HGIEL
We Make People Move...

H.G. Infra Engineering Limited

An ISO 9001:2015, ISO 14001:2015, OHSAS 45001:2018 Certified Company

Enterprise Risk Management Policy

Version -8.0

Prepared by:

H.G. Infra Engineering Limited

Document Owner:

Chief Risk Officer

Contents

1. BACKGROUND

1.1 INTRODUCTION

H.G. Infra Engineering Limited is into construction sector for having primary focus on highways, roads and bridges. Over the years, it has also begun to execute civil construction projects, like extension and grading of runways, railways and land development with diversification into water pipeline projects as well.

Under new Companies Act, 2013 in accordance with Section 134(3)(n) and Section 177(4)(vii) which mandates that the Board of Directors and Audit Committee of the company to make an assertion on:

- Development and implementation of a Risk Management Policy;
- Including identification of risk elements, if any, which in the opinion of Board may threaten the existence of company and further as per Regulation 17 read with Regulation 21 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("SEBI (LODR) Regulations" or "Listing Regulations"), the board of directors shall be responsible for framing, implementing and monitoring the Risk management policy/plan for the listed entity;
- Effectiveness of risk mitigation plans through proper monitoring and evaluation of risk management systems.
- Accordingly, to mitigate and manage risk at "H.G. Infra Engineering Limited" (hereinafter referred to as the "Company" or "HGIEL"), the Company has formed the policy (the "Enterprise Risk Management Policy").
- This document shall be under the authority of the Board of Directors of the Company. It seeks to identify risks inherent in the operations of the Company and provides guidelines to define, measure, report, control and mitigate the identified risks.

1.1. PURPOSE OF RISK MANAGEMENT POLICY

HGIEL views Risk Management as an integral part of its objective of creating and maintaining shareholder value and the successful execution of its strategies, while considering the risk and reward relationship in the management of all activities. In particular, the Company is determined:

- To develop an effective Risk Management framework that will provide guidance on implementing Risk Management processes within the operations and minimizing risks;
- To use best practice to support and enhance organizational activities in all areas of business;
- To regularly identifying and taking advantages of opportunities and minimize adverse effects and continuously striving to improve Risk Management practices and processes;
- To specify roles and responsibilities of all employees and establish linkage to their performance reviews;
- To regularly reviewing and communicating Risk Management philosophy, principles, policies and procedures.
- To prepare a framework for identification of internal and external risks, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Risk Management Committee.

- To ensure proper measures are in place for risk mitigation including systems and processes for internal control of identified risks.
- To take cognizance of risks faced by key stakeholders and the multiplied impact of the same on the company which may impact business continuity while framing risk responses

This Framework will continue to evolve and mature as Risk Management is implemented and experience is gained. It will be reviewed and amended on a regular basis to ensure its ongoing relevance and viability.

1.2 OBJECTIVES OF THE POLICY

The objective of Risk Management Policy at HGIEL is to preserve stakeholders value to the extent practically feasible and to ensure sustainable business growth with stability by identifying and mitigating major operating, and external business risk. In order to achieve the key business objectives, the policy establishes a structured and disciplined approach to Risk Management, including the development of the Risk Register, in order to guide decisions on risk related issues. The specific objectives of the Risk Management Policy are:

- **Aligning risk appetite and strategy** – HGIEL considers its risk appetite in evaluating strategic alternatives setting related objectives, and developing mechanisms to manage related risks.
- **Enhancing risk response decisions** – Risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, distribution, and acceptance.
- **Reducing operational risks and losses** – The entity strives to gain enhanced capability to identify potential events and establish responses, reducing risks and associated cost or losses.
- **Identifying and managing multiple and cross-enterprise risks** – The entity faces a myriad of risks affecting different parts of the organization, and risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.
- **Seizing opportunities** – By considering a full range of potential events, the entity is poised to identify and proactively realize opportunities.
- **Improving deployment of capital** – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

1.3 SCOPE AND APPLICABILITY OF THE POLICY

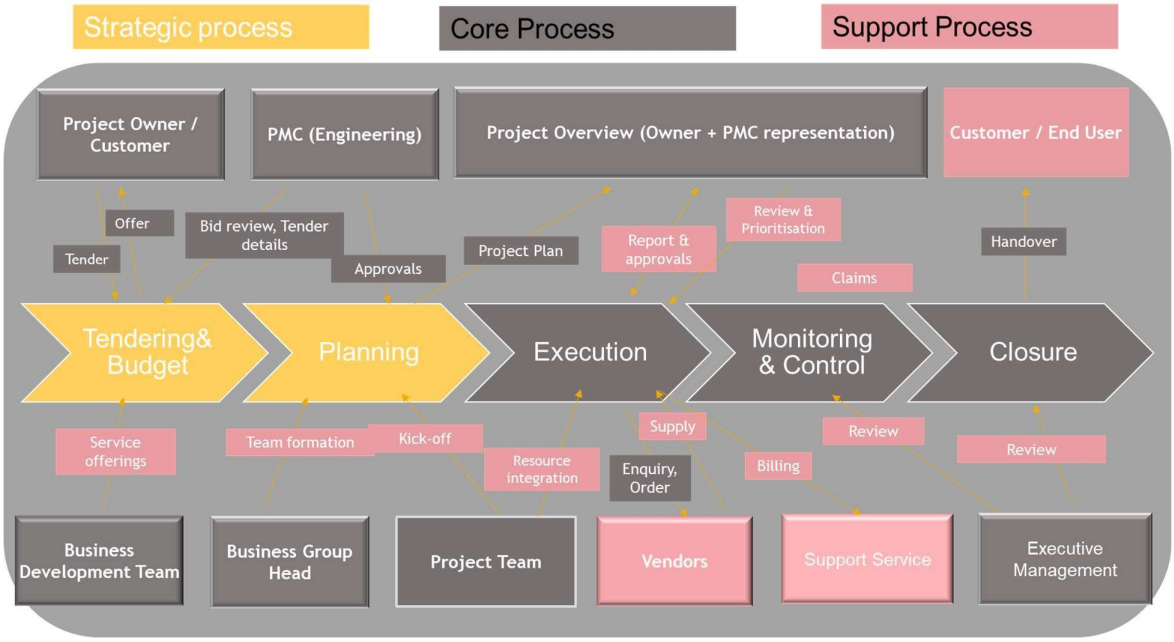
The policy guidelines are devised in context of the organization's growth objectives, business Profile envisaged and new business endeavors including new projects that may be necessary to achieve these goals and the emerging global standards and leading practices amongst comparable organizations.

