# RISK MANAGEMENT POLICY

## Route Mobile Limited

*POLICY EFFECTIVE FROM JANUARY 11, 2019*

*FIRST AMENDMENT EFFECTIVE FROM JULY 28, 2021*

*SECOND AMENDMENT EFFECTIVE FROM SEPTEMBER 20, 2025*

# CONTENTS

# 1. Introduction

## 1.1 Route Mobile

Route Mobile Limited is a listed entity, with its registered and corporate office located in SanRaj Corporate Park - 4th Dimension, Mind Space, Malad (West), Mumbai – 400 064, India. The Securities and Exchange Board of India ("SEBI"), vide its Notification dated September 2, 2015, has issued the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended, ("LODR") which came into force from December 1, 2015.

The Board of Directors of Route Mobile Limited ("Company"), at its meeting held on January 11, 2019, approved this policy with regard to Risk Management Policy ("Policy"). The policy was further amended pursuant to Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) (Second Amendment) Regulations, 2021 which came into effect from May 5, 2021. The policy was subsequently revised and updated to align with the ISO 31000 Risk Management standards, effective September 20, 2025.

## 1.2 Risk Management

Risk management is an attempt to identify and then manage threats that could severely impact or bringdown the organization in terms of turnover, market share, goodwill, profitability, competition, technology obsolescence, investments, human resources and such other factors.

Route Mobile defines **risk** as "**the effect of uncertainty on objectives**".

- An effect is a deviation from the expected. It can be positive, negative or both, and can address, create, or result in opportunities and threats.
- Objectives can have different aspects and categories and can be applied at different levels.
- Risk is usually expressed in terms of risk sources, potential events, their consequences, and their likelihood.

**Risk management** is the **systematic approach to proactively identify, assess, and mitigate potential risks and uncertainties**.

The purpose of risk management is to enable the management to **make informed strategic and operational decisions**, based on best available information, and **allocate resources accordingly** to safeguard the stakeholders' interests.

Risk management requires individuals and teams within an organization to take accountability for identifying and managing risks within their areas of expertise, preventing costly disruptions, maintaining continuity, etc.

## 1.3 Policy objectives

1. **Establish an integrated risk management framework** for identifying, assessing, treating, monitoring, and reporting of risk and promote the use of common methods throughout the organization based on appropriate standards.
2. **Ensure all material risks of the company are identified, analyzed, appropriately mitigated, and managed** to avoid bad surprises and capitalize on opportunities.
3. **Embed risk management into the culture** of Route Mobile, integrate risk management into policy, planning and informed decision making at all levels of the organization.
4. **Instil confidence in regulators, customers, and other stakeholders** regarding its adherence to relevant laws, regulations, and industry standards.

### 1.3.1 Scope and extent of policy application

The framework and methodology described in this document defines a common ground which should be **applied in all domains of activity and in all entities within Route Mobile** and defines the **minimum required risk management activities** for all domains.

This iteration of the policy focuses on development of a common understanding of **risk terminology** and **aligning on risk process and methods** used for its implementation.

This policy will operate **in conjunction with other domain policies which may include domain-specific risk management requirements.** These domain-specific risk management requirements will be described in the respective domain risk policies (e.g., Cyber Security Risk Management Methodology).

# 2. Risk management framework

## 2.1 Organization

### 2.1.1 The three lines model

Governance at Route Mobile includes risk management, internal control, and assurance activities. The **organizational structure is aligned with the IIA's Three Line Model**[1].

### 2.1.2 Risk management governing bodies at Route Mobile

#### Board of Directors

- Responsible for framing, implementing and monitoring the risk management plan
- Be informed about risk assessment and minimization procedures
- Responsible for constituting a Risk Management Committee
- Define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit such function shall specifically cover cyber security

#### Audit Committee (ACC)

- Evaluates internal financial controls and risk management systems

#### Risk Management Committee

- Formulate a detailed risk management policy 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.
- Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;
- Monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;
- Periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;
- Keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken;
- The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee;
- Seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

[1] https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf

### 2.1.3 Risk management responsibilities at Route Mobile

#### Route Mobile Leadership Team (RLT) members

RLT members hold direct responsibility for critical decision-making regarding risk acceptance, approval of mitigation plans, and ensuring significant risks are identified and communicated. They are responsible for both first- and second-line activities when it comes to Risk Management. As such they must ensure risk management is effectively integrated into daily operations while maintaining oversight at higher levels. Operational aspects of risk management, including the implementation of risk plans, conducting assessments, and monitoring mitigation actions, can be delegated to appropriate team members.

