J Kumar

Risk Management Framework

Document Name	: Risk Management Policy and Procedures
Issued By	: Risk Management Committee
Authorized By	: Managing Director

Version History

Version	Date	Prepared by	Changes and Reasons for change
1.0	25-Jul-2021		Initial document by M/s KPMG

PROPRIETARY NOTICE

Contents	Pg. No.

Foreword

Need for Risk Management

J. Kumar Infra Projects Limited ('JKumar' or 'the Company') operates in a business environment that is characterized by increasing globalization of markets and intensifying competition.

JKUMAR is exposed to a number of risks in ordinary course of business. This is inevitable, as there can be no entrepreneurial activity without the acceptance of risks and associated profit opportunities.

Accordingly, risk management activities at JKUMAR are not aimed at eliminating all risks in their entirety, but rather at helping to identify and assess the risks the Company encounters in its daily business. This allows the company to manage the risks in an efficient manner to take informed decisions, to exploit the opportunities available and thereby enhance the value of the Company and its stake holders.

Mandates for Risk management framework

1. Companies Act, 2013 mandates development and implementation of risk management framework.
   - As per section 134 (3)(n): The Board of Directors report must 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): Every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, inter alia, include evaluation of internal financial controls and risk management systems.
2. SEBI (Listing Obligations & Disclosure Requirement) Regulations, 2015 mandates risk assessment and minimization procedures. As per regulation 17 (9): The listed entity shall lay down procedures to inform members of Board of Directors about risk assessment and minimization procedures and the Board of Directors shall be responsible for framing, implementing and monitoring the risk management plan for the Company.

Benefits of Integrated Enterprise Risk Management (ERM)

- *Increasing the range of opportunities:*
  Management can identify new opportunities and unique challenges associated with current risks by considering all possibilities.
- *Identifying and managing risk entity-wide:*
  Sometimes a risk can originate in one part of the entity but impact a different part. Consequently, management identifies and manages these entity-wide risks to sustain and improve performance
- *Increasing positive outcomes and advantage while reducing negative surprises:*
  ERM allows entities to improve their ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses, while profiting from advantageous developments.
- *Reducing performance variability:*
  ERM helps to anticipate the risks that would affect performance and enable them to put in place the actions needed to minimize disruption and maximize opportunity.
- *Improving resource deployment:*
  Obtaining robust information on risk allows management to assess overall resource needs, prioritize resource deployment and enhance resource allocation.
- *Enhancing enterprise resilience:*
  Entity's medium- and long-term viability depends on its ability to anticipate and respond to change, not only to survive but also to evolve and thrive. This is, in part, enabled by effective ERM.

Scope and Purpose of this Policy

The key objectives of this policy are to:

- Provide an overview of the principles of risk management
- Explain approach adopted by the Company for risk management
- Define the organizational structure for effective risk management
- Provide a sound basis for integrated enterprise-wide risk management as a component of good corporate governance
- Improve business performance by informing and improving decision making and planning
- Promote a more innovative, risk awareness culture in pursuit of opportunities to benefit the organization

This policy applies to all employees of JKUMAR and every part of JKUMAR's business and functions.

This policy has been designed to complement other specific risk management programs, policies and risk register already in use within JKUMAR.

This policy is intended to ensure that an effective risk management framework is established and implemented within JKUMAR to ensure compliance to various requirements under the Companies Act 2013 and SEBI (Listing Obligations & Disclosure Requirement) Regulations, 2015.

Definitions

This Risk Management policy is formed around a common understanding of terminology used in this document.

Risk

"The possibility that events will occur and affect the achievement of strategy and business objectives"
Risk is the potential for loss or harm – or the diminished opportunity for gain – that can adversely affect the achievement of an organization's objectives. Risk may be a direct or indirect effect on an organization resulting from inadequate or failed internal processes, people & systems or from external events.

Gross/Inherent Risk

Gross/Inherent risk is the risk to an entity in the absence of any direct or focused actions by management to alter its severity

Residual Risk

Residual risk is the risk remaining after management has taken action to alter its severity.

Risk Appetite Statement

Risk appetite may encompass a single depiction or several depictions that align and collectively specify the acceptable types and amount of risk. It is the articulation of risk appetite in written form.

Contributing Factors

Contributing factors are the possible proximate causes which jointly or severally accentuate the chances of the occurrence of a risk event or increase the level of impact of the risk on the organization

Enterprise Risk Management

The culture, capabilities, and practices, integrated with strategy-setting and performance that organizations rely on to manage risk in creating, preserving, and realizing value. It helps the organization identify, prioritize, and focus on those risks that may prevent value from being created, preserved, and realized, or that may erode existing value.

