RBI Master Direction on Cyber Resilience and Digital Payment Security Controls, 2024

Non-bank Payment System Operators

Digital Trust, Financial Services

October 2024

KPMG. Make the Difference.

Table of contents

01

Introduction

Introduction of the Circular

The Reserve Bank of India (RBI) has issued Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators (PSO) on 30 July 2024.

Applicability

- Clearing Corporation of India Limited
- National Payments Corporation of India (NPCI)
- NPCI Bharat Bill Pay Limited
- Card Payment Networks
- Large Prepaid Payment Instrument (PPI) Issuers
- Payment Aggregators (PA)
- Trade Receivables Discounting System Operators (TReDS)
- Bharat Bill Payment Operating Units
- Non-Bank ATM Networks
- White Label ATM Operators (WLAOs)
- Cross-border (in-bound) Money Transfer Operators under Money Transfer Service Scheme (MTSS)
- Medium PPI Issuers
- Instant Money Transfer Operators
- Small PPI Issuers

Legend

- Large Non-Bank PSOs
- Medium Non-Bank PSOs
- Small Non-Bank PSOs

Key Stakeholders Impacted

- Board of Directors
- Sub-committee of Board (in case)
- Senior Management (CISO, CRO, IT Head etc.)
- Application Owner

Objective

- Authorised non-bank PSOs should be resilient to information and cyber security risks.
- Robust governance mechanisms for identification, assessment, monitoring, and management to be in place.
- Ensure baseline security for system resiliency and secure digital payment transactions.
- PSOs linked with unregulated entities (part of digital payment ecosystem) shall effectively identify, monitor, control, and manage cyber and technology related risks.
- PSO organisational policy should be approved by the Board for the digital payment ecosystem.

Timelines

Regulated Entity	Timeline
Large Non-Bank PSOs	April 1, 2025
Medium Non-Bank PSOs	April 1, 2026
Small Non-Bank PSOs	April 1, 2028

Note:

- If a PPI issuer moves to a higher category, the timeline of the category to which it moves into, would apply.
- Unregulated entities which are part of PSO's digital payments ecosystem shall adhere to these Directions, **subject to mutual agreement.**
- **A draft Master Direction** was published on 2 June 2023 seeking feedback from industry. Based on the feedback received, final directions were published by RBI.

02

MD 2024 vs Draft MD 2023

Master Direction 2024 v/s Draft Master Direction 2023

	MD 2024	Draft MD 2023	Impact
Risk Assessment & Monitoring	Timely review of IT Assessment Reports by dedicated sub-committee	Limited to drafting and formulation of IT Assessment Reports	Sub-committee now accountable for reviewing IT Assessment Reports
Network Security	Devices to be admitted to network only if they meet prescribed measures	Limited to whitelisting solutions, but lacks clarity over admissibility aspect	Moving beyond the requirement of simply having provisions for device admissibility to thorough checks
Application Security Life Cycle	Obtaining source code has been prioritised over having an escrow	Limited to having escrow arrangement	Instead of escrow, organisations will have to first seek source-code from vendor
Vendor Risk Management	Certificate from Independent auditor necessary for critical processes	Does not specify the type of auditor for certified assurance	Certification from Independent Auditor will only be accepted
Data Security	Periodic testing of backed-up data, recovery verification, and transaction & audit trail integrity	Limited to adherence and compliance with PCI-DSS guidelines and certification	Organisation will have to test their data twice a year and the PSO needs to ensure successful recovery of transaction data
Security Testing	Security Audits, in addition to security testing, critical for deployment	Does not bear provisions for deployment of new /existing services	Details out pre-requisites for deployment / re-deployment like security audits and VAPT tests
Cloud Security	Cloud-operation policy, data security, and independent information/cyber security audits	Excluded from Draft MD 2023 altogether	Cloud Operation Policy documentation, data security, and periodic independent audits have been made mandatory

03

Overview of Master Direction

Overview of Master Direction

Governance Controls

- Cybersecurity Preparedness
- Risk Assessment and Monitoring

Baseline Information Security Measures / Controls

- Inventory Management
- Identity and Access Management
- Network Security
- Application Security Life Cycle
- Cloud Security
- Security Testing
- Vendor Risk Management
- Data Security
- Patch and Change Management
- Other Security Measures
- Incident Response
- Business Continuity Plan (BCP)
- Application Programming Interfaces (APIs)
- Employee Awareness / Training

Digital Payment Security Measures / Controls

- Mobile Payment
- Card Payments
- Prepaid Payment Instruments

Governance Controls

Governance Controls

Baseline Information Security Measures / Controls

Digital Payment Security Measures / Controls

Structure

Board of Directors

InfoSec Risk | Cyber Risk | Cyber Resilience

Primary Oversight Sub-Committee/s

Formulating Information Security Policy

- Roles & Responsibilities
- Measures for Cyber Security Risks
  - Identify
  - Assess
  - Manage
  - Monitor
- Processes for training and awareness of employees / stakeholders

