RISK MANAGEMENT POLICY

OF

NAVI TECHNOLOGIES LIMITED

Version No	2.0
Originally adopted Date of Policy	March 06, 2022
Amended / Modified Date of Policy	June 16, 2025
Policy owner	Risk Management Department
Approved by	Board of Directors
Signature	Sd/-

Table of Contents

1. Policy Statement

This Risk Management Policy ("the Policy") establishes the risk governance principles, structures, and processes applicable to Navi Technologies Limited (hereinafter referred to as "the Company" or Navi" or "NTL") in its roles as:

- A **Third-Party Application Provider (TPAP)** under UPI/NPCI framework
- A **technology infrastructure and service provider** to its regulated subsidiaries engaged in NBFC, AMC, and General Insurance operations

The Company recognizes that a sound risk management framework is essential to protect its systems, people, operations, and reputation, especially given its critical role in supporting regulated financial institutions and operations in the payments industry.

2. Objectives

The key objectives of this Policy, based on the underlying principles of risk management, are as listed below:

- Enhance stakeholder value by pinpointing critical events and risks affecting the Company's business goals and strategies.
- Proactively recognize and address internal and external risks that could disrupt operations or the delivery of secure and compliant technology services.
- Ensure compliance with applicable[1] NPCI's TPAP guidelines, RBI's cyber security guidelines, and leading IT risk governance practices.
- Establish clear control responsibilities while upholding operational independence between the Company and its regulated subsidiaries.
- Maintain high availability, confidentiality, integrity, and resilience for all vital systems and data environments.

[1] It is noted that these guidelines will need to be reviewed to identify the latest circulars / notices / master directions from the regulators as applicable for the Company.

3. Scope

This Policy is applicable to:

- All departments and employees of the Company.
- All technology platforms and systems owned or managed by the Company.
- All services provided to external stakeholders, including:
    - UPI and other payment services offered as a TPAP.
    - Hosting and technology support provided to regulated subsidiaries.
- All contractors, consultants, and vendors involved in service delivery.

This Policy excludes internal risk management frameworks of subsidiary companies, though it governs risks related to infrastructure, data, and systems operated on their behalf by the Company.

4. Risk Governance Structure

The Risk Management Framework, as part of this Policy, shall provide for comprehensive governance identifying the structure, charter, roles and responsibilities of key departments, Committees or specific personnel.

The governance structures shall enable oversight on various risks and allow for bubbling up of risks to the right level of leadership. The Audit Committee may provide oversight and review the Risk Management Policy from time to time.

Personnel / Department / Committee	Responsibility
Board of Directors	Oversight of enterprise risk strategy and policy approval

Personnel / Department / Committee	Responsibility
Audit Committee of the Board	Provide the Board with assurance and oversight regarding the effectiveness of the Risk Management Policy.
Risk Management Department	• Implement risk programs, conduct risk assessments, and report any critical risks. • Oversee, review, and escalate significant risk incidents to Senior Management & the Board
Head, Technology	Evaluation of technology risks, assessment of security posture, and development of infrastructure resilience strategies.
Head, Information Security	Adherence to cybersecurity, data privacy regulations, and regulatory security compliance.
Business Unit Heads	Oversight of risk management pertaining to individual operational areas.
Internal Audit	Conduct periodic oversight and review of the risk management policy

5. Risk Categories

To mitigate operational, technological, cybersecurity, compliance, third-party, and reputational risks, thereby ensuring stakeholder confidence and regulatory adherence, the Company shall implement a suite of risk management strategies.

These shall comprise Standard Operating Procedures (as appropriate), audits, rigorous access controls, compliance monitoring, vendor risk management, and crisis communication protocols. In accordance with its operational directives, the Company has identified critical risks and shall adopt appropriate, independent policies (where required) and procedures.

S. No	Risk Type	Definition	Mitigation Strategies
1	Operational Risk	• Process failures impacting service delivery (e.g., change mismanagement) • Inadequate internal controls • Errors in deployment of patches, APIs, or version upgrades	• SOPs for incident response and change management • Automated testing and rollback procedures • Periodic internal audits
2	Liquidity Risk	• Inability to repay external obligations • Insufficiency of funds for the purpose of operational expenses, and commitments to external parties • Lack of liquidity to support operations within Group subsidiaries	• Active liquidity monitoring, with alerts defined for early warnings of stress • Establishing liquidity buffers to help plan for contingencies
3	Technology Risk	• System downtime or platform unavailability • Legacy systems and infrastructure bottlenecks • Lack of redundancy in critical environments	• Load balancing, and real-time monitoring • Defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) • Cloud-native architectures and containerized deployments
4	Cybersecurity Risk	• Unauthorized system access • Data breaches or leaks • Malware, ransomware, DDoS attacks	• Role-based access, MFA, and log monitoring (SIEM)

S. No	Risk Type	Definition	Mitigation Strategies
			• Regular VAPT[2], patch management, endpoint protection • Employee awareness and phishing simulation
5	Compliance & Regulatory Risks	• Non-compliance with applicable NPCI TPAP guidelines, RBI circulars • Data localization breaches • Inadequate audit trails or log retention	• Regulatory compliance calendar and monitoring tools • Internal reviews of compliance to security and IT requirements
6	Third-Party Vendor Risk	• SLA breaches by infrastructure partners • Insecure third-party libraries or APIs • Poor onboarding of vendors without due diligence	• Vendor risk management processes • Contracts with SLA & indemnity clauses • Continuous monitoring of third-party integrations
7	Reputational Risk	• Incidents affecting the trust of PSP banks, subsidiaries, or end-users • Mismanagement of public relations in times of breach or failure	• Crisis communication protocol • Incident response team coordination with PR / Legal • Proactive stakeholder updates and transparency
8	Fraud Risk and AML	• Account takeover or identity fraud • Use of fake or dormant KYC accounts	• Customer Due Diligence (CDD) & KYC Controls

[2] Vulnerability Assessment and Penetration Testing

S. No	Risk Type	Definition	Mitigation Strategies
		• Use of platform for layering (e.g. rapid pass-through transactions) • Use of mule accounts for fund movement	• AI/ML rules to detect and block suspected mule accounts • Conduct regular AML program reviews and gap assessments.

6. TPAP - Specific Risk Framework

As a Third-Party Application Provider (TPAP), the Company is required to:

- Adhere to all operational and technical guidelines issued by the National Payments Corporation of India (NPCI).
- Create and maintain secure integration channels with Payment Service Provider (PSP) banks.
- Track and analyze failed transaction rates and system downtime logs.
- Implement tokenization, secure customer onboarding processes (including Know Your Customer (KYC) verification and device binding), and robust payment authentication procedures.
- Conduct daily reconciliation with PSPs and resolve disputes in a timely manner.

7. Technology Services to Subsidiaries

The Company mandates the following to ensure risk and compliance, even though subsidiaries are responsible for their own risk and compliance management:

- Infrastructure must be logically and physically segregated between business entities.
- Access controls must prevent cross-entity privilege elevation.
- Each platform/service must have defined SLAs and uptime commitments.
- Subsidiaries must conduct pre-deployment UAT as part of change management processes.

- Incident reporting and resolution timelines must be mapped according to severity.

8. Risk Identification & Assessment Process

A. Risk Identification

The purpose of risk identification is to identify internal and external risks specifically faced by the Company, and identify all other events that can have an adverse impact on the achievement of the business objectives.

B. Risk Assessment and Control

On a periodic basis risk, external and internal risk factors shall be assessed by the Business and Controls Functions (Risk, Technology, Infosec, Compliance and Internal Audit) across the Company. The risks that are identified in Section 5, 6 & 7 shall be assessed and formally reported through mechanisms such as operation reviews. Internal control is exercised through policies and systems to ensure timely availability of information that facilitate risk management.

C. Risk Mitigation

All identified Risks should be mitigated using any of the following risk mitigation plan:

a. Risk avoidance: Risk avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed.
b. Risk transfer: Mitigation by having another party to accept the risk, either partially or totally, typically by contract or by hedging / Insurance.
c. Risk reduction: Employing methods / solutions that reduce the severity of the loss.
d. Risk retention: Accepting the loss when it occurs. Risk retention is a viable strategy for minor risks where the cost of insuring against the risk would be greater than the total losses sustained. All risks that are not avoided or transferred are retained by default.

9. Limitation, Amendment and Effective Date

In the event of any conflict between the provisions of this Policy and of applicable regulatory guidelines or any other statutory enactments, rules, the provisions of such regulatory guidelines or statutory enactments, rules shall prevail over this policy.

Any subsequent amendment / modification in the regulatory guidelines and/or applicable laws in this regard shall automatically apply to this Policy.

10. Communication of this Policy

This Policy shall be posted on the website of the Company i.e. www.navi.com.

11. Review of this Policy

This Policy shall be reviewed at least on an annual basis or as warranted, by considering the changing industry dynamics and evolving complexity.