Risk Assessment

Risk Assessment refers to the quantification of the impact of risks to determine its potential severity and the probability of occurrence of the risk to determine its potential frequency.
It is process of determining the possibility of occurrence of the risk event (Likelihood) and the magnitude of their consequences (Impact)

Risk Prioritization

The process used to determine risk management priorities by comparing the level of risk against risk appetite, target risk levels or other criteria, to generate a prioritized list of risk for further monitoring and mitigation.

Risk Category

Risks are classified into various categories for better management and control. Each risk category is appropriately defined for the purpose of common understanding. An illustrative list of risk category along with the probable questions to identify them is attached in Annexure-3. This list maybe modified in future to add/modify as new risk categories that may emerge.

Risk Capacity

The maximum amount of risk that JKUMAR is able to absorb in the pursuit of strategy and business objectives while remaining within constraints implied by capital and funding needs and the expectation of shareholders.

Risk Appetite

The types and amount of risk, on a broad level, JKUMAR is willing to accept in its pursuit of value. Generally, risk appetite falls within the risk capacity of the company

Risk Tolerance

The boundaries of acceptable variation in performance related to achieving business objective

Risk Impact

Result or effect of a risk. There may be a range of possible impacts associated with a risk.

Risk Likelihood

The possibility of a risk occurring. This may be expressed in terms of a probability or frequency of occurring.

Risk Management Framework

The Risk Management framework has been developed and approved by senior management in accordance with the business strategy. The key elements of the framework include Risk Structure, Strategy and Objective setting, Risk Identification, Risk Assessment, Risk Prioritization, Risk Treatment, Risk Review and Revision, Risk Reporting, Risk forms & MIS. The overall objective of risk management process is to optimize the risk-reward relationship. Formal authority, responsibility, and accountability for designing, implementing and sustaining effective risk management processes rests with the Board of Directors. The Audit Committee, Risk Management Committee (RMC), Internal Audit Department, Management and other employees support and assist the Board of Directors in fulfilling this responsibility.

RISK STRUCTURE

JKUMAR has established an operating structure and designed reporting lines to carry out the strategy and business objectives. The Risk management Structure is headed by the Board of Directors and flows down to individual risk owners, through communication channels moving through the RMC, respective Department Heads and Risk Coordinators.

A formal Risk Structure with defined roles and responsibilities for risk management activities is an essential prerequisite for effective risk management framework. The risk management structure at JKUMAR is represented in Annexure 1. The roles and responsibilities of JKUMAR personnel are detailed in Annexure 5.

The effectiveness of risk management depends on the employees of the Company. Factors promoting risk awareness culture within an organization include:

- Corporate philosophy and management style
- Integrity, values, competence, and abilities of employees
- Effective lateral and vertical communication
- Key actions driven by the top management to help embed a risk structure

Composition and functioning of RMC

A robust organizational structure for identifying and reporting risks is a prerequisite for an effective risk management process

The organization structure needs to be supported by clearly defined non overlapping roles and responsibilities which are communicated and understood.

To ensure that this policy is followed in letter and spirit, a Risk Management Committee (RMC) is constituted comprising of:

- Managing Director
- Non-Executive Director- Independent Director
- Non-Executive Director- Independent Director
- Chief Risk Officer

The RMC will be chaired by Non-Executive - Independent Director. The RMC shall meet at least twice in a year or as needed for urgent or other matters. Reports of RMC's activities (agendas, decisions) and meetings (including attendance) will be dealt by the Company Secretary.

STRATEGY AND OBJECTIVE SETTING

1. Analyze business context

JKUMAR considers business context when developing strategy to support its vision and mission. “Business context” refers to the trends, relationships, and other factors that influence an organization’s current and future strategy and business objectives. It consists of the following:

a. External environment and external stakeholders: External environment is anything, including external stakeholders, outside the entity that can influence the entity’s ability to achieve its strategy and business objectives. The external environment comprises several factors that can be categorized by the acronym PESTLE: political, economic, social, technological, legal, and environmental.
b. Internal environment: Internal environment consists of capital, people, process and technology.

Internal Environment Categories and Characteristics	
Categories	Internal Environment Characteristics
Capital	Assets, including cash, equipment, property, patents
People	Knowledge, skills, attitudes, relationships, values, and culture
Process	Activities, tasks, policies, or procedures; changes in management, operational, and supporting processes
Technology	New, amended, and/or adopted technology

2. Defines risk appetite

JKUMAR develops strategy and risk appetite in parallel and aligns it to vision and mission of the company. JKUMAR considers a number of parameters to frame its risk appetite:

- *Strategic parameters*, such as new products to pursue or avoid, the investment for capital expenditures, and merger and acquisition activity.
- *Financial parameters*, such as the maximum acceptable variation in financial performance, return on assets or risk-adjusted return on capital, target debt rating, and target debt/equity ratio.
- *Operating parameters*, such as environmental requirements, safety targets, quality targets, and customer concentrations.
- *Risk profile* provides information on the JKUMAR’s current amount of risk and how risk is distributed across the entity, as well as on the different categories of risk for the entity.

In addition, JKUMAR has also developed risk appetite statements by considering the following:

- Strategy and business objectives that align with the vision and mission.
- Business objective categories.
- Performance targets of the entity.

With the support of the board, management also revisits and reinforces risk appetite over time in light of new and emerging considerations. JKUMAR’s “appetite” or tolerance for risk will vary with its strategy, evolving conditions in the industry and markets, organizational culture as well as other external factors.
JKUMAR cascades risk appetite through statements aligned with high-level business objectives that, in turn, align with the overall entity strategy.

3. Evaluate alternate strategies

JKUMAR selects strategy that supports vision and mission of the company and is aligned with their risk appetite. When evaluating alternative strategies, JKUMAR seeks to identify and understand the potential risks and opportunities of each strategy being considered. The identified risks collectively form a risk profile for each option; that is, different strategies yield different risk profiles. Management and the board use these risk profiles when deciding on the best strategy to adopt, given the entity's risk appetite.
JKUMAR uses a number of approaches to evaluating alternative strategies are SWOT analysis, modeling, valuation, revenue forecast, competitor analysis, and scenario analysis. JKUMAR selected the strategy which is within the risk appetite of the company.

4. Formulating business objectives

- Establishing business objectives: JKUMAR develops business objectives that are specific, measurable, or observable, attainable, and relevant which are aligned with the achievement of the selected strategy, risk appetite, vision, and mission of the company.
- Setting Performance Measures and Targets: JKUMAR sets targets to monitor the performance of the entity and support the achievement of the business objectives.
- Establishing tolerances: It is a range of acceptable outcomes related to achieving a business objective within the risk appetite and is applied to all business objectives. Performance measures related to a business objective help confirm that actual performance is within an established tolerance. It is expressed in measurable units (preferably in the same units as the business objectives).
  In setting tolerance, the organization considers the relative importance of each business objective and strategy. For those objectives viewed as being highly important to achieving the entity's strategy, the organization may wish to set a lower range of tolerance. Operating within defined tolerance provides management with greater confidence that the entity remains within its risk appetite and provides a higher degree of comfort that the entity will achieve its business objectives.

RISK IDENTIFICATION

Risk identification refers not only to the systematic identification of risks but also to the identification of their root causes. JKUMAR identifies new, emerging, and changing risks to the achievement of the entity's strategy and business objectives. It undertakes risk identification activities to first establish an inventory of risks, and then to confirm existing risks as being still applicable and relevant. Frequency of risk identification exercise conducted by JKUMAR depends on how quickly risks change or new risks emerge.

New, emerging, and changing risks include those that:

- Arise from a change in business objectives
- Arise from a change in business context (Internal and External)
- Were previously unknown
- Were previously identified but have since been altered due to a change in the business context, risk appetite, or supporting assumptions.

Risk can be identified in a number of ways:

1. Cognitive computing allows JKUMAR to collect and analyze large volumes of data to detect future trends and meaningful insights in new and emerging risks as well as changes in existing risks more efficiently than a human.

2. Data tracking from past events can help predict future occurrences. While historical data typically is used in risk assessment—based on actual experience with severity—it can also be used to understand interdependencies and develop predictive and causal models

3. Interviews solicit the individual's knowledge of past and potential events. For canvassing large groups of people, questionnaires or surveys may be used. Sample questions are listed in Annexure 3.

4. Workshops bring together individuals from different functions and levels to draw on the group's collective knowledge and develop a list of risks as they relate to the entity's strategy or business objectives

5. Process analysis involves developing a diagram of a process to better understand the interrelationships of its inputs, tasks, outputs, and responsibilities

6. Key indicators are qualitative or quantitative measures that help to identify changes to existing risks. Risk indicators should not be confused with performance measures, which are typically retrospective in nature

Type of Risk	Cognitive Computing	Data Tracking	Interviews	Key Indicators	Process Analysis	Workshops
Existing	✔	✔	✔	✔	✔	✔
New	✔	✔			✔	✔
Emerging	✔		✔	✔		✔

Once risks are identified, they are categorized into various categories. JKUMAR identifies and categorizes risks into

- Strategic Risk
- Operational Risk
- Reputation Risk
- Compliance Risk
- Financial Risk
- Information Risk
- New / Other Risk

JKUMAR will document its risks in the Risk Register. The Risk Register acts as a central repository for risks. The purpose of the Risk Register is to record identified risks and related information in a structured manner. JKUMAR structures the risk inventory by category to provide standard definitions for different risks. This allows similar risks to be grouped together, such as financial risks, reputational risks, or compliance (or more broadly, obligation) risks. The risk register includes Risk Category, Risk Statement along with contributing factor, Risk Owner, Risk Manager, Inherent Risk Evaluation, Risk Mitigation Owner, Existing mitigation, Mitigation measures in progress or proposed along with timelines, Resource requirement and Residual Risk Evaluation. The Risk Register is the key document used to communicate the current status of all known risks and is vital to all management control, reporting and reviews. The Risk Register is owned by the Risk Coordinator. Risk owners are assigned to each identified risk and are responsible for the execution of risk managing actions. The risk inventory is updated on once a quarter and reported to management quarterly.

