

RISK MANAGEMENT POLICY

1. Definitions

1.1. Risk

Risks are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives. The exposure to the consequences of uncertainty constitutes a risk.

1.2. Risk Management

Risk Management is the process of systematically identifying, quantifying, and managing all risks and opportunities that can affect achievement of a corporation's strategic and financial goals.

1.3. Risk Strategy

The Risk Strategy of a company defines the company's standpoint towards dealing with various risks associated with the business. It includes the company's decision on the risk tolerance levels, and acceptance, avoidance or transfer of risks faced by the company.

1.4. Risk Assessment

Risk Assessment is defined as the overall process of risk analysis and evaluation.

1.5. Risk Estimation

Risk Estimation is the process of quantification of risks.

1.6. Risk Tolerance/Risk Appetite

Risk tolerance or Risk appetite indicates the maximum quantum of risk which the Company is willing to take as determined from time to time in accordance with the Risk Strategy of the company.

1.7. Risk Description

A Risk Description is a comprehensive collection of information about a particular risk recorded in a structured manner.

1.8. Risk Register

A 'Risk Register' is a tool for recording the risks encountered at various locations and levels in a standardized format of Risk Description.

2. Objectives of the Policy

The main objective of this policy is to ensure sustainable business growth with stability and to promote a pro- active approach in reporting, evaluating and resolving risks associated with the business. In order to achieve the key objective, 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:

- a) To ensure that all the current and future material risk exposures of the Company are identified, assessed, quantified, appropriately mitigated and managed
- b) To establish a framework for the company's risk management process and to ensure companywide implementation
- c) To improve decision making, planning and prioritization by comprehensive and structured understanding of business activities, volatility and opportunities/ threats.
- d) To ensure systematic and uniform assessment of risks related with construction projects and operational power stations
- e) To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices
- f) To assure business growth with financial stability

3. Risk Management Policy

Risk management is a central part of any organisation's strategic management. It is the process whereby an organisation methodically addresses the risks attaching to their activities with the goal of achieving sustained benefits within each activity and across the portfolio of all activities.

The focus of good risk management is the identification and treatment of these risks. Risk management should be a continuous and developing process which runs throughout the organisation's strategy and the implementation of that strategy.

3.1. Principles of Risk Management

In order to fulfil the objectives of this policy and lay a strong foundation for the development of an integrated risk management framework, the policy outlines the following guiding principles of Risk Management:

- a) All business decisions will be made with the prior information and acceptance of risk involved.
- b) The Risk Management Policy shall provide for the enhancement and protection of business value from uncertainties and

