RISK ASSESSMENT POLICY

The policy is applicable to BEIL Infrastructure Limited and its group companies (hereinafter referred to as BEIL Group). BEIL Group consists of BEIL Infrastructure Limited, Enviro Technology Limited, BEIL Research and Consultancy Private Limited, Kerala Enviro Infrastructure Limited, Shivalik Solid Waste Management Limited, Coimbatore Integrated Waste Management Company Private Limited, Gharpure Engineering and Constructions Private Limited, Gharpure Engineering Vasai Virar STP Private Limited and Tatva Global Water Technologies Private Limited.

"Compliance Officer" wherever mentioned in this document refers to Compliance Officer of the Group.

1.1. Risk assessment and reviews

1.1.1. Risk assessment is the foundation of an Integrity Compliance Program. It is a proactive approach that allows BEIL Group to understand and identify the risk exposure with regards to the business operations. It allows us to identify structural weaknesses that may facilitate corruption as well as provide a framework that identify risk factors and measures. The ineffective ways of mitigating risks of fraud, corruption or other Misconduct may affect the organization's revenue, culture and reputation. Compliance Officer shall be responsible for monitoring the sufficiency and operating effectiveness of the risk assessment.

1.1.2. An Integrity Risk Assessment focuses on fraud risk exposure which includes bribery, corruption, money laundering and criminal conspiracy, among others.

1.1.3. The Risk assessment process designed will look for ways and means to minimise the risks by providing appropriate counter measures. Mitigation and preventive measures are to be developed to minimise the risks identified in the assessment. The BEIL Group shall conduct risk assessment activity periodically with a maximum gap of 3 years.

1.1.4. Having identified the relevant areas of risk, BEIL Group has defined the need and develop the following mitigation and preventive action plans:

a) Detailed rules, procedures and policies that address the potential areas of misconduct including fraud, corruption and so on.

b) Provide communication and training to ensure that employees understand the organisation's policies and procedures as well as the leadership's commitment. Learnings and experiences gained from past incidents shall be covered as case studies during training programs to educate the employees and thereby prevent occurrence of such misconduct.

c) Awareness initiatives such as posters/screensavers/intranet wall messages, emailers to concurrently educate the employees and thereby strengthen the compliance program to help mitigate the risk of misconduct.

d) Carry out regular reviews of the Integrity Programme including internal audits, focused reviews encompassing areas identified based on past incidents.

1.1.5. Common fraud and corruption-related activities are:

- unlawful assignment of donations, benefits, cash transfers, etc.;
- manipulation of the procurement process by favouring one vendor over others, or selectively supplying information to some vendors;
- tax evasion, money laundering, insider trading;
- payment or receipt of secret commissions (bribes), in money or in some other form of value, to the receiver and possibly relating to a specific decision or action by the receiver;
- overcharging for goods and services in invoices rendered to customers and clients;
- theft of cash, plant, equipment, inventory, information, or intellectual property by employees;
- false invoicing, accounts-receivable fraud, false accounting;
- the release of misleading, inaccurate, or confidential information in order to deceive, mislead, or conceal wrongdoing, or in exchange for benefits or advantage;
- payment or solicitation of donations for improper political purposes;
- conflict of interest involving the senior executive of an entity, or other entity, acting in his or her own self-interest rather than the interests of the entity to which he or she has been appointed;

- bribery to officials (locally or in foreign jurisdictions) in order to secure a contract for the supply of goods or services;
- manipulation of the procurement process through collusive tendering (in preparation of bids);
- the facilitation of payments – small one-off payments in cash or in kind intended to secure prompt delivery of goods or services.
- the receipt or giving of gifts or entertainment intended to achieve an unstated objective;
- the appointment of friends and associates to positions of authority, without proper regard to their qualifications.

1.2. RISK ASSESSMENT FRAMEWORK

1.2.1. Introduction

(a) Complexity, uncertainty and changes are prevalent in all businesses. Identifying, assessing and managing risk at all levels of the organisation will enable BEIL Group to improve its business by maximizing opportunities and reducing the time spent on reacting to surprises. The Risk assessment process can increase the value of BEIL Group by supporting decision-making, providing assurance to stakeholders and increasing the ability to meet the objectives.

(b) The risk assessment process supports effective establishment of a risk-based internal control framework through consideration of occurrence of fraud, corruption or other Misconduct in the business and operations its compliance and related reporting risks. It is designed to ensure that BEIL Group actively considers and manages internal and external risks across the business portfolio. It is an integral part of good management practice.

1.2.2. Purpose

(a) The purpose of this document is to set down the responsibilities, processes and methodologies for identifying, managing, monitoring and reporting significant risks faced by the Departments/functions in respect of occurrence of fraud, corruption or other Misconduct in the business and operations.

1.2.3. Structure, Roles, Responsibilities

(a) The overall Risk Escalation Process is shown in **Exhibit – A**. The Board of Directors has responsibility for the management of risk in BEIL Group Companies / Entities, through the system of internal control, and for internal control effectiveness. The Board discharges its responsibility through the Audit Committee/ Compliance Committee (wherever applicable) and Compliance Officer.

(b) The Audit Committee (wherever applicable) maintains an overview of the operation of internal controls within BEIL Group Entities / Companies (including risk management), by periodically evaluating the design and effectiveness of all internal controls and recommending the results of their assessment to the Board of Directors. The Audit Committee reviews the effectiveness of internal controls by assessing the significant risks facing the company and the effectiveness of its controls in managing them. In the entities where Audit Committee is not applicable, Board of Directors maintains an overview of the operation of internal control within the company.

(c) The Compliance Committee (wherever applicable) supported by the Compliance Officer is responsible for identifying overarching risks and general risk trends which may impact BEIL Group.

(d) The Compliance Officer should review and challenge the perspective of key risks of various departments/functions and if necessary, should provide the necessary support to help the Companies/entities departments/functions to mitigate the risks. The Compliance Officer shall maintain a Risk Assessment Document which will be updated on a periodical basis with a maximum gap of 3 years relating to the key risks.

(e) If any risk is considered significant from a Company / Entity /Department / function perspective, it should be updated in the risk assessment document.

(f) The Compliance Officer is responsible for defining, developing, communicating and implementing the BEIL Group's risk assessment process.

1.2.4. Risk escalation matrix

(a) The overall risk management structure works on the basis of significant risks escalating upwards from function / department levels to the company level and generic risk categories cascading downwards through the organisation. External risks would also be identified at the company level to make the assessment fully comprehensive. Individual functions either at the department level would also need to assess their risks and report upwards.

1.2.5. Identify uncertainties, circumstances and events

(a) The risks could be identified at each level of the organisation, through a combination of approaches, which may include as appropriate:

- Holding a facilitated risk workshop
- Brain storming techniques
- Interview techniques
- Conducting risk analysis as part of an overall business planning or project planning meeting(s)
- Feed from other management reporting processes
- Ad-hoc risk reporting – all staff should be encouraged to report risks identified in the course of their day-to-day business
- Risk checklists drawn up using past experience
- Engage external Consultants
- Risk registers from similar projects undertaken in the past.

(b) Event identification techniques should consider both the past and the future. Events could range from the obvious to the obscure and the effects from the inconsequential to the highly significant. It is important not to ignore any low probability events that could have significant impact on the business objectives. It is also important to understand that events often do not occur in isolation. One event can trigger another and events can occur concurrently. It may be useful to group similar events into categories to get a better understanding of the risks.

1.2.6. Risk Evaluation

(a) Once the events, circumstances and uncertainties have been identified, the next stage is to understand the nature and importance of each of these events so that they can be managed appropriately. BEIL group has adopted three key criteria for evaluating risks:

- Likelihood
- Impact criteria

- Control Environment.

1.2.7. Analysis of likelihood

(a) Likelihood represents the chance or possibility that a given event will occur.

(b) The following table, **Figure 1**, can be used to categorise an event for Likelihood. These definitions are intended to be mutually exclusive.

Figure 1: Likelihood criteria

LIKELIHOOD	1	2	3
Description 1	Low	Possible	Probable / Very High
Description 2	Unlikely	Below Average	Above Average
Description 3	<10%	10-49%	> 50%

1.2.8. Analysis of impact

(a) When evaluating risks in terms of Impact, the team should consider the objectives stated in the business or project plan and then determine its risk appetite in both financial and nonfinancial terms. In order to achieve a consistent evaluation of all risks, the team should agree a set of impact descriptions to use as a guide.

(b) This may vary considerably between different projects but the following provides an example of impact descriptions based on financial loss, health and safety, and reputation. Other factors may be considered such as impact on strategy, approval delays, sourcing / production, capex, etc. depending on the scope. Financial figures below are indicative only and can be based in % terms of the profit, capex, etc.

Figure 2: Impact Criteria

IMPACT	1	2	3
Description	Low	Moderate	Significant
Financial	<=₹ 10 lakhs	Between ₹ 10 to 50 lakhs	Above ₹ 50 Lakhs
HSSE	Minor / No Injury	Reportable injury	Fatality / Major Injury

Schedule	< 1 month delay	1-6 month delay	> 6 month delay
Reputation	Internal knowledge only of incident	Adverse coverage at local and industry level	Adverse coverage at national / international level

1.2.9. Control Environment

(a) The third criterion for assessment of each event is the effectiveness of the existing internal controls that have been designed to mitigate the risk. The control environment takes into account the internal controls placed by the Organisation to ensure the mitigation of identified risks.

1.2.10. Gross and Residual Risks

(a) Gross (Inherent) Risk is the risk in the absence of any actions that management might take to either alter the Likelihood or Impact. The scoring takes into consideration that control measures are not present or one or two key control measures are ineffective or fail. Although this is a useful measurement of the risk profile, the approach is to consider residual risk (i.e. Net Risk) in carrying out risk assessments.

(b) Net Risk is the risk that remains after management's response to the risk. The scoring takes into consideration that all the key controls have been communicated, are effective and action plans are 'fully' implemented. The net risk can be looked at from a 'current' perspective or a 'target' perspective.

(c) BEIL Group's approach is to assess the Likelihood and Impact using the current net ratings viz., taking into consideration the fully implemented controls at the time of the assessment or review.

1.2.11. Controls and Mitigation

(a) In order to confirm whether the existing controls in place are appropriate and adequate and, if not, how urgently action should be taken to enhance them. The four 'T's model sets out the strategies for managing risks namely:

- **Treat** – Add control measures or contingency plans to manage the probability and impact of events to mitigate the risk through

the normal control measures employed in day-to-day management

- **Transfer** - To transfer and share the risk with another party, for example, by insurance, contractual risk transfer or outsourcing
- **Tolerate** - Some risks may be unmanageable, but a conscious decision may be taken to accept a risk if it is a necessary part of that business activity
- **Terminate** - Cease the activity related to the risk viz., abandon project

(b) For many risks, appropriate response options will be obvious and well documented. However, for other risks, options available might not be readily apparent, requiring investigation and analysis. It will be necessary to develop appropriate action plans to mitigate the risks. In developing risk responses, management should assess the effects on the probability and impact, costs versus benefits and possible opportunities to achieve entity objectives going beyond dealing with the specific risk.

(c) Where a new action plan is required, it will be necessary to fully define the risk at the outset, identify surrounding issues and then identify appropriate actions, risk owners and due dates to mitigate the risk.

1.2.12. Risk assessment and maps

(a) Risk assessment document is a convenient way of recording risks and providing a formal note of the actions taken or intended to manage risks. Risk assessment document as a minimum should include the the risk description, scoring for Impact, Likelihood and Control Environment...

(b) Key risks of the businesses and its functions are escalated and reported to the Audit Committee (wherever applicable) / Board of Directors. This high-level reporting and escalation process is the key to ensuring that risks are visible to the appropriate level in the organisation for action to be taken.

1.2.13. Execute action plans

(a) For the key risks and action plans, management will ensure that there is adequate communication of the mitigation strategies and that sufficient and skilled resources (monetary and people) have been

provided for fulfilling the action plan. Implementation of action plans may last several weeks or months depending on the complexity of the risk. The discussion and progress of actions should be part of the regular management team meetings.

1.2.14. Monitoring and assurance

(a) The risk assessment document should be monitored at regular intervals by way of management reviews, functional reviews, or local internal audit reviews. The purpose of the monitoring is to ensure that stated actions are being carried out and that the identified controls are effective in controlling risks. Internal audit, as a function employed to monitor and review the effectiveness of internal control, may be performed within all operating divisions and departments. Where monitoring reveals a weakness in any control, action should be taken to investigate, re-define control procedure and communicated.

1.2.15. Reporting and performance

(a) Significant risks will be reported to management from respective departments /functions on a regular basis. Any control failings or weaknesses identified should also be notified including the impact that they have had or may have and the actions being taken to rectify them.

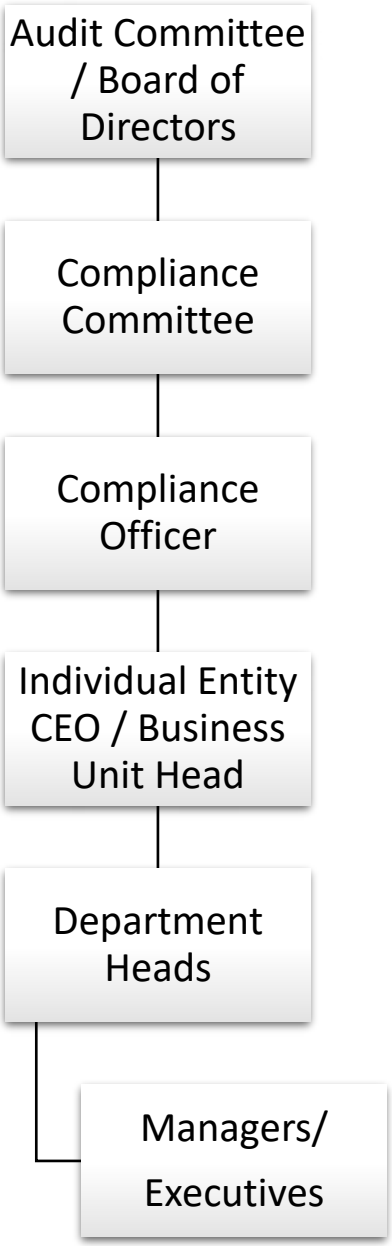
(b) Key risks from department / functions / entities / companies are cascaded upwards and reported to the Compliance Committee on a quarterly basis. The financial and non-financial criteria for reporting will be fixed and appropriate criteria will be applied.

****

Revision History

Issue	Date	Description of amendment
R-0	01/01/2021	--- x --- x --- x ---
R-1	06/09/2021	guidelines to conduct a risk assessment to be performed on periodic interval and areas to be covered and process for identification, assessment and mitigating such risks
R-2	01/01/2023	Update in Risk Assessment Register
R-3	01/01/2024	Reference of Audit Committee, Analysis criteria for likelihood, impact, control environment

Exhibit - A


Audit Committee / Board of Directors
Compliance Committee
Compliance Officer
Individual Entity CEO / Business Unit Head
Department Heads
Managers/ Executives