# PROLIFIC RESOLUTION PRIVATE LIMITED

## RISK MANAGEMENT POLICY

Pursuant to Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 and as approved by the Risk Management Committee on August 01, 2023 and adopted by the Board of Directors on August 01, 2023

## CONTENTS

## 1. PREAMBLE

In accordance with Section 134(3)(n) of the Companies Act, 2013, a Company is required to include a statement indicating development and implementation of a Risk Management Policy for the Company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company. Further as per Regulation 17 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, the Board of Directors shall be responsible for framing, implementing and monitoring the Risk management Plan for the Listed Entity.

Accordingly, to mitigate and manage risk at "Prolific Resolution Private Limited" (hereinafter referred to as the "Company"), the Company has formed the Risk Management Policy ("Policy") for the same.

This Policy 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.

This Policy is disclosed on the Website of the Company at www.prolificresolution.com

## 2. SCOPE AND APPLICABILITY OF POLICY

The objective of this Policy is 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 Matrix, in order to guide decisions on risk related issues. The specific objectives of the Risk Management Policy are:

- To ensure that all the current and future material risk exposures of the Company are identified, assessed, mitigated, monitored and reported.
- To establish a framework for the Company's Risk Management process and to ensure companywide implementation.
- To ensure systematic and uniform assessment of risks related with recovery, assessment and management of claims (including arbitral awards), decrees, orders, and/or beneficial interest.
- To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices.
- To assure business growth with financial stability.
- The effectiveness of Risk Mitigation plans shall be ensured through proper monitoring, evaluation of outcomes of Mitigation Plans and to look for the scope of its applicability in other areas in order to achieve overall objective of this Policy.

To achieve the above objectives, the Company shall adhere to the following core principles:


## 3. DEFINITIONS

**a.** **"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.

**b.** **"Risk Management"** is a set of coordinated activities to direct and control an organization with regard to risk. Risk management includes risk assessment, risk treatment, risk acceptance and risk communication.

**c.** **"Risk Identification"** is the process of identifying the organization's exposure to uncertainty.

**d.** **"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.

**e.** **"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.

f. **"Risk acceptance/ Retention"**– the acceptance of the burden of loss or benefit or gain, for a risk.

g. **"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.

h. **"Risk Matrix"** is a matrix that is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity to increase visibility of risks and assist management decision making.

## 4. ENTERPRISE RISK MANAGEMENT FRAMEWORK (ERMF)

Enterprise Risk Management is a definitive plan-based strategy that aims to identify, assess, and prepare for any potential risks. It enables Management to deal with uncertainties and challenges head-on and empowers them to build more value. Based on the organization's structure and needs, the approach to mitigate against these risks differ.

The 8 core principles of ERMF consist of the following:

### a) Company's Code of Conduct

The Company's core values and code of conduct play a major role in defining the risk aptitude. A healthy work culture sets the tone for employees' work standards and the ability to deal with risks. The managerial skills of the leaders will ensure that none of the risks are overlooked in the light of completion of assignments.

### b) Objective setting and goals

The Company has set a mission and vision to ensure that everyone is working towards a common goal. When these objectives are cascaded across the enterprise, every senior and junior employee is aware of their roles and responsibility.

These common business objectives act as a guidebook while forming Risk Management Plan. The following aspects can be ascertained:

- Risk tolerance: The maximum level of risk that the Company can take to fulfil its mission and goals.
- Risk appetite: The level of risk the Company is willing to take to pursue its goals and objectives.

### c) Identification of Risks and Opportunities

It is one of the most crucial components of the ERM framework. Risks can disrupt the Company's progress, while opportunities can give some tangible benefits. Analysing these events is at the core of the risk mitigation strategy.

**d) Risk assessments and its categorization**

Risks can be of different types based on the several areas of business they can impact. It includes strategic risks, i.e., it poses a threat to the business sustainability, operational risks, i.e., it can cause inefficiency in resource management, compliance risks, i.e., it violates the rules and regulations of a business, and cyber security risks which relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation).