RISK ASSESSMENT

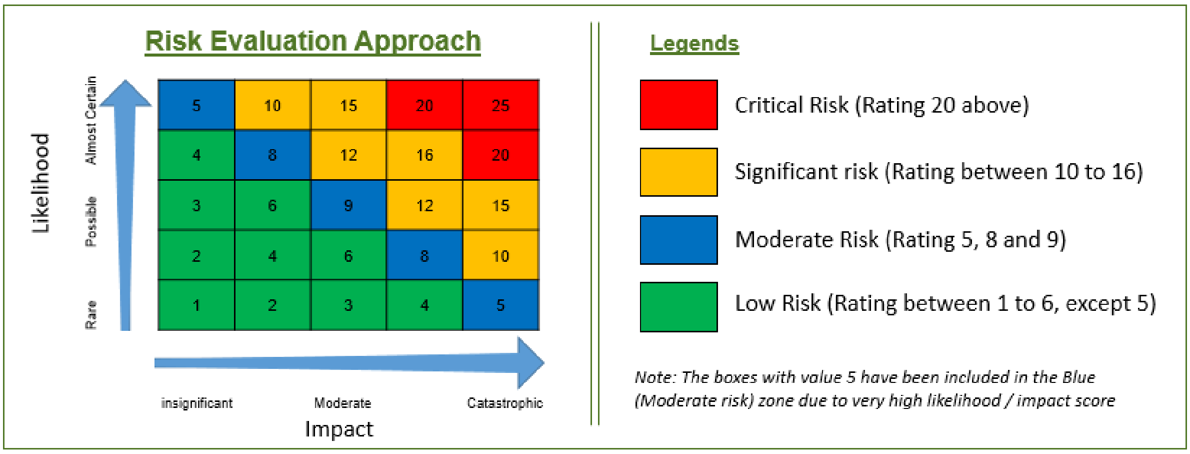
Risks identified and included in an JKUMAR risk inventory are assessed in order to understand the severity of each to the achievement of an entity's strategy and business objectives.
The risks will be assessed on qualitative two-fold criteria. The two components of risk assessment are (a) Impact (b) Likelihood. The likelihood and impact should be rated over a period of 12 to 18 months.

The combination of likelihood of occurrence and the magnitude of impact provides the inherent risk level. The magnitude of impact of an event, should it occur, and the likelihood of the event and its associated consequences, are assessed in the context of the existing controls. As a part of the assessment process, management considers potential combinations of likelihood and impact. The time horizon used to assess risks is the same as that used for the related strategy and business objectives. Impact and likelihood may be determined using statistical analysis and calculations. Alternatively, where no past data are available assessment approaches, such as interviews, workshops, surveys, and benchmarking are used for risk assessment.
Where needed, guidance as provided in Annexure 2 may be used for assessment Risk.

RISK EVALUATION AND PRIORITIZATION

Product of impact and likelihood provides the level of inherent risk which is classified into 4 zones as below

- Critical Risk-Risks that score within a red zone are considered "unacceptable" or "critical" and require immediate action plans to bridge significant control gap (if any). Further the same should be monitored on continuous basis.
- Significant Risk – Risk that score within the amber zone are "significant" and require continuous (quarterly) monitoring where controls needs to be reviewed or revived.
- Moderate Risk - Risks that score within the blue zone are considered "cautionary" or "Moderate Risk" where action steps to develop or enhance existing controls is also needed and periodic (half yearly) monitoring is required.
- Low Risk-Risks that score within the green zone are considered "acceptable" or in control. Such risk can be reviewed on an annual basis.



The objective of risk evaluation is to create prioritized list of risks for further action or treatment. Through prioritizing risks, management also recognizes that there are risks the entity chooses to accept; that is, some are already considered to be managed to an acceptable limit for the entity and for which no additional risk response will be contemplated. JKUMAR prioritize risks on an aggregate basis where a single risk owner is identified, or a common risk response is likely to be applied. This allows risks to be clearly identified and described using a standard risk category, which enables common risks to be prioritized consistently across the entity.

Once the inherent risk rating is done and risk evaluation score is arrived, the management consider the following criteria to determine the order of risk treatment:

- Adaptability: The capacity of an JKUMAR to adapt and respond to risks (e.g., responding to changing demographics such as the age of the population and the impact on business objectives relating to product innovation).
- Complexity: The scope and nature of a risk to the JKUMAR's success. The interdependency of risks will typically increase their complexity (e.g., risks of product obsolescence and low sales to a company's objective of being market leader in technology and customer satisfaction).
- Velocity: The speed at which a risk impacts JKUMAR. The velocity may move the entity away from the acceptable variation in performance. (e.g., the risk of disruptions due to strikes by port).
- Persistence: How long a risk impacts JKUMAR (e.g., the persistence of adverse media coverage)
- Recovery: The capacity of JKUMAR to return to tolerance (e.g., continuing to function after a severe flood or other natural disaster).
- Risk Appetite: Risks that result in JKUMAR approaching the risk appetite for a specific business objective are typically given higher priority. Additionally, performance levels that approach the outer bounds of tolerance may be given priority.

RISK TREATMENT / MITIGATION

Risk Treatment/Mitigation is a process of managing the exposure of various risks and bringing them in line with the risk appetite of the company. I.e. treatment of inherent risk to bring the residual risk within the risk appetite of the company.

Risk Treatment/Mitigation involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them

For all risks identified, management selects and deploys a risk response.

Management considers the following criteria for selection of a management response:

- Severity and prioritization of the risk as well as the business context and associated business objectives.
- Performance targets of the organization.
- Anticipated costs and benefits
- Risk response either brings risk (residual) within risk appetite of the entity.

Risk responses fall within the following categories:

- *Accept:* No action is taken to change the severity of the risk. This response is appropriate when the risk to strategy and business objectives is already within risk appetite. Risk that is outside the entity's risk appetite and that management seeks to accept will generally require approval from the board or other oversight bodies.
- *Avoid:* Action is taken to remove the risk, which may mean ceasing a product line, declining to expand to a new geographical market, or selling a division. Choosing avoidance suggests that the organization was not able to identify a response that would reduce the risk to an acceptable level of severity.
- *Pursue*: Action is taken that accepts increased risk to achieve improved performance. This may involve adopting more aggressive growth strategies, expanding operations, or developing new products and services. When choosing to pursue risk, management understands the nature and extent of any changes required to achieve desired performance while not exceeding the boundaries of acceptable tolerance.
- *Reduce*: Action is taken to reduce the severity of the risk. This involves any of myriad everyday business decisions that reduces risk to an amount of severity aligned with the target residual risk profile and risk appetite.
- *Share*: Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk. Common techniques include outsourcing to specialist service providers, purchasing insurance products, and engaging in hedging transactions. As with the reduce response, sharing risk lowers residual risk in alignment with risk appetite

Upon treatment of the risk, JKUMAR re-evaluates the risk rating to identify the residual risk. JKUMAR selects that risk response which brings the residual risk within the risk appetite of the company. Monitoring of the risk (immediate, quarterly, half yearly and annually) is done based on the residual risk rating,

In some instances, management may need to consider another course of action, including the following:

- *Review business objective*: The organization chooses to review and potentially revise the business objective given the severity of identified risks and tolerance. This may occur when the other categories of risk responses do not represent desired courses of action for the entity.
- *Review strategy*: The organization chooses to review and potentially revise the strategy given the severity of identified risks and risk appetite of the entity. As with a review of business objectives, this may occur when other categories of risk responses do not represent desired courses of action for the entity.

RISK REVIEW AND REVISION

A risk review involves the re-examination of all risks recorded on the Risk Register to ensure that the current assessments remain valid and review the progress of risk reduction actions.
Also, Risk Management action should also be undertaken to identify risks associated with changes to current business processes or changes in external environment.
The organization identifies and assesses changes that may substantially affect strategy and business objectives. The extent of any corrective actions must align with the magnitude of the deviation in performance, the importance of the business objective, and the costs and benefits associated with altering risk responses. Factors that can lead to review and revision

1. Internal Environment

   Rapid growth: When operations expand quickly, existing structures, business activities, information systems, or resources may be affected. Information systems may not be able to effectively meet risk information requirements because of the increased volume of transactions. Risk oversight roles and responsibilities may need to be redefined in light of organizational and geographical changes due to an acquisition.

   Innovation: Whenever innovation is introduced, risk responses and management actions will likely need to be modified

   Substantial changes in leadership and personnel: A change in management may affect enterprise risk management. A newcomer to management may not understand the entity's culture and may have a different philosophy or may focus solely on performance to the exclusion of risk appetite or tolerance.

2. External Environment

   Changing regulatory or economic environment: Changes to regulations or in the economy can result in increased competitive pressures, changes in operating requirements, and different risks.

3. Entity Performance

   Reviewing performance confirms whether risks were previously identified, or whether new, emerging risks have occurred. The organization also reviews whether the actual risk levels are within the boundaries established for tolerance. If JKUMAR determines that performance does not fall within its acceptable variation, or that the target performance results in a different risk profile than what was expected, it may need to review business objectives, strategy, culture, reassess severity of risk results, review how risks are prioritized, revise risk responses, revise risk appetite.

RISK REPORTING

JKUMAR uses various channels that are available to the organization for communicating risk data and information to internal and external stakeholders.

1. Internal Communication to employees and the board
   Internally, management communicates the entity's strategy and business objectives clearly throughout the organization so that all personnel at all levels understand their individual roles. Management also communicates any information (along with the Top 20 risks) that helps the board fulfill its risk oversight responsibilities.

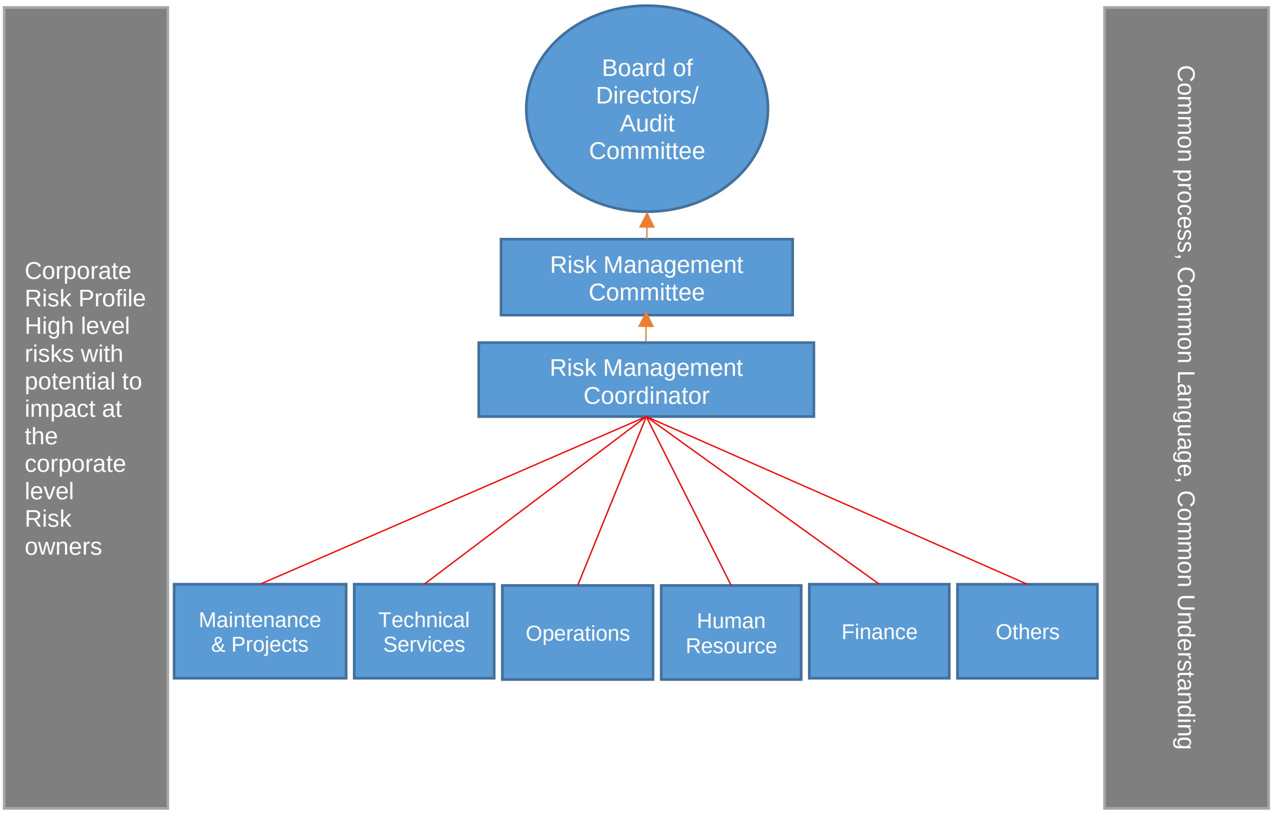
   Also, Risk Communication and Escalation are embedded in the culture of an organization to make it effective. At JKUMAR, the Board of Directors drive the Risk Management Process by adopting the following communication and escalation procedure:

   - Employees continuously identify needs to update / modify the risks and escalate them to their respective Unit / Functional Head.
   - The respective Unit/ Functional Head or designated personnel collate the identified risks/ modifications and forward the same to the respective Risk Coordinator for collation and escalation to Risk Management Committee. Standard forms for identification/ modification/ deletion of risks are used for this purpose
   - The Risk Coordinator collates the risks and forwards the same to the Risk Management Committee on a quarterly basis.
   - The Risk Management Committee (RMC) is responsible for reviewing and validating the risks/ modifications for all departments.
   - The RMC categorizes and rates the risks (using the risk categories and impact and likelihood rating criteria).
   - Risk Owners for each risk are identified and approved by RMC. Risk Owners may be at any level in the organization depending on the nature and categorization (e.g. strategic, operational, compliance or reporting) of the risk
   - Designated Risk Coordinator updates the Risk Register based on the approvals obtained from the RMC.
   - RMC reviews all the risk where the inherent risk rating is critical/ significant and presents the same to the Audit Committee and Board of Directors on quarterly basis along with the status of the action plans for mitigating these risks. Further risk whether the inherent rating has changed will also be presented to the Audit Committee and Board of Directors on quarterly basis

   The escalation of key risk information will assist in ensuring that critical/significant risks identified at the line level are available for consideration in the context of the overall operations of the business. Risk Management Process as defined above is illustrated in Annexure 4.

2. External Communication to stakeholders and other external parties
   Management also communicates information about the entity's strategy and business objectives to shareholders and other external parties. This information may come through email communications, public forums, blogs, hotlines, annual report or other channels.

Annexure 1 – Risk Organization Structure



Annexure 2 – Risk Impact and Likelihood Criteria

Rating Criteria – Likelihood

Rating	Occurrence	Probability
5	Almost Certain	80-100% probability of risk occurring Ongoing risk
4	Likely	60-80% probability of risk occurring Risk likely to occur Weekly basis
3	Moderate	30-60% probability of risk occurring Risk likely to occur on monthly basis
2	Rare	10-30% probability of risk occurring Risk likely to occur once a year
1	Unlikely	0-10% probability of risk occurring Risk likely to occur on occasional circumstances

Rating Criteria – Impact

Particulars	Consequence Category				
	1	2	3	4	5
Financial (Average Net Profit)- Impact on profitability	< Rs. 25 Lacs	Rs. 25 Lacs - Rs. 1 Cr.	Rs. 1 Cr. - Rs. 5 Cr.	Rs. 5 Cr. - Rs. 25 Cr.	> Rs. 25 Cr.
Health & Safety	Minor Bruises	Minor Injury (Fracture)	Serious Injury (Multiple Fractures)	Permanent Disability	Fatal Injury
Environment	Minor Environmental Damage	Serious Environmental damage	Multiple Environmental damage	Major environmental damage/ possibility of prosecution	Major environmental damage & prosecution
Regulatory	Routine issues raised by Ministry/regulatory authorities	Caution/ instruction from Ministry	Penalties/ intensive scrutiny	Heavy penalties/restrictions on activity	Prosecution / loss of rights to operate
Loss of Talent	General attrition - Negligible impact	Higher than usual level of attrition- gap can be filled easily	Exit of key individual affecting operations in short term	Exit of several key individual affecting operations in short term in various departments	Exit of several key individual at senior and middle management level adversely affecting operations

Annexure 3 – Sample questions for Risk Identification

Risk Identification	
Sample questions for Risk Identification	
Strategic Risk	✓ Are the critical strategies appropriate to enable the organization to meet its business objectives? ✓ What are the risks inherent in those strategies, and how might the organization identify, quantify, and manage these risks? ✓ How much risk is the organization willing to take? ✓ What risk result from e-business developments?
Operational Risk	✓ What are the risks inherent in the processes arising out of chosen strategies?
Reputation Risk	✓ What are the risks to brand and reputation inherent in how the organization executes its strategies?
Compliance Risk	✓ What risks are related to compliance with regulations or contractual arrangements —not just those that are financially based?
Financial Risk	✓ Have operating processes put financial resources at undue risk? ✓ Has the organization incurred unreasonable liabilities to support operating processes? ✓ Has the organization succeeded in meeting business objectives?
Information Risk	✓ Is our data/information/knowledge reliable, relevant, and timely? ✓ Are our information systems reliable? ✓ Do our security systems reflect our e-business strategy?
New/ Other Risk	✓ What risks have yet to develop? (These might include risks from new competitors or emerging business models, recession risks, relationship risks, outsourcing risks, political or criminal risks, financial risk disasters (rogue traders), and other crisis and disaster risks.)

Annexure 4 – Risk Management Procedure

Responsibility	Process	Frequency
Process Personal	Event Identification / modification / deletion	Event Driven
Risk Owner (Head of the department as defined in the risk management structure)	Collation of required information about risk → Are controls in Place? No → Action plan is formulated and approved by the HOD. Risk is entered in the online risk register; Yes → next step	Event Driven
Risk Co-coordinator	Collates all the risk and submits the same to Risk Management committee for review	Quarterly
Risk Management Committee (along with Managing Director)	Reviews and approves the risk → Collates the risk report in accordance with SEBI regulations 2015 and Companies Act, 2013	Quarterly
Audit Committee / Board	Review the report submitted by RMC	Quarterly

