

# **RISK MANAGEMENT**

## **POLICY**

## 1. Purpose

The purpose of this Risk Management Policy is to provide a structured and proactive approach to identifying, assessing, mitigating, and monitoring risks that could impact **VeeFin Solutions Limited's** ability to achieve its strategic and operational objectives. As a global leader in **Digital Supply Chain Finance (SCF)** and **Lending Solutions**, operating in a dynamic fintech landscape, VeeFin is committed to safeguarding its technological assets, customer trust, reputation, and shareholder value. This policy underpins VeeFin's commitment to sustainable growth, technological excellence, and regulatory compliance.

## 2. Scope

This policy applies to all business units, departments, employees, and functions of **VeeFin Solutions Limited**, across all geographies where the company operates. It encompasses a broad spectrum of risks including, but not limited to:

- Financial Risk
- Technological & Operational Risk
- Regulatory & Compliance Risk
- Strategic & Market Risk
- Reputational Risk
- Cybersecurity Risk

Given VeeFin's focus on scalable, white-labelled digital platforms and mission-critical infrastructure for clients, particular attention is placed on **technology and data security risks**, as well as **client delivery and service continuity**.

## 3. Objectives

- To **proactively identify and assess** risks that may impact business continuity, client delivery, and growth.
- To implement **robust mitigation strategies** ensuring technology resilience, data security, and client satisfaction.
- To embed **risk awareness into corporate culture**, empowering all employees to act as custodians of risk.
- To **regularly report, review, and update** risk responses in alignment with business strategy and external changes.

#### 4. Risk Management Framework

Veefin adopts an **enterprise-wide risk management (ERM)** approach to ensure alignment with global best practices and fintech regulatory standards.

##### a. Risk Identification:

Risks are identified through internal audits, stakeholder consultations, regulatory monitoring, market intelligence, and feedback from clients and partners.

##### b. Risk Assessment:

Each risk is evaluated on likelihood, impact, velocity, and control effectiveness. This includes cyber threat analysis, platform scalability reviews, and compliance readiness.

##### c. Risk Mitigation:

Control measures, technology upgrades, business continuity planning (BCP), and crisis response protocols are developed and maintained for key risks.

##### d. Risk Monitoring:

A continuous monitoring process using internal dashboards, governance reviews, and audit reports tracks the effectiveness of controls and risk exposure.

##### e. Risk Reporting:

Risk-related insights are periodically reported to the **Board of Directors**, with urgent issues escalated immediately through a predefined risk escalation matrix.

#### 5. Key Risk Areas Identified

The Board recognizes the following key risks, relevant to Veefin's fintech-led, platform-driven operating model:

- **Technology & Cybersecurity Risk:** Vulnerabilities in infrastructure, data breaches, downtime affecting client operations.
- **Market & Strategic Risk:** Shifts in financial services demand, evolving client expectations, new entrants and innovation cycles.
- **Operational Risk:** Platform delivery issues, third-party integrations, process failures, or talent attrition.
- **Financial Risk:** Credit exposure, delayed receivables from clients, FX volatility due to global operations.

- **Compliance & Regulatory Risk:** Changing fintech regulations (RBI, SEBI, global fintech norms), GDPR compliance, data localization rules.
- **Reputational Risk:** Loss of trust due to service disruption, compliance failures, or negative media attention.

## 6. Board's View on Risk to Company Continuity

The **Board of Directors** of Veefin Solutions Limited conducts periodic reviews of risk exposure and mitigation effectiveness. Based on the current assessment, **there are no identified risks that pose a threat to the continued existence** of the company. However, the Board remains vigilant given the fast-evolving fintech ecosystem, and is committed to proactive and dynamic risk management to safeguard the company's mission and stakeholders.

## 7. Roles and Responsibilities

- **Board of Directors:**  
Provide strategic oversight and approve the Risk Management Policy. Review material risks and mitigation effectiveness.
- **Executive Management:**  
Own implementation of the risk management framework. Allocate resources, lead mitigation plans, and ensure reporting to the Board.
- **Chief Technology Officer & CISO:**  
Lead identification and management of cybersecurity and platform risks, ensure compliance with security standards, and implement best practices in data governance.
- **Risk Management Committee:**  
Operationalize risk strategy, conduct regular assessments, coordinate with business units, and maintain the risk register.
- **All Employees:**  
Adhere to policies, participate in training, and promptly report risk events or concerns through established communication channels.

## 8. Policy Review

This policy will be **reviewed annually**, or more frequently as required, to ensure continued relevance in light of internal developments, technological changes, and regulatory updates. Recommendations for updates will be presented to the Board for approval.