The categorization of these risks enables the Company to prioritize them and decide a course of action.

**e) Risk response and mitigation**

After careful assessment and categorization of risks, ways in which the Company can respond to risks are:

- Reduce – reduce the risks to minimize its impact
- Accept– accept the impact if it's negligent or minimal.
- Avoid– eliminate or forego the risk.
- Transfer– assign the mitigation to a competent third party.

The onus is on leaders to ensure that employees are implementing the right risk response in favour of the strategic planning process.

**f) Checks and balances**

Checks and balances are necessary to ensure that the response activities are carried out according to the policies. The company's ethics and values are as important as risk mitigation measures. If any employee deviates from the defined laws, it will not go unnoticed.

As a part of the framework and risk management strategy, the Board of Directors must clarify the roles and responsibilities with transparency.

**g) Information and Communication**

Communication is the essence of any business. Especially in the digitally advanced world, it holds immense value.

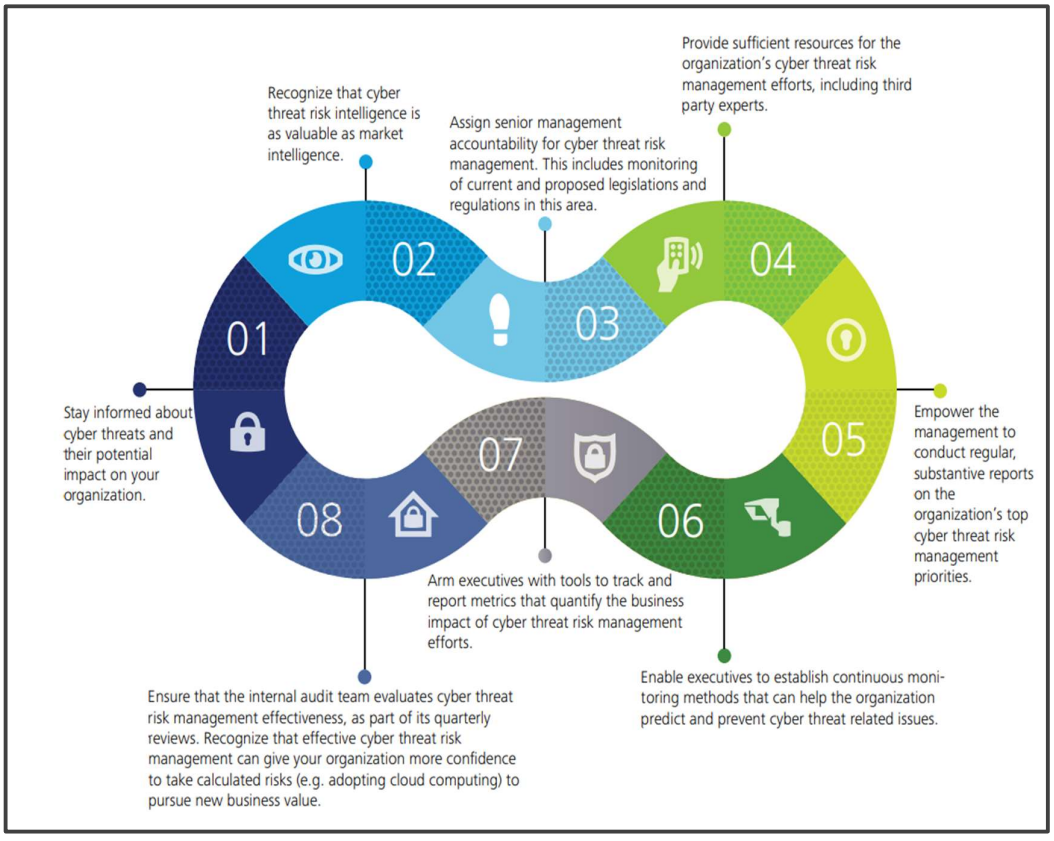
**h) Monitoring and call to Action**

The Company must monitor and review the Risk Management Strategy at regular intervals to introduce improvements that will be beneficial in mitigating risks. Risk Management is always a Work in Progress.

