भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA
www.rbi.org.in

RBI/DPSS/2026-27/475
CO.DPSS.CSD.No.S825/01-01-078/2026-2027 November 05, 2026

The Chairman / Managing Director / Chief Executive Officer
Authorised Non-bank Payment System Operators

Madam / Dear Sir,

Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators

The safety and security of payment systems is a key objective of the Reserve Bank of India (RBI). To ensure that the authorised non-bank Payment System Operators (PSOs) are resilient to existing and emerging information systems and cyber security risks, RBI issued Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators on July 30, 2024. In order to provide a single reference point for the entities, it has been decided to consolidate the directions listed below, issued from time to time on the subject, into a single Master Direction on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators.

2. The following guidelines have been consolidated under the revised Master Directions:

a) Cyber Security controls for Third party ATM Switch Application Service Providers, RBI/2019-20/130/DoS.CO/CSITE/BC.4084/31.01.015/2019-20, dated December 31, 2019; and
b) System Audit of Payment Systems operated under the Payment and Settlement Systems Act, 2007 – Review of Scope and Coverage, dated January 10, 2020.

3. The consolidated Master Directions cover governance mechanisms for identification, assessment, monitoring and management of these risks. The Directions

also cover baseline security measures for ensuring system resiliency as well as safe and secure digital payment transactions. However, they shall endeavour to migrate to latest security standards. The existing instructions on security and risk mitigation measures for payments done using cards, Prepaid Payment Instruments (PPIs) and mobile banking continue to be applicable as hitherto. In case of any discrepancy in applicability of guidelines, the instructions provided in this Master Direction shall prevail.

4. These Directions are issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

Yours faithfully,

(Saurabh Nath)
Chief General Manager

Index	Page
Section I – Preliminary	4
Introduction	4
Short Title and Commencement	4
Applicability	4
Purpose	5
Section II – Governance Controls	5
Cyber Security Preparedness	5
Risk Assessment and Monitoring	6
Section III – Baseline Information Security Measures / Controls	6
Inventory Management	6
Identity and Access Management	7
Network Security	8
Application Security Life Cycle	8
Security Testing	9
Vendor Risk Management	9
Data Security	10
Patch and Change Management Life Cycle	11
Incident Response	11
Business Continuity Plan (BCP)	12
Application Programming Interfaces (APIs)	12
Employee Awareness / Training	13
Cloud Security	13
Other Security Measures	13
Section IV – Digital Payment Security Measures / Controls	14
Mobile Payments	15
Card Payments	16
Prepaid Payment Instruments	17
Section V – System Audit of Authorised Payment System Operators- Scope and Coverage	17
Section VI - Cyber Security controls for Third party ATM Switch Application Service Providers	22
Repeal	30
Acronyms	31

Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators (PSOs)

Section I
Preliminary

Introduction

1. In exercise of the powers conferred under Section 10 (2) read with Section 18 of the Payment and Settlement Systems Act, 2007 (PSS Act), the Reserve Bank of India (RBI, Bank) being satisfied that it is necessary and expedient in the public interest so to do, issues the Master Directions hereinafter specified.

Short Title and Commencement

2. These Master Directions shall be called the Reserve Bank of India (Cyber Resilience and Digital Payment Security Controls for non-bank PSOs) Master Directions, 2026.

3. The Directions shall come into effect on the day they are placed on the official website of the RBI for Large[1] and Medium[2] non-bank PSOs. For small non-bank PSOs[3], the directions shall come into effect from April 01, 2028.

Applicability

4. The provisions of these Directions shall apply to all authorised non-bank PSOs.

5. To effectively identify, monitor, control and manage cyber and technology related risks arising out of linkages of PSOs with unregulated entities who are part of their digital payments ecosystem (like payment gateways, third party service providers, vendors, third party ATM Switch Application Service Providers (ASPs), etc.), PSOs

[1] For the purpose of these Directions, 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) and Payment Aggregators (PAs) are considered as large non-bank PSOs.

[2] Cross-border (in-bound) Money Transfer Operators under Money Transfer Service Scheme (MTSS) and Medium PPI Issuers are considered as medium non-bank PSOs.

[3] Small PPI Issuers and Instant Money Transfer Operators are considered as small non-bank PSOs. Categorisation of authorised non-bank PPI Issuers into small, medium and large is as per the Oversight Framework for Financial Market Infrastructures (FMIs) and Retail Payment Systems (RPSs). If a PPI Issuer moves to a higher category, the timeline of the category to which it moves into, would apply. For instance, if a small PPI issuer moves into medium category (or large), it will need to comply with these Directions within a period of one year from the time of new categorisation, as the case may be.

shall ensure adherence to these Directions by such unregulated entities as well, subject to mutual agreement. An organisational policy in this respect, approved by the Board, shall be put in place.

Purpose

6. These Directions aim to improve safety and security of the payment systems operated by PSOs by providing a framework for overall information security preparedness with an emphasis on cyber resilience.

Section II

Governance Controls

7. The Board of Directors (Board) of the PSO shall be responsible for ensuring adequate oversight over information security risks, including cyber risk and cyber resilience. However, primary oversight may be delegated to a sub-committee of the Board, headed by a member with experience in information / cyber security, which shall meet at least once every quarter.

