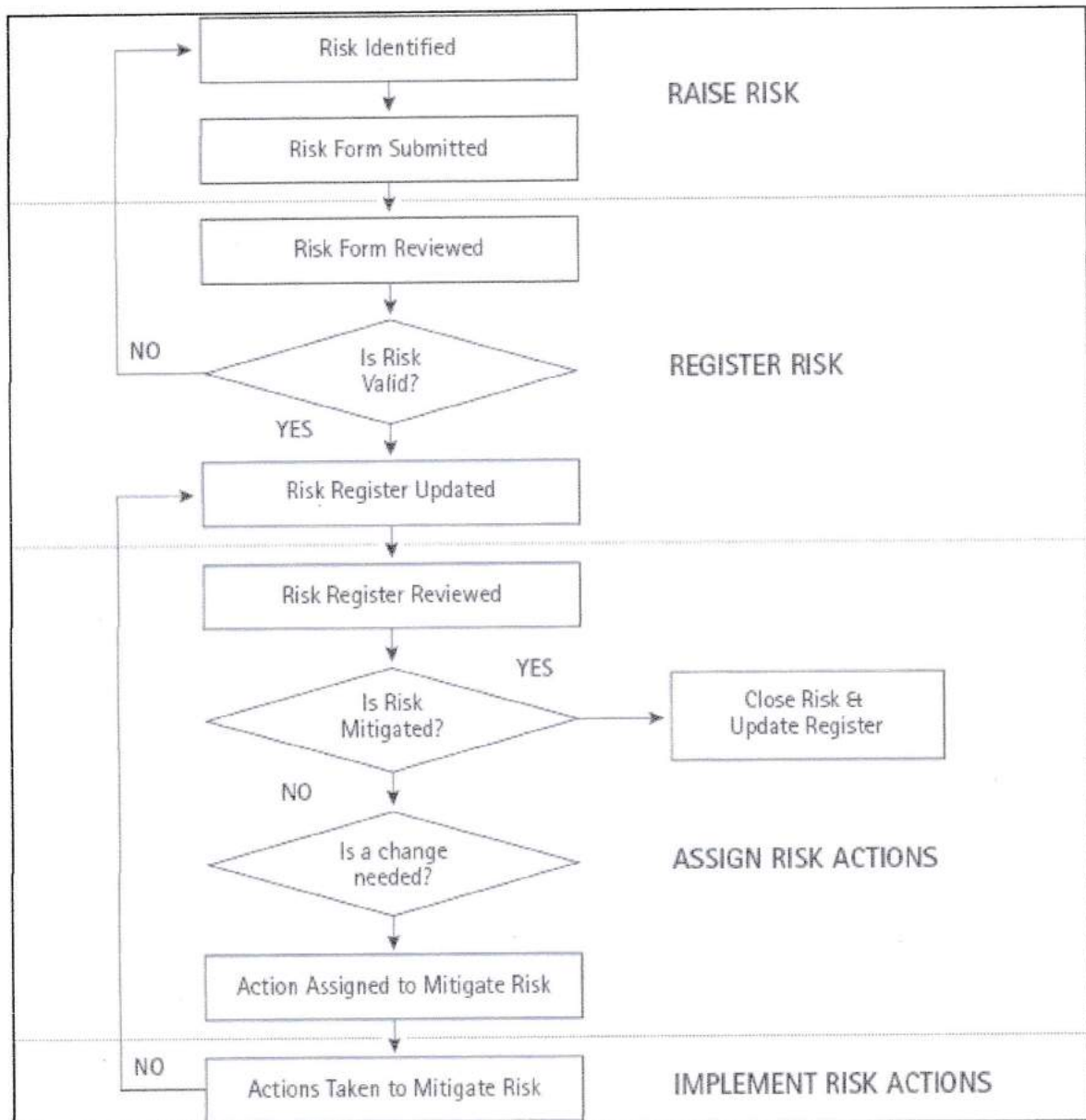
*S. K. Sharma*

- a) Critical risks relevant to the function wherein the complete mitigation is possible at RMC level
  - b) Critical inter-dependent risks wherein intervention of RMC / Board is required for smooth implementation of the mitigation plan. It is desired that Risk Owner prepares risk mitigation plan at the unit/function level for such risks which may be considered by RMC / Board for integrated response/mitigation plan
2. The CRO shall select risks to be escalated to RMC based on the inputs received from respective RMCs. This would include:
  - a) Risk submitted by individual RMCs as crucial for their respective function
  - b) For critical interrelated risks the CRO need to present to the RMC an aggregate / consolidated view of the risks after thorough analysis and consultation with RMC heads of relevant Business Unit / Corporate Function
3. RMC will review the risks submitted by CRO and will identify and escalate strategic risks to the Board.





## 4. Flowchart Depicting Risk Management Process



## 11 ORGANISATION STRUCTURE



## 12 ACTION PLAN

1. Risk Management in the company will look into all organizational processes involved in advanced detection of risks as well as in identifying and taking suitable action to counter them.
2. Deployment of integrated planning, control and monitoring systems and corporate governance systems and fine tune them on an ongoing basis to ensure that risks are detected at early stage and properly assessed and appropriately managed.
3. Risk management, a key success factor will form an integral component of IRCTC's management system. To promote risk awareness throughout the company, risk culture at all levels shall be developed through the mechanism of review framework, progress monitoring and discussions in open forums.
4. All identified risks will be assigned: impact, probability, category, timescale and action to be taken. This will be complemented with focus on quantitative reporting. A key element of early warning system will be regulated through a mechanism in which Risk Managers will inform the Risk Controllers, who in turn will report to the Chief Risk Officer about the probable/potential risk.

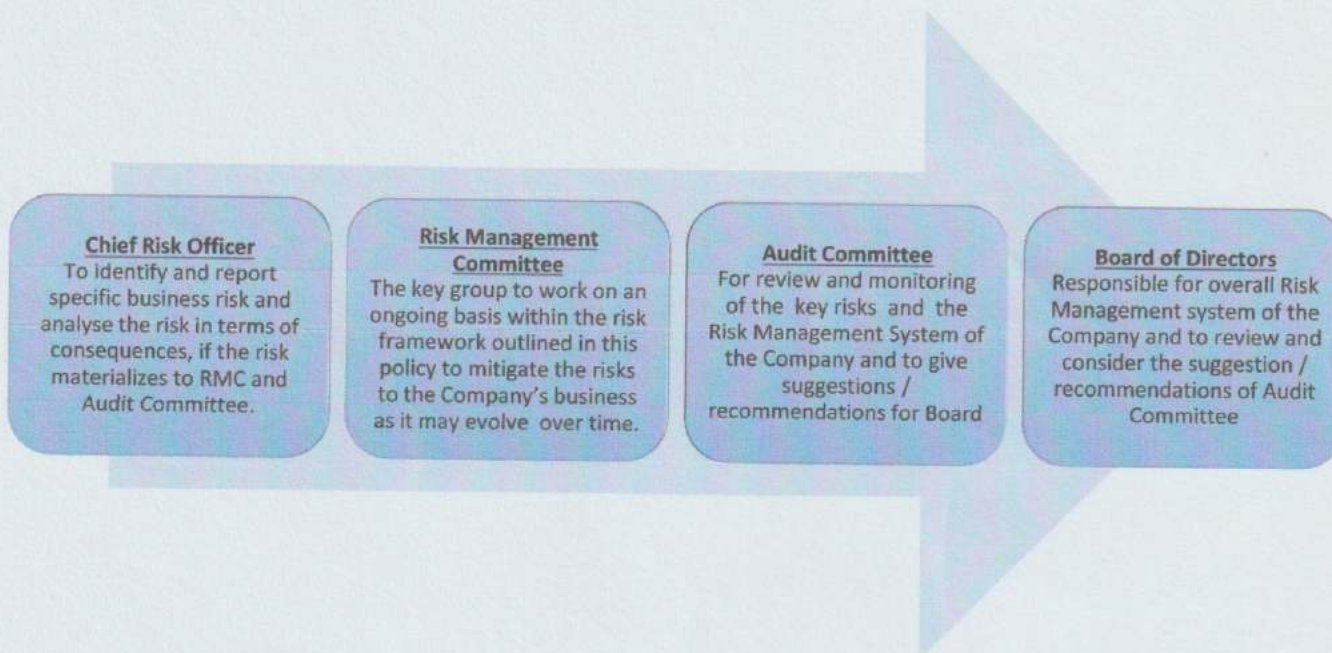




5. Chief Risk Officer shall compile all reported risks on quarterly basis with such details about risks in tabular form. This analysis will form an integral part of reporting and will be periodically reviewed by the Audit Committee/Board.

### 13 RISK MANAGEMENT INFORMATION SYSTEM (MIS)

IRCTC will have an enterprise-wide integrated Risk Management Information System (MIS) implemented. The structure of the MIS will be as follows:



### 14 APPROVAL OF THE POLICY

The Board 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.

### 15 REVIEW OF THE POLICY

The policy will be the guiding document for risk management at IRCTC and will be reviewed as and when required due to the changes in the risk management regulations/ standards/ best practices as appropriate.

Any changes to the Policies and Procedure are required to be approved by the Board of Directors.



## 16 PUBLICATION OF THE POLICY

This Policy will be published on the Company's website.