The Scope of the Policy shall cover:

- All functions and departments of HGIEL, operational at Head offices & at any other location
- All functions and departments across all Projects sites
- All events, both external and internal which shall have an impact on the business objectives of the organization.

Applicability of the Policy: The Risk Management Policy is applicable to the Registered Office, Corporate Office & Liaison Offices and all Construction Projects including SPV's of HGIEL.

1.4 COVERAGE OF THE POLICY



1.5 DEFINITIONS

1.5.1 Board

It shall mean the board of directors of the company

1.5.2 Audit Committee

It means "Audit Committee" constituted by the Board of Directors of the Company, from time to time in compliance with the provisions of the Companies Act, 2013 and the rules made thereunder, as amended, and the Listing Regulations.

1.5.3 Company/Entity

It shall mean H. G. Infra Engineering Limited and its SPVs

1.5.4 SPV

Special purpose vehicle (SPV) as the name says, is formed for a special purpose. Its powers are limited to what might be required to attain that specific purpose and its life is destined to end when the purpose is attained. The operations are limited to the acquisition and financing of specific assets.

1.5.5 Risk

Risk is the effect of uncertainty on objectives. It is expressed as a combination of the probability of an event and its consequence. Events with a negative impact represent risks, which can prevent value creation or erode existing value.

1.5.6 Risk Management

Risk management is a set of coordinated activities to direct and control an organization with regard to risk. Risk management includes risk identification, roles, risk treatment and risk monitoring.

1.5.7 Risk Identification

Risk identification is the process of identifying the organization's exposure to uncertainty.

1.5.8 Risk Assessment

Risk assessment is the overall process of risk analysis and risk evaluation. It allows an entity to consider the extent to which potential risk events have an impact on achievement of objectives.

1.5.9 Risk Treatment

Risk treatment determines the way to deal with risk. Various mechanisms to treat risk are:

- **Risk Avoidance/ Termination** – decision not to become involved in, or action to withdraw from a risk situation.
- **Risk Transfer** –sharing with another party the burden of loss or benefit or gain, for a risk.
- **Risk Reduction/ Mitigation -** actions taken to lessen the probability, negative consequence, or both, associated with a risk.
- **Risk Acceptance/ Retention**–the acceptance of the burden of loss or benefit or gain, for a risk.

1.5.10 Risk Assessment Team

Risk Assessment team compromises of Risk Co-ordinators & Process Owners who shall identify risks.

1.5.11 Risk Appetite

Risk Appetite is the broad-based amount of risk a company or other entity is willing to accept in pursuit of its business objectives and goals.

1.5.12 Risk Tolerance

Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. Operating within risk tolerances provides management greater assurance that entity remains within its risk appetite, which, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

Risk tolerance is being considered as "Low" impact in Risk Measurement Matrix. Accordingly, risks are managed with the effort to bring them within "Low" impact criteria.

1.5.13 Limitations of Risk Management

Effective RM, provides only reasonable assurance and not absolute assurance to the senior management and the Board of Directors regarding achievement of an entity's objectives. Achievement of objectives is affected by limitations inherent in all management processes, which include:

- Human Judgement in decision making, which can be faulty and that breakdowns can occur because of human failures.
- Management's ability to override the risk management decisions.
- Decisions on responding to risk and establishing controls depend on their related costs and benefits.

1.5.14 Risk Register

A Risk Register' is a document for recording the risks in a standardized format.

