**TRIDENT LIMITED**

| | |
|---|---|
| **Name of the Policy** | **Risk Management Policy** |
| **Policy Custodian** | **Company Secretary** |
| **Date of latest amendment** | **November 14, 2023** |
| **Date of review** | **January 06, 2026** |

# RISK MANAGEMENT POLICY

## 1. PROCESS

Risk management is a continuous process that is accomplished throughout the life cycle of a Company. It is an organized methodology for continuously identifying the future uncertainty; developing mitigation options; selecting, planning, and implementing appropriate risk mitigations; and tracking the implementation to ensure successful risk reduction. Effective risk management depends on risk management planning; early identification and analyses of risks; early implementation of corrective actions; continuous monitoring and reassessment; and communication, documentation, and coordination.

## 2. STEPS IN RISK MANAGEMENT

Risk management is a shared responsibility. The risk management process model includes the following key activities, performed on a continuous basis.

### 2.1 Risk Assessment

This step involves understanding and listing of the potential threats that may affect the realization of the key success parameters, including the objectives of the organization or a project. Risk assessment involves identification and prioritization of risks. Likelihood and Impact of risk events have to be assessed for the purpose of analyzing the criticality. The potential impact may include:

- Financial loss;
- Non-compliance to regulations and applicable laws leading to imprisonment, fines, penalties etc.
- Loss of talent;
- Health, Safety and Environment related incidences;
- Business interruptions / closure;
- Loss of values, ethics and reputation.

The likelihood of occurrence of risk is rated based on number of past incidences in the industry, previous year audit observations, Government Policies, information from competition, market data, future trends or research report.

Risk may be evaluated based on whether they are internal and external, controllable and non- controllable, inherent and residual.

#### 2.1.1 Risk Identification

Once the objectives and assumptions of the organization or proposed scheme/activity have been established, the potential risks that may have an adverse effect on the achievement of these objectives are identified.

This involves continuous identification of events that may have negative impact on the

Company's ability to achieve goals. Processes have been identified by the Company and their key activities have been selected for the purpose of risk assessment. Identification of risks, risk events and their relationship are defined on the basis of discussion with the Business Heads & Heads of Department and secondary analysis of related data, previous internal audit reports, information from competition, market data, Government Policies, past occurrences of such events etc.

### 2.1.2 Risk Prioritization

Risk prioritization is the process of identifying the key risks. Risks are determined as priority depending on their analysis which is based on significance of their impact on the realization of the objectives of the organization/event/activity/scheme.

### 2.2 Risk Analysis

Risk Analysis is to be conducted using a risk matrix for likelihood and Impact, taking the existing controls into consideration. Risk events assessed as "high" or "very high" criticality may go into risk mitigation planning and implementation; low and medium critical risk to be tracked and monitored.

### 2.3 Risk Appetite

Risk appetite is the amount of risk an organization is willing to accept in pursuit of value. There are certain risks that the management may accept and tolerate. Delay in the recovery of dues from sundry debtors is a very high risk on the financial management front.

### 2.4 Proposed Enterprise Risk Management framework

Enterprise Risk Management framework is proposed to be designed in Trident Limited ("Trident"/"Company") to manage and monitor the risks and progress of risk mitigation plans.

Risks in Trident are proposed to be managed at 2 levels (Enterprise risks and Operating risks):

**Enterprise risks**

- Enterprise risks are the risks which are applicable to the entire company.
- Risk registers will be maintained containing risks, names of risk owners and mitigation owners and the related mitigation plans with timelines for closure.
- Enterprise risks will be monitored every month through risk meetings with the risk owners and mitigation owners.

- Status update on the enterprise risks and its mitigation plans will be presented to Chairman and Managing Director every month and to Risk Management Committee every quarter.
- Deep dives on 2 enterprise risks will be presented every quarter to the Chairman and Managing Director and to Risk Management Committee.

**Operating risks**

- Operating risks are the risks which are applicable at the operating unit level. These are the risks which pertain to day to day working of a business unit.
- Operating risk registers will be prepared separately for each of the business units and functions.
- Risk register will contain risks, names of risk owner and mitigation owners and the related mitigation plans with timelines for closure.
- Operating risks will be monitored every month through risk meetings with the risk owners and mitigation owners.
- Status update on the operating risks and its mitigation plans will be presented to Chairman and Managing Director every month and to Risk Management Committee every quarter.