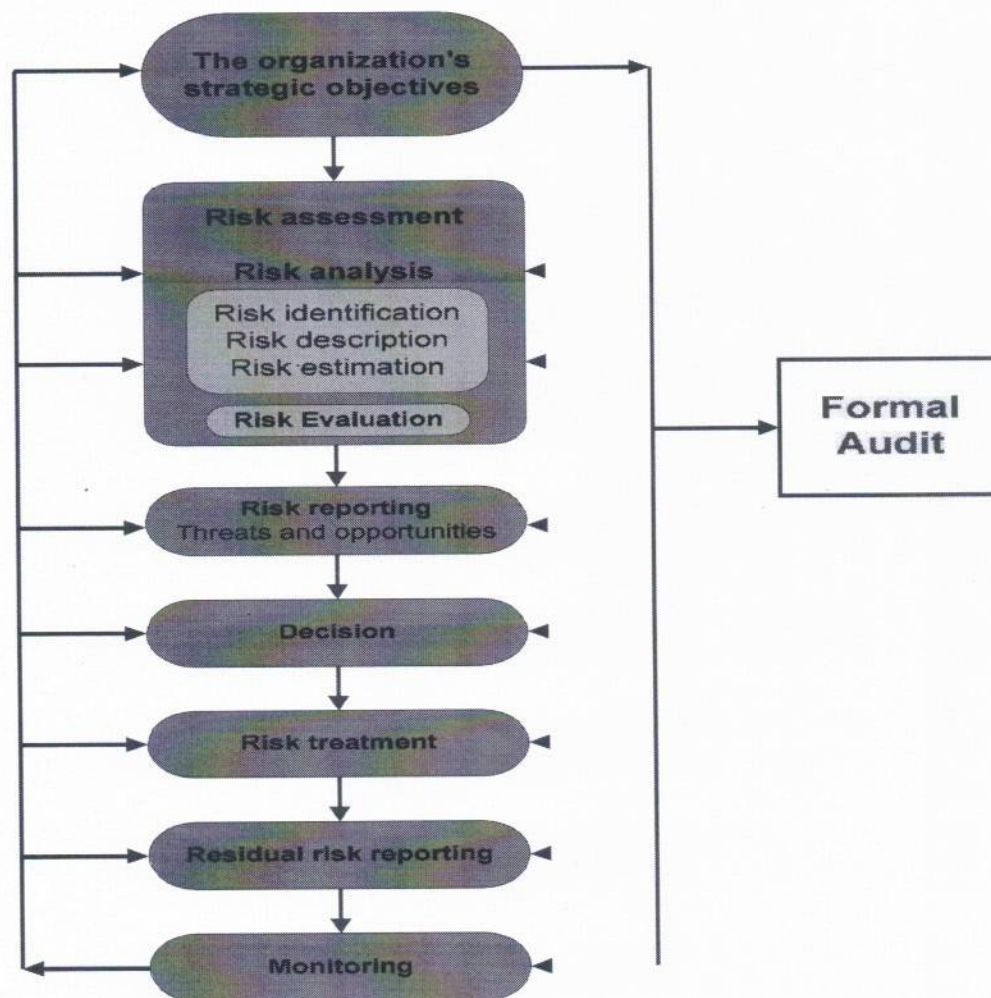
consequent losses.

- c) All employees of the company shall be made aware of risks in their respective domains and their mitigation measures.
- d) The risk mitigation measures adopted by the Company shall be effective in the long-term and to the extent possible be embedded in the business processes of the company.
- e) Risk tolerance levels will be regularly reviewed and decided upon depending on the change in the Company's strategy.
- f) The occurrence, progress and status of all risks will be promptly reported and appropriate actions be taken thereof.

3.2. Risk Management Policy Statement

1. To ensure protection of shareholder value through the establishment of an integrated Risk Management Framework for identifying, assessing, mitigating, monitoring, evaluating and reporting of all risks, which shall include:
 - a. A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee.
 - b. Measures for risk mitigation including systems and processes for internal control of identified risks.
 - c. Business continuity plan.
2. To provide clear and strong basis for informed decision making at all levels of the organisation.
3. To continually strive towards strengthening the Risk Management System through continuous learning and improvement.
4. To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity.
5. To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken.
6. The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.
7. The committee to meet at least twice in a year in such a manner that on a continuous basis not more than one hundred and eighty days shall elapse between any two consecutive meetings.

3.3 Risk Management Process



4. Scope and Extent of Application

The policy guidelines are devised in the context of the future growth objectives, business profile envisaged and new business endeavours including new products and services that may be necessary to achieve these goals and the emerging global standards and best practices amongst comparable organizations.

This policy is meant to ensure continuity of business and protection of interests of the investors and thus covers all the activities within the Company and events outside the Company which have a bearing on the Company's business.

The policy shall operate in conjunction with other business and operating/administrative policies.

5. Risk Mitigation

Mitigating measures have been identified for majority of the perceived risks. There is however always a residual risk attached to any business. The Company has implemented a continuous monitoring mechanism to deal with such risks on an ongoing basis. Details of various initiatives taken towards achieving this objective are as follows:

5.1 Strategic Planning

The Company has a strong strategic planning and budgeting process in place supported by budgetary controls at operational level.

Company's management meets periodically for a detailed strategic & operational review of each business segment, taking into account the business environment. These reviews by the top management are held every month and updated to the BOD on a quarterly basis.

5.2 Communication & Reporting

Members of the core management team review the implementation of these strategies and also ensure that adequate efforts are being made to mitigate the risks perceived.

Actual performance is measured against budgets by the management on a Monthly basis. The monthly and quarterly MIS has been designed to ensure timely dissemination of information and highlight possible risk of non-achievement of business objectives to key management.

5.3 Operational Initiatives for Managing Risk

Policies & Procedures – To strengthen internal controls over business processes the Company has designed Policies and Procedures and circulated them across the organisation. A few such examples are provided below:-

- ✓ Approval Limits - Authorisation matrix document specifying the financial powers for every nature of expense and every executive
- ✓ Foreign Exchange Risk Management Policy (FERM)
- ✓ Policies and procedures manuals for:
 - Accounting Policies and Procedures
 - EHS
 - Purchasing
 - Sales
 - Employee Benefits
 - Travel
 - Bill Passing

5.4 Audits & Reviews

Internal Audits: A firm of Chartered Accountants or any other Competent person as the Board may decide and whose appointment shall be approved by the Board, conducts regular internal audit. The observations and recommendations are reviewed and discussed with top management. The

implementation status is reviewed regularly for each department.

These observations are also presented every quarter to the Audit committee. The Audit Committee also reviews action taken by the management on the observations and recommendations made by the auditors. Follow-up audits are conducted at regular intervals and Action Not Taken Reports presented to the Audit Committee.

6 Risk Assessment

6.1 Risk Identification and Categorisation

The risk associated with Graphisads business activities and decisions are classified as:

Operational Risk

These concern the day-to-day issues that the organization is confronted with as it strives to deliver its strategic objectives.

Financial Risk

These concern the financial transactions entered by the organization in domestic as well as foreign currency.

Sectoral Risk

'Sectoral Risk' refers to the factors that can impact (both positively and negatively) a particular industry/ sector, which can in turn affect companies within the sector. Just as the economic performance of economies can vary widely, the performance of industries across the spectrum too can differ considerably.

Sustainability Risk

Sustainability risk is defined as the exposure to practices that negatively impact the environment and the people involved in the process chain. Climate change, water scarcity, disease, and poor labor conditions are some key factors that increase sustainability risk.

Information Risk

Information risk is a calculation based on the likelihood that an unauthorized user will negatively impact the confidentiality, integrity, and availability of data that you collect, transmit, or store

Cyber Security Risk

Cybersecurity risk is the probability of exposure or loss resulting from a cyber attack or data breach on your organization. A better, more encompassing definition is the potential loss or harm related to technical infrastructure, use of technology or reputation of an organization.

Other Risks

Any other risk which affects the business negatively and cannot be categorized in any of the above classifications.

6.2 Risk Description

A risk description helps in understanding the nature and quantum of risk and its likely impact and possible mitigation measures. Risk descriptions for each of the risks identified in the Risk Matrix are to be documented and recorded in structured format in each area where the risk is identified. The suggested format is provided in table below:

Table 6.2.1 – Risk Description

1	Name of Risk	
2	Scope of Risk	Qualitative description of the events, their size, type, number and dependencies
3	Nature of Risk	E.g. strategic, operational, financial, knowledge or compliance
4	Stakeholders	Stakeholders and their expectations
5	Quantification of Risk	Significance and Probability
6	Risk Tolerance / Appetite	Loss potential and financial impact of risk
		Value at risk
		Probability and size of potential losses/gains
7	Risk Treatment & Control Mechanisms	Objective(s) for control of the risk and desired level of performance
		Primary means by which the risk is currently managed
		Levels of confidence in existing control
8	Potential Action for Improvement	Identification of protocols for monitoring and review
9	Strategy and Policy Developments	Recommendations to reduce risk
		Identification of function responsible for developing strategy and policy

6.3 Risk Evaluation

In this process, the consequences of the risk occurrences have to be quantified to the maximum extent possible, using quantitative, semi-quantitative or qualitative techniques.

Table 6.3.1 – Risk Evaluation Criteria – Probability / Likelihood for Existing Events

Grading	Description	Qualitative Criteria
5	Almost Certain	Event occurred multiple times in previous year
4	High Probability/ Likely	Event occurred regularly (Once in a year) in past 3 years
3	Possible	Event occurred not more than once in past 3 years
2	Low Possibility/ Unlikely	Event never occurred in past for Graphisads
1	Rare	Event never occurred in past for Pigment Industry

Table 6.3.2 – Risk Evaluation Criteria – Probability / Likelihood for Events not relevant in past

Grading	Description	Qualitative Criteria
5	Almost Certain	Event occurred multiple times in a year for Pigment Industry
4	High Probability/ Likely	Event occurred regularly (Once in a year) for Pigment Industry
3	Possible	Event occurred not more than once in 3 years for Pigment Industry
2	Low Possibility/ Unlikely	Event never occurred in past for Pigment Industry
1	Rare	Event never occurred in past for Chemical Industry

Table 6.3.3 – Risk Evaluation Criteria – Consequences / Impact in Nonmonetary Terms

Grading	Description	Qualitative Criteria
1	Insignificant	Impact expected to be negligible
2	Minor	Impact is minor and can be contained
3	Moderate	Potential to cause reasonable damage
4	Major	Could cause substantial damage in the short and medium term without threatening the survival of the business
5	Critical	Significant threat to the survival of the business

Table 6.3.4 – Risk Evaluation Criteria – Consequences / Impact in Monetary Terms

Level	Grading	Description	Qualitative Criteria
Company	1	Insignificant	Impact is <1% of PBT // <0.10% of Net Fixed assets // <0.10% of Total T/O
	2	Minor	Impact is 1% to 2.5% of PBT // 0.10% to 0.25% // Net Fixed Assets or 0.10% to 0.25% of Total T/O
	3	Moderate	Impact is 2.5% to 3.75% of PBT // 0.25% to 0.5% of NetFixed Assets // 0.25% to 0.5% of Total T/O
	4	Major	Impact is 3.75% - 5% of PBT or 0.5% to 1% of Net FixedAssets // 0.5% to 1% of Total T/O
	5	Critical	Impact is >5% of PBT // >1% or more of Net Fixed Assets // >1% of Total T/O

Table 6.3.5 – Risk Factor – (Probability) * (Impact)

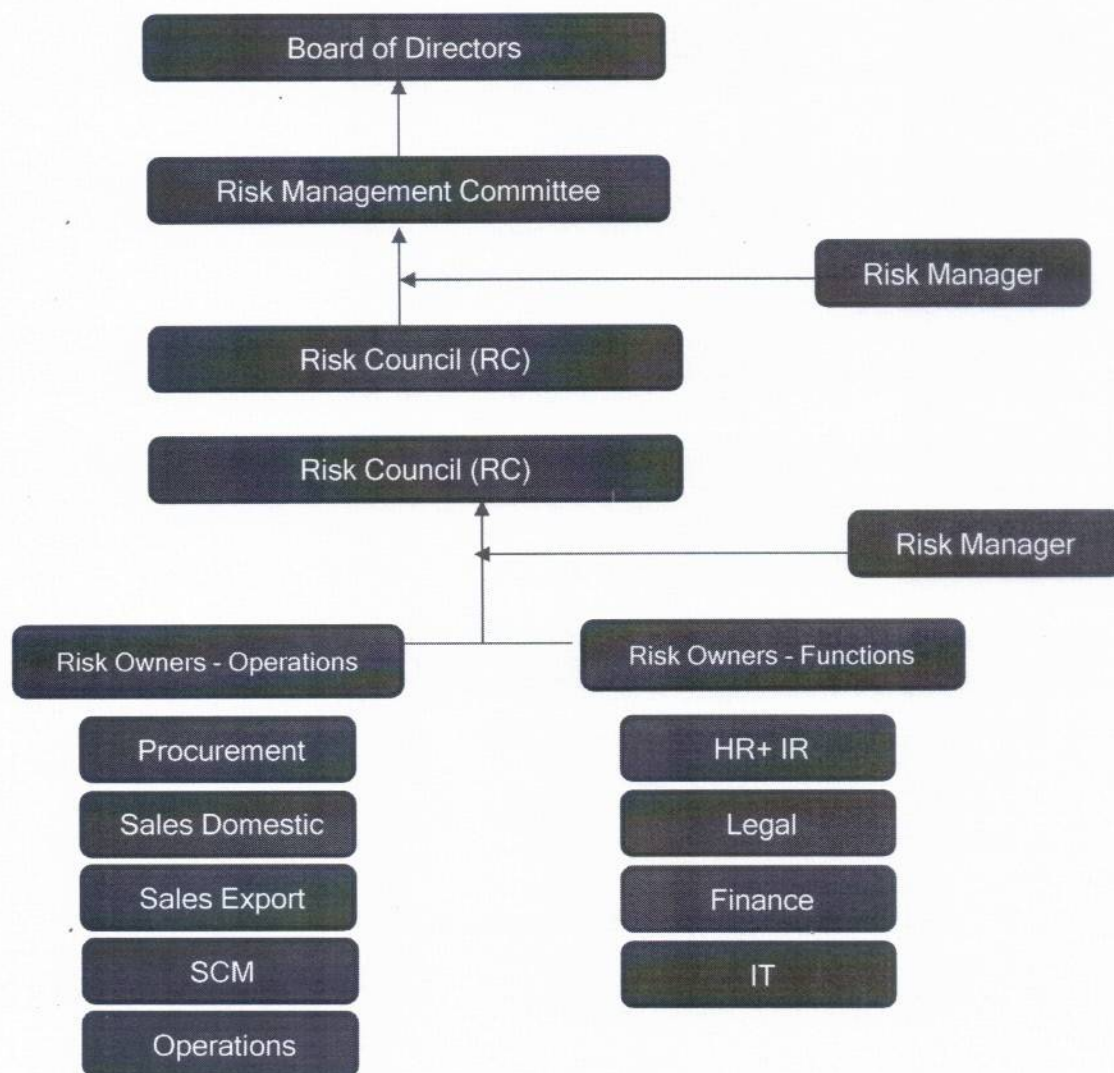
(L)	Low	1 – 8
(M)	Medium	9 – 15
(H)	High	16 – 25