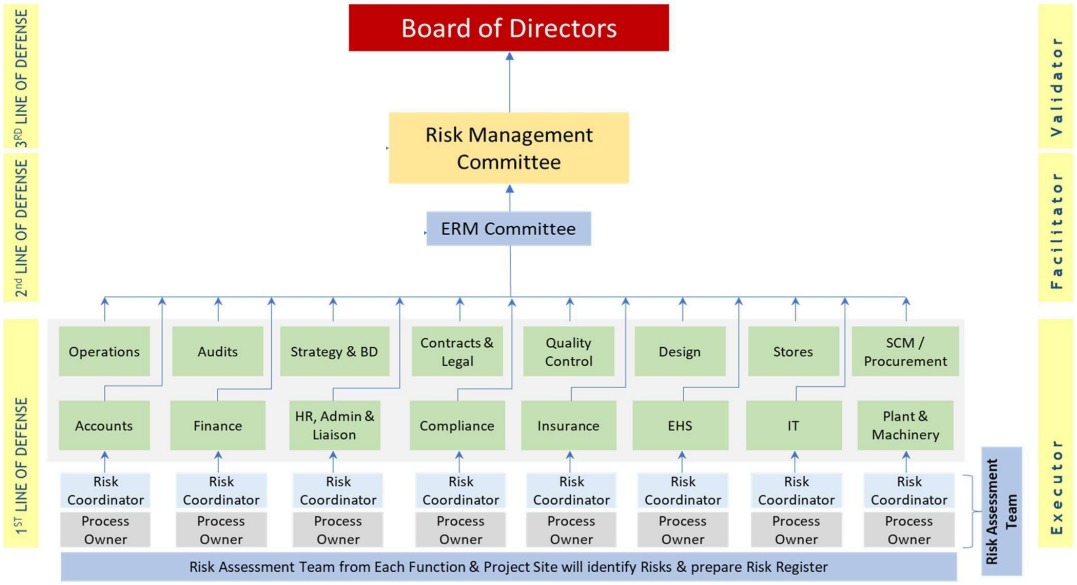
2. RISK GOVERNANCE FRAMEWORK

2.1 RISK GOVERNANCE STRUCTURE

- A well-defined risk governance structure serves to communicate the approach of risk management throughout the organization by establishing clear allocation of roles and responsibilities for the management of risks on a day-to-day basis. In order to develop and implement a Risk Management framework, a Risk Assessment Teams has been constituted.
- Risk Assessment Team shall identify the key risks and report them to the Risk Management Committee which shall ensure that risk management activities are undertaken as per this policy. The main objective of the Risk Assessment Team shall be to provide a wide view of key risks within the organization to the Risk Management Committee.

RISK GOVERNANCE → 3 LINES OF DEFENCE			
Provides Assurance	3rd LINE OF DEFENSE	***RISK PROCESS AND CONTENT Monitoring*** ➲ Provide oversight on risk-management content/processes, followed by second line of defense (as practical) ➲ Liaise with RMC and/or Board ➲ Provide assurance that risk-management processes are adequate and appropriate	Validators
Standard Setters	2nd LINE OF DEFENSE	***RISK PROCESS Accountability*** ➲ Establish policy and process for risk management the enterprise in terms of risk ➲ Provide guidance and coordination among all constituencies ➲ Identify enterprise trends, synergies, and opportunities for change ➲ Initiate change, integration operationalization of new events ➲ Liaison between third line of defense and first line of defense ➲ Oversight over certain key risk areas and in terms of certain enterprise objectives (e.g., compliance with regulation)	Facilitators
Business Owners	1st LINE OF DEFENSE	***RISK CONTENTS Accountability*** ➲ Manage risks/implement actions to manage and treat risk ➲ Comply with risk-management process ➲ Identify control breakdowns and inadequate processes ➲ Implement internal control procedures and RISK MANAGEMENT processes where applicable ➲ Execute risk assessments and identify emerging risk	Executors

2.2 STRUCTURE



2.3 RISK MANAGEMENT COMMITTEE

- The Risk Management Committee shall be appointed by and will serve at the discretion of the Board. The Risk Management Committee shall consist of no fewer than three members, majority of whom shall consist of members of the Board and composition shall include at least one independent director.
- The Chairman of the Risk Management Committee shall be a member of the Board.
- The members of the Risk Management Committee shall meet the Regulation 21 (3A) of SEBI (LODR) Regulations.
- The Risk Management Committee comprises of the members of the Board of Directors, including Independent Director(s) and senior executives of the company as approved by the Board.

2.4 RISK ASSESSMENT TEAM

The Risk Assessment Team shall comprise of heads (HOD's) of key departments.

The Risk Assessment team shall have the key role of identifying the key risks, suggest mitigation measures, monitoring and supervising the implementation of the Risk Management Policy and maintain wide view of the key risks faced by the organization.

- Identify, evaluate and assess the key risks anticipated for the organization and suggest mitigation measures to the risk coordinators.
- Ensure that effective risk mitigation plans are in place and the results are evaluated and acted upon.
- Report the key risks faced by the organization and their mitigation plans to the Risk Assessment Team.
- Appoint the Risk Coordinators for the identified risks.
- Ensure that the *Risk Coordinators* is informed about any new/emerging risks faced by the organization in case of exigencies/emergent conditions.
- Assist the Risk Management Committee in overseeing and monitoring the development and implementation of the Risk Management Policy.
- Prioritize the risks reported according to their risk ratings and assist the Risk Management Committee in decision making for risk management responses for identified key risks.

Roles and Responsibilities of Risks Assessment Team :

- Communicating and managing the establishment and ongoing maintenance of risk management policy pursuant to the organization's risk management vision.
- Designing and reviewing processes for risk management.
- Communicating with the Process owners regarding the status of risk management and reporting the key risks faced by the organization.
- Coordinate with all the *Process Owners* to compile the status of risks and mitigation measures taken.
- Convene the Process Owners meeting and facilitate discussions among the Team to fulfill its responsibilities.

2.5 RISK GOVERNANCE MEETINGS

Sr. No.	Meetings	Frequency
1	Board of Directors and Risk Management Committee	Half yearly or earlier if needed
2	Risk Management Committee	Half-yearly
3	Internal ERM Committee & Risk Assessment Team	Quarterly
4	Process Owners and Risk Coordinators	Monthly

2.6 RISK CO-ORDINATORS TEAM

The *Risk Coordinators* located at Corporate Office / Project Office shall be the representative not below the rank of Manager of respective departments members who shall report directly to the Risk Management Committee.

