Indo Count Industries Limited

Policy Name:
Enterprise Risk Management

This Policy on Risk Management is approved by the Risk Management Committee of the Company at their meeting held on March 21, 2023.

Policy Description	
Objective	This policy is intended to ensure that an effective Enterprise Risk Management (ERM) program is established and implemented within Indo Count Industries Limited (hereinafter referred to as company / organization) to identify enterprise level risk. This program will provide regular reports on: 1. The performance of the ERM program, including any exceptions, to key stakeholders. 2. The movement of identified Risk, to give an overview of the Risk Profile of the company as on a date. The ERM framework aims to realize the following benefits for the organization: 1. Enhance risk management for the organization including strategy setting 2. Facilitate risk-based decision making 3. Improve governance and accountability 4. Enhance credibility with key stakeholders such as investors, employees, government, regulators, society, etc. 5. Create, protect and enrich stakeholder value
Policy Summary	The policy contains the objectives of risk management, companies approach to risk management and the risk organization structure for identification, management and reporting of risks. The policy also specifies the roles and responsibilities of key stakeholders and other key personnel of the company with regards to risk management.
Policy Scope	The policy complements and does not replace other existing compliance programs, such as those relating to quality, health & safety, legal and regulatory compliance matters.

Members of Central Risk Office				
Name	**Role**	**Function**	**Sign**	**Date**

TABLE OF CONTENTS

1 Introduction

1.1 Applicability

This policy applies to all business segments, functions and units across the company including its subsidiaries.

Any new activity or new departments or new plants or new capital projects/ initiatives that are made part of the organization shall comply with this policy from the date of creation of such departments.

This policy is applicable only for enterprise wide and high-level operational risks that have a strategic impact on company. The process level risks that have an impact on day-to-day operations are excluded from the purview of this policy and will be governed by the respective policies and standard operating procedures documented for those processes.

1.2 Objective of Enterprise Risk Management

The objective of embarking on the Enterprise Risk Management journey by organization is to strengthen and formalize risk management practices at company level to manage risks in a structured and consistent manner. The specific objectives include:

1. To enable organizational sustainability taking cognizance of the impact of its products, services & operations on society and the environment
2. Reduce potential gaps in achieving company's objectives
3. Align and integrate existing risk management practices in the organization
4. Build confidence of investment community and stakeholders
5. Enhance Corporate Governance
6. Successfully respond to changing business environment

1.3 Benefits of Risk Management

ERM has following benefits for the organization:

1. Greater awareness about the risks facing the organization and the ability to respond effectively
2. Enhanced confidence about the achievement of strategic objectives
3. Improved compliance with legal, regulatory and reporting requirements
4. Increased efficiency and effectiveness of operations

2 Enterprise Risk Management Framework Overview

The ERM framework is a systematic application of risk management procedures and practices for establishing ERM in organization.

The ERM framework is a continuous cycle beginning with risk identification and followed sequentially by risk assessment, risk evaluation and risk response. The framework also lays down activities for risk monitoring, review, control and managing materialized risks to support the entire ERM process across the organization.

2.1 Internal and External Environment

Risks may arise from changes or developments in organizations internal and external environment. In order to ensure an effective risk management, it is imperative to understand and identify signals of change in internal and external context of the organization.

Internal Environment

The following are indicative factors/ signals of change from an internal environment perspective:

- Organizational strategy and objectives
- Inherent strengths and weaknesses/ vulnerabilities of company's businesses
- Organization structure and roles & responsibilities
- The organization values & belief system
- Incentive and development mechanisms, and how it is expected to drive employee behavior
- Internal Systems and processes
- Internal control and monitoring mechanisms

External Environment

The following are indicative factors/ signals of change from an external environment perspective:

- New/ changes in government regulations and/ or policies
- Competitive landscape including local competitors
- Vendor group, partners, alliances
- Geo-Political scenario at the domestic and international level
- Socio-economic condition
- Technological changes and advancements
- Trade wars between countries
- Extreme weather, Climate Change and Natural disasters
- Man-made hazards / disaster including epidemic / pandemic like COVID, SARS, MERS

The external environment in which the organization operates can be determined using the following techniques:

- Porters 5 forces model – Five forces include threat of entry of new competitors, intensity of competitive rivalry, bargaining power of customers, bargaining power of suppliers and threat of substitute products or services. It is a framework for industry analysis and business strategy development. It draws upon Industrial Organization economics to derive five forces that determine the competitive intensity and therefore attractiveness of a market. Three of Porter's five forces refer to competition from external sources and the remainder are internal threats
- PESTLE analysis – Political, Economic, Social, Technological, Legal and Environmental analysis. It is a part of the external analysis when conducting a strategic analysis or doing market research and gives an overview of the different macro environmental factors that the Company has to take into consideration. It is a useful strategic tool for understanding market growth or decline, business position, potential and direction for operations
- SWOT analysis – It is a strategic planning method used to evaluate the Strengths, Weaknesses, Opportunities and Threats involved in a project or in a business venture. It involves specifying the objective of the business venture or project and identifying the internal and external factors that are favorable and unfavorable to achieve that objective

3 Enterprise Risk Management Governance Structure

The ERM Governance Structure identifies the key internal stakeholders responsible for creating, implementing and sustaining ERM in the organization. The structure leverages existing organizational structure within the company in order to align individuals, teams and departments with the intent of:

- Integrating ERM into the organization culture
- Establishing responsibility and accountability for ERM
- Facilitating and monitoring effective implementation of the ERM framework
- Ensuring that the ERM framework and its components are up to date
- Providing clarity over roles and responsibilities across the ERM processes

The risk governance structure is presented below, and the distinct roles and responsibilities are included in *Section 4.*

Figure 1: Risk Governance Structure

4 Roles and Responsibilities

4.1 Board of Directors

With respect to Risk Governance, the Board of Directors have the following responsibilities:

- Determine the strategic direction of the organization
- Establishing expectations with respect to Enterprise Risk Management
- Reviewing and approving risk management related policies, procedures and parameters
- Allocating adequate resources for treating critical risks and/ or risk events at the organization level
- Owning risks of strategic importance impacting company at an organizational level, and establishing a risk environment that is consistent with accepted practices of the organization and fulfils the expectations of the shareholders
- Reviewing the critical aspects of the company's overall risk profile through the periodic review of high-level reports that address material risks and strategic implications
- Endorsing the Enterprise Risk Management organization structure and authorizing roles and responsibilities for key stakeholders
- Independent review of the Central Risk Office (CRO) and its activities pertaining to Enterprise Risk Management

Board may decide to execute these responsibilities through Risk Management Committee (RMC). The composition of RMC should be in accordance to clause 21 of Listing Obligations and Disclosure Requirements ('LODR').

4.2 Risk Management Committee

RMC will act as a sponsor for risk management in the organization and in doing so carry out the following responsibilities:

A. Overall

- Set policy and strategy for risk management
- Approve changes to risk appetite parameters
- Communicating with Risk Management Officer ("RMO") significant developments / changes to business and other key decisions
- Monitor the effectiveness of the Enterprise Risk Management process

B. Risk Management

- Providing necessary support to the RMO in performing risk management activities as envisaged
- Track the emergence of new risks and the progress of the risk response plans on a half-yearly basis in collaboration with respective business functions
- Monitor compliance with risk limits/ appetite established for the organization
- Enabling risk assessment and prioritization
- Review risk response strategies with respective business functions for sufficiency, implementation status and effectiveness
- Managing materialized risks
- Build risk awareness culture across the organization

The Risk Management Committee shall be constituted as per clause 21 of LODR and accordingly shall comprise of: (Reference Clause 21 of Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015)

Core Committee (Majority member to be from board of directors)

- Independent Director (Chairman)
- Independent Director
- Managing Director
- Whole Time Director
- Business / Functional Heads (invited on need basis)

Consultation

- Head of Internal Audit

Convener

- Chief Financial Officer / CCRO

4.3 Central Risk Office

The role of the Central Risk Office will be to facilitate development, implementation and monitoring of risk management across the organization and ensure meetings / activities are carried out as per calendar defined in Annexure 14.6. The central risk office may be headed by single person or jointly by more than one person who shall be the Company Chief Risk Officer and be part of Risk management committee.

Kolhapur Plant, Bhilad Plant, & Spinning Plant will have a nominated Divisional Chief Risk Officer (DCRO) who shall roll-up into the Company Chief Risk Officer/s (CCRO). However, the Plant Heads will ultimately be responsible for the division and its risks.

Key responsibilities of CCRO and DCRO		
Area	**Responsibility of CCRO**	**Responsibility of DCRO**
ERM Program Management:		
Program Leadership	Providing overall leadership to ERM process in line with directions of the Board of Directors and Audit Committee	Providing overall leadership to Divisions ERM process in line with directions of the CCRO
Program Ownership	Developing and assuming ownership of the risk management policy, framework and process	Assuming ownership of the divisional risk management policy, framework and process as directed by CCRO
Implementation of ERM framework	Program manage implementation of the ERM framework	Assist CCRO is implementing ERM framework at divisional level
Define risk appetite	Provide necessary information and feedback to facilitate definition of risk appetite at the business line/ function, entity and organization level	Provide necessary information and feedback to CCRO to facilitate definition of risk appetite at the division level
Reporting / Consultation	Liaising with Risk Management Committee at various levels for deploying the ERM process	Liaising with CCRO for deploying the ERM process at division level
Review and updation of policy	Periodically review and enhance ERM policies and proposing necessary updates	Bring to the notice of CCRO if any change needed in policy due to changes at division level
Deviation management	Reviewing significant deviations from the ERM framework or other procedures and bringing it to the attention of Board of Directors, Audit Committee and Management Committee as appropriate	Reviewing significant deviations from the ERM framework or other procedures and bringing it to the attention of CCRO
Support	Rendering support to the Board of Directors and Audit Committee for effecting changes to the risk management organization and process	Rendering support to the CCRO for effecting changes to the risk management organization and process
Implementing procedures for review	Assisting with implementation of procedures for proactive review of risks for projects, transactions, new businesses, etc.	Assisting CCRO with implementation of procedures for proactive review of risks for projects, transactions, etc. at division level
Monitoring trends	Monitoring external trends and factors that may have significant impact on the risk profile of the organization and communicating the information to all key stakeholders	Monitoring external trends and factors that may have significant impact on the risk profile of the division and communicating the information to all key stakeholders and CCRO

Key responsibilities of CCRO and DCRO		
Area	**Responsibility of CCRO**	**Responsibility of DCRO**
Risk Management:		
Reporting	Co-ordinate risk reporting to the Risk Management Committee, Board and the Audit Committee	Assist CCRO for divisional risk reporting
Risk Management	Co-ordinate with DCRO and HO functions on activities which rely on the risk management for risk related inputs	Seek inputs from CCRO on risk management
Risk Identification	Facilitating risk identification, assessment, prioritization and profiling activities	Facilitating risk identification, assessment, prioritization and profiling activities for division
Continuous monitoring and updation	Coordinating with DCRO and HO Risk Owners for new risks identified or changes to risks	Update CCRO for new risks identified or changes to risks at division level
Maintenance of register	Maintain the risk registers and the risk response plan tracker	Assist CCRO to maintain divisional risk registers and risk response plan tracker
Risk response plans	Providing input and feedback on proposed risk response plans and initiatives	Providing input and feedback on proposed risk response plans and initiatives to CCRO
Monitoring risk response plans	Monitoring progress of implementation of risk response plans and strategies	Assist CCRO to monitor progress of implementation of risk response plans and strategies for division
Periodic risk reviews	Ensuring that risk reviews are carried out on a periodic basis in order to maintain continuity of the enterprise risk management process	Ensuring that risk reviews are carried out on a periodic basis in order to maintain continuity of the divisional enterprise risk management process
Risk and mitigation plan reporting	Preparing and communicating risk reports with risk mitigation measures to relevant stakeholders	Assisting CCRO for preparing and communicating divisional risk reports with risk mitigation measures
Loss event database	Updating the loss event database based on information on materialized risks from DCRO and HO Risk Owners risk owners	Co-ordinating with CCRO to get the loss event database base updated for any materialized risks
Risk escalation	Risk escalation as per the process in Annexure 14.5	Risk escalation as per the process in Annexure 14.5
Risk Training, Competencies and Culture:		
Training	Training and collaborating with the business lines and divisions in executing ERM framework on a regular basis to aid management in decision making	Assist CCRO in executing ERM framework at division level

Key responsibilities of CCRO and DCRO		
Area	**Responsibility of CCRO**	**Responsibility of DCRO**
Promote culture	Promoting risk management culture through trainings, reporting and other internal communications	Promoting risk management culture at division through reporting and other internal communications
Training calendar	Developing an annual risk management training calendar to ensure that individuals engaged in risk management are: 1. Developed with appropriate risk management skills and competencies 2. Developing the analytical systems and data management capabilities to support the ERM program	Assist CCRO to develop content and ensure that all relevant personnel from division attend the training

4.4 Risk and Mitigation Owners

All the business functions and units of the company have a primary responsibility for managing risk on a day to day basis. The role of risk owner and mitigation owner is as follows:

Risk Owner

- Overall ERM responsibility
  - Promote risk awareness and introduce risk management objectives within their business function/ unit
  - Timely escalation of challenges, concerns or unforeseen developments pertaining to the risk to the CCROs / DCROs office who shall then evaluate the situation and accordingly report to the RMC and Board
  - Identify new emerging risks quarterly and report to the DCROs / CCROs office (for assessment, prioritization and response planning)
  - Ensuring responsibility and action are assigned to mitigation owner
  - Ensure that risk management is incorporated in the business decision making process
  - Reporting significant breakdowns in risk mitigation measures and actions to prevent their recurrence
  - Risk escalation as per the process in Annexure 14.5
- Risk Profiling and Mitigation
  - Assuming overall responsibility for mitigating the individual risk, that is overall management of the risk response as agreed in the risk profile
  - Ensure responsibility and actions are assigned to appropriate mitigation owners against agreed upon risk response plans
  - Monitoring the progress of the risk treatment plans against the agreed milestones
  - Periodically evaluating the impact of the mitigation plan on the risk, against the risk threshold level, risk evaluation/ prioritization parameters, and the subsequent impact on the residual risk

- Report to the DCROs / CCROs office on the status of the risk and its treatment plan
- Periodic updation of Risk Profiles
- Proactively reporting significant breakdowns in risk mitigation measures and actions to prevent their recurrence

Mitigation Owner

- Overall ERM responsibility
  - Assuming overall responsibility for mitigating the individual risk as agreed in the risk profile
  - Identify new emerging risks periodically and report to the DCROs / CCROs office (for assessment, prioritization and response planning)
  - Risk escalation as per the process in Annexure 14.5
- Risk Profiling
  - Following are the critical characteristics of a SMART risk profile:
    - Specific: The plan should be clear and not general in nature
    - Measurable: The output of the plan should be easy to 'quantify' to monitor its performance
    - Achievable: The plan should be attainable by the existing and available resources
    - Relevant: The plan should be focused towards mitigating the risk identified
    - Time bound: The plan should be executed within a period to contain any adversity from the risk
- Risk Mitigation
  - Assuming the role of a SPOC (single point of contact) for managing the mitigation of an individual risk as identified in the risk register
  - Periodically updating the risk owner on status of execution along with relevant KPI's
  - Timely escalation of challenges, concerns or unforeseen developments to risk owner
  - Proactively reporting significant breakdowns in risk mitigation measures and actions to prevent their recurrence

4.5 Internal Audit

Internal Audit (IA) provides independent assurance of the risk management system and the processes supporting it. Its role is essentially to review the overall effectiveness of the risk management measures and controls. The position of Internal Audit within the company also puts it in a good position to assist the Board of Directors/ Audit Committee in their monitoring function and to play an integral part in the promotion of risk management generally.

Internal Audit is specifically responsible for:

- Aligning internal audit plans to risk profiles to ensure that risk management activities for all key risks are covered as a part of the internal audit process
- Identifying and putting emphasis on the potential impact of weaknesses in the ERM system;
- Supporting the risk management process in all business functions by providing advice about risk management standards and best-practice procedures.

In order to enable Internal Audit to effectively leverage the ERM output and vice versa:

- ERM department shall share the list of risks identified on a periodic basis or as requested by IA. Internal audit may use this information as an input for developing a risk-based Audit plan

IA shall share the respective audit reports with the ERM function on a need basis. The ERM function may use this information as an input for risk treatment plans.

5 Risk Appetite

Risk appetite is the amount of risk that company is willing to pursue or retain for pursuing its objectives. The understanding of risk appetite is based on the following key parameters:

- **Financial parameters**
- **Regulatory parameters**
- **Reputation parameters, including brand image**
- **Non – Financial and other qualitative parameters**

Risk appetite is an integral part of the risk management framework to assist in consistently measure and treat risks across all business lines.

6 Risk Identification

Risk Management begins with Risk Identification, which involves identifying any possible threat or vulnerability which may adversely affect companies Vision or Mission.

Risk identification is the mechanism of identifying exposure to uncertainty across the organization. This involves assessment of the external and internal environment in which the company operates. Risk identification entails creating a comprehensive list of risks. These risks are based on historical and anticipated events which may prevent, degrade, accelerate or delay the achievement of the company's strategic and operational objectives, and may have an adverse reputational impact on the brand.

6.1 Level of Risk Identification

Risks identified can be segregated into two levels:

6.1.1. Enterprise-wide Risks

These are strategic risks that have a mid to long term impact on company, including operational risks that have a strategic impact on the organization. An example of such a risk is 'Reputational risk' which can have a long-term impact on the entire organization. *This ERM policy lays down the framework and procedures for addressing such risks (and not process level risks)*.

6.1.2. Process level Risks

These are operational risks that have a current to short term impact on the operational activities and tasks. These risks are faced by the operational teams on a periodic basis due to the ongoing operations of the company. An example of such a risk is 'duplicate invoices from vendors. These risks can also arise from change of business offerings, processes, activities etc. In order to mitigate such risks, the process owner needs to update the Standard Operating Procedures (SOPs) to include mitigating checks and controls.

As a part of the company's internal assurance program, the Internal Audit department must test these checks and controls to gauge the operational effectiveness of the processes and business functions.

6.2. Risk Register

Risks for entire business shall be documented in a risk register. A risk register acts as a central repository for risks. The purpose of the risk register is to identify and record risks and related information in a structured manner. The ownership of the risk register shall lie with the CRO's office while the ownership of individual risks will lie with individual process owners within each business line/ function.

As a part of the risk identification process, it is important to identify the sources, events or situations leading to these risks, i.e. the root cause. The purpose of identifying potential root causes is to give direction to risk response/ treatment measures. The fact that one risk might have multiple root causes also needs to be considered.

The format for maintaining risk registers is appended in Annexure 14.1.

6.3. Maintenance and Regular updates to Risk Register

The Central Risk Office shall assist in risk identification, creating and updating risk registers. However, it is the responsibility of each business line and function to identify risks relevant to their organizational setup and objectives.

A risk once identified shall not be deleted. In case a risk becomes irrelevant, the status of the risk shall be updated in the risk register to reflect the same.

6.4. Techniques of risk identification

For a focused risk identification activity, the following risk identification techniques can be deployed:

- Preliminary hazard analysis/ "What Can Go Wrong (WCGW) analysis"
- Structured interview and brainstorming
- Root cause analysis
- Scenario analysis
- Business impact analysis

7. Risk Assessment

Risk assessment refers to the process followed for understanding the nature and level of risk. It involves the determination of quantitative or qualitative value of risk related to a situation and a recognized threat. It also requires the calculation of the potential loss or impact, and the likelihood that the loss will occur. It should be performed for each risk identified. The onus of risk assessment lies with the risk identifier/ owner, who may choose to consult with the Central Risk Office for assistance.

Risk assessment is based on the following parameters:

- Calculate likelihood of risk events
- Calculate potential impact of the identified risk scenarios

a) Calculate likelihood of risk events

The term “likelihood” is defined as a probability of an event. This is defined, measured or determined objectively or subjectively, qualitatively or quantitatively. Likelihood may be described using general terms (e.g. high, medium or low likelihood) or even mathematically (such as a probability or a frequency over a given time period).

A realistic evaluation of risk likelihood is essential, because it guides the allocation of resources in the company. When deciding upon a probability factor, the following guidelines should be considered:

- Consider how many similar incidents have occurred in the company across entities and business lines
- Consider, and research if necessary, how many similar incidents have occurred across the industry
- Consider the effectiveness of our existing preventative controls for the risk

b) Calculate potential impact of the identified risk scenarios

The impact of the risk on various parameters such as reputational, financial and other qualitative parameters, need to be calculated at this stage. Various scales of impact that are relevant according to the prevalent categories of risk such as reputation damage, media coverage, strategic and operational impact must be considered during assessment of potential impact.

Please note:

i. Risks do not normally exist in isolation and usually have a potential effect on related functions, business processes and risk categories. In many cases, the cross-functional effects of the risks may not be easily identifiable and will require a formal approach for the cause-and-effect analysis. Once identified, the aggregated effect of these risk groupings and linkages (created based on the cause and effect analysis) should be analyzed and documented.

ii. The Risk Register has to be updated based on the risk assessment carried out by the risk owners

Each identified risk has to be assessed on a 5-point scale with respect to the following criteria for determining inherent and residual exposure:

a) Potential impact of the identified risk scenarios

b) Likelihood of risk events

The assessment of each risk on the above two criteria would be done in two stages:

1. Considering the impact and the likelihood of the events without taking any mitigation actions
2. Considering the impact and the likelihood of the events if action for mitigation are taken

The first stage of Risk Assessment is called the Inherent or Gross Risk and the second stage would be Residual Risk

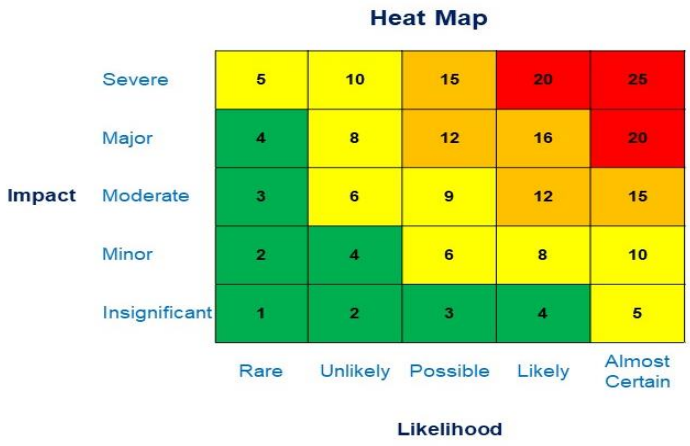
In order to visually depict the risk assessment based on 'residual risk', a "heat map" (graphical representation of impact and likelihood) maybe used based on the risk analysis (i.e. Likelihood * Impact) wherein each risk will be plotted on the "heat map" based on its relative likelihood and impact. The placement of the risks on the "heat map" will indicate the risk zone (High/ Medium/ Low) for each of the respective risks. The heat map shall also form the basis of escalation as and when new risks are identified.

A five by five matrix shall be used for measuring likelihood and impact. The risk shall be evaluated as:

Risk Priority = Likelihood * Impact

The risk measurement scale in terms of impact and likelihood has been defined in Annexure 14.2.

Please Note: A single risk may have an effect on a number of impact parameters. In such a scenario, the risk shall be evaluated for all impact parameters and the highest score shall be used for escalation and prioritization purposes.



The overall risk me[illegible]

Likelihood*Impact (Range)	Risk zone
Score – less than or equal to 4	**Low**
Score – greater than or equal to 5 but less than 12	**Medium**
Score – greater than or equal to 12 but less than 17	**High**
Score – greater than or equal to 17	**Extreme**

Heat Map helps to inform particular stakeholders of the current state of key risks and its mitigation, here key risks are plotted and is supported by the detailed risk profiles. Refer Annexure 14.3 for illustrative map.

8. Incident Reporting / Loss Reporting

8.1. Definition of an incident

Incident can be defined as an instance of something happening; an event or occurrence. Incident can be an instance of employee injury, property damage, improper conduct, security breach, fraud or other reasons. For the organization incident which falls within the parameters defined in Annexure 14.2. can be termed as incident meant to be reported or anything else which the Risk owners or unit heads deem fit.

8.2. Purpose of incident reporting

Incident reports are one of the most important forms of documentation for a corporation to employ in their day to day operations for a multitude of reasons. Whether reporting an instance of employee injury, property damage, improper conduct, security breach, fraud or other reasons, it is increasingly important for a company to keep an effective Incident reporting process. Some of the key benefits include:

1. Provide valuable feedback to risk assessments. One of the primary challenges is that risks may be assessed on an overly optimistic basis. Having effective Incident reporting enables risks to be objectively tracked for occurrence and impact.

2. Avoiding unnecessary fines and claims where there is appropriate documentation in place, along with mitigation plans. This is particularly important if incident reporting is regulated, such as in the case of Medical Care providers.

3. Captures intelligence for Prevention Strategies – this includes identifying gaps in the existing business processes and provide opportunities for improvements in efficiency and quality.

8.3. Incident reporting process

In case of an incident the mitigation owner will report the incident, its nature and its implication to the respective Risk owner who shall then ultimately report to CRO and in turn CRO will report into the Board / Audit Committee. The incident if related to plant will also be informed to plant head who shall also take immediate action to ensure same is mitigated. In case a incident is not reported by employee then necessary action can be taken against such employee wherein he / she can be monetarily penalized or suspended for certain period or terminated from job as determined by management.

8.4. Senior management reporting and analyzing incident

Senior management i.e. CRO and the team identified as senior management for this purpose shall discuss and deliberate on the incident and action to be taken to mitigate the risk. This action to be taken shall be proposed to the board which shall then either approve the action or suggest alternate action after analyzing the incident.

9. Risk Prioritization and Mitigation

9.1. Risk Prioritization

Risk prioritization is the process for prioritizing risks having a residual risk, based on whether the risk and its magnitude is acceptable or tolerable within companies' risk appetite.

The intent of risk prioritization is to:

- Enable escalation to the appropriate level of management as per risk measurement criteria
- Prioritize the implementation of the risk response

Risk prioritization helps ensure appropriate resource allocation within an acceptable 'potential cost of risk mitigation' for the purpose of creating an ongoing risk response and channeling of management focus towards

risks of significant concern. The management may choose to override the risk ranking to raise the rank of certain other risks justified by non-financial influences such as media implications, social responsibilities or regulatory pressures. The ranking of risks should be shaped by strategic and business objectives. The prioritized risks must be correlated with the risk appetite and all risks falling beyond the acceptable appetite must be short listed for risk response.

9.2. **Risk Mitigation**

Risk mitigation is treatment of the risk identified post assessment and prioritization. This requires the mitigation owner to select one or more options for managing and treating risks and implementing the agreed mitigation/ action plans. This phase of the ERM process is intended to:

- Understanding and ensuring existing controls/ mitigation mechanisms are in place for managing and treating risks
- Generate a new risk response plan if the existing controls are ineffective and/ or need to be strengthened to respond to the identified risk
- Continuously assess the effectiveness of such response plans

A risk mitigation may fall into any of the 4 following categories namely:

- Avoid - Exiting the activity giving rise to the risk
- Reduce - Action is taken to reduce risk likelihood or impact, or both
- Share - Reducing risk likelihood / impact by transferring /sharing a portion of the risk
- Accept - No action is taken to affect risk likelihood or impact

Risk mitigation can be a choice from the above or a combination of multiple options. For example, a combination of partially sharing the risk (through insurance) and partially accepting the risk can be the chosen treatment for a risk.

The choice of an appropriate mitigation option must consider the following:

- Net effect of potential response on risk likelihood and impact
- Cost versus benefit of potential response

High Level steps for risk mitigation:

- Evaluate the mitigations in place for key risks
- Evaluate control requirements
- Verify and evaluate the controls currently in place for key risks
- Identify and evaluate the post event measures in place for risk
- Review the financial risk protection measures in place to respond to the consequences of risk events
- Take decisions on the acceptability of identified risks and controls
- Document action plans for risk mitigation
- Use the outputs of risk assessments for budgeting and capital allocation processes

Each risk might have multiple root causes emanating from different business functions and so will need multiple risk mitigation actions. Hence, accordingly such risks will have multiple **'Mitigation Owners'**. In addition, each risk will also have a '**Risk Owner**' for monitoring the overall risk response in terms of the performance of the mitigation steps taken by different mitigation owners, and the effect of these steps on the risk prioritization. Each risk can also have multiple risk owners in case a particular root cause for a risk is recurring and attributable to a specific business department.

9.3. Risk profiling

Individual risk profiles (Refer Annexure 14.4) detail out the response plans, responsibility (risk and mitigation owner), risk limits and monitoring plans for each risk. These profiles should be prepared for the prioritized risks for serving as a descriptive record of each key risk. The Central Risk Office may assist in preparing risk profiles for each key risk but these risk profile should be owned, regularly updated and reported to the Risk Management Committee by the risk owner.

The chosen risk response option has to be supported by a detailed implementation plan in the risk profile. This implementation plan should clearly outline:

- Activity plan with the various steps to be performed
- Intended outcome of the activity plan
- Resource requirements to achieve successful implementation
- Accountability and responsibility for the activity plan
- Implementation time schedule

Performance evaluation criteria to measure implementation status and the effectiveness of the response plan (success of the response).

10. Risk Escalation and Control

A critical element of ERM is an effective system of escalation which ensures that specific issues are promptly communicated to relevant authorities. The escalation process links the results of risk assessment with the risk organization structure and responsibility levels. Section 3 – Enterprise Risk Organization Structure establishes clear reporting lines and defines responsibilities of the various levels of the ERM structure.

Risk escalation may stem from one or more of the following:

- Identification of new risks at business line and entity level
- Change in impact/ likelihood of identified risks causing a change in the risk evaluation
- Unforeseen contingencies

In order to bring risks to the notice of appropriate levels of Management, the process to be used has been depicted in Annexure 14.5. It is to be noted that at each level of escalation, the risk shall be reassessed so that only the key risks are filtered upwards on a timely basis.

Risk control refers to policies and procedures that help ensure that the risk responses identified as determined by the risk owners are carried out.

11. Risk Reviews

Periodic risk monitoring, review and reporting are critical components for the success of the ERM process. The intent of monitoring and reviewing risks and their respective response plans is to:

- Analyze and track events, changes, trends which effect identified risks
- Assess the impact of such changes to risk assessment and evaluation
- Assess the impact of such changes on response plans

Risk monitoring should be conducted by each business line and function on a monthly basis, for identified risks, in order to track the status of response plans and to consequently update changes to risk profiles.

Risk reviews involves re-examination of the risk register, risk assessment and risk response including the risk profiles. The risk review is conducted by the management to monitor the effectiveness of the ERM framework. Risk reviews entail updation of the risk registers with updated risk assessment, new/ emerging risks, and the related responses and profiling. The risk reviews should be carried out on a quarterly basis (minimum) and updated in the risk report.

The Central Risk Office shall initiate and assist the risk monitoring and risk review process. However, the responsibility of updation of the risk register, risk assessment and risk response, including risk profiles, lies with the respective risk and process owners.

12. Managing Materialized Risks

It is necessary to have a crisis/ incident response plan for timely and effective management of an event of a risk materializing. The incident management plan is a set of well-coordinated actions aimed at preparing and responding to unpredictable events with adverse consequences. The intention of this plan is to preserve the confidence of internal and external stakeholders in companies risk readiness for potentially adverse events.

The crisis management plan should detail out the following:

- The situations for which action plans shall be invoked
- The manner in which such plans shall be actioned
- The individuals/ departments involved in such planning and execution

Tracking data pertaining to materialized risks is an essential input to the development and functioning of ERM. Such data is crucial for effective risk reviews based on actual historical experience.

The data pertaining to materialized risks shall be captured in a “Loss event database”. Typical loss events can include (but may not be restricted to):

- Unforeseen political or regulatory changes
- Damage/ loss of critical network assets resulting in network outage or deteriorating quality
- Environment, Health and Safety incidents
- Loss of key customers/ vendors/ alliances
- Technology/ system failures or Cyber-attacks including Hacking

The format for the “Loss event database” is appended in Annexure 14.7.

13. Document Management

The ERM framework is owned by the Central Risk Office. Changes to the document need to be processed through the CROs office and require the consensus of the Board of Directors and Audit Committee.

The Central Risk Office shall ensure that updates to the framework are communicated across the organization and shall also be responsible for promoting risk awareness across the company.

Record retention

For the purpose of ensuring traceability of ERM activities, documentation shall be maintained in physical or electronic form and retained for period mandated by law for financial data under companies and/ or income tax act.

Records, both physical and electronic, at the organization level shall be maintained by the Central Risk Office on behalf of the Audit Committee and Board of Directors.

14. Annexure

14.1. Risk Register Format

Please Note: Risks identified and assessed can arise from multiple categories, termed under 'Risk type/ category'. The risk categorization as per the COSO framework:

- Effectiveness and efficiency of operations (**Operational**)
- Reliability of financial reporting (**Reporting**)
- Compliance with applicable laws and regulations (**Compliance**)
- Sustenance/ Safeguarding of Assets (**Strategic**)

Risk #	Risk type/ category	Risk Title	Risk Impact	Risk Description/ Root causes	Risk owner	Mitigation Owner	Likelihood	Impact	Risk response	Risk Timelines

14.2. Risk Assessment Parameters

Risk Impact

Ref.	Scale	Calculation	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
1. Financial Parameters							
1.1	**Financial** - Potential impact on Revenue	% of 'Last 3 years Total Revenue'	Less than or equal to 1%	More than 1 % but less than or equal to 3 %	More than 3 % but less than or equal to 5 %	More than 5 % but less than or equal to 10 %	More than 10 %
1.2	**Financial** - Potential impact on Profitability	% of 'Last 3 years EBITDA'	Less than or equal to 2 % of EBITDA	More than 2 % but less than or equal to 5 % of EBITDA	More than 5 % but less than or equal to 10 % of EBITDA	More than 10 % but less than or equal to 15 % of EBITDA	More than 15 % of EBITDA
2. Compliance Parameters							
2.1	**Regulatory Impact**	Potential financial	Regulatory and legal non compliances	Regulatory and legal non compliances with	Regulatory and legal non compliances with	Regulatory and legal non compliances with	Regulatory and legal non compliances with

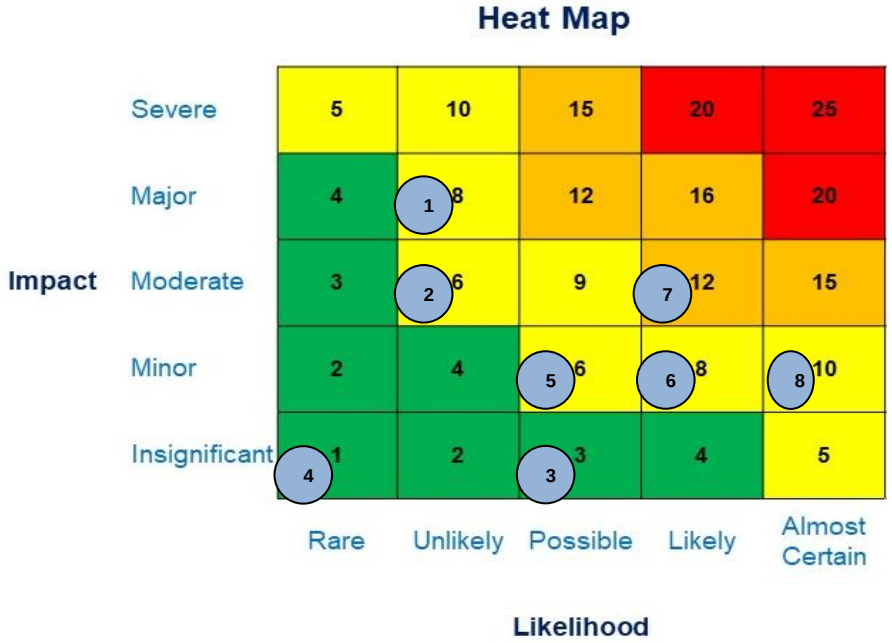
Ref.	Scale	Calculation	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
	- Potential impact on business owing to applicable regulations	penalties from regulator	resulting in a notice/ warning from the regulator	potential financial penalties upto INR 5 Lacs	potential imprisonment and/or financial penalties between INR 6 Lacs and INR 50 Lacs	potential imprisonment and/or financial penalties upto INR 51 Lacs to INR 1 Cr	potential imprisonment and/or financial penalties greater than INR 1 Cr
3. IT System or Vulnerability Parameters							
3.1	**Operations Impact** - Potential impact on business owing to IT system downtime or vulnerabilities	System downtime leading to difficulty in continuing business	Insignificant impact on business continuity, loss of information or data, business disruption up to 1 hour of downtime.	Minor impact on business continuity, loss of information or data, business disruption up to 4 hours of downtime.	Moderate impact on business continuity, loss of information or data, business disruption up to 1 day of downtime	Major impact on business continuity, loss of information or data, business disruption for more than 1 day of downtime	Critical impact on business continuity, loss of information or data, business disruption for more than 1 day of downtime
3.2	**Data Leakage** - Potential impact on business owing to data leakage	Nature of document	Documents easily available to public / containing non-confidential data	Documents not available to public but containing non-confidential data	Documents not available to public and leakage impacting business to minimum	Documents not available to public and leakage impacting one divisions competitiveness	Documents not available to public and leakage impacting more than one division competitiveness
4. Reputation Parameters							
4.1	**Brand Image** - Potential impact on brand image	Qualitative impact (Reputational)	Impact on brand image but can be prevented through immediate corrective action	Impact on brand image but contained within the organization within a specific circle	Reputational loss contained within the organization but with a reach across multiple circles	Reputational loss at circle level, with mass reach (i.e. media and public)	Reputational loss at national/ international level/group level
4.2	**Non-Financial** - Potential impact on the control environment and relationships (internal and external)	Qualitative and Quantitative Impact	a) No risk of litigation b) Disruption in relation with 10% of non-strategic vendor c) Impacts < 5% of the customer base d) Geopolitical situation with no impact	a) Arbitration with financial penalty as above b) Disruption in relation with 20% of non-strategic vendor c) Impacts 5% to 10% of the customer base d) Geopolitical situation with minor impact	a) Court litigation with possible penalty as above b) Disruption in relation with 30% of non-strategic vendor c) Impacts 10% to 20% of the customer base d) Geopolitical situation with temporary closure of operations	a) Court litigation with possible penalty as above b) Disruption in relation with 5% of strategic vendor c) Impacts 20% to 30% of the customer base d) Geopolitical situation with long term closure of operations	a) Court litigation with possible penalty as above b) Disruption in relation with 10% of strategic vendor c) Impacts > 30% of the customer base d) Geopolitical situation with permanent closure of operations
4.3	**Financial** - Potential impact on Sales and Purchase due to customer / vendor	Quantitative Impact	a) Loss of sales due to departure / dependence on Brands < 2% of total sales	a) Loss of sales due to departure / dependence on Brands 2% to 5% of total sales	a) Loss of sales due to departure / dependence on Brands 5% to 10% of total sales	a) Loss of sales due to departure / dependence on Brands 10% to 20% of total sales	a) Loss of sales due to departure / dependence on Brands > 20% of total sales

