TOUCAN

Payment Service Operations – Governance - Risk Management

Document History

Date	Version	Prepared by	Reviewed by	Approved by
26 June 2024	1.0	Sastry Lanka	Chakrapani D	Srikanth Mopidevi

Table of Content

1. Risk Governance Framework

- **Risk Governance Structure**:
  - **Board of Directors (BoD)**: Oversee risk policies and strategies.
  - **Risk Management Committee (RMC)**: Monitor and address operational, financial, compliance, and cybersecurity risks.
  - **Internal Audit Team**: Perform regular audits of risk management policies and controls.
- **Risk Management Policies**:
  - Comprehensive policies for handling operational, financial, legal, and reputational risks.
  - Align policies with RBI guidelines, such as **Circular on Guidelines for Payment Aggregators**.

2. Risk Categorization

A. Operational Risk

- **Key Risks**:
  - Transaction failures.
  - Delays in merchant settlements.
  - System downtime.
- **Mitigation Measures**:
  - Establish a disaster recovery (DR) site and backup systems.
  - Monitor reconciliation and settlement processes in real-time.
  - Conduct stress testing for peak transaction loads.

B. Cybersecurity Risk

- **Key Risks**:
  - Data breaches.
  - Phishing and malware attacks.
  - Unauthorized access to systems.

- **Mitigation Measures**:
    - Implement **end-to-end encryption**, firewalls, and intrusion detection systems.
    - Use **multi-factor authentication (MFA)** for access control.
    - Perform **Vulnerability Assessment and Penetration Testing (VAPT)** regularly.

C. Fraud Risk

- **Key Risks**:
    - Fraudulent transactions by merchants or customers.
    - Account takeover fraud.
    - Chargeback fraud.
- **Mitigation Measures**:
    - Employ **AI/ML-based fraud detection** systems for real-time monitoring.
    - Conduct KYC/AML verification for merchants and customers.
    - Set fraud escalation and reporting mechanisms.

D. Regulatory and Compliance Risk

- **Key Risks**:
    - Non-compliance with RBI guidelines or data localization laws.
    - Delays in AML reporting.
- **Mitigation Measures**:
    - Monitor regulatory updates and ensure adherence to **Payment and Settlement Systems Act, 2007**.
    - Conduct regular audits to validate adherence to PCI DSS and other standards.

E. Financial Risk

- **Key Risks**:
    - Insolvency of third-party vendors or banks.
    - Settlement delays leading to financial loss.
- **Mitigation Measures**:
    - Maintain the minimum net worth requirement of ₹15 crore as per RBI norms.
    - Conduct credit risk assessments of banking partners and service providers.
    - Maintain an escrow account for timely settlements.

F. Reputational Risk

- **Key Risks**:
    - Negative publicity from service disruptions or data breaches.
- **Mitigation Measures**:
    - Transparent communication with merchants and customers during incidents.
    - Proactive resolution of disputes and grievances.
    - Build strong public relations and crisis management protocols.

3. Risk Identification and Assessment

- **Risk Identification**:
    - Use industry benchmarks and historical data to identify emerging risks.
    - Gather inputs from stakeholders, including merchants, customers, and employees.
- **Risk Assessment Tools**:
    - Conduct **Risk and Control Self-Assessments (RCSAs)**.
    - Use quantitative models to assess financial and fraud risks.
    - Classify risks based on likelihood and impact:
        - High, Medium, Low.

4. Risk Mitigation Strategies

Technology Controls

- Implement robust IT infrastructure with redundancy to ensure 99.9% system availability.

Compliance Measures

- Ensure automated KYC/AML processes to reduce manual errors.
- Conduct periodic compliance training for employees and merchants.

Operational Controls

- Use real-time dashboards for transaction and settlement monitoring.
- Automate reconciliation processes to reduce human errors.

5. Risk Monitoring and Reporting

- **Monitoring Tools**:
  - Real-time dashboards for fraud, compliance, and operational risk metrics.
  - Incident management systems to log and track risk events.
- **Key Risk Indicators (KRIs)**:
  - **Transaction Success Rate**: Target >99%.
  - **System Uptime**: Maintain >99.9%.
  - **Fraud Detection Rate**: >95% of suspicious transactions flagged.
- **Reporting Framework**:
  - Submit periodic risk reports to the Risk Management Committee.
  - Report fraud incidents and significant operational failures to RBI as mandated.

6. Business Continuity and Disaster Recovery (BCDR)

- **Disaster Recovery Plan (DRP)**:
  - Establish geographically dispersed DR sites.
  - Ensure recovery within stipulated timelines **(e.g., <4 hours).**
- **Business Continuity Plan (BCP)**:
  - Maintain an incident response team (IRT) for immediate action.
  - Conduct periodic drills for all employees.

7. Merchant and Customer Risk Management

- **Merchant Onboarding**:
  - Perform due diligence on merchants, including background checks and financial audits.
  - Mandate contracts specifying compliance requirements.

- **Customer Transaction Monitoring**:
    - Implement anomaly detection to flag high-risk transactions.
    - Provide customers with real-time transaction alerts and grievance redressal mechanisms.

8. Training and Awareness

- Conduct regular risk management training for employees.
- Educate merchants on secure payment practices and compliance requirements.
- Run customer awareness campaigns on fraud prevention and secure payment methods.

9. Escalation and Incident Management

- **Escalation Matrix**:
    - Define escalation levels for operational, cybersecurity, and compliance risks.
- **Incident Response**:
    - Ensure immediate containment, resolution, and root cause analysis of incidents.
    - Report high-severity incidents to RBI within stipulated timelines.

10. Continuous Improvement

- **Periodic Review**:
    - Update risk policies annually or in response to regulatory or technological changes.
    - Use insights from post-incident reviews to improve controls.
- **Emerging Risk Adaptation**:
    - Stay updated on risks like Central Bank Digital Currencies (CBDCs), AI-driven fraud, and new compliance norms.