## 5. CYBER SECURITY RISKS

Unlike other fraud, the motivations for perpetrators of cyber threats extend beyond financial gain and include revenge, personal thrill, activist causes, deep rooted anti-establishment sentiments, and a need to prove self-worth by showcasing professional finesse in hacking complex security systems. The perpetrators of cyber-attacks can, therefore, range from individuals or small groups of insiders, suppliers and activists, to large-scale organized efforts by criminal networks and foreign entities. Hence, cyber-attacks can vary in nature and include scenarios - such as introduction of malicious software like trojans, worms, viruses and spyware; password phishing; and denial-of-service attacks intended to crash websites. Each type of attack presents unique challenges and requires a targeted set of prevention activities. Phishing or social engineering techniques, for instance, are often dependent on employees divulging their password or other sensitive information when requested under false pretence. Thus, education and awareness across the Company of Cyber Crimes and the reasons behind them are of paramount importance in preventing losses.

The following model shall serve as a guide to the Board of Directors for establishing a cyber threat risk governance program:



## 6. CHIEF RISK OFFICER

The Company Secretary shall act as the Chief Risk Officer (CRO) and ensure effective implementation of Risk Management Process.

Roles and Responsibilities of the CRO:

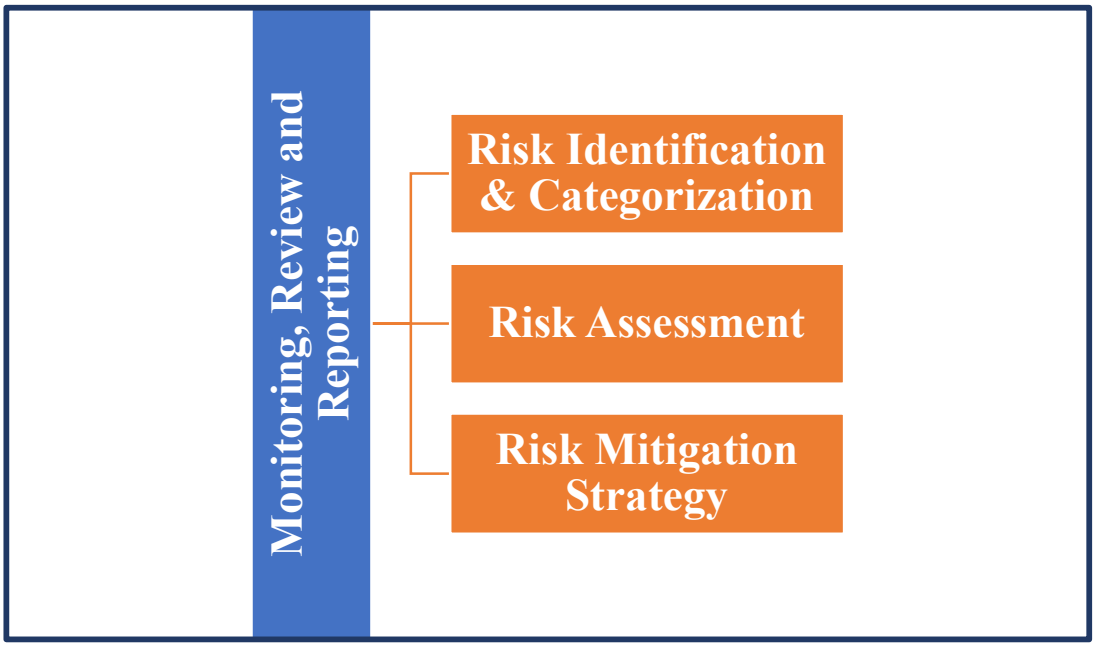
- Communicating and managing the establishment and ongoing maintenance of Risk Management Policy pursuant to the organization's Risk Management Vision.
- Reporting the key risks faced by the organization.
- Coordinate with the organizational heads to compile the status of risks and mitigation measures taken.