Ref.	Scale	Calculation	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
			b) Loss of tonnage / meters / dependence on single customer < 2% of total tonnage / meters c) Loss of vendor / dependence on single vendor < 2% of procurement	b) Loss of tonnage / meters / dependence on single customer 2% to 5% of total tonnage / meters c) Loss of vendor / dependence on single vendor 2% to 5% of procurement	b) Loss of tonnage / meters / dependence on single customer 5% to 10% of total tonnage / meters c) Loss of vendor / dependence on single vendor 5% to 10% of procurement	b) Loss of tonnage / meters / dependence on single customer 10% to 20% of total tonnage / meters c) Loss of vendor / dependence on single vendor 10% to 20% of procurement	b) Loss of tonnage / meters / dependence on single customer > 20% of total tonnage / meters c) Loss of vendor / dependence on single vendor > 20% of procurement
4.4	**Attrition** - Potential impact on operations of company due to Attritions	Qualitative Impact (Critical Employees are defined as CEO / COO and any employee who has been identified as critical to the business Key Employees - Defined as employees who have been rated as exceptional performers for a continuous period of 2 years)	a) Limited attrition of non-key employees – can be managed through normal recruitment	a) Moderate attrition of non-key employees - may require focused effort on recruitment	a) Extensive attrition of non-key employees - may require focused effort on recruitment b) Loss of 2 key employees	a) Loss of > 2 key employees b) Loss of 1 critical employee	a) Loss of > 1 critical employee

Likelihood of Occurrence

Scale	Probability	Velocity (No. of Years)	Description
Almost certain (5)	> 80%	Multiple times a year	Very likely. The event is expected to occur in most circumstances as there is a history of regular recurrence and lapse of control
Likely (4)	51 - 80%	Once in a year	More than an even chance of occurring. There is a strong possibility the event will occur as there could be a history of frequent occurrence and/ or similar occurrences
Possible (3)	26 - 50%	1 – 3	More than likely to occur. The event might occur at some time as there could be a history of casual occurrence &/or similar occurrences.
Unlikely (2)	11 - 25%	3 – 5	Small likelihood, Not expected, but there's a slight possibility it may occur at some time.
Rare (1)	0 - 10%	5 – 10	Neither expected to happen nor has it occurred in the past – event would be a surprise; it may occur in exceptional circumstances. It could happen, but probably never will