Both the enterprise risks and operating risks will be further categorized into following categories in accordance with SEBI LODR Regulations:

- Sectoral risks
- Operational risks
- Financial risks
- Sustainability (including ESG risks)
- Information/cyber security risks

**Risk registers**

**Operating risk registers**

These risk registers will contain risks for running a business, function and related risk mitigation plans. Risk registers will be maintained for each of the businesses and corporate functions. Business risk registers will be separately maintained for each of the plants and branch locations.

**Enterprise risk registers**

Enterprise risk registers will be maintained at the company level and it will contain risks which are common to all or most of the businesses, risks which are applicable to the company as a whole.

**Risk register format**
Risk register will capture the following details:

1. **Risk statement**
   Risk statement will give clear description of risk
2. **Cause of risk**
   For each of the risk, the reason which is causing the risk will be mentioned
3. **Impact of risk**
   The impact which the risk is expected to have on the operations will be mentioned
4. **Risk mitigation plan**
   The plan for mitigating the risk will be mentioned in the risk register
5. **Risk Owner**
   Risk owner will be defined. Risk owner is the person who owns the function which is bound by Risk
6. **Mitigation Owner**
   Mitigation owner is the person who is responsible for mitigating the risk
7. **Timelines**
   Timelines by which risk mitigation plans are to be implemented will be mentioned
8. **Likelihood score**
   The level indicating probability of occurrence of the risk will be mentioned
9. **Impact**
   The level of impact which the occurrence of risk will have on the operations will be mentioned
10. **Risk score**
    Risk score will be mentioned which is the product of likelihood level and impact level.

**Risk prioritization**

All risks will be prioritized by assigning risk score to each of the risks. Risk score will be assigned to each of the risks based on product of likelihood and impact of the risk

Risk score will be calculated by the following formula:
Risk score= Likelihood X Impact

Matrix for determining severity of impact of risk is tabulated below:

| Grading | Very low (1) | Low (2) | Medium (3) | High (4) | Critical (5) |
|---|---|---|---|---|---|
| Financial | Annual impact of less than INR 0.05 lacs | Annual impact >INR 0.05 lacs<= INR 0.50 lacs | Annual impact >INR 0.51 lacs < = INR 5 lacs | Annual impact >INR 5 lacs<=INR 10 lacs | Annual impact >INR 10 lacs |
| Business continuity | Temporary interruptions of some operations | Temporary interruptions of business in some facilities | Interruption of business in one facility | Interruption of business in multiple facilities | Interruption of business in all facilities |
| Environme | Minor | Minor | Environmental | Major | Major |

| | | | | | |
|---|---|---|---|---|---|
| nt | environmental damage effects due to non toxic factors | environmental damage effects due to non toxic factors | damage effects due to toxic/non toxic factors | environmental damage effects due to toxic/non toxic factors and prosecution | environmental damage effects due to toxic/non toxic factors and prosecution & suspension of operations |
| Laws and Regulations | Routine issues raised by regulatory authorities | Cautions /instructions from regulatory authorities | Penalties below INR 0.5 Lacs and intensive scrutiny | Penalties above INR 0.5 Lacs restrictions on activity | Prosecution / loss of right to operate |
| Reputation /Brand | Insignificant brand damage at regional level | Temporary reputational impact at country level | Significant reputational impact at country level | Significant reputational impact at multi countries level | Significant reputational impact across the world |
| Safety | Minor injuries not leading to hospitalization | Minor injuries leading to hospitalization | Major injuries leading to hospitalization and temporary physical injuries | Major injuries leading to hospitalization and permanent physical injuries | Safety incidents leading to death |

Matrix for determining likelihood is tabulated below:

| Likelihood | Description | Probability |
|---|---|---|
| Almost certain (5) | Event expected to occur in most circumstances | 75-100% |
| Likely (4) | Event will probably occur in most circumstances | 51-75% |
| Possible (3) | Event should occur at sometime | 26-50% |
| Unlikely (2) | Event could occur at sometime | 6-25% |
| Rare (1) | Event may occur but only under exceptional circumstances | 1-5% |

**Risk rating matrix**

Risks will be categorized into following 4 categories based on the risk score (calculated by multiplying likelihood level with impact level):
Critical: Risk with score =>20
High: Risk with score =>10 and less than 20
Medium: Risk with score =>4 and less than 10
Low: Risk with score <4

| | | Impact | | | | |
|---|---|---|---|---|---|---|
| | | Very Low (1) | Low (2) | Medium (3) | High (4) | Critical (5) |
| Likelihood | 5 Almost certain | Medium (5) | High (10) | High (15) | Critical (20) | Critical (25) |
| | 4 Likely | Medium (4) | Medium (8) | High (12) | High (16) | Critical (20) |
| | 3 Possible | Low (3) | Medium (6) | Medium (9) | High (12) | High (15) |
| | 2 Unlikely | Low (2) | Low (4) | Medium (6) | Medium (8) | High (10) |
| | 1 Rare | Low (1) | Low (2) | Low (3) | Medium (4) | Medium (5) |

Enterprise Risk Management (ERM) program will be automated to enable better visibility, tracking and governance.