## 7. RISK MANAGEMENT APPROACH

Risk Management is the process which shall enable the organization to identify, assess and treat risks. The primary objective(s) of establishing a Risk Management Process is to ensure that:

- Risks faced by the organization shall be identified in the risk matrix, enabling the top management to take a comprehensive view of the same
- Risks identified shall be assessed, mitigated, monitored and reviewed on an ongoing basis.

Risk Management Approach is as depicted below:




### A. RISK IDENTIFICATION & CATEGORIZATION

Risk identification sets out to identify an organization's exposure to uncertainty. This requires an in-depth knowledge of the economic, legal, regulatory, social, political, technological and cultural environment in which it exists, as well as the development of a

sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

Risk identification shall be approached in a methodical way to ensure that all significant activities within the organization have been identified and all the risks flowing from these activities defined.

The following methodologies can be used to identify risks:

- Brainstorming
- Surveys /Interviews/Working groups
- Experiential or Documented Knowledge
- Risk Lists - Lessons Learned
- Historical risk event information

Risks shall be classified under the following risk categories –

- **Contractual Risks** - Risk of loss resulting from Contractual matters. These risks adversely affect the achievement of contractual objectives and may impair overall value.

- **Financial Risks** - Risk directly impacting the balance sheet and access to capital.

- **Cyber- Security Risks -** Cybersecurity risk is the probability of exposure, loss of critical assets and sensitive information, or reputational harm as a result of a cyber-attack or breach within an organization's network.

## B. RISK ASSESSMENT

Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives.

Subject to deliberations with the Board of Directors, the risks identified may be evaluated on an appropriate risk rating as per the criteria given below:

| Severity | Score | Impact |
|---|---|---|
| Very Insignificant | <0.25 | Financial implications of the risk are very low and are comfortably within the ability of the risk owner to manage locally. |
| Minor | 0.25-0.5 | Financial implications of the risk are low (<10% of the budget/turnover). It remains within any contingency set. |
| Significant | 0.5-1 | Financial implications of the risk are medium (10% -<25% of the budget/turnover). It may exhaust or be larger than contingencies made but can be managed without additional funds. |
| Major | 1-2 | Financial implications of the risk are high (25% - <50% of the budget or turnover). It is not possible to meet the cost within the approved budget and further funding would be required. |
| Catastrophic | More than 2 | The impact on finance is critical (>50% of the budget or turnover). Increased cost would negate benefits of activity and may destabilize the reporting unit. Impacts upon Cashflow would be adverse. |

## C. RISK MITIGATION STRATEGY

There are four common strategies for treating risk. There is no single "best" response strategy and each risk must be considered on its own merits. Some risks may require a combination of strategies and multiple responses, whereas others may need only one strategy with a single response.

- **Risk avoidance/ termination:** This involves doing things differently and thus removing the risk. This is particularly important in terms of contractual risks and strategic risks.

- **Risk reduction/ mitigation:** Reduce or treat the risk. This is the most widely used approach. The purpose of treating a risk is to continue with the activity which gives rise to the risk but to bring the risk to an acceptable level by taking action to control it in some way through either.

- **Risk acceptance/ retention:** Accept and tolerate the risk. Risk Management doesn't necessarily mean risk reduction and there could be certain risks within the organization that it might be willing to accept and continue with its operational activities. The organization shall tolerate such risks that are considered to be acceptable, for example (i) risk that cannot be mitigated cost effectively (ii) risk that opens up greater benefits than loss (iii) Uncontrollable risk.