Roles and Responsibilities of the Risk Coordinators:

- Assist the head of Risk Assessment Team in organizing Risk Assessment Team meetings.
- Ensure strategic level and process level risks are identified and acted upon continuously
- Support the Risk Assessment Team by providing appropriate risk related information
- Identify, assess, manage, report and monitor risk and controls on a regular basis
- Participate in risk management programs and co-ordinate with Risk Assessment Team in risk management
- Communicate the importance of risk management and foster a risk culture within the departments/ process
- Monitor and implement the actions planned during risk management.
- Compile the status of risks and mitigation measures taken as reported by Risk Coordinators
- Record the key risks and their mitigation plans in the risk register as agreed by the Risk Assessment Team.

The risk register shall contain:

- Function/Department wise record of key Risks
- Risk category wise record of key Risks
- Treatment plans for the key Risks

3. RISK MANAGEMENT APPROACH

Risk Management is the process used to identify, assess, and treat the risks. It is the responsibility of the line management function and applies to all departments, missions and operations within the Company and is performed at all hierarchical levels.

01	02	03	04
Identification	Assessment	Mitigation	Monitoring
How do we identify and Prioritize risk?	What are the Key causes & consequences of the risks?	What are the Internal controls or mitigation measures in the place to manage the risks?	How do we monitor the risks and who do we report them to ?
Risk Awareness		Understanding controls or activities undertaken by management to respond, mitigate or manage risk by reducing its impacts, its likelihood of occurrence or both, in case some of the residual risks are not	Risk should be reviewed on a periodic basis, providing management and board with up-to-date perspective on key risk faced by HGIEL.
Finding , Recognizing and describing the risk (Including short to long term and emerging) that may have an impact on the strategic objectives	Prioritization and understanding of key risks to HGIEL, including likelihood and potential impact of the risk		

3.1 RISK IDENTIFICATION

Risk identification is the process of finding, recognizing, describing and recording risk. This step consists of identifying the risk sources, events, their causes and their potential consequences.

Risk identification will be done at HGIEL by adopting a top-down and bottom-up approach involving people at the middle and senior management level of all key business and support functions, to achieve a holistic view of risks.

3.1.1 Approach to be used for Risk identification:

One or more combination of event identification techniques may be applied in preparing an event Inventory following approach / techniques may be used to identify events that may impact the achievement of objectives.

- Reviewing internal data such as history of loss events, existing risk assessments, business plans and accounting records
- Brainstorming
- Internal/External Audit reports
- Surveys /Interviews/Working groups
- Experiential or Documented Knowledge
- Risk Lists – Lessons Learned
- Historical risk event information

3.1.2 Risk Identification- ongoing basis

There will be an ongoing application of the risk process in response to changing operations due to both internal and external factors. Following are the specific instances for continuous risk identification:

- Change in regulatory / political framework and their policies
- Any major change in Business dynamics or Opportunities
- Introduction of any major Product or expansion to new geographies
- Mergers / acquisition etc. of new businesses
- Occurrence of a Critical Risk

This ongoing application enables staff to identify, assess and respond to risks within their direct responsibility. Risk co-ordinators from different departments will be responsible in keeping the risks registers current and ensuring that all the new/emerging risks are updated.

3.1.3 Risk Identification Quarterly

In this process, the existing risks listing will be updated by addition/ deletion/ modification based on discussions with function heads and key people within the organization. Inputs will also be taken from other sources like external reviews, including benchmarking, input from external parties etc.

3.1.4 Documenting Risks

All new risks identified will be recorded in Risk Register for each business process.

3.2 RISK CLASSIFICATION AND CATEGORISATION

All the risks that have been identified shall be classified as:

Reputational Risk	Risks which may cause failure due to potential for adverse publicity, public perception or uncontrollable events causing an adverse impact To be treated with mitigation plan at RMC level within 1 year.
Strategic Risk	Risk which may cause failure of Business due to faulty or wrong Business Decisions or inadequate strategic roadmap. To be treated with mitigation plan at RMC level within 1 year.
Functional Risk	Risk due to abrupt changes in Business Environment.Such Risks differ from strategic risk as it is based on real time events for dealing with current business environment. To be treated with mitigation plan at Functional level within 6 months.
Operational Risk	Risks which an organization faces during its day-to-day activities. To be treated with mitigation plan at site level within 3 months.

All the classified risks can be **categorized** as under:

Enterprise & Governance	Enterprise & inter-organizational risks (Strategic, Governance, Decision making)
Business & Commercial	Business set-up and ongoing commercial risks (budgeting, contracting, material, approvals, dependence on natural resources etc.)
Execution	Construction & operational risks (like Design, project delays, land unavailability, obtaining clearances from statutory authorities, etc.)
Regulatory	Regulations Changes, Non-compliance of applicable laws and regulation and emerging regulations, Environment, Social and Governance
Financial	Funding (accessibility and cost), Transaction Risk. It also comprises of credit risk, liquidity risk and market risk.
People	Talent Availability, Productivity, Attrition, Dissatisfaction, Skills development & shortage
Security	Assets, Employees Safety, Data Privacy, Cybersecurity, Intellectual property, Climate Change, Natural Calamities

3.3 RISK ASSESSMENT

The risk assessment process provides a standard and consistent approach to understand and evaluate risks impacting objectives across all business divisions. During this process, events with a potential of negatively impacting objectives are assessed and included in the overall risk profile of the respective departments. The purpose of this step is to determine the level of each risk at various stages: inherent risk, residual risk. The level of the risk is assessed for two dimensions:

- The likelihood of occurrence of the event,
- The magnitude of impact of the potential consequences