Responsibilities for RLT:

- Define and implement a risk management plan within their responsibility domain.
- Ensure risk assessments are conducted systematically, aligning with organizational standards, and facilitating collaboration among relevant stakeholders.
- Make decisions regarding the treatment and mitigation of the risk within the risk appetite (e.g. accepting risks and approve mitigation plans).
- Ensure necessary resources and support to ensure control activities and risk mitigating actions are carried out effectively and in a timely manner. Follow-up on risk mitigation actions.
- Report all significant risks, potential deviations from expected performance, or uncertainties that could impact the organization materially to the CEO to seek advice and guidance on appropriate mitigating measures and actions to be taken.
- Ensure root cause analyses are performed for major incidents.
- Ensure maintenance of the risk register for their domain.
- Encourage good risk management practices in their teams.

#### All staff

For risk management to be effective, it requires the co-operation of all staff to

- identifying emerging risks within their areas of responsibility and reporting them through the appropriate hierarchical channels or other designated reporting mechanisms.
- Provide guidance on, contribute to and report on the implementation of mitigation actions.

### 2.1.4 Risk management at Route Mobile subsidiaries

The framework described in this document applies for all Route Mobile subsidiaries. Depending on the size of the subsidiary, the above-described governance bodies and roles assigned should be implemented to a maximum extent within the subsidiary's organization, although we acknowledge that for smaller organizations some of the roles/governance bodies might be bundled.

We define the following subsidiaries, based on the nature of their activities, their regulatory environment, the complexity of its operations, or the extent of its exposure to external events.

- RML UK, Routesms Solutions FZE, Mr Messaging-UAE, Masivian, 365Squared, Malta.

General guidelines for risk management in the subsidiaries:

The CEOs or Managing Director (MD) of the subsidiary will by default be responsible for overseeing the risk management process within the subsidiary. A CEO/MD can appoint a dedicated risk SPOC within the subsidiary's organization. In case a dedicated SPOC is appointed, he/she reports risk findings directly to the subsidiary's management team.

Subsidiaries are expected to report significant risks through the established Group risk reporting channels on a regular basis, at least annually, and must immediately escalate any emerging or critical risks to the appropriate Group functions.

# 3. Risk management process and methods

The risk management process used within Route Mobile should be aligned with the guidelines set forth in "ISO 31000: 2018 – Risk Management Guidelines".

The risk management process and methods outlined in this document serve as the overarching framework for all risk management activities across Route Mobile and its subsidiaries. They establish the minimum standards to be followed—such as the use of a common risk rating scale—and provide a consistent foundation for risk-related practices. Upholding key risk management principles is essential, including clear understanding of risks, accountability at all levels, and the ability to apply the process consistently and repeatably.

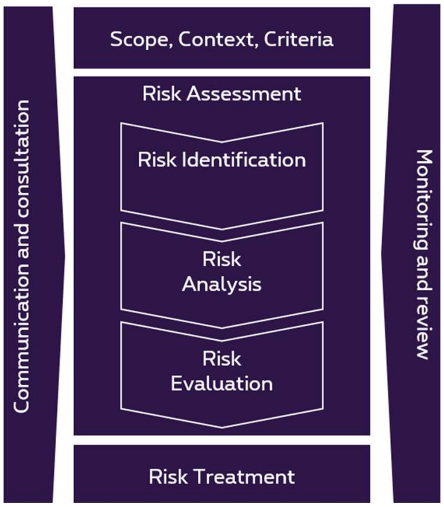
Any governance domain may modify or depart from this methodology to address unique requirements or stakeholder expectations (e.g., specific risk rating levels). Such domain-specific approaches will be outlined in their respective policies (e.g., Cyber Security Risk Management Policy).

As part of the Route Mobile's approach to risk mitigation, business continuity plans (BCPs) are maintained to ensure the timely recovery of critical operations in the event of significant disruptions. The BCP framework is embedded within the risk management process and undergoes regular review, testing, and enhancement under the supervision of the Risk Management Committee. Route Mobile has established IT services and Business Continuity/Disaster Recovery plans to maintain the highest possible service levels for uninterrupted message delivery, enable rapid recovery from disruptions, and reduce both the likelihood and impact of potential interruptions.

## 3.1 Process overview

The main steps are:

1. Setting scope, context and criteria: define how the level of risk is determined and select the appropriate risk assessment tools and techniques.
2. Risk identification: for every risk domain, identify risks that could have an adverse (or beneficial) impact on value drivers, achievement of objectives or protection of assets.
3. Risk analysis: analyze and document the potential causes and consequences for the prioritized risk scenarios and express impact and likelihood.
4. Risk evaluation: rank and prioritize risks, make formal decisions on risk response, whether risks are acceptable or need complementary treatment.
5. Risk treatment: identify complementary measures to reduce risks and create action plans. Assign clear ownership for their execution.
6. Monitor and review: follow-up on open risk mitigating action points. Review risks periodically or when context changes.
7. Communicate and consult: bring different areas of expertise together for each step of the risk management process to build a sense of inclusiveness and ownership among those affected by risk. Report risks to relevant stakeholders.



Consider that a risk assessment is a collaborative exercise. When planning the risk assessment, identify all relevant internal and stakeholders; those that need to be consulted and/or informed and those that will participate in the assessment.

## 3.2 Process steps

### 3.2.1 Risk assessment

The risk assessment phase should have as output:

- A risk inventory or register with a list of relevant, described in a comprehensible way.
- Risk assessment documentation containing detailed analysis of prioritized risks.
- Risk treatment plans documenting risk mitigation actions, responsibilities, timelines, and success indicators.
- Risk communication and reporting containing risk assessment findings, key insights to stakeholders, management, and relevant decision-makers through reports, presentations, or dashboards.

#### Risk identification

The objective is to identify potential risks and capture related information in a structured way that will enable further analysis of the likelihood and consequences. Examining all sources of risk and the perspective of all stakeholders.

#### Risk analysis

The risk analysis is the process to comprehend the nature of risk and to determine the level of risk by understanding the sources and causes of the identified risks; studying probabilities and consequences given the existing controls, to identify the level of residual risk.

The risk analysis provides the basis for risk evaluation and decisions about risk treatment. It involves the development of understanding of the risk, consideration of the causes and risk sources, their positive and negative consequences, the likelihood that those consequences can occur, provides an input to risk evaluation and decision whether risks need to be treated, and on the most appropriate risk treatment strategies and methods.

Wherever feasible, risks should be assessed using quantitative analysis methods—such as statistical modeling, correlation analysis, regression techniques, Monte Carlo simulations, Value at Risk, or reliability engineering—to enable data-driven decision-making.

When quantitative analysis is not practical due to limited data, time, or resources, a qualitative assessment using predefined scales (e.g., Very high, high, Medium, Low, Very low) should be applied as an alternative. Qualitative analysis may also be used for preliminary risk screening before a more detailed evaluation.

#### Risk Evaluation

The level of risk (the “risk rating”) is defined by the relationship between the impact (of the consequences) and the likelihood (of the causes). We distinguish between:

- **Inherent risk:** The level of risk that exists before any controls or risk treatments are applied. It reflects the natural level of risk associated with an activity, process, or asset—assuming no risk management measures are in place.
- **initial residual risk**: The level of risk that considers a baseline environment—assuming some foundational or minimum controls are always present (e.g., industry-standard practices, effective policies, etc.).
- **Residual Risk**: The level of risk that remains after controls or risk treatments have been applied. The risk that an organization chooses to retain because it is within the risk appetite, or because it is impractical or too costly to eliminate entirely.

  The residual risk considers the effectiveness of controls. If there is more than one control linked to the risk, the aggregated control effectiveness score is calculated.

| Control effectiveness | Description |
|---|---|
| Effective | Allows effective management of the risk and reduces the impact or the likelihood of the risk. |
| Partially Effective | Allow effective management of the risk, thereby partially reducing the likelihood or impact of the risk. However, there are opportunities for improving the control to reduce further the residual risk. |
| Ineffective | Does not allow effective management of the risk, there is no reduction in the likelihood or impact of the risk. Under high-stress conditions, it is not expected to be effective in detecting/avoiding failures. |

After completing control effectiveness scoring, the residual risk value can be identified by using lookup matrix between inherent risk assessment and control effectiveness below:

| Inherent Likelihood or Impact | Control Effectiveness | Residual Likelihood or Impact |
|---|---|---|
| 🟥 Very High | Effective | 🟨 Moderate |
| 🟥 Very High | Partially Effective | 🟧 High |
| 🟥 Very High | Ineffective | 🟥 Very High |
| 🟧 High Risk | Effective | 🟩 Low Risk |
| 🟧 High Risk | Partially Effective | 🟨 Moderate |
| 🟧 High Risk | Ineffective | 🟧 High Risk |
| 🟨 Moderate | Effective | 🟩 Very Low |
| 🟨 Moderate | Partially Effective | 🟩 Low Risk |
| 🟨 Moderate | Ineffective | 🟨 Moderate |
| 🟩 Low Risk | Effective | 🟩 Very Low |
| 🟩 Low Risk | Partially Effective | 🟩 Very Low |
| 🟩 Low Risk | Ineffective | 🟩 Low Risk |
| 🟩 Very Low | Effective | 🟩 Very Low |
| 🟩 Very Low | Partially Effective | 🟩 Very Low |
| 🟩 Very Low | Ineffective | 🟩 Very Low |

### 3.2.2 Risk treatment

Decisions on how to treat identified risks must be made at the appropriate management level. These decisions should align with the organization's risk appetite and aim to strike a balance between the level of risk and the cost or effort required to mitigate it.

The following are the available risk treatment options:

- Mitigate – reduce the risk through remediation plans
- Transfer – shift the risk through insurance or other mechanisms
- Retain – accept the risk, typically when it falls within tolerance
- Avoid – eliminate the risk by discontinuing the activity or changing the approach

#### Risk mitigation

Identify and apply actions that reduce the threats, vulnerabilities and impacts of a given risk to an acceptable level. Possible actions are:

- Reduce the probability of occurrence or the likelihood a risk materializes or succeeds.
- Limit potential loss by decreasing the amount of damage and liability.

As part of the risk treatment process, one or more action plans shall be developed to address each identified risk. These plans should outline the specific measures to be taken to reduce the risk by decreasing its likelihood, its consequences, or both.

The selection of treatment options should be based on a cost-benefit analysis, the level of risk, and the organization's risk criteria. For each action plan, a target completion date shall be defined in proportion to the urgency and severity of the risk.

Each treatment plan must be clearly documented, assigned to a responsible owner, and monitored to ensure effective implementation and accountability in line with the organization's overall risk management framework.

#### Risk transfer

Risk transfer involves shifting the consequences of a risk, and in some cases the responsibility for specific risk responses, to a third party. Common methods include insurance, outsourcing of services or processes, and contractual arrangements such as indemnity clauses or service level agreements.

Risk transfer can be applied to a variety of risks—not only financial, but also operational, legal, or reputational. However, it is important to note that the organization retains overall accountability for the risk. Transferring risk does not eliminate the need to identify, assess, and monitor the risk as part of the organization's risk management framework.

#### Risk retention (risk acceptance)

Risk retention—also referred to as risk acceptance—is an appropriate risk treatment option when the cost of mitigation exceeds the potential benefits, or when no effective treatment options are available (e.g., the risk falls outside the organization's span of control). In such cases, the organization deliberately chooses to retain the risk while continuing to monitor it.

Retaining a risk contributes to the organization's overall risk exposure. Therefore, depending on the level of potential impact, risk retention must be approved by the appropriate level of management—particularly the leadership of the affected entity (e.g., legal entity, division, or business unit).

Risk retention may take two forms:

- Unconditional retention: The risk is accepted as-is, with no immediate plans for further treatment.
- Conditional or temporary retention: The risk is accepted under specific conditions or for a defined period. In such cases, the risk must be reviewed at least every six months, or sooner if there are significant changes in context or exposure.

All retained risks shall be subject to periodic review to ensure they remain within acceptable risk levels and continue to align with the organization's risk appetite and strategic objectives.

All risk retention decisions must align with the organization's Risk Acceptance Criteria outlined in the Risk Framework. These criteria define the necessary approval levels based on residual risk and potential impact, ensuring that accountability matches the severity of potential outcomes and adheres to the organization's governance structure.

#### Risk avoidance

Eliminate the risk entirely by discontinuing the associated activity or altering plans to remove exposure. Consider this option when risk exceeds acceptable thresholds and cannot be mitigated to an acceptable level.

### 3.2.3 Risk register

The risk register supports the whole tracking and risk treatment process. The risk register is part of the risk management plan and should contain all information about each identified risk, such as the nature of that risk, level of impact risk, who owns it and what are/ is the risk response mitigation measures in place to respond to it.

Goals of the risk register

- Evaluate the risks, take decisions on the response, eyes wide open, at the appropriate level in the organization.
- Ensure ownership of risk and risk mitigation action plans.
- Monitor and review risks periodically.
- Promote awareness and understanding of risks.

Risk register elements include,

- Risk ID
- Risk level
- Risk description
- Risk control measures in place
- Risk likelihood
- Risk impact
- Response type (Mitigate, Transfer, Accept or Avoid)
- Response description
- Risk owner
- Risk mitigation plan owner
- Status

## 3.3 Risk monitoring, reporting, communication

An important component of the risk management life cycle is continuously monitoring, evaluating, assessing, reporting risk and keeping the risk register (status) up-to date is the primary role of the risk owner. The results and status of this on-going activity need to be documented and reported to senior management and the appropriate governance bodies. The results of these activities might serve as an input to reassess risks.

Monitoring contains many activities including tracking new external risk factors, following up status of risks, controls, exceptions, and treatments.

Risk communication has the following goals:

- Raise awareness among all stakeholders, internal and external, regarding risk management.
- Ensure the views and experience from the different stakeholders and organizational structures involved is collected.
- Ensure prompt notification of risk events to those responsible; and
- Contribute to the continuous improvement of the risk management program.

****************