Cyber Security Preparedness

- Preparing *Cyber Crisis Management Plan*
  - Detect
  - Contain
  - Respond
  - Recover
- Reference Guidelines
  - CERT-In
  - NCIIPC
  - IDRBT

Risk Assessment & Monitoring

- CISO's Responsibilities
  - Implementing IS Policy
  - Implementing Cyber Resilience Framework
  - Continuous Assessment of Overall Cyber Security Posture
- Define KRIs & KPIs
- IT Assessment Reports
- Cyber Risk Assessment Exercise

Baseline Information Security Measures/Controls

Governance Controls

Baseline Information Security Measures / Controls

Digital Payment Security Measures / Controls

Inventory Management	Record Keeping	Process Flow Diagram	Asset Management			
Identity & Access Management	Access Rights	System Access	Multifactor Authentication	Whitelist Mechanism	System Termination Procedure	Physical & Environmental Safeguards
Network Security	Device Configuration	Automated Mechanisms	Anti-Malware Solutions	Network Segmentation	Network Device Checks	Multi-Layered Boundary Defenses
ASLC	"Secure by Design" Approach	Multi-Tier Application Architecture	Source-Code Procurement			
Security Testing	Rigorous Security Testing	Security Deficiency Reporting	Security Audits			
Vendor Risk Management	Security Controls to prevent network infiltration	Adherence to legal and regulatory requirements	Certified assurance for vendor's cyber resilience capabilities			
Data Security	Data Leak Prevention Policy	Visibility of Data Assets	ISMS Development	Data Encryption	PCI-DSS Adherence	Backup Testing

Baseline Information Security Measures/Controls

Governance Controls

Baseline Information Security Measures / Controls

Digital Payment Security Measures / Controls

Patch & Change Management Life Cycle	Security Patches	Robust Change Management Process	Patch Testing		
Incident Response	Board approved incident response mechanism	Post Incident Analysis	Unusual Incident Reporting to RBI		
Business Continuity Plan	Near-Zero RPO	Disaster Recovery (DR)	DR Drills	Recovery Time Objective Recovery Point Objective	
APIs	Authentication & Authorisation	Confidentiality	Integrity	Availability & Threat Protection	
Employee Awareness/ Training	Periodic repeated trainings / awareness programs	Periodic Evaluation of Cyber Security awareness	Training for Board Members and Key Senior Management Personnel		
Cloud Security	Cloud Operation Policy	Protecting Data	CSP Cyber Security Audits		
Other Security Measures	Ensuring secure configuration of entire IT infrastructure	Real time/ near real time fraud monitoring solution	Capture, analyse, store and archive audit logs	Robust & scalable architecture	Secure Mail and Messaging Systems	Creating public awareness on measures

Digital Payment Security Measures/Controls

Governance Controls

Baseline Information Security Measures / Controls

Digital Payment Security Measures / Controls

PSOs must configure online alerts for various suspicious activities and parameters, such as failed transactions or unusual IP addresses. When sending alerts to customers, PSOs and participants must redact confidential information and clearly mention merchant names, transaction amounts, and beneficiary details.

Mobile Payments

- Ensure mobile app integrity, secure authenticated sessions, and revalidate device binding if unused for a set period.
- Automatically terminate inactive sessions and set a limit for failed login attempts, with a secure reactivation process.
- Identify and block remote access applications during live sessions.
- Implement a 12-hour cooling period for changes to registered mobile numbers or email IDs before allowing transactions.