6.4Risk Analysis

After completion of risk analysis process, compare the estimated (residual) risk against various risk criteria i.e. associated costs and benefits, legal requirements, socio-economic and environmental factors, concerned of stakeholders etc. Based on risk evaluation management should decide whether the risk should be accepted or treated.

6.5Risk Reporting And Communication

The following approach should be used for risk reporting and communication:



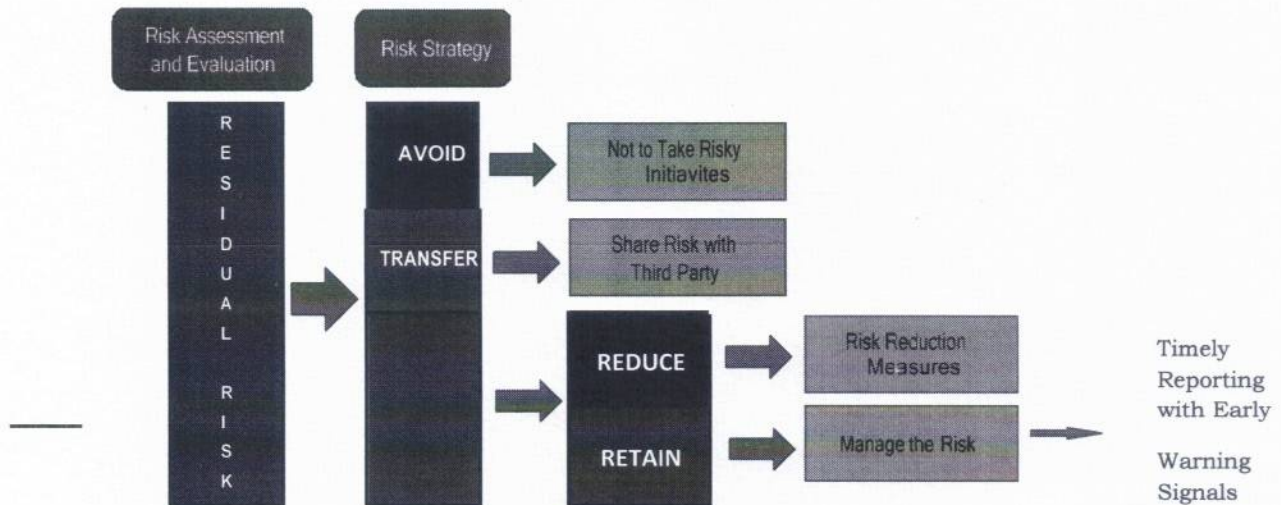
6.6 Role & Responsibility of Risk Organization

