TRANSCORP INTERNATIONAL LIMITED

Risk Management Policy

Updated as on May' 2024

Table of Contents

I. Overview

Transcorp International Limited ("the Company" or "Transcorp" or "TIL"), is a Company incorporated under the Companies Act 1956 with its registered office at Jaipur, Rajasthan. The Company is a licensed Prepaid Payment Instruments (PPI) issuer under the RBI's Master Directions on PPIs ("PPI Master Directions"), as updated from time to time, and is authorized to issue co-branded cards to its customers.

Under the PPI Master Directions, every company is required to lay down a detailed risk management policy duly approved by the Board of Directors ("Board"). This policy overarchingly prescribes the risk management mechanisms that the Company may use in identification, assessment, mitigation, and monitoring the identified risks arising from the operation of its business.

To meet challenges of fraud and ensure customer protection, the Board has adopted this Risk Management Policy ("Policy") which will be applicable at all levels.

II. Objectives

This Policy aims to safeguard the Company from the ever-evolving risks arising out of the business it operates in and the various risks associated with it. To this front, the Policy is formulated with the objective outlining its approach to identifying, assessing, mitigating and monitoring risks. This Policy aims to help ensure that the Company operates in a structured and proactive manner, making informed decisions to protect its stakeholders and assets, and achieve its objectives by:

- Establishing and implementing this company-wide robust and comprehensive risk management policy
- Ensuring compliance with all relevant laws, regulations, and industry best standards to mitigate compliance-related risks
- Allocating financial, human, technological, and other relevant resources to effectively manage and mitigate risks by efficiently coordinating between them
- Establishing mechanisms for continuous monitoring of current and expected risk indicators and exposures in the Company
- Ensuring that these risks are identified, reported, evaluated, analyzed, and mitigated in a timely manner
- Helping the relevant decision-makers of the Company to develop a response plan for managing risks when they materialize, to minimize their impact
- Fostering a risk-aware culture within the organization where employees at all levels understand their role in risk management

III. Definitions

For the purpose of this Policy, the following terms may be defined to mean:

a. **"Customer"** means the individual or the end user who has availed the PPI issued by Transcorp for purchase of goods and services.
b. **"Merchant"** means individuals or legal entities with whom either the Company has entered into a contract directly to accept the PPI issued by the Company against the sale of goods and services, financial services, etc. or entities who have been on-boarded by the card networks with whom Transcorp has tied up.
c. **"Agent"** means the entities who, on behalf of Transcorp, facilitate loading/reloading of PPI issued by Transcorp and/or, help distribute PPIs to the customers and/or authenticate customer's identity via biometric devices provided by the Company.
d. **"User"** includes Customer, Merchants, and Agents.

IV. Key Roles and Responsibilities

The Board, Risk Management Committee, Risk Head and Risk Management Team of the Company will have designated roles and responsibilities and will comprise of the following:

a. Board

The Board plays a crucial role in overseeing and shaping the Company's risk management policy. The Board will be responsible in setting the strategic direction, establishing a risk governance framework, and ensuring that risks are appropriately managed across the Company.

To ensure this, the Board will define and delegate the roles and responsibilities across the Risk Management Team to monitor and review the risk management plan and such other functions as it may deem fit.

In addition to the above, the Board will perform the following duties to maintain effective governance and risk oversight:

- Review the business plan at regular intervals and develop the Risk Management Strategy
- Recommend and approve the annual budget and policies
- Establish a risk governance framework that includes policies, procedures, and risk management guidelines
- Allocate resources, including budget and personnel, to support effective risk management activities
- Approve financial, Company-wide procedures and Internal Control measures and all relevant frameworks covering various nature of risks detailed in Para V below

- Approve Compliance Risk Management framework ensuring that the Company is compliant with all relevant laws, regulations, and industry standards related to risk management and governance
- Receive regular and comprehensive risk reports from management, providing insight into the Company's risk profile, key risk indicators, and risk mitigation progress
- If applicable, appoint and oversee the activities of the audit committee, which plays a role in reviewing internal controls, financial reporting, and risk management processes
- Approve the action plan and guidelines before communication to the personnel for implementation.
- Communicate Risk Management Strategy to various levels of management for effective implementation
- Periodically review, update and approve the Company's risk management policies and procedures to reflect changing risks and regulatory requirements.

b. Risk Head

- Lead the Risk Committee to ensure smooth functioning of all activities
- Oversee the functioning of the Risk Management Team
- Formulate Risk Categorization Levels (High, Medium or Low)
- Undertake periodic performance reviews of the risk team members, including the Risk Manager and the Risk Team
- Ensuring that appropriate mechanisms are in place to ensure efficiency in risk operations of the Company
- Undertake continuous review of the process and procedures for identifying, assessing, mitigating and monitoring of risks.

c. Risk Management Team

The Risk Head will have, as its team, 2 or more employees of the Company who will work in the capacity of Risk Team Members. These employees will be responsible for the following:

- Identification assessment, aggregation, reporting, and monitoring of risk in a timely manner
- Categorize Users under the relevant Risk Categorization Levels (High, Medium or Low) based on the recognized risk parameters
- Recognizing possible risks and reporting/ escalating these risks to the Risk Head
- Implementing the risk mitigation measures as laid out by the Risk Head and the Board
- Undertaking any other tasks or responsibilities as assigned from time to time by the Risk Head.

V. Risk Management Framework

The risk management framework not only defines the Company's readiness towards dealing with various risks arising from its operations but also associated with the business involves review of operations, identifying the risks an organization is subject to, deciding how to manage it, implementing the management technique, measuring the ongoing effectiveness of management and taking appropriate correction action

a. Risk Identification

Risk identification is the process of identifying, documenting, and understanding potential risks and uncertainties that may affect an organization's objectives, operations, projects, or initiatives. To identify the Company's exposure to uncertainty arising from its PPI operations, the Company has to document the below for each of the process / functions of the Company:

- Determining whether and which internal or external drivers may cause risk to the Company;
- An indicator or event that will cause a risk to occur;
- Whether the risk is operational, regulatory, fraud, etc., and the areas of its impact;
- Determining the possibility or likelihood of occurrence of a risk

Risk Identification is mandatory for all vertical and functional heads, who with the inputs from their team members, are required to report the material risks (risks which have potential to materially affect the Company's performance) to the Board along with their considered views and recommendations for risk mitigation.

b. Risk Assessment

In a business environment, there are numerous hazards to consider, where each hazard could have multiple consequences. Therefore, a risk assessment process helps in identifying potential hazards and analyze what could happen if a disaster or hazard occurs. Under this step, the Risk Team evaluates and assesses the risks based on the internal or external factors due to which such a risk occurred and whether this risk is controllable or non–controllable. For extensive assessment, the Team will deep dive by:

- Investigating into the potential triggers that led to the occurrence of the risk
- The level of magnitude of the risk
- Putting in place the existing controls to avoid/ manage such risks, if they arise
- Undertaking periodic review of the existing process and controls to ensure their adequacy

c. Risk Mitigation

Upon identification and assessment of risk, the next step is to mitigate the risk. Risk mitigation focuses on selection of remedies that can help minimise the risks that have occurred. The process entails:

- Risk Avoidance: Avoiding starting or continuing with the action that creates the risk
- Risk Transfer: Implementing measures to shift such the impact of the risks identified to an external party to mitigate any significant bearing / impact on the Company
- Risk Reduction: Optimising or reducing the likelihood of suffering loss

- Risk Acceptance: In instances where the cost of taking the risk is less than that of covering the risk, acceptance of unavoidable risks by default may be considered

The Risk Mitigation measures that will be adopted by the Company have been mentioned in the Para VII of this Policy.

d. Risk Monitoring

Risk monitoring ensures the Company's ability to control the risk while guaranteeing efficiency in the entire risk management process. For efficient risk monitoring, the following methods will be implemented:

- Regular monitoring of risk management performance
- Regular review of the Risk Management policy to evaluate its efficacy
- Review of whether this Policy is being consistently followed by the employees / staff
- Analyze deviations from the Risk Management Policy and identify the causes and factors to such deviations

VI. Categorization of Risk

Risks shall be categorised as:

e. **High Risk** - Very high risk and can put adverse effect on the business growth and even on existence of the Company

f. **Medium Risk** - Medium risk which may not have any adverse effect on the existence but may be a risk for growth of business

g. **Low Risk** - Low risk may not put any adverse effect on existence of business growth immediately but on a long term basis, may impact business operations.

VII. Types of Risks and Mitigation Measures

#	Type of Risk	Meaning	Mitigation Measures
a.	Fraud Risk	Primarily arising as a result of an organization's vulnerability to fraudulent behaviour, fraud risk is often accomplished through impersonation or forgery. Fraud risk may arise in situations where:	Fraud can take various forms, including financial fraud, internal fraud, and external fraud. Therefore, fraud risk mitigation involves implementing strategies and controls to prevent, detect, and respond to fraudulent activities within the organization. This is done by: • Putting in place a comprehensive fraud prevention framework tailored to address

#	Type of Risk	Meaning	Mitigation Measures
		• Initiation or acceptance of fraudulent transactions by any of the stakeholders • Incurrence of financial losses due to acts of any of the internal or external individual (Customers, employees, third parties, Users, etc.) • Commission of fraud on the Customer by any stakeholder, resulting in card schemes fining the Company.	the unique risks associated with gift cards also. • Implementing automated transaction monitoring systems to detect unusual or suspicious activities, such as large or unusual financial transactions, including those specific to gift card transactions, as well as procedures to prevent them from occurring again • Database upkeep to ensure the situations of previous frauds do not arise again • Creation of a strong internal fraud and transaction monitoring system with a specific focus on gift card operations. • Putting in place appropriate conflict resolution mechanisms including but not limited to gift card-related fraud incidents. • Conducting appropriate due diligence on Users to ensure their integrity and financial stability, reducing the risk of fraudulent transactions. • Conducting thorough due diligence on gift card users to ascertain their integrity and financial soundness, thereby mitigating the risk of fraudulent transactions. • Performing velocity checks on real-time/automatic basis tailored to include gift card transactions. • Providing regular training to employees on recognizing and preventing fraud. Encourage a culture of vigilance and reporting suspicious activities
b.	Financial Risk	Financial Risk is the one that is tagged to the Company's financial situation, third parties involved with the Company, and the fluctuations arising therefrom. This includes, market, liquidity, credit, valuation risk, and so on.	Financial risk mitigation involves strategies and actions taken by the Company to reduce the potential negative impacts of financial risks on their operations, investments, and overall financial health by:

#	Type of Risk	Meaning	Mitigation Measures
		Financial risk may arise due to any of the following: • Failure/ delay on part of the participating bank to deposit the daily settlement amount into the escrow account for onward payments to Merchants/Billers • Chargeback related transactions wherein the transactions are contested by the customer after the settlement is completed towards the Merchant account for card-based sales transactions • Inflationary conditions causing increase in costs of the projects, resources, etc.	• Ensuring strict compliance with escrow management and Merchant settlement protocols • Ensuring daily transaction reconciliation and follow-up on money with banks • Ensuring putting in place stringent AFA/2FA for PPI transactions (both debit and credit) • Evaluating relevant alternatives where applicable to reduce the overall project, resource, product cost to mitigate inflationary risk.
b.	Compliance Risk	Transcorp, as a regulated entity, is required to comply with extensive new and ever evolving regulations that are generally stem from overlapping information sources which makes compliance with these regulations complex, cost-heavy, and risk-intensive. Compliance risk is the risk of legal or regulatory sanctions, financial loss, or damage to reputation resulting from failure to comply with laws, regulations, or internal policies. Compliance risk arises from: • Changes in applicable regulations • Failure in adhering with the prescribed regulatory timelines, and subsequent delay in	Mitigating compliance risk is essential for the Company to avoid legal issues, financial penalties, damage to reputation, and other adverse consequences associated with non-compliance. The Company aims to mitigate this risk by: • Designating a compliance officer or team responsible for overseeing and managing compliance efforts • Identifying and comprehensively understanding all relevant laws, regulations, and industry standards as applicable to the Company's operations • Conducting regular risk assessments to identify potential compliance risks within the Company and prioritizing the activities based on intensity of risk • Making actionable regulatory updates and regularly review and update the Company's compliance program to reflect these changes

#	Type of Risk	Meaning	Mitigation Measures
		submitting reports to the regulator • Failure in complying with any changes in rules affecting the Company's operations	• Analyzing impact of changes in regulations to the business operations. • Formulate a compliance register to keep track of various obligations emanating from applicable regulations • Ensuring Compliance with regulations governing gift card operations to mitigate fraud risk and ensuring adherence to industry standards and best practices.
c.	Operational Risk	The risk of loss resulting from inadequate or failed internal processes, systems, people, or external events constitute Operational Risk. Operational Risk of the Company inter-alia includes: • Failure of core operating systems, such as IT infrastructure, security (digital & physical), and internal procedures or as a result of external causes • Inadequate reconciliation and record-keeping mechanisms • Incompetence among the Company's personnel, i.e., employees	Mitigating operational risk is crucial for organizations to ensure the continuity of their operations, protect their assets, and maintain their reputation. The Company will undertake following measures to mitigate its operational risks: • Use risk assessment techniques such as risk matrices, risk heat maps, and key risk indicators to prioritize and quantify operational risks • Develop internal strategies, governance procedures, and systems pertaining to the process to be followed by personnel, as well as maintain proper records, compliance, and so on, and guarantee adherence to the same • Provide training and awareness programs to employees to ensure they understand operational risks, compliance requirements, and the importance of adherence to policies and procedures • Conduct internal audits to review compliance with the internal process and systems • Maintain up-to-date documentation of standard operating procedures (SOPs) to guide employees in performing their tasks correctly and consistently. • The Company has adopted a risk-based approach, duly approved by their Board, in

#	Type of Risk	Meaning	Mitigation Measures
			deciding the number of Gift card instruments which can be issued to a customer, transaction limits on gift cards, etc.
d.	Technology Risk	Technology risk refers to the potential threats and vulnerabilities associated with the use of technology within the Company. These risks can have significant impacts on operations, data security, and business continuity. Technology risk includes: • Implementing new technology without proper testing • Inadequate user training for new systems • Compatibility issues when integrating new and existing systems • Non-operation and/ or redundancy of the current technological infrastructure	To ensure that the Company's IT systems and infrastructure is reliable, secure, and stable, it is essential to mitigate the technology risks by: • Keeping all software, operating systems, and applications up to date with the latest security patches and updates • Conducting regular vulnerability assessments to identify and address weaknesses in the Company's IT infrastructure • Implementing detection systems to detect and block unauthorized access attempts and suspicious activities • Educating employees about cybersecurity best practices, including how to recognize phishing emails and potential security threats • Establishing clear incident reporting procedures and a well-defined response protocol to ensure swift and effective action in the event of a security incident • Employ encryption technologies to secure sensitive data associated with PPI card transactions along with gift cards, including card numbers and customer information, to prevent unauthorized access by cybercriminals.
e.	Reputational Risk	Reputational risk arises from the damage to the Company's reputation or brand image, which can result from various factors, including poor customer service or unethical	Mitigating reputational risk is crucial for organizations as damage to reputation can lead to loss of trust, customers, investors, and revenue. The Company aims to mitigate reputational risk by:

#	Type of Risk	Meaning	Mitigation Measures
		behavior, non-compliance with applicable regulations, etc. Reputational risk generally arises when there is: • Involvement of the stakeholders of the Company in unlawful activities and/or questionable business practices that may cause them irreparable harm such as, leak of confidential information, insider trading activities, etc. • Repeated delay or deficiency in providing services • Customer dissatisfaction and negative review and/ or feedback against the Company	• Fostering and inculcating amongst its employees, a strong organizational culture centered on ethics, integrity, and responsible business practices • Prioritizing excellent customer service and satisfaction mechanisms • Monitoring social media channels for the kind of publicity that the Company gets online and respond to inquiries or issues promptly • Educating employees about the importance of their actions and behaviors in safeguarding the organization's reputation • Assessing the reputation and ethical standards of suppliers, vendors, Agents, Merchants, and business partners to ensure that their practices align with the Company's values • Continuously monitor the activities where Company's brand is involved
f.	Legal Risk	Legal risks can arise from various aspects of business operations, contracts, compliance, and more. In the day-to-day functioning of a company, it is exposed to legal action. Therefore, it needs to conduct various legal analysis, opinion and vetting of documents by the experts to examine all relevant legal aspects. Legal risk generally arises due to: • Non-review or assessment of the Rules, Procedure, Agreements & Contracts by the internal authorities appointed by the Company.	Legal risk mitigation involves strategies and actions taken by organizations to minimize their exposure to legal issues, disputes, regulatory violations, and potential legal liabilities. This is mitigated through: • Ensuring timely and accurate regulatory reporting to relevant authorities, as required by applicable regulations • Ensuring compliance with relevant regulations and industry standards governing PPI cards and gift card operations, including data protection laws and consumer protection regulations, to mitigate legal and regulatory risks associated with fraudulent activities. • Develop the Company's solutions and operations in accordance with industry norms and laws

#	Type of Risk	Meaning	Mitigation Measures
		• The Company's failure to comply with any legal agreements or contractual commitments • Legal challenges arising from unintentional/intentional operational breakdowns	• Retaining qualified legal counsel or advisors to provide guidance on legal matters and to represent the Company in legal proceedings. • Creating a system for assessing the legal ramifications of any of its company operations/activities
g.	Settlement Risk	Settlement risk, also known as counterparty risk arises from the possibility that one party in a financial transaction may not fulfill its obligation. Settlement risk arises when: • Settlement as per prescribed timeline of T+1 or T+2 days does not happen due to malfunction or downtime in the systems involved in business operations • The Customer loads money using a form factor that does not support same-day settlement (for example, a debit card) and intends to use the amount for outward payment before the inward credit is settled.	Mitigating settlement risk is essential to ensure the smooth and secure settlement of financial transactions and customer convenience. This can be undertaken by: • Using systems and settlement processes that ensure finality of settlement • Implementing real-time monitoring systems to track settlement activities and quickly identify anomalies or potential issues. • Ensuring establishment of adequate Service Level Agreements (SLAs) iterating the promised uptime as well as remedies or consequences for failure to meet the same • Putting in place a streamlined reconciliation and settlement process • Ensuring prefunding in escrow account to meet such settlement requirements.

VIII. Reporting

The Company will undertake the following reporting to the following on a quarterly basis:

a. Board of Directors
b. Risk Management Committee

IX. Review of Policy

The Policy will be reviewed annually by the Board or in the following situations:

- To incorporate any changes in applicable Laws
- To align the Policy with any major changes to Company's structure or procedures
- After any security incident or breach
- Remediate any deficiencies
- Effect changes in the overall Policy, as and when required

This Policy will be communicated to all vertical/functional heads and other concerned persons of the Company.