8. The PSO shall formulate a Board approved Information Security (IS) policy to manage potential information security risks covering all applications and products concerning payment systems as well as management of risks that have materialised. The policy shall be reviewed annually. It shall cover at the minimum, (i) roles and responsibilities of Board/ sub-committees of the Board, senior management and other key personnel; (ii) measures to identify, assess, manage and monitor cyber security risk which shall also include various types of security controls for ensuring cyber resiliency along with processes for training and awareness of employees / stakeholders.

Cyber Security Preparedness

9. The PSO shall prepare a distinct Board approved Cyber Crisis Management Plan (CCMP) to detect, contain, respond and recover from cyber threats and cyber-attacks. Relevant guidelines from CERT-In / National Critical Information Infrastructure Protection Centre (NCIIPC) / IDRBT and other agencies may be referred for guidance.

Risk Assessment and Monitoring

10. The Board shall entrust the responsibility and accountability for implementing the IS policy and the cyber resilience framework as well as for continuously assessing the overall IS posture of PSO to a senior level executive with expertise in areas of information security including cyber security. [e.g. Chief Information Security Officer (CISO)].

11. The PSO shall define appropriate Key Risk Indicators (KRIs) to identify potential risk events and Key Performance Indicators (KPIs) to assess the effectiveness of security controls. These KRIs and KPIs shall be continuously monitored by the sub-committee of the Board referred to in paragraph 7.

12. IT assessment reports (such as system audit, VA / PT reports, etc.) shall be placed before the sub-committee responsible for IT oversight in the meeting due immediately after such report is available.

13. The PSO shall, undertake a cyber risk assessment exercise relating to launch of new products / services / technologies or undertaking major changes to infrastructure or processes of existing products / services. Action points emanating from such assessment shall be implemented under the oversight of the CISO or equivalent executive.

Section III

Baseline Information Security Measures / Controls

14. **Inventory Management**

(a) The PSO shall maintain a record of all the key roles, information assets (applications, data, infrastructure, personnel, services, etc.), critical functions, processes and third-party service providers, and classify and document their levels of usage, criticality and business value.

(b) A complete process flow diagram of network resources, inter-connections and dependencies, and data flows with other information assets, including any other third-party systems, shall be created and maintained.

(c) Asset information shall necessarily include an identifier, network address, asset location, asset owner name and End of Life Support (EoLS). All assets (hardware or

software) approaching EoLS shall be assessed to evaluate risks associated with the continued use of the unsupported asset.

15. **Identity and Access Management**

(a) Policies, procedures and controls that address access privileges as well as administration of access rights must be established.

(b) All individuals having access to the IT environment of the PSO shall be assigned a digital identity, which shall be maintained and monitored till termination.

(c) Default authentication settings in systems / software / services shall be deactivated and changed before they are rolled out to live environment.

(d) Access to systems and different environments (development, test, production, etc.) shall be based on need-to-have, need-to-know and based on the principle of least privilege[4].

(e) The use of privileged accounts[5] shall be with multi-factor authentication and tightly monitored. Appropriate controls, including rotation policy, shall be implemented.

(f) Necessary security controls, including centralised mechanism to whitelist / blacklist, shall be put in place to ensure secure use of removable media and portable devices (e.g. smartphones, laptops, etc.).

(g) In case of remote / work from home situations, adequate precautions, including multi-factor authentication mechanism, shall be in place.

(h) The PSO shall define and implement procedures that limit, lock and terminate system and remote sessions after a pre-defined period of inactivity.

(i) PSO shall have physical and environmental safeguards, with periodic testing, to protect access to its information assets from natural disasters and other threats.

[4] Principle of least privilege refers to granting a user or a process only those privileges or access to the specific data, resources and applications that are/is necessary for intended function or to complete a required task.

[5] Privileged accounts refer to a user account that has more privileges than ordinary user e.g. Administrator level accounts. Such user may be able to install or remove software, upgrade the operating system, or modify system or application configurations. They might also have access to files that are not normally accessible to standard users.

16. Network Security

The PSO shall put in place the following measures to protect its network and systems from external threats:

(a) Network devices shall be configured and checked periodically for security rules;

(b) A Security Operations Centre (SOC) shall ensure proactive and centralised monitoring of comprehensive network and system logs collected and management of security incidents with effective tools for detection, escalation and quick response;

(c) Automated mechanisms (e.g. Security Information and Event Management (SIEM) system), which correlate all network and system alerts and any other anomalous activity across its business units to detect multi-faceted attacks, shall be established;

(d) Anti-malware solutions shall be implemented so as to prevent, detect and contain malware attacks by scanning all incoming data to prevent malware from being installed and infecting a system;

(e) Multi-layered boundary defences shall be incorporated into IS systems to efficiently monitor the network traffic and filter the flow of data in and out of the organisation. There shall be adequate measures to detect and remedy unusual activities / events;

(f) Network segmentation shall be made based on role, location and environment (production, testing, development, etc.) to segregate systems and data of varying criticality; Whitelisting solutions shall be in place to ensure that only permitted applications and services with validated needs are running. Whitelisting of ports may also be ensured with constant monitoring; and

(g) PSOs shall allow devices (such as laptop, desktop, mobile, etc.) to be connected to its network only after ensuring that they meet the prescribed security measures / requirements.

17. Application Security Life Cycle (ASLC)

(a) The PSO shall follow a ‘secure by design’ approach such as Secure-Software Development Life Cycle (S-SDLC) for design and development of products / services and ensure that no security weaknesses are introduced during the build process.