3.3.1 Basis of Impact Assessment

The risks identified shall be evaluated on an appropriate risk rating for each risk identified as per the criteria below:

Rating	Financial Impact of		Qualitative
	For Project Risks identified	For Functional Risks identified	Description
Critical	More than 0.50% of project Cost	More than INR 5 Cr on the profits	Inability to achieve business objectives, ex. - Loss of significant business capacity - Loss of high value customers, customer loyalty and sales opportunities due to process failure - High costs dramatically impacting profitability and business viability - Material error in books of accounts, significant adjustment to accounts after close - Penalty from regulatory non-compliance related to financial, operating process - Disruption of relationship with a strategic partner (vendor, channel partner) - Serious non-compliance with internal corporate policies and procedures resulting loss of asset, sensitive information, reputation - Significant operational losses leading to significant reduction of market value
High	More than 0.30% and up to 0.50% of project Cost	More than INR 3 Cr and up to INR 5 Cr on the profits	Constrained ability to achieve business objectives, ex. - Inability to recover significant revenue amount; significant profitability erosion - Significant reduction in service and business capacity - Incurring excessive costs that impact current earnings and profitability - Loss or misappropriation of significant assets - Process deviations (compared to SOP) without mitigating controls, high risk rated audit findings - Non-compliance with internal corporate policies and procedures resulting loss of asset, sensitive information, reputation
Moderate	More than 0.10% and up to 0.30% of project Cost	More than INR 1 Cr and up to INR 3 Cr on profits	Moderate impact on achievement of business objectives - Less that material gaps in books of account - Process failure leading to loss of transaction with moderate value restricted to small number of transactions - Delay, Inability to reconcile key vendor, partner accounts impacting short terms transaction - Moderate rated audit findings on process gaps - Short term increase in costs or loss of revenue
Low	Up to 0.10% of project Cost	Up to INR 1 Cr on profits	Limited impact on achievement of business objectives - Policy, procedure non-compliance with low impact - Genuine error in accounting, corrected on scrutiny - Transaction level error in dealing with partner, detected and corrected - Minimal impact to revenue or earnings

Note:
Risk rating must be done as Critical i.e. irrespective of monetary limit, if the consequence is severe having impact on Reputation of Organization, Imprisonment of KMP *or Directors, Threat to Discontinuation of Business or Unit, Financial Mis-statement, Cyber- security Breach, Penalty due to Non-Compliance, etc.*

3.3.2 Likelihood Measurement Parameters

Probability Risk Guidance			
Rating	Inherent Probability of the risk events to occur and lead to assessed consequences		
	Occurrence in Future	% Chances	Occurrence in the past
Expected	Very High, will be almost a routine feature within the immediate next year	Over 80%	Similar instances have commonly occurred in the past
Highly Likely	High, may arise several times within the immediate next year	50% to 80%	Similar instances have occurred several times in past
Likely	Possible, may arise once or twice within the immediate next year	10% to 49%	There have been 1 or 2 similar instances in the year
Not Likely	Not likely, almost impossible to occur or may occur at most once or twice between year 2 (from now) to 5 years	Less than 10%	Similar instances have rarely or never occurred in the past

3.3.3 Inherent Risk considering impact and probability scale

		Impact			
		Low	Moderate	High	Critical
Probability	Expected	Y	A	R	R
	Highly Unlikely	Y	A	A	R
	Likely	G	Y	A	R
	Not Likely	G	G	Y	A

Legend	Level of Inherent Risk	Description
	R	**Red Risk-** Immediate action Required
	A	**Amber Risk**- Needs corporate management attention
	Y	**Yellow Risk**- Needs business unit head's attention
	G	**Green Risk-** Managed through routine procedures

3.3.4 Mitigation Control Effectiveness

Mitigation Effectiveness Rating Guidance	
Rating	Description
Needs Improvement	Mitigation plans though in place but do not ensure any control over risk occurrence and impact
Reasonably Adequate	Mitigation plans involved duly laid down approval and reporting norms though not ensuring complete control over the risk occurrence and impact.
Effective	Mitigation plans involved stringent approval and reporting norms with responsibility for execution duly mapped to various management levels ensuring complete control occurrence.

3.3.5 Final Risk Rating

Overall Final Risk Rating					
Mitigation Effectiveness		Inherent Risk Rating			
		Green	Yellow	Amber	Red
Needs Improvement		Low	Moderate	High	Critical
Reasonably Adequate		Low	Moderate	Moderate	High
Effective		Low	Low	Low	Moderate
Final Risk Rating = Inherent Risk Rating * Mitigation Effectiveness					

3.4 RISK MITIGATION STRATEGY

- Actions taken to reduce the likelihood of occurrence by targeting internal risk factors (e.g., management charts, control procedures etc.) and/or to 16minimize the magnitude of impact bytargeting the consequences of the risk (e.g., disaster recovery plan, backup copies etc.).
- The mitigation plan to be adopted would be based on cost-benefit evaluation. **Risk avoidance/ termination**: This involves doing things differently and thus removing the risk. This is particularly important in terms of project risk, market risk or customer risk but often wishful thinking in terms of the strategic risks.
- This step consists of defining and implementing the necessary controls to reduce the risk to the acceptable levels. There are four major categories of possible decisions: -Management action ensures a disciplined approach to the future management of risks, and should entail at least one of the following:

Treat / Mitigate the risk		Terminate the risk
• Organize; • Pro-active management; • Monitoring; • Implement controls; • Reporting; • Inspection; or • Culture/behavioral changes		• Cease activity; • Pull out of market; • Divest; • Contract out (outsource, assign); • Change or recalibrate objective; • Redesign (e.g. business processes, systems, tools); • Reduce scale
Transfer the risk		**Accept the risk**
• Insure; • Share (joint ventures, alliances, partnerships); • Diversify / spread; or • Hedge		• Intentionally pursue; • Fully accept; • Set reward / loss targets and tolerance levels; • Establish and monitor key risk indicators; • Charge premium price; • Build in contingencies; • Develop recovery plans; • Investigate and take follow-up action; • Develop fall-back arrangements; or • Finance the consequences

3.4.1 Risk Mitigation Process

The risks are identified and if the risk treatment mechanism selected is risk mitigation or risk transfer, the next step shall be to review and revise existing controls to mitigate the risks falling beyond the risk appetite and also to identify new and improved controls.