- A. Risk Management Committee (RMC)** – RMC to promote enterprise risk culture in Graphisads and oversee the risk management process. RMC is also responsible for reviewing and approving risk disclosure statements in public documents or disclosures. Risk Committee is reporting to board on key risk management issues on quarterly basis.
- B. Risk Council (RC)** - RC is accountable to the Risk Management Committee and the Board for enabling the business to balance risk and rewards. RC shall work closely with Risk Owners in deploying risk mitigating measures and maintenance of Risk Register. RC shall update Risk Management Committee on consolidated view of all risks on a periodical basis.
- C. Risk Manager (RM)** – RM shall update Risk Management Committee on consolidated view of all risks, based on deliberations within the RC, on a periodical basis. RM should act as a facilitator between RC and Risk Owners (ROs). RM shall also work closely with ROs and update risks to RC on a periodical basis.
- D. Risk Owners(ROs)** – Risk Owners (Operations and Functions) are

responsible to manage and identify risks in their functional domain, Preparation of mitigating action plans and follow ups. Risk owners shall report on status of implementation plan against identified risks to RM on a periodical basis.

Risk Treatment (Strategy)

The following framework should be used for treating the residual risk:



Based on the Risk Appetite/Risk Tolerance level determined and reviewed from time to time, the Company should formulate its Risk Management Strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. The risk mitigation can be planned using the following key strategies:

Risk Avoidance: By not performing an activity that could carry risk. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed.

Risk Transfer: Mitigation by having another party to accept the risk, either partial or total, typically by contractor by hedging

Risk Reduction: Employing methods / solutions that reduce the severity of the loss e.g., concrete being done for preventing landslide from occurring.

Risk Retention: Accepting the loss when it occurs. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default.

6.7 Risk Management Information System

A company-wide integrated Risk Management Information System (MIS) needs to be implemented by the Risk Manager. Information is needed at all levels of the organization to identify, assess and respond to future occurrences of risk events. Pertinent information from both internal and external sources must be captured and shared in a form and timeframe that equips personnel to react quickly and efficiently. Effective communication would also involve the exchange of relevant data with external parties, such as customers, vendors, regulators and shareholders. Further, both historical and current data needs to be collected. Historical data tracks actual performance against target, identifies trends, correlate results and forecasts performance. Historical data also provides early warning signals concerning potential risk-related events. Current data gives management a real time view of risks inherent in a process or function. This will enable the company to alter its activities as needed in keeping with its risk appetite.

Risk Manager should prepare 'Risk Registers' as an immediate measure. The Risk Registers will be maintained at the Risk Coordinators level for capturing comprehensively all risks in operations and functions. Each risk will be identified, categorized and assessed using the methodology as specified in sections of the policy above.

Each Risk Officer would have access to risk registers of all Risk Coordinators under the span of control and would be responsible for monitoring them. Chief Risk Officer would in turn monitor all risks at the Risk Officer level.


The 'Risk Register' should contain the following information:

S.No.	Column Heading
1	Risk Profile Number
2	Risk Head
3	Risk Description
4	Category
5	Likelihood of occurrence (prior to considering the measures / safeguards)
6	Consequence of occurrence (prior to considering the measures / safeguards)
7	Likelihood x Consequence (Column 5 * Column 6)
8	Inherent Risk rating
9	Describe and comment on the existing measures and safeguards that are presently in place to mitigate against the risk
10	Adequacy of existing measures / safeguards
11	Likelihood of occurrence (after considering the measures / safeguards)

12	Consequence of occurrence (after considering the measures / safeguards)
13	Likelihood x Consequence (Column 11 * Column 12)
14	Residual Risk rating
15	Person Responsible
16	Periodicity of Review
17	Date of Last Review
18	Comments
19	Signature

**For and on behalf of
M/s GRAPHISADS LIMITED**

For GRAPHISADS LIMITED


Shobharam Dhama
Company Secretary
M. No. 23402

**Shobharam Dhama
Company Secretary
M. No.: A23402**