Card Payments

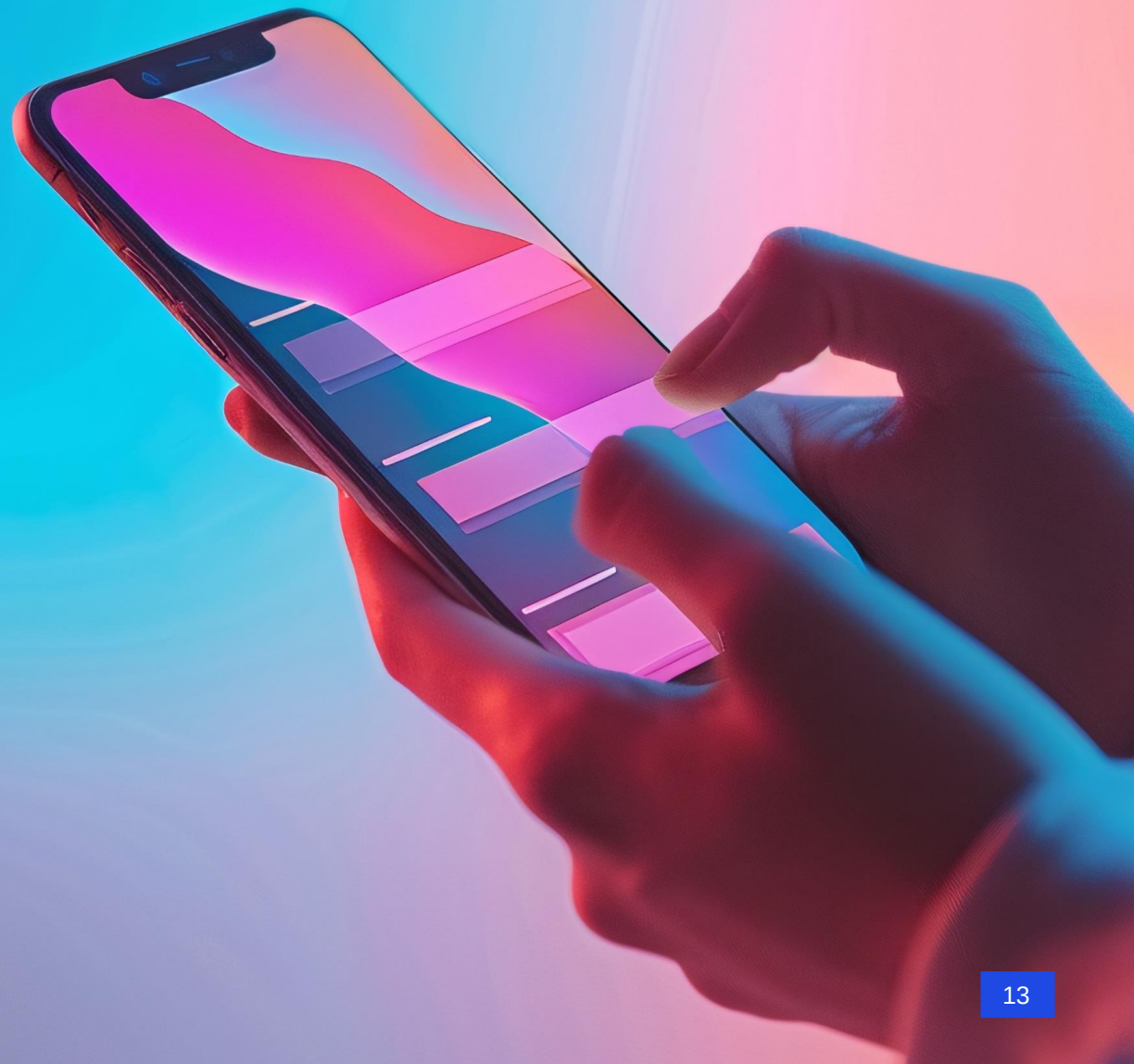
- Terminals at merchants must comply with PCI-P2PE and PCI-PTS standards for capturing card details and PIN entry.
- Card networks must implement transaction limits at various levels and establish a 24/7 alert system for suspicious activities.
- Card details must be encrypted on servers and processed securely by card networks.

Prepaid Payment Instruments

- PPI issuers should provide OTP and transaction alerts in users' preferred languages, including vernacular languages.
- Banks and non-banks issuing PPIs must implement a cooling period for funds transfer and cash withdrawal after electronic loading of funds onto the PPI.

04

Way Forward



Way forward for organisations – aligned to CMMI model

1 Initial

- Initiate GAP assessment
- Create / update the applicable polices and procedures with respect to payment system:
  - Application Programming Interfaces (APIs)
  - Incident response and reporting
  - Identity and Access management
  - Network Security

0 – 45 days

2 Managed

- Key risk indicators to be revisited for focus on cyber security and cyber resilience
- Define Board approved Cyber Crisis Management Plan
- Additional responsibilities for CISO focused on PSO's governance of information security risks

45 – 90 days

3 Defined

- Employee awareness training focused on information and cyber security risks
- Phishing simulation exercises to be conducted
- Payment architecture robustness to be reviewed by Board sub-committee

90 – 180 days

4 Optimised

- OTP alerts with masked customer data and statements to be revisited
- Review of mobile applications robustness, architecture, and security
- Remediation and compliance review of identified gaps reported previously
- POS terminal review against PCI-P2PE* and PCI-PTS* program

180 – 240 days

Acknowledgements

Contributors:

- Aakansha Gupta
- Madhuri Gangaramani
- Jay Goyal
- Sahil Shaikh
- Shubham Sharma

Design and Compliance:

- Shveta Pednekar
- Pooja Patel

Source: Master Directions on Cyber Resilience and Digital Payment Security Controls for non-banking Payment System Operators, Reserve Bank of India, July 2024

KPMG in India contacts:

Akhilesh Tuteja
Global Head
Cyber Security
T: +91 98710 25500
E: atuteja@kpmg.com

Rohan Padhi
Partner and Co-Lead
Digital Risk and Cloud Security
T: +91 99302 24081
E: rohanpadhi@kpmg.com

Atul Gupta
Partner, Head of Function
Digital Trust and Cyber
T: +91 98100 81050
E: atulgupta@kpmg.com

Romharsh Razdan
Partner, Lead Payment Risk and
Co-Lead Cloud Security
T: +91 99755 96366
E: romharsh@kpmg.com

Kunal Pande
Partner, Co-Head - Digital Risk and
Cyber Leader - Digital Trust for FS
T: +91 98926 00676
E: kpande@kpmg.com

Divya Poojari
Director, Digital Risk and
Cloud Security
T: +91 98929 83231
E: divyap@kpmg.com

kpmg.com/in

Access our latest insights
on KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia