

RISK MANAGEMENT POLICY

NATIONAL PROJECTS CONSTRUCTION CORPORATION LIMITED

(A GOVERNMENT OF INDIA ENTERPRISES)

PLOT NO. 67-68, SECTOR 25, FARIDABAD (HARYANA)

WHAT IS RISK AND WHY IT SHOULD BE MANAGED

Risk is inherent in all activities. It is a normal condition of existence. Risk is the potential for a negative future reality that may or may not happen. Risk is defined by two characteristics of a possible negative future event: probability of occurrence (whether something will happen), and consequences of occurrence (how catastrophic if it happens). If the probability of occurrence is not known then one has *uncertainty*, and the risk is undefined.

Risk is not a problem. It is an understanding of the level of threat due to *potential* problems. A problem is a consequence that has already occurred.

In fact, knowledge of a risk is an opportunity to avoid a problem. Risk occurs whether there is an attempt to manage it or not. Risk exists whether you acknowledge it, whether you believe it, whether it is written down, or whether you understand it. Risk does not change just because it is contrary to policy, procedure, or regulation. Risk is neither good nor bad. It is just how things are. Risk can arise from internal or external sources and may include exposure to such things as economic or financial loss or gain, physical damage, failure of a project to achieve its target, client dissatisfaction, unfavourable publicity, and a threat to physical safety or breach of security, mismanagement, failure of equipment or fraud.

Progress and opportunity are companions of risk. In order to make progress, risks must be understood, managed, and reduced to acceptable levels.

OBJECTIVE OF RISK MANAGEMENT POLICY

Every business has risk associated with it. Every decision taken has some risk involved. This is more so in the Public Sector which is currently changing rapidly with more autonomy and more decision making delegated down the line. Hence there is a need to define the risks in the business, evaluate them and document their possible impact. Such evaluation of risks involved needs to be factored in while taking the decision.

The Ministry of Corporate Affairs, Government of India has also accepted the concept of Risk Management and its relevance to the smooth functioning of the Corporate sector in India and has therefore introduced a specific provision on Risk Management under paragraph (II) (C) of Corporate Governance voluntary guidelines, 2009

The objective of the Risk Management Policy is:

- (a) To define a framework for identification, evaluation and mitigation of risk in the decision making process of the business of NPCC;
- (b) To protect NPCC from those risks of significant likelihood and consequence in the pursuit of NPCC's stated strategic goals and objectives;
- (c) To continuously monitor the effectiveness of the management of risks having particular regard to failings/weaknesses reported;
- (d) Provide assistance to and improve the quality of decision making throughout the organization;
- (e) To identify and ensure delivery of effective risk management training programmes.
- (f) Assist in safeguarding the Company's property and reputation.
- (g) To continuously monitor and review risks and controls to cater for external/internal changes.

RISK MANAGEMENT PROCESS

Definitions

- (a) **Risk** – An event which leads to a range of consequences with a negative impact on the attainment of qualitative or quantitative business goals, and financial performance.
- (b) **Risk Management** - It is a systematic application of Management Policies, procedures and practices to the task of identifying, analyzing, assessing, treating and monitoring of risks.
- (c) **Risk Management Process** - This pertains to the systematic application of management policies, procedures and practices to the task of establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating the risks.
- (d) **Risk Strategy** - Company's outlook in dealing with various risks associated with the business and includes company's decision on acceptance of risks, avoidance of risks, transfer of risks and its risks tolerance level.
- (e) **Risk Assessment**- The overall process of risk analysis and risk evaluation.
- (f) **Risk Estimation** - The process of quantification of risks.

- (g) **Risk Description** - A comprehensive collection of information about risks in a structured manner.
- (h) **Risk identification**- process of finding, recognizing and detailing risks.
- (i) **Risk Register** - A tool for recording of risks at various locations/levels in a structured format.
- (i) **Risk Owner**- person or delegate with accountability authority to manage risk.

RISK MANAGEMENT

Risk management is an organized method for identifying and measuring risk and for selecting, developing, and implementing options for the handling of risk. It is a process, not a series of events. Risk management depends on risk management planning, early identification and analysis of risks, continuous risk tracking and reassessment, early implementation of corrective actions, communication, documentation, and coordination. Though there are many ways to structure risk management.

As per ISO 31000 "**Risk management - Principles and guidelines on implementation**" divides risk management process into six steps: (1) identification, (2) planning, (3) mapping out the social scope of the risk management, identifies objectives of the stakeholders, and the background of the risk will be assessed, (4) defining the model for the following action due to risk identification, (5) analyzing the risk in an overall process, (6) reducing or taking any other solution to deal with the risk regarding the situation and available resources. (ISO 2009)

TYPES OF RISKS

Risks can be categorized into following areas:

Strategic Risks

These risks relate to the risks to agency's direction, external environment and risks to the achievement of its plans. Such risks would relate to an assessment of the impact of external environment such as:

- Impact of changes in government policies on the business environment related to NPCC Ltd
- Political risk which may arise due to change of governments in countries where the projects are being executed or even change in state or central governments in India

- Environmental risks that may arise out of changes in environment or some new rules being introduced that may have an adverse impact on the business
- NPCC's decisions on the impact of increase/decrease of competition.
- Impact of introduction of new technologies and new developments in contract delivery

Commercial Risks

These risks relate to various commercial risks which impact the business of the corporation. These could be financial or contractual in nature such as:

- Currency exchange fluctuation risk. This could be a substantial risk if the corporation has large exposure to overseas contracts.
- Inflation risk affects many contracts as the costs may escalate beyond our estimates and adversely impact the profitability of a contract.
- Liquidity risk, such as delays in payments or over expenditure in a contract, which may result in affect the working capital requirements.
- Credit risk needs to be considered if the corporation is financing any of the activities of its associates or others where there is a possibility of a default.
- Risk of failure of a contractual relationship, where an associate may fail to perform thereby adversely affecting the performance of the corporation.

Operational Risks

These are risks which may arise while performing the core business of the corporation. These risks would include:

- Risks in implementing projects due to inadequate human resources.
- Market risks that may arise due to changes in market place, the demand supply, new trends which may impact the projects being undertaken.
- Risk of physical damage to assets or threats to physical safety.
- Risks of delays due to delays by vendors supplying goods/equipment.
- Risk of cost escalations or cost over runs.

Technical Risks

Risks may be technical in nature such as:

- Risk of failure of equipment or risk in management of assets.
- Risk of obsolesce of some technologies currently used by the corporation which may have an adverse impact on its business prospects or efficiencies.

Financial risks

- Risks associated with financial controls.
- Risk of failure of system such as frauds.

Compliance risks

- Environmental risk while executing certain projects and the risks of delay that may be introduced if environmental clearance is delayed.
- Any other risks due to the need to meet regulatory requirements e.g. obtaining completion certificates for the buildings etc.

RISK IDENTIFICATION

In the process of managing risk first step is to identify potential risks. Risks are about events that, when triggered, cause problems or benefits. Hence, risk identification can start with the source of our problems and those of our competitors (benefit), or with the problem itself.

- Source analysis- Risk sources may be internal or external to the system that is the target of risk management (use mitigation instead of management since by its own definition risk deals with factors of decision-making that cannot be managed). The major risk sources of internal could be the employees of the company and external could be the stakeholders.
- Problem analysis - Risks are related to identified threats. For example: the threat of losing money, the threat of abuse of confidential information or the threat of human errors, accidents and casualties. The threats may exist with various entities like shareholders, customers and legislative bodies such as the government.

The Method of identifying risks may depend on culture, industry practice and compliance.

Common risk identification methods

- Objectives-based risk identification - Organizations and project teams have objectives. Any event that may endanger achieving an objective partly or completely is identified as risk.
- Scenario-based risk identification - In scenario analysis different scenarios are created. The scenarios may be the alternative ways to achieve an objective, or an analysis of the interaction of forces in future developments.
- Taxonomy-based risk identification - The taxonomy in taxonomy-based risk identification is a breakdown of possible risk sources. Based on the taxonomy

and knowledge of best practices, a questionnaire is compiled. The answers to the questions reveal risks.

- Common-risk checking - In several industries, lists with known risks are available. Each risk in the list can be checked for application to a particular situation.
- Risk Mapping/charting - This method combines the above approaches by listing resources at risk, threats to those resources, modifying factors which may increase or decrease the risk and consequences. Creating a matrix under these headings enables a variety of approaches. One can begin with resources and consider the threats they are exposed to and the consequences of each.

A risk identification matrix is given in Table-I

Table – I: Risk Management Identification

AREAS OF IMPACT

ASSETS	REVENUE	COST	PEOPLE	COMMUNITY	PERFORMANCE	TIMING	ENVIROMENT	INTANGIBLE	ORG
Commercial and Legal	Ω	Ω	Ω			Ω	Ω		
Economic			Ω						
Human Behaviour			Ω	Ω		Ω			Ω
Natural Calamity								Ω	
Political & Regulatory					Ω		Ω		
Technology	Ω		Ω			Ω			
Competition	Ω	Ω	Ω		Ω	Ω			
Management Activity & Control			Ω	Ω			Ω		
Annual Results	Ω		Ω		Ω				

RISK ASSESSMENT

Once risks have been identified, they must then be assessed as to their potential severity of impact (generally a negative impact, such as damage or loss) and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated decisions in order to properly prioritize the implementation of the risk management plan.

In Risk assessment *Quantitative risk assessment* requires calculations of two components of risk (R):, the magnitude of the potential loss (L), and the probability (p) that the loss will occur. **Acceptable risk** is a risk that is understood and tolerated usually because the cost or difficulty of implementing an effective counter measure for the associated vulnerability exceeds the expectation of loss.

Rate (or probability) of occurrence multiplied by the impact of the event equals risk magnitude.

The above formula can also be re-written in terms of a Composite Risk Index, as follows:

Composite Risk Index = Impact of Risk event x Probability of Occurrence

The impact of the risk event is commonly assessed on a scale of 1 to 5, where 1 and 5 represent the minimum and maximum possible impact of an occurrence of a risk (usually in terms of financial losses). However, the 1 to 5 scale can be arbitrary and need not be on a linear scale.

The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for intangible assets. After all, probability does not imply certainty.

While the severity of loss may be easy to measure and quantify, the probability of occurrence may require educated guesses. However, determining the probability of occurrence is necessary to properly prioritize the implementation of risk management plan.

The table-II below gives the rating of 'Severity of loss' (Impact) on 5 point scale and table-III gives the probability of occurrence (Likelihood) also on a 5 point scale.

Table – II: Quantitative Data and Risk Expressions to measure ‘Impact’

LEVEL	DESCRIPTOR	EXAMPLE DETAIL DESCRIPTION
1.	Insignificant	Low financial loss, no disruption to capability, no impact on community standing.
2.	Minor	Medium financial loss, minor disruption to capability, minor impact on community standing.
3.	Moderate	High financial loss, some ongoing disruption to capability modest impact on community standing.
4.	Major	Major financial loss, ongoing disruption to capability, major impact on community standing.
5.	Catastrophic	Mission critical financial loss, permanent disruption to capability, and ruinous impact on

Table – III: Quantitative Data and Risk Expressions to measure ‘Likelihood’

LEVEL	DESCRIPTOR	EXAMPLE DETAIL DESCRIPTION
1.	Rare	May occur only in exceptional circumstances.
2.	Unlikely	Could occur at some time.
3.	Possible	Might occur at some time.
4.	Likely	Will probably occur in most circumstances.
5.	Almost certain	Is expected to occur in most circumstances

The Composite Index thus can take values ranging (typically) from 1 through 25, and this range is usually arbitrarily divided into three sub-ranges. The overall risk assessment is then Low, Medium or High, depending on the sub-range containing the calculated value of the Composite Index. For instance, the three sub-ranges could be defined as 1 to 8, 9 to 16 and 17 to 25.

The Severity of Risk can then be determined using the formula:

Potential severity of loss (impact) x Probability of occurrence (likelihood) = Risk

The severity of risk can then be assessed as follows:

25 points = E: Extreme Risk, Immediate Action Required at highest level

20 points = H: High Risk, Attention of Board members and Senior Management

15 points = M: Moderate Risk, Action by Departmental Heads

10 points and below=L: Low risk; manage with routine procedures

Further, both the above factors can change in magnitude depending on the adequacy of risk avoidance and prevention measures taken and due to changes in the external business environment. Hence it is absolutely necessary to periodically re-assess risks and intensify/relax mitigation measures, or as necessary. Changes in procedures, technology, schedules, budgets, market conditions, political environment, or other factors typically require re-assessment of risks.

The following may be used to assist in making preliminary judgments regarding risk classifications:

	Low Risk	Moderate Risk	High Risk
Consequences	Insignificant cost, schedule, or technical impact	Affects program objectives, cost, or schedule; however cost, schedule, performance are achievable	Significant impact, requiring reserve or alternate courses of action to recover
Probability of Occurrence	Little or no estimated likelihood	Probability sufficiently high to be of concern to management	High likelihood of occurrence
Extent of Demonstration	Full-scale, integrated technology has been demonstrated previously	Has been demonstrated but design changes, tests in relevant environments required	Significant design changes required in order to achieve required/ desired results
Existence of Capability	Capability exists in known products; requires integration into new system	Capability exists, but not at performance levels required for new system	Capability does not currently exist

ASSESSMENT OF RISK AND ITS TREATMENT PLAN

Depending on the different types of risk in an organization as detailed above, so treat the same, using the different categories of risks. Treatment starts with preparation of risk register having different types of risks elaboration, their identified consequence and with consequence rating and likely hood rating on a five point scale, to arrive at the severity of risk.

Risk Options

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of following 4T strategy, which are:

1. **Treat Risk** in designing a new business process with adequate built-in risk control and containment measures from the start.
2. **Tolerate risks** that are accepted in ongoing processes as a normal feature of business operations and modify mitigation measures.
3. **Transfer risks** to an external agency (e.g. an insurance company/ out sourcing)
4. **Terminate risks** altogether (e.g. by closing down a particular high-risk business area/ eliminate, withdraw from or not become involved)

Treatment of Risk

MANAGEMENT METHOD	OBJECTIVE	FEATURES
Terminate	Risk is eliminated or avoided by changing the parameters of the project	<ul style="list-style-type: none"> ❖ May change the project plan to eliminate conditions creating the risk (risky requirement, work scope, technology, or contractor) or eliminate the risk entirely. ❖ May trade one risk for another lesser risk. ❖ If a lower risk option is available, revise baseline to favor it. ❖ Check that the lower risk is the better choice considering the project as a whole.

Transfer	Risk remains viable but is shifted to another project or organization. Often called risk allocation. Cannot completely “transfer risk” or responsibility.	<ul style="list-style-type: none"> ❖ If full transfer is not possible, consider a partial shift e.g., insurances, performance bond, PI, warranty, or contract guarantee. ❖ Often, results in risk being shared between project and others. ❖ Often best with funding risks. ❖ Must consider costs and benefits of transfer. Must ensure recipient is best equipped and prepared to assume the risk in whole or in part. ❖ Risk is not avoided. Recipient must be willing to assume the risk, in whole or in part.
Treat	Reduced likelihood and/or consequences of a risk (preferably both) by series of control actions.	<ul style="list-style-type: none"> ❖ Most common form of risk management. ❖ Must systematically and carefully identify and attack root causes of the risk. ❖ Control actions are comprehensive and feasible. ❖ Early actions often required for success. ❖ Actions can affect cost, scope, and schedule. ❖ Cost/benefit analysis can be useful in selecting best Control action.
Tolerate	Risk is recognized and simply taken on by the project Residual risks which are not transferred. Develop recovery plans for residual risk.	<ul style="list-style-type: none"> ❖ “Last option” for controlling a risk. No feasible means to mitigate or otherwise control the risk is available. ❖ Benefit is that no changes in project plans are required to address the risk. ❖ Sometimes used when a compellingly large reward could be gained by taking the risk. ❖ Typically used for obdurate, distant, or least-predictable risk e.g. funding levels. ❖ Residual (remaining) risk is always accepted. ❖ Requires special diligence in monitoring, because nothing was done to reduce the risk. ❖ Alternative or acceptable “fall-back” positions are especially crucial if the risk is critical to project success. ❖ Worst case is “passive” acceptance, when no fall-back plans are considered.

RISK MANAGEMENT PLAN

Select appropriate controls or countermeasures to measure each risk. Risk mitigation needs to be approved by the appropriate level of management. For instance, a risk concerning the image of the organization should have top management decision behind it.

The risk management plan should propose applicable and effective security controls for managing the risks. It is just like high risk of computer viruses could be mitigated by acquiring and implementing antivirus software. A good risk management plan should contain a schedule for control implementation and responsible persons for those actions.

RISK MANAGEMENT DOCUMENTATION

The Risk Register (as per format at **Annexure-I**) will track and monitor the status of all risks including probability and consequence of each risk (pre and post-mitigation) and details on the risk control actions. The Risk Manager is responsible for identifying and assessing of risks. This responsibility includes providing regular re-evaluation and a status update of risk entries in Risk Register. The Risk Register is a living document used for the NPCC.

Project risks and the management actions to control them are reviewed and updated periodically by Risk Manager, Chief Risk Manager and Board of Directors of NPCC. New and imminent risks are added into the Register when identified. Risks are closed when the risk is no longer credible or when the risk has been realized and no residual risk remains.

The Risk Manager is responsible for maintenance of the Risk Register for ensuring that Chief Risk Manager monitor and reassess risks regularly, and that the Risk Handling Plans are being implemented in a timely and effective manner.

Items with risk higher severity level must be entered in the NPCC Contingency Analysis, which is the product of the impact and the risk probability.

ANNEXURE-I

Risk Register

Function / Activity: _____

S. No.	Risk Description	Type of Risk	Risk Rating	Likelihood	Mitigating Action	Responsibility
	Force Majeure	Strategic	Low			
	Competition	Operational	Medium			
	Exchange Fluctuation	Compliance	High			
	Time & Cost Over run	Financial	Very High			
	Uncertain Weather Conditions	Environmental				
	Labour Unrest					
	Non-availability/ increase in price of input.					
	Defect in designing					
	Loss of experienced manpower					
	Delay in decision making etc.					

(Note: If Risk description is considered/not available same may be added)

Date of Risk Review: _____

Completed by:_____ **Date:**_____

Reviewed by: _____ **Date:**_____

ORGANISATIONAL STRUCTURE WITH RESPONSIBILITY AND ACCOUNTABILITY FOR RISK MANAGEMENT:

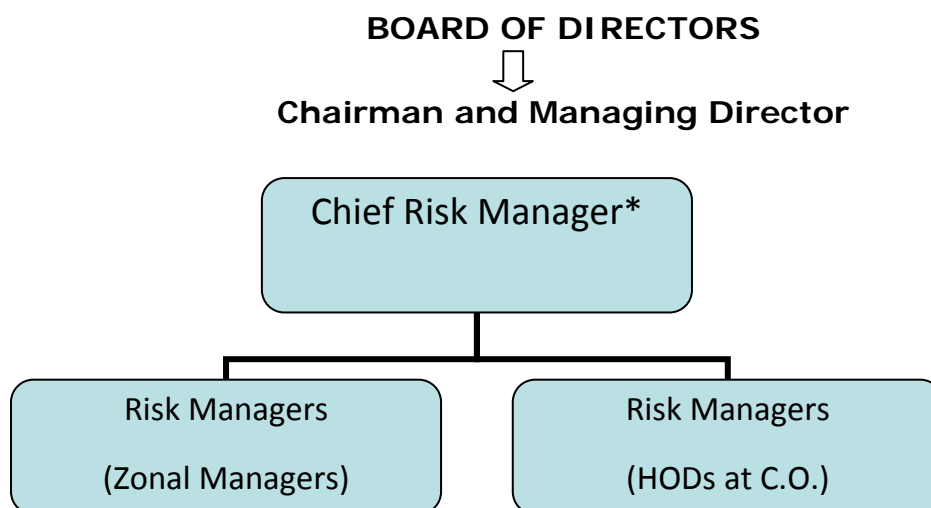
In order that the risk management gets the priority it deserves, the policy needs to be driven and implemented from the board level, with one of the directors being made in-charge. The Chairman and Managing Director, as authority to establish a risk management system in the organization, shall be designated as in-charge of Risk Management.

A high level responsibility for Risk Management will provide the resources and authority to mitigate risks effectively. Risk Management is not just a technical or financial issue but is an organizational management issue.

A Chief Risk Manager (CRM) needs to be appointed who will be responsible for coordinating the development and maintenance of risk management policies, procedures, standards and forms for the NPCC. All HODs and Zonal in-charges will be Risk Managers in respect of projects/ works under their control.

The CRM will ensure that the risk assessment process is performed at least once annually and an update should be carried out. The CRM will ensure that the departmental heads are aware and in agreement with the risk assessment and risk management plan and that they are aware of the risks of failure. The CRM will report to the CMD/ Board of Director on the key risk areas every year and also outline the mitigation measures undertaken.

RISK ORGANISATION CHART



(*Support will be provided to CRM by a Risk Management Group to be established by the CMD with detailed terms of reference)

RISK MANAGEMENT AND STRATEGY ON-GOING

Risk management is simply a practice of systematically selecting cost-effective approaches for minimising the effect of threat realization to the organization. All risks can never be fully avoided or mitigated simply because of financial and practical limitations. Therefore, all organizations have to accept some level of residual risks.

Whereas risk management tends to be preemptive, strategy shall be adopted to deal with the consequences of realised residual risks. The necessity to have strategy in place arises because even very unlikely events will occur if given enough time. Risk management also proposes applicable controls for the observed risks. Therefore, risk management covers several areas that are vital for the strategy planning. However, the strategy process goes beyond risk management's preemptive approach and assumes that the disaster will happen at some point.

RISK COMMUNICATION

Risk communication is a complex cross-disciplinary academic field. Problems for risk communicators involve how to reach the intended audience, to make the risk comprehensible and relatable to other risks, how to pay appropriate respect to the audience's values related to the risk, how to predict the audience's response to the communication, etc. A main goal of risk communication is to improve collective and individual decision making. Risk communication is somewhat related to crisis communication.

Seven cardinal rules for the practice of risk communication

- Accept and involve the public/other consumers as legitimate partners (e.g. stakeholders).
- Plan carefully and evaluate your efforts with a focus on your strengths, weaknesses, opportunities, and threats (SWOT).
- Listen to the stakeholders' specific concerns.
- Be honest, frank, and open.
- Coordinate and collaborate with other credible sources.
- Meet the needs of the media.
- Speak clearly and with compassion.

SPECIFIC RISKS TO THE CORPORATION AND ITS MITIGATION MEASURES ADOPTED

BUSINESS OPERATIONS RISKS:

These risks relate broadly to the company's organisation and management, such as planning, monitoring and reporting systems in the day to day management process namely:

- Organisation and management risks,
- Projects working/ interruption risks,
- Profitability

Risk mitigation measures:

- The Company functions under a well defined organization structure.
- Flow of information is well defined to avoid any conflict or communication gap between two or more Departments.
- Second level positions are created in each Department to continue the work without any interruption in case of non-availability of functional heads.
- Effective steps are being taken to reduce cost of production on a continuing basis taking various changing scenarios in the market.

BUSINESS DEVELOPMENT

State level pressure arising losing of projects

Risk mitigation measures:

- Award of projects should be with transparency.
- Should have strong legally binding agreements with the state Governments/ agencies once the project is allocated/ MoU signed for the same.

NPCC is awarded projects in difficult/ remote areas and private agency awarded with projects with easier areas

Risk mitigation measures:

- Government should support for timely completion of projects in difficult/ remote areas with incentives to off load some risks.

Risk of poor relationship with the clients

Risk mitigation measures:

- Suitable Project Manager may be posted at Project with regular suitable guidance. It will improve the relation for getting further works under the client.

Risk of non workable rate/ agency

Risk mitigation measures:

- As per contract, terms & condition work, the analysis of rates should be made with the consideration of local & other related conditions in the area.
- Credentials of agency/ contractor with financial parameters must be verified as per norms and local conditions.

PROJECT MANAGEMENT

Delays in decision making

Risk mitigation measures:

- Delays in decision making leading to financial loss may be charged with more accountability for the same.
- Internal monitoring mechanism may be developed for the approval of files or system. The key decision points should be identified which delayed and affected the overall project. The estimated time for these decisions and the responsible agency/agent for decision making should be clearly identified. Once the system is in place the company will fix accountability for delays in decision making.

Delays in award of contract because of contract litigations

Risk mitigation measures:

- Uniform tender approval procedure must be developed to avoiding contract litigations that arise due to issues raised on tendering procedures considering all aspects related to tendering.

- Detailed standard contracts agreement covering each factor for avoiding loop holes with the lesson from various contracts should be carried forward to to make them more robust.

Project, time and cost overrun Risks

Risk mitigation measures:

- Clauses for penalties, liquidated damages, performance bonus, completion/ performance guarantees may be added in contract agreement to transfer such risks to agencies/contractor.
- Reduce cost overruns adopting fixed/lump-sum turnkey contracts, and developing contingency plan, and developing scope and risk management.

Upgradation of technology

Risk mitigation measures:

- The manpower at every level may be updated with new technology in the all fields, viz. Finance, Green Engineering technology, Construction Methodology, New machinery & material, Human Resources skill development to cope up these.
- Attending seminars, workshops, technical/ non technical fairs, training in different field to enhance the competency to work new scenario.

Terrorism/ insurgent groups impact on project leading to time and cost overrun

Risk mitigation measures:

- Liaison with State Government (Department of Home), and Ministry of Home Affairs for adequate protection of its project sites
- Ensure that there are no penalty clauses in the working for the project which are likely to be impacted by the acts of terrorism/ insurgent groups.
- Explore the option of taking terrorism coverage policy for projects in States effected by terrorism/ insurgent groups for nullifying any loss of its financial interests

Non availability and/ or price hike of raw materials like cement, steel, bricks, sand etc.

Risk mitigation measures:

- Prescribe minimum inventory norms for critical raw material and monitor regularly its movement. Penalty can be included in the contract conditions for not meeting the average inventory norms by the contractor even without any disruption of project activity on such account

Contractor issues like equipment problems, construction methodology, labor unions, poor labour quality and scarcity of contractor labour

Risk mitigation measures:

- Develop a screening filter for weeding out non-serious bidders and/or put erring contractors under a black list to forbid them in future tenders participation. Publish such list of erring contractors to discourage growth of such vendors.
- Awarding of critical assignments to new contractor may be avoided.
- Offer of assignments to be extensively advertised to allow maximum agencies/ contractor to participate in the tendering process. Expert agencies/ contractors may be encouraged.
- With the implementation of contractors' performance feedback system. Prepare a agencies/ contractors Information and Rating System to allow evaluation of all agencies/contractors.

LIQUIDITY RISKS:

- Financial solvency and liquidity risks
- Borrowing limits
- Cash management risks

Risk Mitigation Measures:

- Proper financial planning in terms of cash flow, is put in place with detailed Annual Plans discussed at appropriate levels within the organisation.
- Annual and quarterly budgets are prepared and put up to management for

detailed discussion and an analysis of the nature and quality of the assumptions, parameters etc.

- These budgets with Variance Analysis are prepared to have better financial planning and study of factors giving rise to variances.
- Daily and monthly cash flows are prepared, followed and monitored at senior levels to prevent undue loss of interest and utilise cash in an effective manner.
- Cash management services are availed from Bank to avoid any loss of interest on collections

CREDIT RISKS:

- Risks in settlement of dues by clients/ contractors
- Provision for bad and doubtful debts

Risk Mitigation Measures:

- Systems put in place for assessment of creditworthiness of clients/ contractors.
- Provision for bad and doubtful debts made to arrive at correct financial position of the Company.
- Appropriate recovery management and follow up.

HUMAN RESOURCE RISKS:

- Labour Turnover Risks, involving replacement risks, training risks, skill risks, etc.
- Unrest Risks due to Strikes and Lockouts.

Risk Mitigation Measures:

- Company has proper recruitment policy for recruitment of personnel at induction levels in the organization.
- Proper appraisal system for revision of compensation on a periodical basis has been evolved and followed regularly to keep the high morale of manpower.
- Employees are trained at regular intervals to upgrade their skills with new developed technologies.

- Activities relating to the Welfare of employees are undertaken.
- Employees are to be encouraged to make suggestions and discuss any problems with their Superiors. So a monthly interactive meeting of teams should be held.

DISASTER RISKS:

- Natural risks like Fire, Floods, Earthquakes, etc.

Risk Mitigation Measures:

- The Properties/ Assets of the company are insured against natural risks, like fire, flood, earthquakes, etc. with periodical review of adequacy, rates and risks covered under professional advice.
- Fire extinguishers have been placed at fire sensitive locations.
- Training of Manpower for fighting with Natural Disasters and usage of First aid medical care in case of accidents at site/ offices.

INFORMATION TECHNOLOGY RISKS:

- System capability
- System reliability
- Data integrity risks
- Coordinating and interfacing risks

Risk Mitigation Measures:

- IT Division maintains repairs and upgrades the systems on a continuous basis with personnel who are trained in software and hardware.
- Password protection is provided at different levels to ensure data integrity.
- Licensed software is being used in the systems.
- Keeping the periodic backup provisions for servers related to all our intranet & internet activities.
- The Company ensures "Data Security", by having access control/ restrictions.

LEGAL RISKS:

These risks relate to the following:

- Contract Risks
- Contractual Liability
- Frauds
- Judicial Risks
- Insurance Risks

Risk Mitigation Measures:

Following are the Risk mitigation measures adopted by the Company to mitigate the risks relating to Legal aspects:

- A study of contracts with focus on contractual liabilities, deductions, penalties and interest conditions is undertaken on a regular basis.
- The Legal department vets all legal and contractual documents with legal advice from Legal retainers for different branches of legislation.
- Contracts are finalized as per the advice from legal professionals and Advocates.
- Insurance policies are audited to avoid any later disputes.
- Timely payment of insurance and full coverage of properties/Assets of the Company under insurance.
- Internal control systems for proper control on the operations of the Company and to detect any frauds.

INTEREST RATE RISK MANAGEMENT:

The Company keeps Project Funds/ Security deposits, EMDs etc with Financial Institutions in the form of Fixed Deposits of different periodicity. This money is also regulating the Cash Flow for the Project/ Corporation.

Risk Mitigation Measures:

All are considered month wise for the current year and quarter wise for later use, accordingly time period is fixed. Besides, the cash flows are prepared and monitored.

DISCLAIMER CLAUSE

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