DSCI
PROMOTING DATA PROTECTION

Brief on

RBI's Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank PSOs



Brief On RBI's Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators

The Reserve Bank of India (RBI) issued the Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators on 05th November 2026 under Section 10(2) read with Section 18 of the Payment and Settlement Systems Act, 2007.

Overview

The Reserve Bank of India (RBI) issued consolidated Master Directions on Cyber Resilience and Digital Payment Security Controls for authorized non-bank Payment System Operators (PSOs) on the 5th November 2026. The 2026 Master Directions build upon the Master Directions issued on 30 July 2024 and consolidate two earlier instruments into a single reference point: the December 2019 cyber security controls for third-party ATM Switch Application Service Providers (ASPs), and the January 2020 review of the scope and coverage of PSO system audits. Six earlier circulars, dating back to 2009, are repealed. Where guidelines conflict, these Directions prevail; existing security instructions for cards, Prepaid Payment Instruments (PPIs) and mobile banking continue to apply.

Background

RBI first issued the Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank PSOs on 30 July 2024. The 2026 Master Directions consolidate the 2024 Master Directions with two instruments: the circular on Cyber Security Controls for Third party ATM Switch Application Service Providers (RBI/2019-20/130, 31 December 2019) and the circular on System Audit of Payment Systems operated under the PSS Act, 2007 - Review of Scope and Coverage (10 January 2020).

Six circulars issued between 7 December 2009 and 10 January 2020 on system audit and ATM Switch ASP controls stand repealed. Existing instructions for cards, Prepaid Payment Instruments (PPIs) and mobile banking continue to apply, and in case of any discrepancy, the Master Directions prevail.

Who it applies to?

All authorized non-bank PSOs, grouped as Large, Medium or Small. PSOs must also extend the Directions to the unregulated entities in their digital payments ecosystem, such as payment gateways, third-party service providers, vendors and ATM Switch ASPs, subject to mutual agreement and under a Board-approved organizational policy.

The five building blocks (one per substantive section of the Directions):

1. **Governance Controls:** The Board is responsible for adequate oversight of information security and cyber risk and may delegate primary oversight to a sub-committee; a senior executive such as a CISO implements the framework.
2. **Baseline Information Security Controls:** Fourteen control areas, from asset inventory and access management to cloud security and fraud monitoring.
3. **Digital Payment Security Controls:** Safeguards for fraud alerts, customer notifications, mobile payments, card payments and PPIs.
4. **System Audit:** An annual System Audit Report (SAR) by a qualified, independent auditor across 20 mandatory areas, testing both design and operation.
5. **Cybersecurity controls for Third-party ATM Switch ASP:** Contractually imposed controls on ASPs that run shared ATM switch services for White Label ATM Operators (WLAOs).

How the framework works

The Master Directions apply to all authorised non-bank PSOs, and the date from which the Master Directions apply depends on the PSO's category.

Category	Who is covered	In force from
Large	CCIL, NPCI, NPCI Bharat Bill Pay Limited, card payment networks, non-bank ATM networks, WLAOs, large PPI issuers, TReDS operators, Bharat Bill Payment Operating Units (BBPOUs) and Payment Aggregators (PAs)	The day the Directions are placed on RBI's website
Medium	Cross-border (in-bound) Money Transfer Operators under MTSS, and medium PPI issuers	The day the Directions are placed on RBI's website
Small	Small PPI issuers and Instant Money Transfer Operators	1 April 2028

If a PPI issuer moves to a higher category, the timeline of that category applies, and the PPI issuer must comply within one year of the new categorisation.

