# [1]Swiggy Limited
# Enterprise Risk Management Policy

[1] Formerly Swiggy Private Limited and Bundl Technologies Private Limited

**Table of Contents**

## 1. Introduction

The Enterprise Risk Management Policy **("Policy")** defines purpose, objective and critical components of the risk management process in use at Swiggy Limited (hereinafter referred to as or **"Company").** The current dynamic and competitive business environment within which Company operates, makes it necessary to establish a robust risk management policy and framework, which will assist in identifying and managing various risks in an effective manner to support the achievement of business objectives.

This Policy has been established by the Company as a comprehensive set of components that provide the foundation and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

## 2. Scope and applicability

This Policy applies to all employees, functions, units and subsidiaries of the Company.

## 3. Purpose

The Board of Directors ("Board") of "the Company has adopted this Policy in compliance with the requirements of Section 134 of the Companies Act, 2013 ("the Act") and Regulation 17(9) and Regulation 21 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("SEBI Listing Regulations"). According to this, the Board shall be responsible for framing, implementing, and monitoring the risk management plans for the Company.

The purpose of this document is to define the objective, requirements and framework for Enterprise Risk Management in the Company. The objective of Risk Management Policy is to ensure that the Company is having a procedure laid down for identifying, evaluating, reporting, and mitigating risks associated with the business.

## 4. Roles and Responsibilities (under Companies Act and SEBI LODR, 2015)

To ensure sustainable business growth, promote efficient risk management practices and protect shareholder wealth, regulatory authorities have placed the responsibility of Enterprise Risk Management on the Board of Directors.

Some of the key regulatory requirements are as follows:

### 4.1. Companies Act, 2013

The Board along with the Audit Committee of a company shall have an oversight on the Risk Management process and Independent Directors oversee and provide inputs on the Risk Management process.

**Board of Directors**

1. Report by its Board of Directors, which shall include a statement indicating

development and implementation of an Enterprise 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. [Section 134 (3) (n)]

2. Independent directors should satisfy themselves on the integrity of financial information and that financial controls and systems of risk management and internal control are robust and defensible and properly understand the Group's activities and associated risks. [Schedule IV]

**Audit Committee of the Board**

3. The Audit Committee shall act in accordance with the terms of reference specified in writing by the Board, which shall, inter alia, include evaluation of risk management systems. [Section 177 (4) (vi)]

### 4.2. Stock Exchange Board of India - Listing Obligations and Disclosure Requirements Regulations 2015 (SEBI-LODR)

The company is required to comply with the standards relating to Enterprise Risk Management (ERM) laid down by SEBI LODR Regulations 2015, detailed below:

**Board of Directors**

1. The Board of Directors of the Company shall have the following responsibilities with respect to risk management:

    - Review the Risk Policy [Regulation 4 (2) (f) (ii) (1)]
    - Ensure integrity of the Risk Management systems [Regulation 4 (2) (f) (ii) (7)]
    - The Board of Directors shall ensure that, while rightly encouraging positive thinking, these do not result in over-optimism that either leads to significant risks not being recognized or exposes the Company to excessive risk. [Regulation 4 (2) (f) (iii) (9)]
    - The Board of Directors shall have the ability to 'step back' to assist executive management by challenging the assumptions underlying: strategy, strategic initiatives (such as acquisitions), risk measurement, exposures, and the key areas of the Company's focus. [Regulation 4 (2) (f) (iii) (10)]

2. The Company shall lay down procedures to inform members of Board of Directors about risk assessment and minimization procedures. [Regulation 17 (9) (a)]

3. The Board of Directors shall be responsible for framing, implementing and monitoring the risk management plan for the Company. [Regulation 17 (9) (b)]

**Risk management Committee**

1. The Risk Management Committee (hereinafter referred to as "the Committee") shall formulate a detailed risk management policy, which should include:

a. a framework for identification of internal and external risks in particular including financial, operational, sectoral, sustainability (particularly ESG related risks), information, cyber security or any other type of risk as determined by the committee.
b. measures for risk mitigation including systems and processes for internal control of identified risks and
c. business continuity plans

2. The Committee shall oversee and monitor the implementation of the risk management policy including evaluation of adequacy of risk management systems

3. Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.

4. Periodically review the risk management policy, at least once every 2 years, including by considering the evolving industry dynamics and increasing complexity.

5. Keep the Board 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 RMC.

7. The Risk Management Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

Additionally, the Board and the Risk Management Committee shall cover all other matters which may be relevant from Company's risk management view or as prescribed by the Companies Act, 2013 & rules made thereunder, SEBI LODR or such other regulation prescribed/applicable to the Company.

**5. Enterprise Risk Management Objectives**

Enterprise Risk management objectives are:

- ***Stakeholder Value Creation & Protection:*** To identify and manage uncertainties that may have potential impact on Company objectives and values.

- ***Uniform Enterprise Risk Management Practice:*** Develop a common understanding of risk and risk management processes across multiple locations, functions, and business units to manage risk effectively and increase competitive advantage.

- ***Governance in line with the regulatory requirements:*** To strengthen corporate governance in-line with principles laid in different regulatory requirements which include Companies Act 2013 & SEBI LODR.

- ***Provide Decision Support:*** Providing senior leadership with visibility to key risks enabling proactive risk-informed decision making, right allocation of resources and maximizing opportunities.

**6. Risk Management Principles**

The Company is committed to adopting a proactive approach to risk management based on the following principles:

- ***Integrated*** - The Risk management processes should be integrated with all operating, strategic and decision-making processes. All parts of the organization and functions shall work in a coherent manner for managing risks in the company.

- ***Ownership and accountability*** - Ownership of all the risks must be clearly defined before further analysis. Risk ownership should lie with the employee whose organisational objective or Key Result Area **(KRA)** is impacted the most and who will be in the best position to coordinate the mitigation responses.

- ***Standardization*** - With respect to definitions - risk impact, risk probability & risk velocity; basic processes of the framework; architecture, tools and governance mechanism to ensure consistency & uniformity in practices across Businesses, functions, geographies and hierarchy.

- ***Systemic*** -Every risk must be dealt with in a systematic manner using the framework for assessment, analysis, mitigation, monitoring and review. Reviews must happen for all risks at the appropriate level.

- ***Comprehensiveness*** - All risks that impact the objective of the company must be addressed as part of the risk management practice. These include operational, strategic, financial, regulatory, sustainability risks etc. & could be external or internal to the organization.

- ***Dynamic*** - The Enterprise Risk Management framework as well as the risk registers should be indicative of changing economic and business conditions, technology and management perspective. At least once in two years review of the framework and policy shall be conducted.

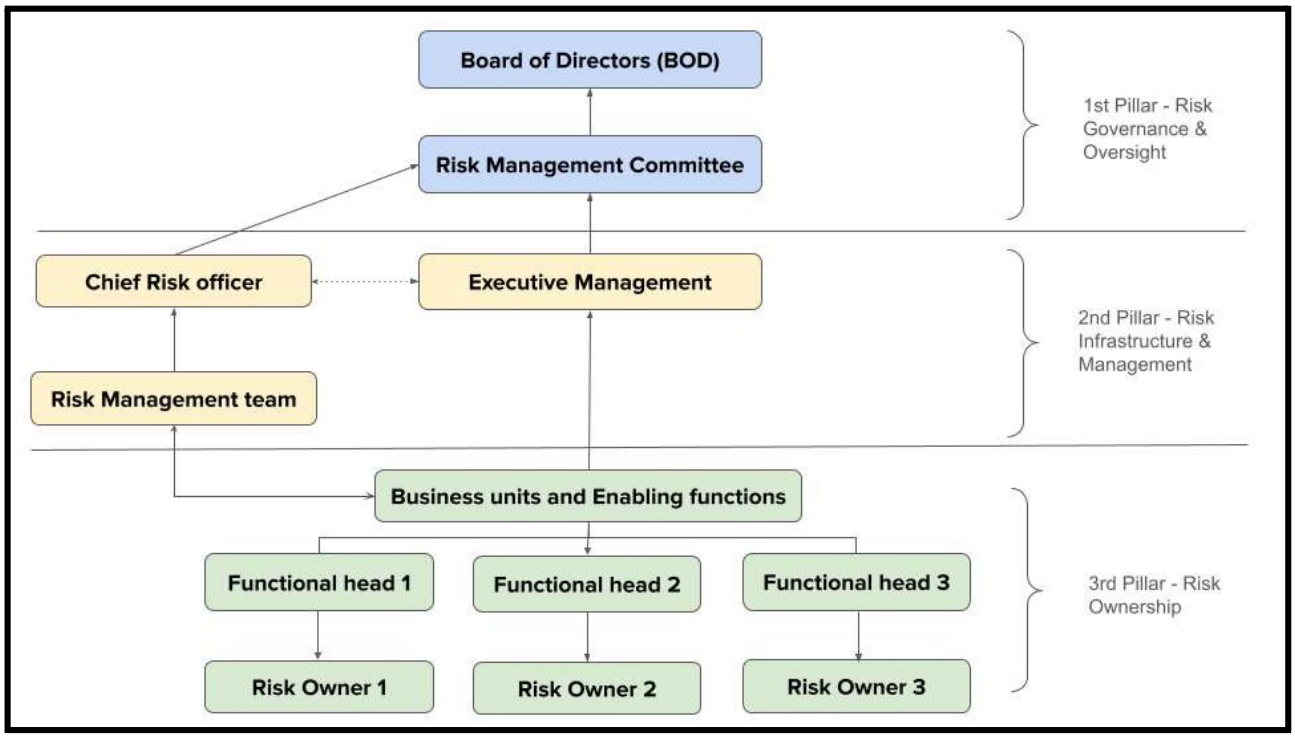
- ***Confidentiality*** -The risk owners must keep all information regarding the risks and its analysis, confidential and follow the company's policy for sharing the information related to risks.

- ***Transparency and Honesty-*** Business units should encourage employees to be transparent and honest in identifying and sharing all the potential risks and all the information regarding the same sufficiently in advance.

- ***No prejudice*** - Risks should not be viewed as inefficiencies, and are events that may or may not occur, therefore identification of a particular risk should not be regarded as a sign of performance inadequacy, and the employee responsible for identifying the risk shall not be treated with any prejudice.

**7. Risk Governance-**

The risk management governance structure has been designed to ensure seamless integration of risk management processes with the existing organizational processes.




**First Pillar - Risk Governance and Oversight**

**1. Board of Directors**

The Board of Directors through the Risk Management Committee play a critical role in overseeing the deployment of risk management processes at an enterprise level and setting the tone and culture towards effective risk management. The Board of Directors shall meet periodically (at least on an annual basis) to review the overall risk management policy, key risks and mitigation status to determine if the total risk exposure is within the company's appetite for risks.

**2. Risk Management Committee (RMC)**

The Risk Management Committee of the Board shall review and approve the risk policy, guide implementation and monitoring of the risk management policy & framework across the organization.

a) **Composition of the RMC:** The Risk Management Committee shall have minimum three (3) members with majority of them being members of the Board of Directors while at least 1 Independent Director. Further, senior executives of the Company may

be members of the Committee.

b) **Chairman:** The Committee will elect a Chairman amongst the Committee members who shall be a director.

c) **Quorum:** The quorum for meetings of the Committee would be at least two members or one third of the total members of the Committee, whichever is higher. Additionally, the quorum shall include at least one member of the Board of Directors in attendance.

d) **Frequency of the meeting:** The Committee shall meet at least twice in a year however, the meetings shall be conducted in such a manner that there should not be any gap of more than 180 days between the two consecutive meetings in a year.

The Risk Management Committee will review the status of high and critical enterprise risks and adequacy of mitigation plans and provide their inputs and recommendations. They will also provide inputs on the company's risk tolerance levels. The Committee may also seek additional information from any employee or obtain inputs from any external professional advice if it considers it necessary to assess the status of the risk.

The committee will also provide annual updates to the Board on the critical and high risks and the effectiveness of the risk management systems. The Committee will also perform such functions as may be delegated by the Board and/or are prescribed under Companies Act, 2013, SEBI (Listing Obligations & Disclosure Requirements) Regulations, 2015 and relevant amendments and any other applicable laws from time to time.

**Second Pillar - Risk Infrastructure and Management**

**1. Executive Committee (Ex- Com)**

The Executive Committee comprises the Group CEO & his DR's includes BUs CEO, CFO, CTO, CHRO. The Executive Committee shall be accountable for designing, initiating implementation and enabling the risk management processes. The Ex-Com is also responsible for developing a risk intelligence culture within the organization that helps improve organization resilience to critical business risks. They would assist in identifying high priority risk, defining the right mitigation strategies and review the status of its mitigation plan on a quarterly basis.

**2. Chief Risk Officer (CRO) & Risk Management team (RMT)**

The Head of Internal Audit function shall also act as Chief Risk officer. The CRO shall be assisted by the Risk Management team who would be working closely with the Functional heads /sub-functional Risk owners.

The key responsibilities of CRO and RMT will be:

A. To ensure that the risk management processes as defined in this policy are executed and to coordinate the effort of various functions to deliver an enterprise level view on risks to the Executive Committee and the Risk Management Committee.

B. To facilitate internal risk review meetings, maintaining risk registers, assisting risk owners in identifying and monitoring Key Risk Indicators (KRls) and suggesting best practices for strengthening the risk management process.
C. Ensure risk registers are periodically reviewed, monitor the risk environment of the company and are updated according to regulatory and business requirements defined in this framework.
D. Assist risk owners in formulation and tracking status of mitigation plans.
E. To provide periodic updates to the Risk Management Committee and Executive Committee on the status of high and critical risks and associated mitigation plans (risk dashboard and heatmap presentation).
F. To organise awareness sessions regarding enterprise risk management to ensure the entire organisation is aligned with respect to risk management programs.
G. Review the Risk Management policy and propose recommendations for changes, if any, to the Risk Management Committee.

**Third Pillar - Risk Ownership**

**1. Functional Head & designated risk owners (at a functional level)**

The ownership of risk identification, monitoring & mitigation shall lie with the respective Functional Heads. The functional heads will be supported by designated risk owners within the function/ BU and will be responsible for:

A. Performing continuous risk assessments for their business units/functions.
B. Identifying, managing and reporting of risk within their area of responsibility.
C. Updating and overseeing the management and maintenance of risk register(s) for their area of responsibility.
D. Providing risk management updates to Executive Committee along with the CRO.
E. Monitoring and follow-up on risk treatment activities and reporting on implementation of the mitigation plans.
F. Regularly discussing questions, concerns, opportunities for improvement including training with the Risk Management Team and CRO.
G. Assisting the risk management team to prepare updates to be presented to the CRO and Exec Committee.

## 8. Risk Management Approach

In order to manage risks in a systematic manner, the Company has incorporated all elements of Enterprise Risk Management process steps as mentioned below:

### 8.1 Risk Identification

Identification of risks is performed based on internal deliberation, industry and market research, scanning the external environment and leadership inputs. The broad categories of risks include Financial, Operational, Reputational, Regulatory, Extended Enterprise, Sustainability, Strategic Technological.

### 8.2 Risk Assessment and Prioritization

Risks are assessed and classified as per the criticality for the business. This helps in prioritizing risks and deciding the right risk management strategies based on risk classifications. The process of assessment is based on two parameters - risk impact and risk likelihood. Additionally, Risk velocity is also taken into consideration in order to identify risks which require immediate attention and contingency plan. (Annexure 2).

### 8.3 Risk Response

Risk response refers to strategies targeted towards reducing the probability of occurrence and/or the impact of a risk event and is classified into mitigation plans. Risk owners are required to formulate the Risk mitigation and contingency plans for the risk identified and documented as a part of the risk register.

## 9. Communication

This Policy and any changes therein shall be communicated and approved by the Board or the Risk Management committee, as authorised by the Board.

## 10. Risk Management Framework

The Enterprise Risk Management Policy should be read with the Enterprise Risk Management Framework which provides the detailed approach to risk management to be followed with respect to risk identification, assessment, monitoring, mitigation & reporting.

## 11. Review and Amendment to the Policy

This Policy shall be reviewed at least once in two years to ensure that it is aligned with the changes in business environment and regulatory requirements. Any change in the Policy shall be approved by the Board of Directors or Risk Management Committee (as may be authorized by the Board). The Board of Directors or any of its authorized Committees shall have the right to withdraw and / or amend any part of this Policy or the entire Policy, at any time, as it deems fit, or from time to time, and the decision of the Board or its Committee in this respect shall be final and binding.

## 12. DOCUMENT CONTROL

| Sl | Version | Approved by | Effective Date | Amendment Summary |
|---|---|---|---|---|
| 1 | I | Board | January 10, 2024 | Policy Drafted |

## Annexures:

### 1. Annexure 1 - Definitions

| S. No. | Terms | Definitions |
|---|---|---|
| 1. | Enterprise Risk Management | Enterprise Risk Management is the capability that involves identifying, assessing, measuring, monitoring, and responding to risks across the enterprise in a way that is aligned with the enterprise's objectives. |
| 2. | Risk | The possibility that events will occur and affect the achievement of strategy and business objectives. |
| 3. | Risk Impact | Result or effect of an event. That may bring a range of possible impacts associated with the event. |
| 4. | Risk Likelihood | The assessment of the probability the risk will occur. However, care must be taken to avoid a recency bias |
| 5. | Risk Velocity | Risk velocity or speed of onset refers to the time it takes for a risk event to manifest itself. It is the time that passes between the occurrence of an event and the point at which the company first feels its effects. |
| 6. | Risk Score | The combined product of risk likelihood and risk impact |
| 7. | Risk Response | A process of determining the strategy for responding to risks, developing, and implementing risk treatment plans & assigning risk owners for each risk; |
| 8 | Risk Register | Compendium of all risks finalized including risk definition, key risk Indicator, risk mitigation and risk owner |
| 9 | Key Risk Indicators | To timely identify, measure and respond to risks, KRI are specific metrics (qualitative or quantitative) that provide early warnings or signals of potential risks e.g., CSAT score, Data security incidence etc. |
| 10 | Mitigation and Contingency plans | Strategies aimed at preventing the occurrence of risk events are called mitigation plans. Plan B (alternate plan) for risks in case of exigency conditions after the risk play is termed as contingency plans |
| 11. | Risk workshop | A risk workshop facilitates a collaborative approach to brainstorm, identify and assess key risks for the concerned unit with the inclusion of all concerned stakeholders |

## 2. Annexure 2- Risk Prioritization

**Purpose:** To have a graded view of risks and ensure a focused approach towards mitigation of risks.

**Procedure:**

- This requires grading the risk as per a two-dimensional scale: Likelihood and Impact
- Overlaying velocity of occurrence to determine prioritization.

❖ **Risk likelihood matrix:** The probability of occurrence of risk event or the risk playing out is to be graded as per risk likelihood matrix. This may require a judgemental call based on the identified causes and existing controls against the risk. However, care must be taken to avoid a recency bias.

| Likelihood | Description |
|---|---|
| Almost Certain (5) | ❖ Event expected to occur in most circumstances |
| Likely (4) | ❖ Events will probably occur in most circumstances. |
| Possible (3) | ❖ Events should occur at some time. |
| Unlikely (2) | ❖ Events could occur at some time. |
| Rare (1) | ❖ Events may occur, but only under exceptional circumstances. |

❖ **Risk impact matrix:** This refers to the quantification of risks identified including its effect on various financial, business (GMV, OPD, CSAT, BCP etc.) and regulatory metrics.

❖ **Risk score:** The product of likelihood rating and impact rating forms the risk score. Risks must be prioritized as per risk score.

❖ **Risk Velocity matrix:** As a modern risk management practice and considering the changing global business environment (incl pandemic) it is important to prioritize those risks which manifest quickly. This has led organizations to further assess and monitor the risks based on Velocity. While risk velocity does not affect the classification of risks, high-velocity indicates the need to have a well-thought-out crisis management plan in place to reduce the consequence/impact of such a risk event.

Risk velocity or speed refers to the time it takes for a risk event to manifest itself. It is the time that passes between the occurrence of an event and the point at which the company first feels its effects. Risks with high velocity (velocity of 3) should

have a rapid response to address the consequence of the impact.

| Rating | Description | Definition |
|---|---|---|
| 3 | **High** | Very rapid Onset, little or no warning, instantaneous from event to impact |
| 2 | Medium | Onset occurs in a matter of weeks to a quarter from event to impact |
| | Low | Very slow onset, occurs over a quarter or more from event to impact |