(b) The PSO shall implement a multi-tier application architecture, that ensures segregation of database layer from other layers, while developing digital payment products and services.

(c) The ASLC guidelines shall apply to procured products / services as well. Further, the PSO shall obtain the source code of all critical applications procured from third-party vendors. In case obtaining source code is not possible, there shall be an escrow arrangement for the source code to ensure continuity of services.

18. Security Testing

(a) The PSO shall ensure that all its applications are subjected to rigorous security testing, such as source code review, VA, PT, etc., through qualified professionals at adequate frequency (at least on annual basis) in authenticated mode.

(b) If the source code is not owned by the PSO, it shall obtain a certificate from the application developer stating that the application is free of vulnerabilities, malwares and any covert channels in the code. Fresh certificate shall be obtained for any changes to source code.

(c) Deficiencies reported in the security testing shall be resolved in a time bound manner. Any recurring observation shall necessarily be reported to the Board sub-committee responsible for IT oversight along with detailed analysis for recurrence and resolution.

(d) Any deployment or redeployment of new or existing services supporting critical functions, applications and infrastructure components must be done only after conducting security audits, including VA / PT, and addressing the resultant observations.

19. Vendor Risk Management

The PSO shall be guided by the Framework for Outsourcing of Payment and Settlement-related Activities by PSOs issued by RBI vide circular dated August 03, 2021 (updated from time to time).

(a) The PSO shall put in place necessary security controls for preventing infiltration into its network from vendor environments.

(b) The PSO shall adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and processing, storage and usage of data and also ensure compliance by their vendors.

(c) In case of vendors involved in critical processes and activities[6], the PSO shall obtain certified assurance from an independent auditor on the vendor's cyber resilience capabilities.

20. Data Security

(a) The PSO shall put in place a comprehensive data leak prevention policy for confidentiality, integrity, availability and protection of business and customer information (both in transit and at rest) in respect of data available with it or at vendor managed facilities, commensurate with the criticality and sensitivity of the information held / transmitted.

(b) The PSO shall employ suitable mechanism to ensure traceability and visibility of data assets.

(c) The PSO shall develop and implement an Information Security Management System (ISMS) based on applicable standards.

(d) Application and database security controls shall focus on secure handling, processing, storage and protection of data, in particular, Personally Identifiable Information (PII). Data in transit and rest shall be secured through either data or channel encryption or both.

(e) The PSO storing card (debit / credit / prepaid) data shall adhere to PCI-DSS guidelines and obtain PCI-DSS certification.

(f) The PSO shall have necessary systems and procedures in place to periodically (at least on a half-yearly basis) test the backed-up data to ensure recovery without loss of transactions or audit-trails.

[6] Critical processes as defined in the Framework for Outsourcing of Payment and Settlement-related Activities by PSOs issued by RBI vide circular dated August 03, 2021 (updated from time to time).

21. Patch and Change Management Life Cycle

(a) The PSO shall put in place a documented policy and process to identify and implement patches to technology and software assets released by OEMs / others.

(b) Security patches shall be applied to the relevant systems and applications within an appropriate time frame from their release. In case of critical patches released to tackle well-known / reported attacks, the PSO shall have a mechanism to apply them immediately.

(c) Any change to system, technology, application, source code, etc., shall be managed using robust change management processes and after ensuring that overall integrity of the IT set-up is not compromised.

(d) Patches and changes shall be implemented in production environment after testing and validating the same in other environments (e.g. development, testing, etc.).

22. Incident Response

(a) The PSO shall put in place a Board approved incident response mechanism, which shall include provisions to promptly notify its senior management, relevant employees and regulatory, supervisory and relevant public authorities, of cyber incidents.

(b) Response strategies shall incorporate readiness to meet various incident scenarios based on situational awareness and potential impact, consistent communication and co-ordination with stakeholders.

(c) Post-incident analysis, including forensic analysis (wherever necessary), shall be conducted to determine the impact and root cause of incidents. Adequate measures shall be taken to avoid recurrence of similar incidents.

(d) Unusual incidents like cyber-attacks, outage of critical system / infrastructure, internal fraud, settlement delay, etc., shall be reported to RBI in the Incident Reporting Format (Annex 1) within 6 hours of detection. Indicative list of types of incidents to be reported is in Annex 2. Any cyber security incident shall also be reported to CERT-In.

23. Business Continuity Plan (BCP)

(a) The PSO shall develop a BCP based on different cyber threat scenarios, including extreme but plausible events to which it may be exposed. It shall be reviewed at least once a year and include a comprehensive cyber incident response, resumption and recovery plan, to manage cyber security events or incidents.

(b) The BCP shall be designed to enable rapid recovery from any adverse event and facilitate safe resumption of critical operations aligned with Recovery Time Objective (RTO) and Recovery Point Objective (RPO) while ensuring the security of processes and data.

(c) The PSO shall strive to achieve near-zero RPO.

(d) The PSO shall set up a Disaster Recovery (DR) facility in a different seismic zone than the Primary Data Centre (PDC). There shall be a defined methodology for reconciliation of data so as to ensure that there is no data loss while resuming operations from the DR.

(e) DR drills shall be conducted on a half-yearly or more frequent basis. Any divergence from the RTO and RPO shall be analysed and the deficiency be rectified on urgent basis.

24. Application Programming Interfaces (APIs)

(a) To safeguard applications against risks emanating from insecure APIs, the PSO shall put in place, inter-alia, the following measures:

(i) Authentication and Authorisation – Establish identity of the communicating applications;

(ii) Confidentiality – Ensure that the message content is not tampered with;

(iii) Integrity – Resources are reliably transferred; and

(iv) Availability and Threat Protection – APIs are available when needed; anomalous[7] activities identified and mitigative action taken.

[7] Activity that is sufficiently different than historical activity.

(b) The PSO shall adhere to relevant standards and globally recognised frameworks on API security.

25. Employee Awareness / Training

(a) The PSO shall ensure periodic repeated training / awareness programs on information security issues for its employees and vendors managing its information assets.

(b) A system of periodic evaluation of cyber security awareness amongst employees shall be operationalised. Employees with an awareness level below a benchmark score may be restricted / prohibited from accessing information assets.

(c) Board members and key senior management personnel shall be provided training and sensitised on information security and cyber risks.

26. Cloud Security

(a) The PSO subscribing to cloud services shall put in place a cloud operation policy (as a part of board approved Information Security Policy), highlighting, inter-alia, activities that can be located in cloud servers, clearly identified roles and responsibilities for cloud service provider (CSP), data localisation, protection and recoverability requirements.

(b) It shall be ensured that data pertaining to the PSO is clearly segregated and stringent access control measures are implemented. Multi-tenancy environments shall be protected against data integrity and confidentiality risks, and against co-mingling of data.

(c) The PSO shall ensure that the CSP is subjected to periodic (at least annually) independent information and cyber security audits. Such audit reports and the CSPs overall performance, its cyber resilience capabilities shall be reviewed annually by the Board sub-committee responsible for IT oversight.

27. Other Security Measures

(a) The PSO shall ensure that all payment transactions, including cash withdrawals, involving debit to the account conducted through electronic modes (bank accounts / debit cards / credit cards / PPIs, etc.) are permitted only by validation through multi-factor authentication, except where explicitly permitted / relaxed.

(b) The PSO shall ensure secure configuration of its entire IT infrastructure. It shall also equip its servers with adequate security measures so that unauthorised / spoofed transactions are not done and the authentication process is robust, secure and centralised.

(c) The PSO shall put in place a real-time / near real-time fraud monitoring solution to identify suspicious transactional behaviour and generate alerts.

(d) The PSO shall have a manned facility to function on 24x7x365 basis for facilitating swift resolution of unauthorised / fraudulent transactions reported by customers and also to provide prompt response to Law Enforcement Agencies (LEAs).

(e) The PSO shall put in place a mechanism to capture, analyse, store and archive audit logs in a systematic manner. Log messages shall provide relevant information to uniquely identify the user that initiated an action, the action and parameters of that particular action. Access to log data shall be provided on a controlled basis. Audit logs shall be preserved for a period of at least five years.

(f) The PSO shall ensure that the payment architecture operated by them is robust, scalable and commensurate with the transaction volumes; this shall be reviewed by the sub-committee of the Board.

(g) The PSO shall employ secure mail and messaging systems to ensure that inbound and outbound traffic through mail, messages or any other media are secure.

(h) The PSO shall subscribe to anti-phishing / anti-rogue app services for identifying and taking down phishing websites / rogue applications.

(i) The PSO shall, on an ongoing basis, either directly or through its participants and service providers, create public awareness on precautionary measures to safeguard against frauds and cyber threats while using digital payment products.

Section IV

Digital Payment Security Measures / Controls

In addition to the extant instructions applicable to PSOs for digital payment transactions, the following instructions shall also be applicable.

28. The PSO shall facilitate its members / participants have mechanisms for online alerts based on various parameters such as failed transactions, transaction velocity, as well as in case of new account parameters (e.g., excessive activity), time zone, geo-location, IP address origin (in respect of unusual patterns, prohibited zones / rogue IPs), behavioural biometrics, transaction origination from point of compromise, transactions to mobile wallets / mobile numbers / VPAs on whom vishing or other types of fraud are registered / recorded, declined transactions, transactions with no approval code, etc.

29. While sending SMS / e-mail alert or any other notification to customers, either by PSO or payment system participants, the following shall be ensured –

(a) Bank account number / card number / other confidential information are redacted / masked to the extent possible.

(b) Online payment transactions shall mention merchant name (not the payment gateway/ aggregator) and amount; for fund transfers, name of the beneficiary and debit amount. The PSO shall ensure that the name is taken from the system of the entity maintaining the beneficiary account.

(c) In cases where the OTP is a factor of authentication, the PSO shall ensure that the OTP is mentioned at the end of the notification message and the message shall also refer the specific transaction.

30. The PSO shall provide a facility on its mobile application / website that would enable customers, with necessary authentication, to identify / mark a fraudulent transaction for seamless and immediate notification to the issuer of payment instrument. It shall also ensure facilitation of such mechanism by the system participants.

Mobile Payments

31. The PSO providing / facilitating / processing mobile payment services transactions shall comply with the following security practices and risk mitigation measures and shall also ensure that the participants in its payment system comply with these instructions:

(a) PSO shall put in place a mechanism to ensure that the mobile application is free from any anomalies or exceptions for which the application was not programmed.

(b) The PSO shall ensure that an authenticated session, together with its encryption protocol, remains intact throughout an interaction with the customer. In case of any interference or if the customer closes the application, the session shall be terminated, and the affected transactions resolved or reversed out.

(c) The PSO shall ensure device binding[8] / finger printing of mobile applications with the device and SIM. In case the mobile application remains unused beyond a policy determined specified period, the PSO shall ensure device binding is performed again.

(d) The PSO shall ensure that an online session on mobile application is automatically terminated after a fixed period of inactivity and customers are prompted to re-login.

(e) The PSO shall, where applicable, set down the maximum number of failed log-in or authentication attempts after which access to the mobile application is blocked. There shall be a secure procedure to re-activate the access to blocked product / service. The customer shall be notified for failed log-in or authentication attempts, immediately.

(f) The PSO shall put in place a control mechanism, to identify any presence of remote access applications (to the extent possible) and prohibit access to the mobile payment application while the remote access is live.

(g) Whenever there is a change in registered mobile number or email ID linked to the payment instrument there shall be a cooling period of minimum 12 hours before allowing any payment transaction through online modes / channels.

Card Payments

32. The PSO shall ensure that terminals installed at merchants for capturing card details for payments or otherwise are validated against the PCI-P2PE program; PoS

[8] The device binding shall be preferably implemented through a combination of hardware, software and service information.

terminals with PIN entry installed at the merchants for capturing card payments (including the double swipe terminals) shall be approved by the PCI-PTS program.

33. The card networks shall facilitate implementation of transaction limits at card, Bank Identification Number (BIN) as well as at card issuer level. Such limits shall mandatorily be set at the card network switch itself. The card networks shall institute an alert mechanism on a 24x7x365 basis, to be triggered to the card issuer in case of any suspicious incident. Card networks shall ensure that card details of the customers are stored in an encrypted form at any of their server locations. They shall also ensure that processing of the card details in readable format is performed in a secure manner.

Prepaid Payment Instruments

34. PPI issuers are encouraged to communicate OTP and transaction alerts with users in a language of their choice, including vernacular languages.

35. The PPI issuers – banks and non-banks – shall put in place suitable cooling period for funds transfer and cash withdrawal after such funds are electronically loaded on to the PPI.

Section (V)

System Audit of Authorised Payment System Operators- Scope and Coverage

36. Authorised entities shall furnish their respective System Audit Report (SAR) conducted by CERT-IN empanelled auditors or a Certified Information Systems Auditor (CISA) registered with Information Systems Audit and Control Association (ISACA) or by a holder of a Diploma in Information System Audit (DISA) qualification of the Institute of Chartered Accountants of India (ICAI),on an annual basis within two months of close of their respective financial year. For entities which follow an April-March financial year, the system audit report should be submitted by 1st June of that year. Entities which follow calendar year annual closing, are advised to submit their SAR by 1st March of the following year.

37. There should not be any conflict of interest, i.e. the firm conducting system audit or any of its sister concerns should not have been engaged in providing any type of service/s to the audited entity during the last two financial years.

38. The scope of system audit must include the items indicated below. Auditors need to comment on each item, indicating any observation (or the lack of it). Controls need to be tested for both Design (Test of Design — TOD) and Operating Effectiveness (Test of Operating Effectiveness — TOE).

i. **Information Security Governance** - Assessment of the top management's role in overseeing the development, implementation, and maintenance of the organization's information security management. It should include the following amongst others:

   a) Policies related to information security;

   b) Defined roles and responsibilities of various governance structure;

   c) Identification and assessment of threats and vulnerabilities;

   d) Management reviews of information security practices;

   e) Additional checks based on the risk perception or threats as they emerge;

   f) Key Risk Indicators (KRIs) by the entity as part of self-assessment.

ii. **Access Control** - Assessment of the access control mechanism in place to restrict and filter access to the IT assets of the organisation. It should include the following amongst others:

   a) Granting access on a "need-to-have" and "need-to-know" basis;

   b) Periodic user access reviews & revocation of access;

   c) Privileged User Access Management;

   d) Controlled access to vendors and service providers;

   e) Maintaining audit trail for system activities.

iii. **Hardware Management** - Assessment of controls with regard to hardware asset management from acquisition through disposal. Validation of effectiveness of controls on secure use of removable media.

iv. **Network Security** - Assessment of the countermeasures in place to protect the network from malicious attacks and minimise or eliminate the possibility of any losses being incurred by the entity as a result of the network being compromised.

v. **Data Security** - Assessment of the security measures implemented across the information life cycle starting from collection/ creation of data to storage, access, transmission and its eventual archival and/or deletion.

vi. **Physical and Environmental Security** - Assessment of the physical and environmental security controls in place to protect assets from internal and external threats.

vii. **Human Resource Security** - Assessment of the controls pertaining to human factors to prevent threats such as data leakage, data theft and misuse of data. It should include the following amongst others:

   a) Recruitment (background checks, roles and responsibilities);

   b) Information security training and user awareness;

   c) Termination (removal of access to data and systems).

viii. **Business Continuity Management** - Assessment of the disaster recovery capabilities of the audited entity and regular BCP drills. Controls should be designed so as to enable the entity to recover rapidly from any disrupting event and safely resume critical operations aligned with recovery time and recovery point objectives while ensuring security of processes and data is protected.

ix. **System Scalability -** Assessment of controls relating to scalability of systems from a growth perspective and Turn Around Time (TAT) of transaction processing.

x. **IT Project Management** - Assessment of controls in place for developing or acquiring new systems focusing on project risk. Examine whether systems are based on sound design principles which have built in security functionality such

as Secure Software Development Life Cycle (S-SDLC) and are able to withstand malicious attacks by design and ensure that no security weaknesses have been introduced during the build process.

xi. **Vendor/Third Party Risk Management** - Assessment of controls in place to ensure that outsourcing related risks are managed through adequate oversight measures that should include the following amongst others:

a) Service level agreement (it should mandatorily include right of audit / inspection by the home country regulators);

b) Assessment of the security controls during on-boarding or off-boarding;

c) Implementation of baseline cyber security controls by the service provider;

d) Responsibility of service providers to get their systems audited to ensure error-free operation;

e) Mandatory disclosure of any security incident specific to the entity's systems or processes.

xii. **Incident Management -** Assessment of the entity's response mechanism in the event of a security incident. Examine the organisation's capability to identify the incident, contain the damage, investigate the incident, effectively respond and restore normal operations as quickly as possible with the least possible impact. Also, verify the effectiveness of controls around determination and elimination of the root cause to prevent the occurrence of repeated incidents.

xiii. **Change Management -** Assessment of controls in place for ensuring that changes are applied appropriately and do not compromise the information security of the organisation.

xiv. **Patch Management** - Assessment of the mechanism in place to consistently monitor and configure systems and applications against known vulnerabilities in operating systems and other software.

xv. **Log Management** - Assessment of the security controls around generation, transmission, access, analysis, storage, archiving and ultimate disposal of log data.

xvi. **Secure Mail and Messaging systems** - Assessment of controls in place to ensure that the entity's inbound and outbound traffic in the form of mail, messages or any other media are secure.

xvii. **Mobile and/or other Input / Output Device Management Policy -** Assessment of security controls with regard to portable devices (e.g. smartphones, laptops etc.) having access to sensitive data.

xviii. **Security Testing and Source Code Review -** Assessment of the adequacy of system performance under stress-load scenarios, security controls including vulnerability assessment, penetration testing, configuration review and source code review.

xix. **Online Systems Security** - Assessment of controls in place to ensure security of payment information processing systems and Application Programming Interfaces (APIs) provided to internal/ external applications.

xx. **Mobile Online Services (applicable for entities offering services through mobile applications) -** Assessment of the controls in place to protect mobile applications provided by the entity to its customers from malicious attacks.

39. The auditors need to check open observations and compliance noted in the previous system audit so as to ensure sustained compliance.

40. Deviations, if any, in the processes followed by the entity from the process flow submitted to RBI while seeking authorisation should be mentioned by the auditor.

41. The SAR and compliance status must be placed before the Board of the entity. For each open observation, specific time-bound (maximum 3 months) corrective action must be taken and reported to RBI. It is imperative that timelines of compliance should be given adequate importance. SAR observations shall be closed only after receiving closure acceptance from the auditor.

Section VI

Cyber Security controls for Third party ATM Switch Application Service Providers

42. White label ATM Operators (WLAOs) managing their ATM Switch ecosystem through shared services of third party ATM Switch Application Service Providers (ASPs) shall ensure that the contract agreement signed between them and the ASP shall necessarily mandate the ASP to comply with the following cyber security controls on an ongoing basis and to provide access to the RBI for on-site/off-site supervision. It may be mentioned that these controls are applicable to the ASPs limited to the IT ecosystem (such as physical infrastructure, hardware, software, reconciliation system, network interfaces, security solutions, hardware security module, middleware, associated people, processes, systems, data, information, etc.,) providing ATM switch services as well as any other type of payment system related services to the WLAOs.

43. **Preventing access of unauthorised software**

a) Put in place a mechanism to control installation of software/applications on endpoints. Also, put in place a mechanism to block/prevent and identify installation and running of unauthorised software/applications on such devices/systems.

b) Continuously monitor the release of patches by various vendors / Original Equipment Manufacturers (OEMs), advisories issued by CERT-In and other similar agencies and expeditiously apply the security patches as per the patch management policy of the ASP. If a patch/series of patches is/are released by the OEM/manufacturer/vendor for protection against well-known/well publicised/reported attacks exploiting the vulnerability patched, the ASPs must have a mechanism to apply them expeditiously following an emergency patch management process.

c) Have a clearly defined framework including requirements justifying the exception(s), duration of exception(s), process of granting exceptions, and authority for approving, authority for review of exceptions granted on a periodic basis by officer(s) preferably at senior levels who are well equipped to understand the business and technical context of the exception(s).

44. **Environmental Controls**

d) Put in place appropriate controls for securing the physical location of critical assets, providing protection from natural and man-made threats.

e) Put in place mechanisms for monitoring of breaches/compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc.

45. **Network Management and Security**

a) Prepare and maintain an up-to-date network architecture diagram at the organisation level including wired/wireless networks.

b) Maintain an up-to-date/centralised inventory of authorised devices connected to ASP's network (within/outside ASP's premises) and authorised devices enabling the ASP's network. The ASP may consider implementing solutions to automate network discovery and management.

c) Have mechanisms to identify authorised hardware / mobile devices like laptops, mobile phones, tablets, etc. and ensure that they are provided connectivity only when they meet the security requirements prescribed by the ASP.

d) Ensure that all the network devices are configured appropriately and periodically assessed to ensure that such configurations are securely maintained.

e) The default passwords of all the network devices/systems should be changed after installation.

f) The infrastructure of ASP should be designed with adequate network separation controls.

g) Have mechanism to automatically identify unauthorised device connections to the ASP's network and block such connections.

h) Boundary defences should be multi-layered with properly configured firewalls, proxies, De-Militarized Zone (DMZ) perimeter networks, and network-based IPS and IDS. Mechanism to filter both inbound and outbound traffic must be put in place.

i) Establish Standard Operating Procedures (SOP) for all major IT activities including for connecting devices to the network.

j) Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.

k) Firewall rules shall be defined to block unidentified outbound connections, reverse TCP shells and other potential backdoor connections.

46. **Secure Configuration**

a) Document and apply baseline security requirements/configurations to all categories of devices (end-points/workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically,

b) Periodically evaluate the configuration of all such devices (such as firewall, network switches, security devices, etc.) and patch levels for all systems in the ASP's IT ecosystem.

c) Disable remote connections from outside machines to the network hosting the ATM Switch infrastructure.

d) Enable IP table to restrict access to the clients and servers in SWIFT and ATM Switch environment only to authorised systems.

e) Ensure the software integrity of the ATM Switch related applications.

47. **Application Security Life Cycle (ASLC)**

a) Incorporate/Ensure information security across all stages of application life cycle.

b) Secure coding practices must be implemented for internally /collaboratively developed applications.

c) The development/test and production environments need to be properly segregated. The data used for development and testing should be appropriately masked.

d) Software/Application development approach should be based on threat modelling, incorporate secure coding principles, security testing (based on global standards) and secure rollout.

e) Ensure that adoption of new technologies is adequately evaluated for existing/evolving security threats and that the IT/security team of the ASP achieve reasonable level of comfort and maturity with such technologies before introducing in the IT ecosystem.

f) ASPs shall certify any new products, updates, upgrades as having been developed following secure coding practices. The application architecture shall be tested to safeguard the confidentiality and integrity of data being stored, processed and transmitted. An assurance to this effect shall be shared with the RBI as and when requested.

g) In respect of critical business applications, ASPs shall conduct source code audits by professionally competent personnel/service providers. They shall provide assurance to the WLAO that the application is free from embedded malicious / fraudulent code.

h) The ASPs shall ensure that their software/application development practices address common vulnerabilities highlighted in baselines such as Open Web Application Security Project (OWASP) proactively and adopt the principle of defence-in-depth to provide layered security mechanism.

48. **Patch/Vulnerability and Change Management**

a) Follow a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.

b) Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes that ensure integrity of any changes thereto.

c) Periodically conduct Application security testing of web/mobile applications throughout their lifecycle (pre-implementation, post implementation, after changes) in an environment closely resembling or a replica of the production environment.

d) As a threat mitigation strategy, identify the root cause of incident and apply necessary patches to plug the vulnerabilities.

e) Periodically evaluate the access device configurations and patch levels to ensure that all access points, nodes between (i) different VLANs in the Data Centre (ii) LAN/WAN interfaces (iii) ASP's network to external network and interconnections with partner, vendor and service provider networks are securely configured.

f) ASPs should have a robust change management process in place to record/ monitor all the changes that are moved/ pushed into the production environment. Such a change management process must clearly mention the test cases, chain of approving authority for the particular change, deployment plan and rollback plan.

49. **User Access Control / Management**

a) Provide secure access to the ASP's assets/services from within/outside the ASP's network by protecting data/information at rest (e.g. using encryption, if supported by the device) and in-transit (e.g. using technologies such as VPN or other standard secure protocols, etc.)

b) Carefully protect access credentials such as logon user-id, authentication information and tokens, access profiles, etc. against leakage/attacks.

c) Implement controls to monitor and minimize invalid logon counts and deactivate dormant accounts.

d) Implement a centralised authentication and authorisation system through an Identity and Access Management solution for accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication

depending on risk assessment, securing privileged accesses following the principle of least privileges and separation of duties.

e) Access to critical servers, network and security devices/systems shall be provided through Privileged User Management Systems /Identity and Access Management systems.

f) Monitor any abnormal change in pattern of logon.

g) Mechanism to monitor the database security events, backend access to the databases shall be put in place to ensure access to the database is restricted and the activities carried out through the backend are logged and reviewed.

h) Trivial and/or default passwords shall not be used.

50. **Data Leak prevention strategy**

a) Develop a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.

b) This shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.

51. **Audit Logs**

a) Enough care is to be taken to capture audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be.

b) Implement and periodically validate settings for capturing of appropriate logs/audit trails of each device, system software and application software, ensuring that logs include sufficient information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or event and/or transaction.

c) Logs generation from various devices/applications/database and capturing should always be automatic and by default.

d) An alert mechanism should be set to monitor any change in the log settings.

e) Manage and analyse audit logs in a systematic manner so as to detect, respond, understand or recover from an attack.

52. **Incident Response and Management**

a) ASPs must have a mechanism/ resources to take appropriate action in case of any cyber security incident. They must have written incident response procedures including the roles of staff / outsourced staff handling such incidents; Response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication and co-ordination with stakeholders, including specifically the WLAO, during response.

b) ASP's BCP/DR capabilities shall adequately and effectively support the ASP's cyber resilience objectives and should be so designed to enable the ASP to recover rapidly from cyber-attacks/other incidents and safely resume critical operations aligned with recovery time objectives while ensuring security of processes and data is protected.

c) ASPs are responsible for meeting the requirements prescribed for incident management and BCP/DR even if their IT infrastructure, systems, applications, etc., are managed by third party vendors/service providers. ASPs shall have necessary arrangements, including a documented procedure for such purpose. This shall include, among other things, to inform the WLAO about any cyber security incident occurring in respect of the WLAO on timely basis to early mitigate the risk as well as to meet extant regulatory requirements.

53. **Advanced Real-time Threat Defence and Management**

a) Build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise.

b) Implement Anti-malware, Antivirus protection including behavioural detection systems for all categories of devices – endpoints, servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-

gateways, Wireless networks, etc. including tools and processes for centralised management and monitoring.

54. **Vulnerability assessment and Penetration Test**

a) Periodically conduct Vulnerability Assessment/ Penetration Testing (VA/PT) of applications, servers and network components.

b) The vulnerabilities detected are to be remedied promptly in terms of the ASP's risk management/treatment framework so as to avoid exploitation of such vulnerabilities.

c) The VAPT report(s) and compliance to its findings shall be shared with the WLAO/ Reserve Bank of India as and when requested.

55. **Forensics**

a) The ASP shall have support/ arrangement for network forensics/forensic investigation/DDOS mitigation services on stand-by.

56. **Arrangement for continuous surveillance - Setting up of Cyber Security Operation Center (C-SOC)**

a) Constant and continuous monitoring of the environment using appropriate and cost-effective technology tools, clearly defined policies and procedures based on best practices and monitored by technically competent and capable manpower is essential. ASPs are mandated that a C-SOC (Cyber Security Operations Center) be set up at the earliest, if not yet set-up. It is also essential that this Centre, among other things, ensures seamless collection of the logs relevant to the IT ecosystem, storing, processing and correlation of the logs through appropriate Security Information and Event Management (SIEM) solution for continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats.

57. **Compliance with various standards**

a) The ASP shall comply with the relevant standards including PCI-DSS and PA-DSS, as applicable to the IT ecosystem.

58. **Repeal**

The list of circulars / directions that are repealed are listed below.

Sl. No.	Circular No	Date	Subject
1.	DPSS.AD.No./1206/02.27.005/2009-2010	December 7, 2009	System Audit of the Payment Systems operated under the PSS Act,2007
2.	RBI/2010-11/340-DPSS.CO.OSD. No. 1444 /06.11.001/2010-2011	December 27, 2010	Directions for submission of system audit reports from CISA qualified Auditor
3.	RBI/2010-11/476 DPSS.CO.OSD. No. 2374 /06.11.001/ 2010-2011	April 15, 2011	Submission of system audit reports
4.	RBI/2010-11/563-DPSS.CO.OSD. No. 2764 /06.11.001/ 2010-2011	June 14, 2011	Directions for submission of system audit reports from CISA qualified Auditor
5.	RBI/2019-20/130 DoS.CO/CSITE/BC.4084/31.01.015/2019-20	December 31, 2019	Cyber Security Controls for Third Part ATM Switch Application Service Providers
6.	DPSS.CO.OD.No. 1325/06.11.001/2019-20	January 10, 2020	System Audit of Payment Systems operated under the Payment and Settlement Systems (PSS) Act, 2007 – Review of Scope and Coverage

Acronyms

API	Application Programming Interface
ASLC	Application Security Life Cycle
ATM	Automated Teller Machine
BCP	Business Continuity Plan
BIN	Bank Identification Number
CCMP	Cyber Crisis Management Plan
CERT-In	Indian Computer Emergency Response Team
CISO	Chief Information Security Officer
CSP	Cloud Service Provider
DR	Disaster Recovery
EoLS	End of Life support
IDRBT	Institute for Development and Research in Banking Technology
IP	Internet Protocol
IS	Information System
ISMS	Information Security Management System
IT	Information Technology
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LEA	Law Enforcement Agency
NCIIPC	National Critical Information Infrastructure Protection Centre
OEM	Original Equipment Manufacturer
OTP	One Time Password
PCI	Payment Card Industry
PCI-DSS	Payment Card Industry-Data Security Standard
PCI-P2PE	Payment Card Industry-Point to Point Encryption
PCI-PTS	Payment Card Industry-PIN Transaction Security
PDC	Primary Data Centre
PIN	Personal Identification Number
PoS	Point of Sale
PPI	Prepaid Payment Instrument
PSO	Payment System Operator
PSS	Payment and Settlement Systems
PT	Penetration Testing

RBI	Reserve Bank of India
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDLC	Software Development Life Cycle
S-SDLC	Secure-Software Development Life Cycle
SIEM	Security Information and Event Management
SIM	Subscriber Identification Module
SMS	Short Message Service
SOC	Security Operations Centre
VA	Vulnerability Assessment
VPA	Virtual Payment Address
WLAO	White Label ATM Operator
SWIFT	Society for Worldwide Interbank Financial Telecommunication
ASP	ATM Switch Application Service Providers