The governance chain runs from the Board to a senior-level executive, with defined reporting lines:

Layer	Role	Cadence
Board of Directors	Overall oversight of information security, cyber risk and cyber resilience. Approves the Information Security (IS) policy, Cyber Crisis Management Plan (CCMP), incident response mechanism and the policy for unregulated ecosystem entities	IS policy reviewed annually

Layer	Role	Cadence
Board sub-committee	Primary oversight may be delegated to the sub-committee. Headed by a member with experience in information or cyber security. Continuously monitors KRIs and KPIs; receives IT assessment reports (such as system audit and VA/PT reports) and recurring security testing observations; reviews CSP audit reports and performance annually; reviews the payment architecture	Meets at least quarterly
CISO or equivalent	Responsible and accountable for implementing the IS policy and the cyber resilience framework and for continuously assessing the overall IS posture; oversees implementation of action points from cyber risk assessments	Continuous

The IS policy must cover all applications and products concerning payment systems and the management of risks that have materialized. At minimum, the IS policy must set out the roles and responsibilities of the Board, its sub-committees, senior management and other key personnel, and the measures to identify, assess, manage and monitor cyber security risk, including security controls and processes for training and awareness of employees and stakeholders. A separate Board-approved CCMP must cover detection, containment, response and recovery, and relevant guidelines from CERT-In, NCIIPC, IDRBT and other agencies may be referred to. A cyber risk assessment must be undertaken relating to the launch of new products, services or technologies, or major changes to the infrastructure or processes of existing ones.

Baseline Information Security Controls

Section III sets fourteen baseline control areas for every PSO:

Control area	Key requirements
Inventory Management	Record of key roles, information assets, critical functions, processes and third-party providers; network and data flow diagram; asset records with identifier, address, location, owner and End of Life Support (EoLS)
Identity and Access Management	Digital identity for all users; default authentication settings changed before go-live; need-to-know and least-privilege access; MFA for privileged accounts and remote access; session time-outs; physical and environmental safeguards
Network Security	Security Operations Centre (SOC); SIEM; anti-malware; multi-layered boundary defences; network segmentation; application and port whitelisting; network access only for compliant devices
Application Security Life Cycle	Secure-by-design approach such as S-SDLC; multi-tier architecture segregating the database layer; source code of critical procured applications, or an escrow arrangement
Security Testing	Source code review, VA and PT at least annually in authenticated mode; developer certificate where source code is not owned; VA/PT before deploying services supporting critical functions

Control area	Key requirements
Vendor Risk Management	RBI outsourcing framework for PSOs (3 August 2021); controls against infiltration from vendor environments; independent certified assurance for vendors in critical processes
Data Security	Data leak prevention policy; ISMS based on applicable standards; encryption of data in transit and at rest; PCI-DSS certification where card data is stored; backup testing at least half-yearly
Patch and Change Management	Documented patch policy; security patches within an appropriate time frame and critical patches immediately; testing in other environments before production
Incident Response	Board-approved mechanism; post-incident and forensic analysis; unusual incidents reported to RBI within 6 hours of detection; cyber security incidents also reported to CERT-In
Business Continuity Plan	Annual review; RTO and RPO alignment, striving for near-zero RPO; DR site in a different seismic zone from the primary data centre; DR drills at least half-yearly
APIs	Authentication and authorization, confidentiality, integrity, availability and threat protection; adherence to recognized API security frameworks
Employee Awareness and Training	Periodic training for employees, vendors, Board members and senior management; employees below a benchmark score may be restricted from accessing information assets
Cloud Security	Cloud operation policy within the IS policy; segregation of PSO data; independent CSP audits at least annually, reviewed by the Board sub-committee
Other Security Measures	MFA for all electronic debit transactions unless relaxed; real-time or near real-time fraud monitoring; 24×7×365 manned facility for fraud complaints and LEAs; audit logs kept at least five years; anti-phishing and anti-rogue app services; public awareness

Digital payments, system audit and ATM switch providers

Digital payment security (Section IV)