Annexure 5 – Roles and Responsibilities

Category	Description of Roles and Responsibilities
Board of Directors	• Inculcate Risk Management philosophy in the organization • Support an environment that does not tolerate behavior which might compromise prudent risk management practice • Define Risk Appetite, assess organization wide risk portfolio against the risk appetite, review and approve changes in the risk appetite of the company • Approve risk policy and risk management strategy • Present Board Disclosures as mandated by per SEBI (Listing Obligations & Disclosure Requirement) Regulations, 2015 and Companies Act, 2013 and its amendments • Review adequacy and effectiveness of business risk management and risk reporting • Periodic review of operating structure, Periodic review of skills, expertise and composition of the board • Setting up of contingency plans for succession
Audit Committee	• Review adequacy and effectiveness of Risk Management at operational/ process level • Review and approve (internal and external) audit plans • Monitor business risk reporting
Risk Management Committee	• Guide integration of enterprise wide risk management with other business planning and management activities • Establishing risk management policies, including defining roles and responsibilities and ensure compliance with the policy • Advise business divisions / support functions on risk initiatives • Suggest improvements to risk management techniques and lift management awareness • Ensure validity and completeness of the risk assessment • Approve and allocate resources for risk mitigation • Setting up of performance targets and their monitoring activities • Ensure appropriate internal controls, risk management and legal compliance systems including standards, training and communications are in place for all high-risk compliance and ethical areas, including but not limited to those areas deemed to be significant risks • Ensure communication of policies and standards to successive levels of management • Provide quarterly updates to the Board / Audit Committee on the current risk management procedures and status of key risks • Submit reports as requested by Audit Committee on changes in risk profile, controls established, etc.
Risk Owners	• Responsible for identifying risks at department's level • Ensure that the Risk Profiles are filled and key risks are escalated to the respective RMC for their approval of proposed mitigation plan • Ensure preparation of a suitable risk response plan keeping in mind the current controls mechanism in place, proposed mitigation measures and organizational priorities in bringing the risks within tolerable limits • Identify resource requirements for risk mitigation/treatment and escalate to RMC for approval • Recommend training programs for staff with specific risk management responsibilities • Ensure that the approved plans are implemented within the specified budgets and reported regularly

Category	Description of Roles and Responsibilities
Risk Managers	• Responsible for identifying risks, assist in preparing risk register and risk profile • Responsible for reassessing risks on a periodic basis • Suggest mitigation plans and ensure implementation of approved mitigation plans • Assist the Risk Owner in understanding the gaps in controls and developing action plans • Assist the Risk Owner in implementation of action plans as approved by the management • Escalate risks to SBU/ corporate function through the Risk Coordinator on a need basis
Risk Coordinator	• Implementing the risk management initiatives across the entire organization • Liaise with the Risk Owners and Risk Managers to coordinate flow of information and escalation of key risk issues/concerns between the RMC and Functional Heads (Risk Owners) • Ensure that meetings of the RMC are held regularly and present updates / changes to Risk Assessment to the RMC on a quarterly basis for approval • Prepare and maintain relevant documentation and RM Reports for the Company • Update Risk Register based on approvals from RMC
All Employees	• Responsible for identifying risks • Responsible for managing risks • Ensure risk profile is current and up to date • Exercise reasonable care to prevent loss, to maximize opportunity and to ensure that the operations, reputation and assets are not adversely affected.

Annexure 6 – Risk Register Template

BACKGROUND			
Risk Ref No:			
Risk Category:			
Business Process / Department(s) / Function			
Risk Statement:			
Contributing Factors:			
Risk Owner(s) / HODs			
Risk Manager(s)			
Overall Risk Criticality (Inherent)	Critical / Significant / Moderate / Low	Impact Rating (A)	
		Likelihood Rating (B)	
		Overall Inherent Risk Rating (A*B)	
Mitigation plan owner(s) / HODs			
Involvement of other departments in risk management / mitigation			
Date of validation:			
Date of next review:			
Description of existing mitigating controls:			
Residual risk assessment			
RISK ASSESSMENT SUMMARY (By all risk owners and risk mitigation plan owners)			
Overall Risk Criticality (Residual)	Critical / Significant / Moderate / Low	Impact Rating (A)	
		Likelihood Rating (B)	
		Overall Residual Risk Rating (A*B)	
Do the controls address the risk effectively (Yes/No)			
Are the controls documented and communicated? (Yes/No)			
Are the controls operating, applied consistently and monitored? (Yes/No)			
Controls Effectiveness Rating:			

RISK TREATMENT/MITIGATION PLAN (By all risk owners and risk mitigation plan owners)					
Recommendation	Accept	Avoid	Pursue	Reduce	Share

Proposed Risk Treatment/Mitigation Actions (By all risk owners and risk mitigation plan owners):

Sr. No	Description	Target date	Mitigation plan owner
Sr. No	**Resource Requirements**	**Responsibility**	**Budgeted Amount**

REVIEW AND MONITORING OF RISK TREATMENT/MITIGATION PLAN (By all risk owners and risk mitigation plan owners)			
Sr. No.	Risk Treatment/Mitigation Plan	Status of Implementation/ monitoring	As on Date

Signature of Risk Manager(s)	Signature of Risk Owner(s) / HOD(s)	Signature of mitigation plan owner(s) / HOD(s)