**2.5 Areas for Risk Management Initiatives**

Risk management requires a broad understanding of internal and external factors that can impact achievement of strategic and business objectives. Historically, risks to the Company's success have been categorized as Strategic, Operational, Compliance, and Financial & Reporting. However, as the world in which we operate becomes more complex and unpredictable, the corresponding risks and their potential impact have increased. To ensure that the Risk Management Policy of the Company appropriately incorporates the evolving risk landscape, our risk categories now also address Environmental, Social and Governance related risk and Cyber security risks.

Our thinking about risk categories is also informed by the results of internal risk assessments and risk assurance work, as well as insights from various industry sources. Although it is difficult to define every specific type of risk, however, the potential/ existing risk that exist in our industry areas follows:

- Strategic
- Financial
- Operational
- Social
- Governance
- Cybersecurity
- Sectoral
- Sustainability(Particularly ESG related Risk)
- Information
- Adverse Exchange rate movement
- Commodity Price Risk

This framework has been designed to address the above risk and to work upon the mitigation of adverse affect.

### 2.6 Risk Management and Internal Control

Effective risk management depends on risk management planning; early identification & analysis of risks; early implementation of corrective actions; continuous monitoring & reassessment; communication, documentation, and coordination.

#### 2.3.1 Risk Monitoring

Refers to the review and monitoring of the execution of the Risk management processes at defined periodicities (monthly/quarterly/annually etc) and ensuring that the key risks are being effectively addressed by the laid down action plan. It also focuses on identification of additional risks and concerns that may arise during the implementation of the scheme and taking the necessary action required to address them.

#### 2.3.2 Risk Assurance

Refers to an independent assurance on the effectiveness with which risks are addressed and internal controls are operating in the programme. This is done through audit and special reviews carried out by agencies appointed by the organization.

#### 2.3.3 Control and Monitoring Mechanism

Internal Auditor to review the internal controls and systems periodically and report their observations and suggestions for improvement. Audit Committee of the Board reviews the observations of internal auditors and gives suitable advice to the management.

#### 2.3.4. Evaluation of Internal Controls

The internal audit evaluates the effectiveness of risk management and Internal Controls relating to the organization's governance, and specifically relating to:

➢ Reliability and integrity of financial and operational information,

➢ Effectiveness and efficiency of operations and programs,
➢ Safeguarding of assets,
➢ Compliance with laws, regulations, policies, procedures and contracts,
➢ The potential for the occurrence of fraud and how the organization manages fraud risk.

**Internal controls** are safeguards that are put in place by the management of an organization to provide assurance that its operations are proceeding as planned. Internal Control is the responsibility of the management and the role of Internal Audit is to assess and evaluate them. Evaluation of Internal control helps to provide reasonable assurance that the organization:

➢ Adheres to laws, regulations and management directives;
➢ Promotes orderly, economical, efficient & effective operations & achieves planned outcomes;
➢ Safeguards resources against fraud, waste, abuse and mismanagement;
➢ Provides quality products and services consistent with the organization's mission;
➢ Develops & maintains reliable financial & management information and timely reporting.

**4. Responsibilities**

Responsibility for risk management is shared across the organisation. Key responsibilities include:

Risk Ownership and management – Management should perform and monitor day-to-day risk management activity. The Management is responsible for periodically reviewing the group's risk profile, fostering a risk-aware culture and reporting to the Risk Management Committee on the effectiveness of the risk management framework and of the company's management of its material business risks.

More specifically, Management is responsible for:

➢ Promoting Risk Policy Framework;
➢ The design and implementation of cost effective risk management and internal control systems in accordance with the guidelines to manage risk, encourage efficiencies and take advantage of opportunities;
➢ Continuous monitoring and reporting of the effectiveness of risk controls;
➢ Monitoring compliance, investigating breaches, recommending and/or approving improvement opportunities.
➢ Create a positive control environment by:
  - Setting a positive ethical tone
  - Removing temptations for unethical behavior
➢ Preparing a written code of conduct for employees
➢ Ensure that personnel have/ maintain a level of competence to perform their duties.
➢ Clearly define key areas of authority and responsibility
➢ Establish appropriate lines of reporting

➢ Establish management control policies and procedures based on analysis of risk
➢ Use training, management communications to reinforce the importance of control management

**4.1 Employees** are accountable for actively applying the principles of risk management within their areas of responsibility and fostering a risk-aware culture. More specifically, Employees are responsible for:

➢ Report to their immediate leader or supervisor, any real or perceived risks that become apparent and may significantly affect the Company's: Commercial viability; Profitability; Assets; Business continuity; Customers; Regulatory and/or legal obligations; Reputation; and/or People and/ or their safety.
➢ Report to their immediate leader or supervisor, any real or perceived risks that company's operations may significantly affect the broader: Environment; and/or Community.
➢ Look for opportunities to improve operational efficiencies and optimize outcomes.

**4.2. Measures of Risk Mitigation through Risk Management Committee:**

➢ Maintain oversight and monitor the effectiveness of internal controls and risk management activities.
➢ Risk Management Committee assists the Company in overseeing the company's risk profile and is responsible for overseeing the effectiveness of management's actions in the identification, assessment, management and reporting of material business risks.
➢ Ensure independence of Internal Audit from management of subsidiaries & Units.
➢ Any deviations will be reported by Risk Management Committee to Audit Committee.

**4.3. Internal Control of Identified Risk:**

Internal Audit provides independent assurance on the effectiveness of internal controls and the Risk Management Framework. It is responsible for:
➢ Developingandimplementinganannualauditplanhavingregardtomaterialrisks
➢ Reviewing the effectiveness of company's risk management policy and risk management processes; and Notifying Group Risk of new and emerging risks identified in the course of implementing the audit plan and, where necessary, modifying the audit plan to take account of the impact of new risks. Ensure professional competence of audit staff
➢ Advise management on areas of risk
➢ Establish auditing strategic plans and goals
➢ Perform audit of operations
➢ Evaluate adequacy and effectiveness of Internal Control mechanism
➢ Recommend ways to improve operations and strengthen controls
➢ Follow up to ensure recommendations are fully and effectively implemented.

### 4.4. Common Internal Control practices:

➢ Performance indicators are developed & monitored
➢ Secure and safe guard all vulnerable assets
➢ An organization's workforce is effectively trained and managed so as to achieve results
➢ Key duties and responsibilities are divided among people to reduce the risk of error & fraud.
➢ Information processing is controlled Eg. Audit checks of data entry
➢ Access to resources and records is limited to authorized individuals. Accountability for their custody and use is assigned and maintained
➢ Internal control and all transactions and other significant events are clearly documented and the documentation is readily available for examination
➢ Transactions & other significant events are authorized and executed only by authorized person
➢ Transactions are promptly recorded to maintain the irrelevance and value to management in controlling operations and making decisions

### 4.5. Risk Organization Structure

As per the provisions of Regulation 17 (9) of SEBI LODR Regulations, 2015 and in order to inform Board of Directors about risk assessment and minimization procedures, periodic workshops will be conducted to ensure awareness of the policy and the benefits of following them. This will ensure that risk management is fully embedded in management processes and consistently applied. Senior management involvement will ensure active review and monitoring of risks on a constructive 'no-blame' basis.

### 4.6. Business Continuity Plan

While Business Continuity Plan encompasses the whole gamut of business processes needed to get the business back on track in the event of a disaster, there are two main aspects to it:

1) Infrastructure-that includes data and applications/software
2) Business Processes- Under this, one needs to look at the value chain to identify the critical areas to be addressed. To manage day to day operations during a disaster, the Business continuity plan should be agile, effective and highly responsive

Business continuity plan should address and protect the above two critical resources of the Company and ensure that Company/ business does not loose its identity in any potential adverse scenario. In Trident Limited, we have incorporated the Business Continuity plan under the following process:

**Business Impact analysis**- A business impact analysis identifies key business areas within an organisation and their critical functions to devise a plan that outlines how each will operate in the event of a major disruption. During this initial phase, we have tried to identify the potential losses that Company might face i.e financial, legal, regulatory and what impact those losses could have on the company over different lengths of time. The

same must be done at regular intervals in the Company.

**Business Continuity Plan-**The report will be placed before the risk management committee of the Company and accordingly the preventive and correction steps will be taken to ensure that in any adverse situations, continuity of Trident Business should not suffered.

**Test and Re-test-**In the current unpredicted scenario, adoption and change is a need of an hour. Company cannot predict a static long term plan for its business continuity. Business continuity plan has to revisit and modified as per the highly volatile scenario of Industry. Evaluation of the Plan is the only key source for continuity. Trident will keep evaluate its business continuity plan on regular intervals over the course of the year to make sure it's not outdated or unrealistic.

**********