3.4.1.1 Identify Mitigation controls

New control activities are designed in addition to existing controls post assessment of risk exposure at current level to ensure that the risks are within the accepted risk appetite.

Control activities are categorized into Preventive or Detective on the basis of their nature and timing:

- **Preventive controls** – focus on preventing an error or irregularity.
- **Detective controls** – focus on identifying when an error or irregularity has occurred. It also focuses on recovering from, repairing the damage from, or minimizing the cost of an error or irregularity.

3.4.1.2 Evaluate Controls

The controls identified for each risk event shall be evaluated to assess their effectiveness in mitigating the risks falling beyond the risk appetite.

3.4.1.3 Implement Controls

It is the responsibility of the Risk Assessment Team to ensure that the risk mitigation plan for each function/department is in place and is reviewed regularly.

3.5 RISK MONITORING

The Risk Assessment Team shall work on an ongoing basis within the risk management framework outlined in this policy to mitigate the risks to the organization's business as it may evolve over time.

3.5.1 Risk Monitoring Methodology

Frequency of Risk Reviews:

- Risk Review will be done at Pre-Bid Stage for each Bid
- During the execution stage Risk review will be done depending on Project Duration
  - For Projects duration 18 Months & above, Risk Review will be done at every 6 months
  - For Projects duration less than 18 Months, Risk Review will be done at every 3 months

As the risk exposure of any business may undergo change from time to time due to continuously changing environment, the risks with their mitigation measures shall be updated on a regular basis (Prebid time/ Quarterly/ Half Yearly).

3.5.1.1 Quarterly

- The Department Heads/ Project heads shall review and report the status of risks and treatment actions to the Risk Coordinators with a copy to head of Risk Assessment Team on

quarterly basis. In addition, Risk Coordinators shall identify and report any new or changed risk to the head of Risk Assessment Team on quarterly basis.

- The Risk Assessment Team shall monitor and supervise the development and implementation of the Risk Management Policy and maintain wide view of the key risks and their mitigation measures faced by the organization on quarterly basis.
- The head of Risk Assessment Team along with the other members of the Risk Assessment Team shall identify the key risks and suggest mitigation measures to the concerned risk coordinators on quarterly basis.

3.5.1.2 Half yearly

- The Risk Assessment Team shall report the key risks and their mitigation plans to the Risk Management Committee on bi-annual basis.
- The Risk Management Committee shall apprise the Board on the key risks faced by the organization and the mitigation measures taken on biannual basis.

3.5.2 Risk Escalation Principle

Inherent Risk Exposure	Reporting Responsibility	Stakeholder
All risks (Critical, High, Medium, Low)	Process Owners	Risk Co-Ordinators
All risks (Critical, High, Medium, Low)	Risk Assessment Team	Internal ERM Committee
Selected Risks	Internal ERM Committee	RMC
Selected Top Risks	RMC	Board

The suggested key reporting principles are summarized in following table:

Stakeholder	Nature of Information	Responsibility	Periodicity	Reporting Format
Risk Assessment Team (comprise of Risk-Co-Ordinators & Process Owners)	• Confirmation/ Revised Risk Profile of respective Business Function & Projects • Control Evaluation result of control activities	Process Owner to prepare and risk Co-Ordinator to approve	Monthly	Risk Register
	• Implementation status of additional control activities identified			
Internal Enterprise Risk Management (ERM) Committee	• Risk Profile of events identified as risk at inherent level Implementation status of additional controls • Control evaluation scores of control activities including validation result by Audit	Risk Co-Ordinator to prepare and Internal ERM Committeeto approve	Quarterly	Risk Register
Risk Management Committee (RMC)	• Risk Profile of events identified as high risk at inherent level Implementation status of additional controls • Control evaluation scores of control activities including validation result by Internal Audit	Internal ERM Committeeto discuss with RMC	Half yearly	Control Evaluation Checklist Compliance report on Corporate Governance
	• Outcome of validation of controls vs control evaluation scores			
	• Shall confirm in their quarterly filing of compliance report on corporate governance in lieu of SEBI LODR-Regulation 27 whether they have complied with the Risk Management Committee requirements.			
Board	• Selected Top risks • Summary of implementation of additional controls • Summary of validation results and control evaluation scores	RMC will present top Risks to Board	Half yearly	Board Risk Report Board Control Summary Report

3.6 RISK REVIEW

Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place. Regular audits of policy and standards compliance shall be carried out and standards performance reviewed to identify opportunities for improvement. It shall be remembered that organization is dynamic and operate in dynamic environment. Changes in the organization and the environment in which it operates must be identified and appropriate modifications made to risk management practices. The monitoring process shall provide assurance that there are appropriate controls in place for the organization's activities and that the procedures are properly understood and followed.

The Risk Coordinators along with project heads shall review the progress on the actions agreed to mitigate the risk and make an assessment of the current level of risk including:

- Establishing whether actions have been completed or are on target for completion.
- Report the status of implementation of mitigation plans to the head of Risk Assessment Team. Risk monitoring and review process shall also determine whether:
- The measures adopted resulted in what was intended.
- The procedures adopted and information gathered for undertaking the assessment was appropriate.
- The acceptability of each identified risk and their mitigation plan shall be assessed and risks shall then be ranked to identify key risks for the organization.
- Proposed actions to eliminate, reduce or manage each material risk shall be considered and agreed.
- Responsibilities for the mitigation measures for key risks management of each risk shall be assigned to appropriate departmental head

4. Roles and Responsibility

4.1 Team Composition

Category		Composition
Board of Directors (BOD)	➲	Mr. Harendra Singh – Chairman & Managing Director
	➲	Mr. Vijendra Singh – Whole Time Director
	➲	Mr. Dinesh Kumar Goyal – Whole Time Director
	➲	Mr. Ashok Kumar Thakur – Independent Director
	➲	Ms. Pooja Hemant Goyal – Independent Director
	➲	Mr. Manjit Singh – Independent Director
Audit Committee (AC)	➲	Mr. Ashok Kumar Thakur – Chairman
	➲	Mr. Harendra Singh – Member
	➲	Mr. Manjit Singh – Member
Risk Management Committee (RMC)	➲	The Risk Management Committee comprises of the members of the Board of Directors, including Independent Director(s) and senior executives of the company as approved by the Board.
Internal Enterprise Risk Management (ERM)Committee	➲	Chief Risk Officer
	➲	Operations - Head(s)
	➲	Other Designated Senior Executives
Chief Risk Officer	➲	Chief Financial Officer of the company will also act as Chief Risk Officer
Internal Audit (IA)	➲	Internal Auditor of HGIEL
Risk Assessment Team	➲	Head of Departments (HoD) as Risk Co-Ordinators & Process Owners
Risk Co-Ordinators	➲	Managers and above
Process Owners	➲	Below Managers

4.2 Roles and Responsibilities

Department / Committees	Roles and Responsibilities
Board of Directors (BOD)	*The Board provides oversight regarding Risk Management.* The Board has a key role in the oversight of Risk Management. The Board should be apprised on a timely basis of the most significant risks, management's assessment, and its planned response. Key roles and responsibilities are outlined below: ➲ Initiate and sponsor the Risk Management process and set the risk management philosophy ➲ Reviewing the most significant risks and appropriateness of management response ➲ Reviewing the entity's portfolio view of risk and considering it against the entity's risk Appetite ➲ Ensures the requisite systems and practices are in place to manage all risks to which the Company is exposed.
Risk Management Committee (RMC)	As per the guidelines of SEBI under Schedule II Part D of amendments to SEBI (LODR) Regulations: Key roles and responsibilities are outlined below: ➲ Formulate a detailed Risk Management policy, which would include: • Measures for risk mitigation, including systems/processes for internal control of identified risks. • A Business Continuity Plan to review the Risk Management Framework & risk mitigation measures from time to time. • A framework for identification of internal and external risks faced by the Company, including financial, operational, sectoral, sustainability (particularly Environment Sustainability and Governance - ESG -related risks), information, cybersecurity risks and any other risk determined by the RMC. Ensure that appropriate methodology, processes, and systems are in place to monitor and evaluate risks associated with business of the company. ➲ Monitor and oversee implementation of the risk management policy, including evaluation of the adequacy of risk management systems. ➲ Periodically review the policy, at least once in two years, considering the changing industry dynamics and evolving complexity. ➲ Keep the board of directors informed about the nature and content of RMC discussions and recommendations, as well as the actions to be taken. ➲ Review the process of appointment, removal and terms of remuneration of Chief Risk Officer (CRO), if any.
Chief Risk Officer	Will own the Enterprise Risk Management Policy and related Documents.
Risk Assessment Team	Under the guidance of RMC, the Risk Assessment Team is to help / support effect risk management. Thus, Risk Assessment acts as a facilitator by assisting management in performing RISK MANAGEMENT activities, monitoring the progress and acting as a risk reporting channel. Key roles and responsibilities are outlined below: ➲ Design, develop and periodically update the RISK MANAGEMENT framework and procedure under the guidance of Sponsors / Internal Risk Management Committee ➲ Ensure appropriateness of risk culture and understanding across the company at all levels ➲ Plan and organize risk management programs in co-ordination with senior management, process owners ➲ Conduct adequate training and development programs for various stakeholders ➲ Ensure adherence to Risk Management policies and procedures within ➲ Facilitate Validators in preparation and execution of control validation plan.

