

TLDR

The RBI's Master Directions on Cyber Resilience and Digital Payment Security Controls have significant implications for digital merchants in India. While the Directions are specifically targeted at non-bank Payment System Operators (PSOs), they will indirectly impact digital merchants who rely on these PSOs for payment processing and digital payment services.

Merchants can expect the following benefits from their PSOs going forward:

1. **Improved** compliance with baseline security measures.
2. **Continuing compliance with risk mitigation measures** for card payments, prepaid payment instruments (PPIs) and mobile banking.
3. **Enhanced risk management** with stricter controls like IT system audits and compliance requirements.
4. **Data security** focusing on secure handling, processing, storage, and protection of data, particularly Personally Identifiable Information (PII) and card data.
5. **Incident response** including prompt notification of cyber incidents.

Introduction

On July 30, 2024, the Reserve Bank of India (RBI) issued the Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank PSOs¹. To ensure that the authorised non-bank PSOs are resilient to existing and emerging information systems and cyber security risks, it was announced in the Statement on Developmental and Regulatory Policies issued as part of Monetary Policy Statement dated April 08, 2022 that RBI will issue directions on Cyber Resilience and Payment Security Controls for PSOs.² These Directions were proposed to enhance the security and resilience of digital payment systems against existing and emerging cyber threats. This subsequent section of this briefing note summarises the key elements of the directions, focusing on governance, baseline security measures, and implementation timelines.

The governance framework outlined in the Directions emphasises corporate boards' responsibility for overseeing information security risks, developing a Cyber Crisis Management Plan (CCMP) and continuously assessing the overall information security posture. The baseline security measures cover critical areas such as inventory management, identity and access management, network security, application security life cycle, security testing, and vendor risk management. The Directions also specify security controls for specific digital payment channels like mobile payments, card payments, and PPIs to ensure safe and secure transactions. The RBI's Master Directions align closely with ISO standards ISO 31000 and ISO/IEC 27001 related to information security, cybersecurity and privacy protection, particularly in their emphasis on governance, risk assessment, baseline security measures, incident response, and continuous improvement. Both frameworks advocate for a structured and proactive approach to managing information security risks, ensuring the resilience in organisational systems against cyber threats.

The issuance of these Master Directions marks a step towards enhancing the security and resilience of digital payment systems in India. All authorised non-bank PSOs must ensure compliance with these Directions to mitigate cyber risks effectively.

Key Objectives

¹ Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank PSOs, available at: <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12715&Mode=0>

² Governor's Statement: April 8, 2022, available at: <https://www.rbi.org.in/commonperson/english/Scripts/PressReleases.aspx?Id=3352>

The primary objectives as evinced by the Master Directions are:

- To establish robust governance mechanisms for identifying, assessing, monitoring, and managing cyber security risks.
- To ensure baseline security measures are in place for safe digital payment transactions.
- To facilitate compliance with related ISO standards related to risk management while maintaining existing security protocols for card payments, Prepaid Payment Instruments (PPIs), and mobile banking.

Governance Structure

The governance structure outlined in the Directions mandates the following:

- **Board Responsibility:** The Board of Directors of each PSO are tasked with overseeing information security risks, including cyber resilience. A sub-committee may be formed to handle these responsibilities, meeting at least on a quarterly basis.
- **CCMP:** Each PSO must develop a Board-approved CCMP to effectively respond to cyber threats and incidents.
- **Risk Assessment:** PSOs are required to continuously assess their information security posture and establish Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) to monitor security controls.

Baseline Information Security Measures

The directions specify comprehensive baseline security measures that all PSOs must implement, including:

- **Inventory Management:** Maintain a detailed record of all information assets, including their criticality and business value.
- **Identity and Access Management:** Establish strict policies for access control, ensuring that access privileges are granted based on the principle of least privilege and continuous monitoring.
- **Network Security:** Implement measures such as Security Operations Centers (SOCs) for centralised monitoring, multi-layered defences against external threats, and network segmentation based on role and environment.
- **Application Security Life Cycle (ASLC):** Adopt a 'secure by design' approach in the development of digital payment products, adopting rigorous security testing and compliance with security standards.

Digital Payment Security Measures

Specific security safeguards for digital payments include:

- **Mobile and Card Payments:** Adhere to established security protocols for mobile and card transactions, ensuring data protection and compliance with PCI-DSS guidelines.
- **Vendor Risk Management:** Implement security controls to prevent risks from third-party vendors, including obtaining independent audits of vendors involved in critical processes.

Implementation Timeline

Implementation of Master Directions will follow a phased timeline as mentioned below:

- **Large non-bank PSOs:** Compliance by April 1, 2025
- **Medium non-bank PSOs:** Compliance by April 1, 2026
- **Small non-bank PSOs:** Compliance by April 1, 2028

Additional Notes

- The categorisation of enterprises is based on the Oversight Framework for Financial Market Infrastructures and Retail Payment Systems.
- If a PPI Issuer moves to a higher category, the compliance timelines of the new category will apply. For example, if a small PPI issuer becomes a medium PPI issuer, it must comply with the regulations within the timeline designated for medium PSOs.
- This classification is crucial for implementing the Master Directions effectively, as it determines the compliance timelines and specific security requirements applicable to each category of PSO.

Categorisation of PSOs

Large Non-Bank PSOs	Medium Non-Bank PSOs	Small Non-Bank PSOs
<ul style="list-style-type: none"> ● Clearing Corporation of India Limited (CCIL) ● National Payments Corporation of India (NPCI) ● NPCI Bharat Bill Pay Limited ● Card Payment Networks ● Non-bank ATM Networks ● White Label ATM Operators (WLAOs) ● Large PPI Issuers ● Trade Receivables Discounting System (TReDS) Operators ● Bharat Bill Payment Operating Units (BBPOUs) ● Payment Aggregators (PAs) 	<ul style="list-style-type: none"> ● Cross-border (in-bound) Money Transfer Operators (under the Money Transfer Service Scheme (MTSS)) ● Medium sized PPI Issuers 	<ul style="list-style-type: none"> ● Small PPI Issuers ● Instant Money Transfer Operators