Report for <Entity/ Business Unit/ Function> as on DD-MM-YYYY



<Risk 1> Shortage of skilled manpower

<Risk 2> Inadequate network planning

<Risk 3> Erosion of brand and reputation

<Risk 4> Poor forecasting and MIS

<Risk 5> Litigation due to regulatory violation

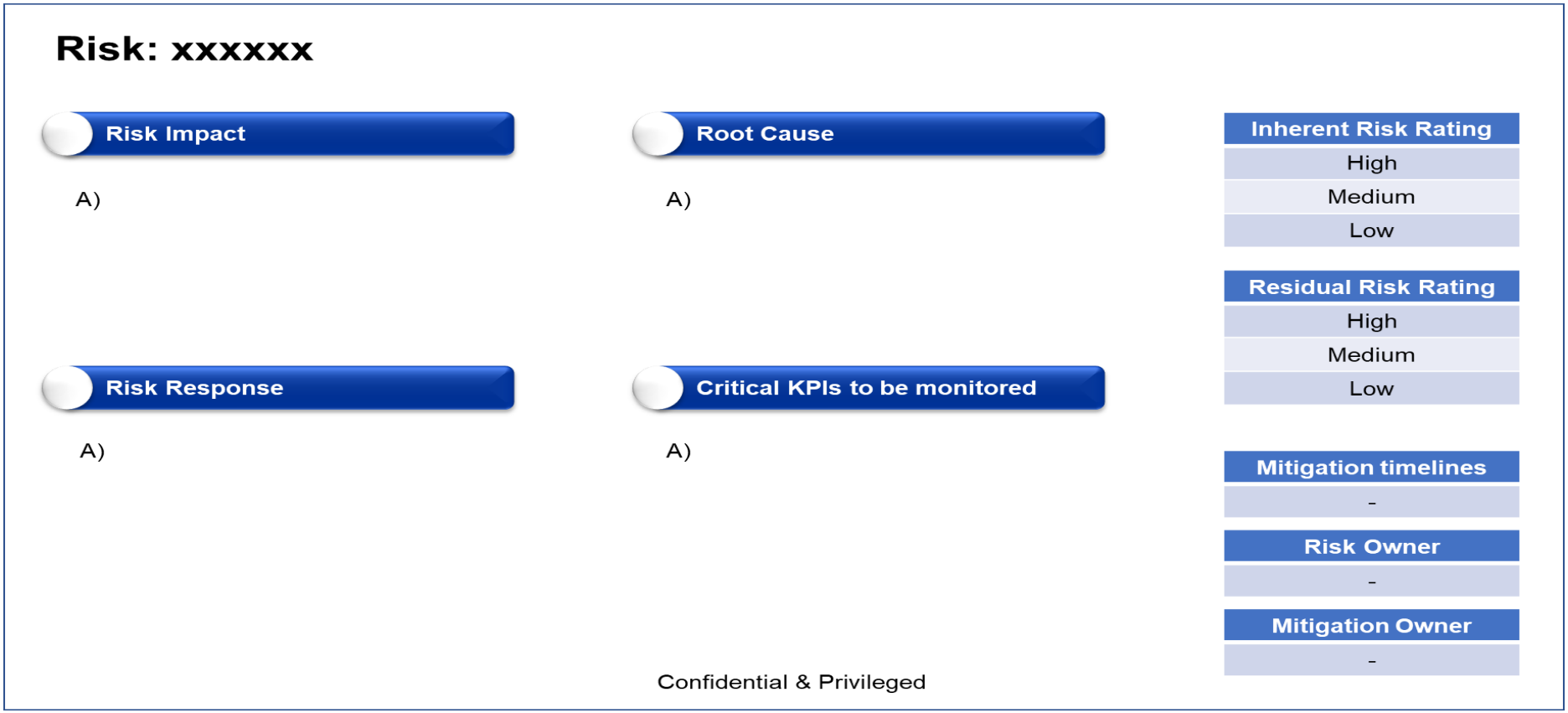
<Risk 6> Time and cost overruns

<Risk 7> Lack of innovation

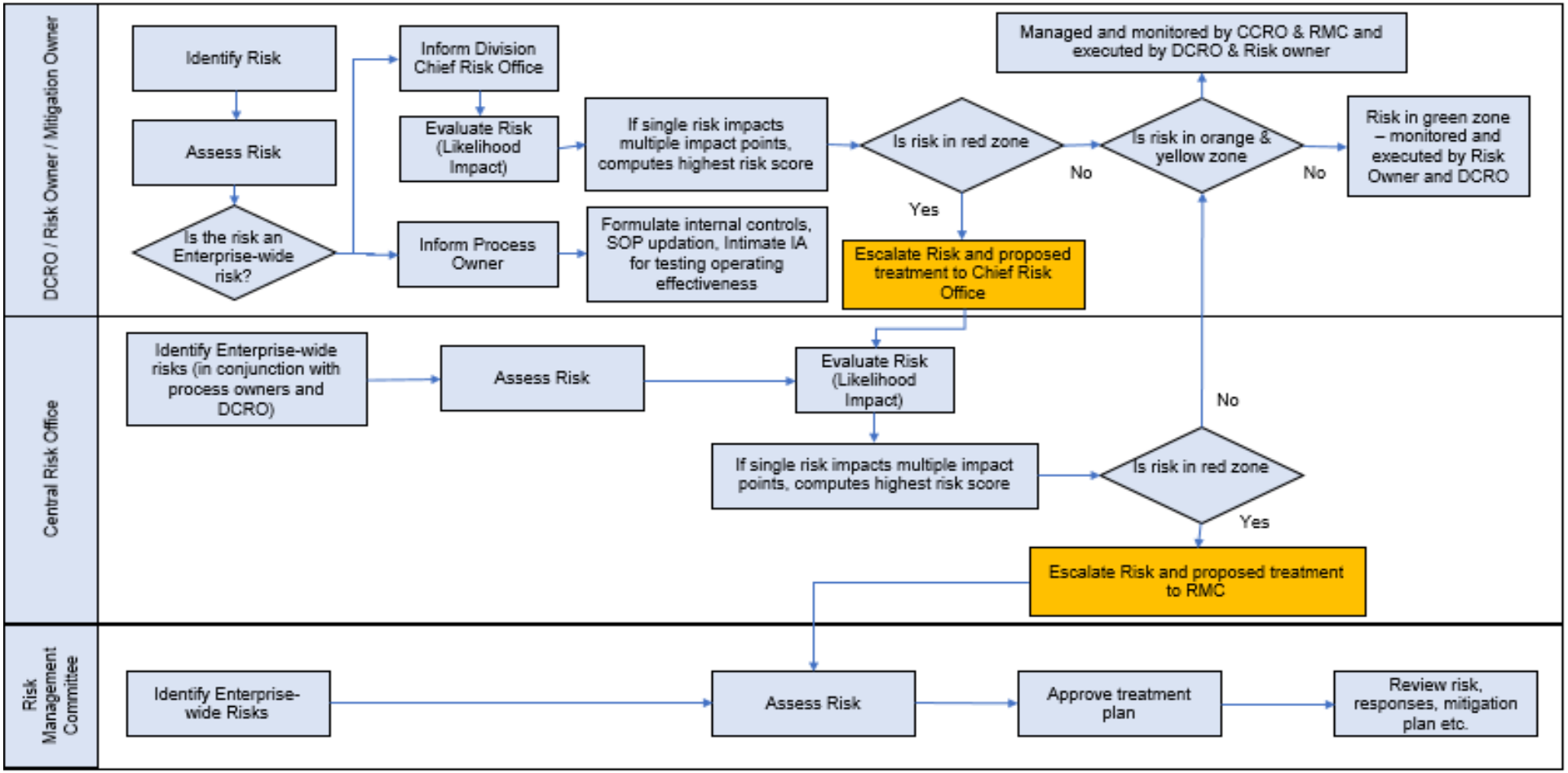
<Risk 8> Inconsistent quality of service

Note: This is an Illustrative "heat map & Risks"

14.3.Risk Profile Format



14.4. Risk Escalation Process



Please Note: Refer to Section 6.1 for definitions of enterprise-wide risk and process risk

14.5. ERM Calendar

#	Activities of the Central Risk Office (CRO)	Resp.	Frequency
1	**Assessment and approval of companies' Risk Appetite** (including risk assessment parameters)	RMC	Annual
2	**Revaluate top enterprise risks** of strategic impact	RMC & CCRO	Annual
3	Review, update (where necessary) and communicate the **ERM policy**	RMC & CCRO	Annual
4	**Inputs on risk from CCRO** in preparation of AOP **& Risk identification (new risk)/ Risk Validation (existing risk)** based on the Annual Operating Plans at company	CCRO, DCRO & Business	Annual
5	**Risk identification** based on 'Signals of Change'	CCRO / DCRO	Ongoing
6	**Monthly assessment of risk & incidents** and report to be sent to CRO	DCRO / Plant Head	Monthly
7	**Periodic self-certification** that risks are monitored on periodic basis	CCRO & DCRO	Quarterly
8	**Inputs to Audit Committee** for consideration in development of IA plan	CCRO, DCRO & IA	Half Yearly
9	**Risk Assessment** for calculating **'Gross or Inherent Risk' and 'Residual Risk'**	CCRO & DCRO	Ongoing
10	Review and update the **Risk Register**	CCRO	Ongoing
11	Updation of the **Loss Event Database**	CCRO	Need Based
12	**Risk Reporting** to the RMC	CCRO	Quarterly
13	**Risk Reporting** to the AC/ BOD	CCRO	Half Yearly

Note: *RMC – Risk Management Committee; CCRO – Company Central Risk Office; DCRO - Division Chief Risk Officer, IA – Internal Audit; AC – Audit Committee; BOD – Board of Directors*

14.6. Loss event database

Incident description	Incident type	Incident owner	Incident cause	Reporting month (MMM/YY)	Total actual cost to date (INR)	Worst case potential loss (INR)	Realistic loss expected (INR)	Actions	Action complete	Incident open/ closed

Terminology & Abbreviations		
S. No.	**Short form**	**Full form**
1	CFO	Chief Financial Officer
2	CRO	Central Risk Office
3	CCRO	Company Chief Risk Officer
4	DCRO	Division Chief Risk Officer
5	ERM	Enterprise Risk Management
6	IA	Internal Audit
7	SWOT	Strengths, Weakness, Opportunity and Threat
8	PESTLE	Political, Economic, Social, Technological, Legal and Environmental
9	RMC	Risk Management Committee
10	LODR	Listing Obligations and Disclosure Requirements