Department / Committees	Roles and Responsibilities
Risk Co-ordinators	*Management in charge of organizational units has responsibility for managing risks related to their units' objectives.* Function heads are responsible for identifying, assessing, and responding to risk relative to meeting the unit's / division's / department's objectives. They ensure that processes utilized are in compliance with the entity's risk management policies and that their unit's / division's / department's activities are within established risk tolerance levels. Key roles and responsibilities of Risk Coordinators are outlined below: ➲ Ensure strategic level, process level and branch level risks are identified and acted upon continuously ➲ Set risk management principles for process / risk owners and measure performance ➲ Support the Risk Assessment team by providing strategic risk information ➲ Communicate the importance of risk management and foster a risk culture within their division / department ➲ Review risk management results on a periodic basis obtain periodic assurance on the adequacy of risk mitigation measures ➲ Escalate / report significant risks from business processes or projects to the attention of Internal Risk Management Committee and Risk Assessment team for discussion and monitoring. ➲ Review the status of implementation plan and validation results Key roles and responsibilities of function heads / process owners are outlined below: ➲ Ensure strategic level and process level risks are identified and acted upon continuously ➲ Support the Risk Assessment Team by providing appropriate risk related information ➲ Identify, assess, manage, report and monitor risk and controls on a regular basis ➲ Participate in risk management programs and co-ordinate with Risk Assessment Team in risk management ➲ Communicate the importance of risk management and foster a risk culture within the departments/ process ➲ Monitor and implement the actions planned during risk management.
Internal Audit (IA)	*Internal auditors play a key role in the ongoing functioning of RM by providing objective monitoring of its application and effectiveness.* Internal auditors conduct examinations for providing an objective assessment of the entire Risk Management process or subsets thereof. In this role, internal auditors may support management by providing assurance on: ➲ Risk management processes – both design and function ➲ Effectiveness and efficiency of risk responses and related control activities ➲ Completeness and accuracy of RM reporting Key roles and responsibilities are outlined below: ➲ Assists Internal Risk Management Committee and Audit Committee in fulfilling responsibilities in monitoring systems of internal controls and risks ➲ Ensures Risk Management Policy has been fully complied with and implemented ➲ Understand the risks within various facets of the Company and takes account of such risks in audit work ➲ Evaluates the adequacy and effectiveness of risk responses and control activities ➲ Keeps abreast of global industry best practices and recommends such practices to the Company, where appropriate ➲ To plan and validate effectiveness and existence of controls.

5. GLOSSARIES

TRMs	Description
Compliance	Used with "objectives": having to do with conforming with laws and regulations applicable to an entity.
Component	The RM components are: Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Risk Reporting, Information and Communication, and Monitoring.
Consequence	The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event
Control Evaluation Checklist	A technique used to assess control strengths and weaknesses in a given process. The "self" assessment refers to the involvement of management and staff in the assessment process, often facilitated by experienced professionals.
Criteria	A set of standards against which RM can be measured in determining effectiveness.
Event	An incident or occurrence, from sources internal or external to HGIEL CCL that could affect the implementation of strategy or achievement of objectives.
Event Identification	A RM Component which is designed to develop a consistent and sustainable approach to identify events that could impact, positively or negatively, HGIEL ability to achieve corporate strategy and objectives.
Exposure	The susceptibility to loss, perception of Risk, or a Threat to an asset or asset-producing process.
Frequency	A measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time. See also Likelihood and Probability.
General Controls	Policies and procedures that help ensure the continued, proper operation of computer information systems. They include controls over information technology management, information technology infrastructure, security management, and software acquisition, development, and maintenance. General controls support the functioning of programmed application controls. Other terms sometimes used to describe general controls are general computer controls and information technology controls.
Impact	Result or effect of an event that materializes the risk. There may be a range of possible impacts associated with an event. The impact of an event can be positive or negative relative to the HGIEL related objectives.
Inherent risk	The risk to the HGIEL in the absence of any action's management might take to alter either the risk's likelihood or impact.
Integrity	The quality or state of being of sound moral principle; uprightness, honesty, and sincerity; the desire to do the right thing, to profess and live up to a set of values and expectations.
Internal Control	A process, effected by the HGIEL Board of Directors, management and staff, designed to provide reasonable assurance regarding the achievement of objectives
Key controls	Set of controls that provide assurance on the reliability of financial reporting even if all the other controls in the process are not operating as intended
Likelihood	The possibility that a given event will occur.
Manual Controls	Controls performed manually, not by computer.
Monitoring	A process that assesses the presence and effectiveness of the HGIEL Framework components over a period.
Opportunity	The possibility that an event will occur and positively affect the achievement of objectives.

TRMs	Description
Policy	Management's dictate of what could be done to effect control. A policy serves as the basis for procedures for its implementation.
Procedure	Action(s) taken to implement a policy.
Probability	The likelihood of a specific event or outcome measured by the ratio of specific events or outcomes to the total number of possible events or outcomes.
Reporting	Used with "objectives": having to do with the reliability of the entity's reporting, including both internal and external reporting of financial and non-financial information.
Residual Risk	The remaining risk after management has acted to alter the risk's frequency of occurrence or impact.
Risk	The possibility that an event will occur and adversely affect the achievement of objectives.
Risk Appetite	The impact of risk HGIEL is willing to accept in pursuit of its vision.
Risk Assessment	The process that enables management to understand the frequency and impact of the potential events and associated risks.
Risk Measurement	The evaluation of the magnitude of risk.
Risk Response	An RM Component which relates to management's decision to avoid, reduce, share or accept risks associated with specified future events taking into consideration the risk tolerances of the organization and the cost vs. benefit including the effectiveness on event frequency and impact.
Risk management processes	The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk
Risk management	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects
Risk Tolerance	The acceptable level of variation relative to the achievement of objectives.
Uncertainty	Inability to know in advance the exact likelihood or impact of future events.

6. APPENDICES

6.1 Reporting Templates

- Risk Register
- RMC Risk Report
- Board Risk Report

6.2 Sampling Guidance

Description	Frequency
Update on Risk Register by Risk Assessment Team	Monthly
Review of Risk Register by Internal ERM Committee	Quarterly
Review of Risk Register by RMC	Half-yearly
Review of Risk Register by Board	Half-yearly

Effective Date: 6th November 2023

Date of the approval of Board: 6th November 2023

Version: 08

Authorized Signatory