- **Alerts and notifications:** PSOs must facilitate online alerts for participants based on parameters such as transaction velocity, geo-location, IP origin, behavioural biometrics and payments to accounts linked to recorded fraud. Customer alerts must mask account and card numbers, name the merchant or beneficiary and the amount, and place any OTP at the end of the message.
- **Fraud reporting:** Customers must be able to mark a transaction as fraudulent on the PSO's app or website for immediate notification to the issuer.
- **Mobile payments:** Device and SIM binding; secure sessions and automatic time-outs; limits on failed log-ins; blocking of access while remote access apps are live; and a cooling period of at least 12 hours after a change of registered mobile number or email ID.
- **Cards and PPIs:** Merchant terminals validated under PCI-P2PE and PIN-entry terminals approved under PCI-PTS; card networks set limits at card, BIN and issuer level at the switch and store card data encrypted. PPI issuers must set a cooling period after funds are loaded electronically.

System audit (Section V)

Entities must submit an annual System Audit Report (SAR) within two months of financial year close: by 01st June for an April–March year, or by 01st March of the following year for a calendar-year closing. The audit must be conducted by a CERT-In empanelled auditor, a CISA registered with ISACA, or a DISA holder of ICAI, and the audit firm and its sister concerns must not have provided any service to the entity in the last two financial years. The audit covers 20 areas, with controls tested for both design and operating effectiveness: information security governance, access control, hardware management, network security, data security, physical and environmental security, human resource security, business continuity management, system scalability, IT project management, vendor risk management, incident management, change management, patch management, log management, secure mail and messaging, mobile and input/output device management, security testing and source code review, online systems security, and mobile online services.

Third-party ATM Switch ASPs (Section VI)

WLAOs using shared ATM switch services of third-party ASPs must contractually require the ASP to comply with prescribed controls on an ongoing basis and to give RBI access for on-site and off-site supervision. The controls cover unauthorised software, environmental controls, network security, secure configuration, application security, patch and change management, user access, data leak prevention, audit logs, incident response, anti-malware defences, VA/PT, forensic and DDoS support, a Cyber Security Operations Centre, and compliance with PCI-DSS and PA-DSS, as applicable.

Reporting and key timelines

Requirement	Timeline
Unusual incidents reported to RBI (Annex 1 format)	Within 6 hours of detection
Board sub-committee meetings	At least once every quarter
IS policy and BCP review	Annually
Security testing; independent CSP audit	At least annually
Backup data testing; DR drills	At least half-yearly
SAR submission	1 June (April–March FY) or 1 March of the following year (calendar year)
Corrective action on open SAR observations	Maximum 3 months, reported to RBI
Audit log retention	At least five years

The SAR and compliance status must be placed before the Board, and SAR observations close only after closure acceptance from the auditor.

Standards and related instruments

The Master Directions require PCI-DSS, PCI-P2PE, PCI-PTS and, for ATM Switch ASPs, PA-DSS, as applicable, and refer to OWASP for ASP development practices. PSOs shall endeavour to migrate to the latest security standards, and CERT-In, NCIIPC and IDRBT guidelines may be referred to for the CCMP.

Impact of the Master Directions

The Master Directions bring cyber governance, baseline controls, digital payment security, system audit and ATM Switch ASP controls into a single Master Direction, in force for Large and Medium PSOs from the day the Master Directions were placed on RBI's website and for Small PSOs from 1st April 2028. Under the earlier July 2024 Directions, compliance was due from 1st April 2025 for Large PSOs and 1st April 2026 for Medium PSOs.

- **PSOs:** Board-level oversight, fourteen baseline control areas, 6-hour incident reporting and an annual 20-area system audit.
- **WLAOs and ATM Switch ASPs:** Contracts must mandate ASP compliance with Section VI and RBI supervisory access.
- **Vendors and cloud providers:** Adherence subject to mutual agreement; independent assurance for critical vendors and annual CSP audits.
- **System auditors:** A prescribed 20-area scope with design and operating-effectiveness testing, and a two-year independence requirement.
- **Merchants and customers:** PCI-validated terminals, device binding, a 12-hour cooling period after contact detail changes, clearer alerts and a fraud-marking facility.