- **Risk transfer:** Transfer some aspects of the risk to a third party. Examples of risk transfer include insurance and hedging. This option is particularly good for mitigating financial risks or risks to assets.

  The following aspects shall be considered for the transfer of identified risks to the transferring party (i) Internal processes of the organization for managing and mitigating the identified risks (ii) Cost benefits analysis of transferring the risk to the third party (iii) Insurance can be used as one of the instruments for transferring risk.

  **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.


**IDENTIFY 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.

**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.

**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.

## D. RISK MONITORING AND REVIEW

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).

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.

## 8. BUSINESS CONTINUITY PLAN

The objective of the Business Continuity Plan is to coordinate recovery of critical business functions in managing and supporting the business recovery in the event of a facilities (office building) disruption or disaster. This can include short or long-term disasters or other disruptions, such as fires, floods, earthquakes, explosions, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, and other natural or man-made disasters.

***A disaster is defined as any event that renders a business facility inoperable or unusable so that it interferes with the organization's ability to deliver essential business services.***

A draft Proforma of a Business Continuity Plan is enclosed as **"Annexure A".**

## 9. REVIEW OF POLICY AND AMENDMENTS

Where the terms of this Policy differ from any existing or newly enacted law, rule, regulation or standard governing the Company, the law, rule, regulation or standard will take precedence over this Policy and procedures until such time as this Policy is changed to conform to the law, rule, regulation or standard.

The Board shall at least once in every two years, review the Risk Management Policy including by considering the changing industry dynamics and evolving complexity.

The Company shall be free to devise and implement any supplementary or other policies and guidelines in respect hereof for better implementation of this Policy. In case of any amendment(s), clarification(s), circular(s) etc. issued by the relevant authorities, not being consistent with the provisions laid down under this Policy, then such amendment(s),

clarification(s), circular(s) etc. shall prevail upon the provisions hereunder and this Policy shall stand amended accordingly from the effective date as laid down under such amendment(s), clarification(s), circular(s) etc.

## 10. DISCLAIMER

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

## ANNEXURE A

## DRAFT PROFORMA OF A BUSINESS CONTINUITY PLAN

### 1. BUSINESS FUNCTION RECOVERY PRIORITIES

Disaster recovery teams use this strategy to recover essential business operations at an alternate location site. The information system and IT teams restore IT functions based on critical business functions.

### 2. RELOCATION STRATEGY

An organization uses the alternate business site and relocation strategy in the event of a disaster or disruption that inhibits the continuation of the business processes at the original business site. This strategy should include both short-term and long-term relocation sites in the case of both types of disruptions.

### 3. RECOVERY PLAN & PHASES

These are the activities most needed for the business to continue, and the recovery plan should target these essential business functions. The recovery plan should proceed as follows:

- Disaster Occurrence - The company declares a disaster.
- Plan Activation - During this phase, the company puts the business continuity plan into effect. This phase continues until the company secures the alternate business site and relocates the business operations.
- Alternate Site Operations - This phase continues until the business can restore the primary facility.
- Transition to Primary Site - This phase continues until the company can appropriately move business operations back to the original business site.

### 4. RESTORATION PLAN

Disaster recovery/It teams maintain, control, and periodically check on all the records that are vital to the continuation of business operations and that would be affected by facility disruptions or disasters. The teams periodically back up and store the most critical files at an offsite location.

## 5. RECOVERY PROCEDURES

The company details the specific activities or tasks needed to recover normal and critical business operations. It describes each strategy by enumerating the specific set of activities and tasks needed to recover appropriately.

## 6. POTENTIAL RECOVERY PROCEDURES

- Disaster Occurrence
- Notification of Management
- Preliminary Damage Assessment
- Declaration of Disaster
- Plan Activation
- Relocation to Alternate Site
- Implementation of Temporary Procedure
- Establishment of Communication
- Restoration of Data Process and Communication with Backup Location
- Management of Work
- Transition Back to Primary Operations
- Cessation of Alternate Site Procedures