Baseline Technology-related Recommendations

Indicative baseline technology-related recommendations for adoption by the PAs (mandatory) and PGs (recommended) are:

1. Security-related Recommendations

The requirements for the entities in respect of IT systems and security are presented below:

1.1. Information Security Governance: The entities at a minimum shall carry out comprehensive security risk assessment of their people, IT, business process environment, etc., to identify risk exposures with remedial measures and residual risks. These can be an internal security audit or an annual security audit by an independent security auditor or a CERT-In empanelled auditor. Reports on risk assessment, security compliance posture, security audit reports and security incidents shall be presented to the Board.

1.2. Data Security Standards: Data security standards and best practices like PCI-DSS, PA-DSS, latest encryption standards, transport channel security, etc., shall be implemented.

1.3. Security Incident Reporting: The entities shall report security incidents / card holder data breaches to RBI within the stipulated timeframe to RBI. Monthly cyber security incident reports with root cause analysis and preventive actions undertaken shall be submitted to RBI.

1.4. Merchant Onboarding: The entities shall undertake comprehensive security assessment during merchant onboarding process to ensure these minimal baseline security controls are adhered to by the merchants.

1.5. Cyber Security Audit and Reports: The entities shall carry out and submit to the IT Committee quarterly internal and annual external audit reports; bi-annual Vulnerability Assessment / Penetration Test (VAPT) reports; PCI-DSS including Attestation of Compliance (AOC) and Report of Compliance (ROC) compliance report with observations noted if any including corrective / preventive actions planned with action closure date; inventory of applications which store or process or transmit customer sensitive data; PA-DSS compliance status of payment applications which stores or processes card holder data.

1.6. Information Security: Board approved information security policy shall be reviewed atleast annually. The policy shall consider aspects like: alignment with business objectives; the objectives, scope, ownership and responsibility for the policy; information security organisational structure; information security roles and responsibilities; maintenance of asset inventory and registers; data classification; authorisation; exceptions; knowledge and skill sets required; periodic training and continuous professional education; compliance review and penal measures for non-compliance of policies.

1.7. IT Governance: An IT policy shall be framed for regular management of IT functions and ensure that detailed documentation in terms of procedures and guidelines exists and are implemented. The strategic plan and policy shall be reviewed annually. The Board level IT Governance framework shall have-

1.7.1. Involvement of Board: The major role of the Board / Top Management shall involve approving information security policies, establishing necessary organisational processes / functions for information security and providing necessary resources.

1.7.2. IT Steering Committee: An IT Steering Committee shall be created with representations from various business functions as appropriate. The Committee shall assist the Executive Management in implementation of the IT strategy approved by the Board. It shall have well defined objectives and actions.

1.7.3. Enterprise Information Model: The entities shall establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with board approved IT strategy. The model shall facilitate optimal creation, use and sharing of information by a business, in a way that it maintains integrity, and is flexible, functional, timely, secure and resilient to failure.

1.7.4. Cyber Crisis Management Plan: The entities shall prepare a comprehensive Cyber Crisis Management Plan approved by the IT strategic committee and shall include components such as Detection, Containment, Response and Recovery.

1.8. Enterprise Data Dictionary: The entities shall maintain an “enterprise data dictionary” incorporating the organisation’s data syntax rules. This shall enable sharing of data across applications and systems, promote a common understanding of data across IT and business users and prevent creation of incompatible data elements.

1.9. Risk Assessment: The risk assessment shall, for each asset within its scope, identify the threat / vulnerability combinations and likelihood of impact on confidentiality, availability or integrity of that asset – from a business, compliance and / or contractual perspective.

1.10. Access to Application: There shall be documented standards / procedures for administering an application system, which are approved by the application owner and kept up-to-date. Access to the application shall be based on the principle of least privilege and “need to know” commensurate with the job responsibilities.

1.11. Competency of Staff: Requirements for trained resources with requisite skill sets for the IT function need to be understood and assessed appropriately with a periodic assessment of the training requirements for human resources.

1.12. Vendor Risk Management: The Service Level Agreements (SLAs) for technology support, including BCP-DR and data management shall categorically include clauses permitting regulatory access to these set-ups.

1.13. Maturity and Roadmap: The entities shall consider assessing their IT maturity level, based on well-known international standards, design an action plan and implement the plan to reach the target maturity level.

1.14. Cryptographic Requirement: The entities shall select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, reputable security vendors or government agencies.

1.15. Forensic Readiness: All security events from the entities infrastructure including but not limited to application, servers, middleware, endpoint, network, authentication events, database, web services, cryptographic events and log files shall be collected, investigated and analysed for proactive identification of security alerts.

1.16. Data Sovereignty: The entities shall take preventive measures to ensure storing data in infrastructure that do not belong to external jurisdictions. Appropriate controls shall be considered to prevent unauthorised access to the data.

1.17. Data Security in Outsourcing: There shall be an outsourcing agreement providing ‘right to audit’ clause to enable the entities / their appointed agencies and regulators to conduct security audits. Alternatively, third parties shall submit annual independent security audit reports to the entities.

1.18. Payment Application Security: Payment applications shall be developed as per PA-DSS guidelines and complied with as required. The entities shall review PCI-DSS compliance status as part of merchant onboarding process.

2. Other Recommendations

2.1. The customer card credentials shall not be stored within the database or the server accessed by the merchant.

2.2. Option for ATM PIN as a factor of authentication for card not present transactions shall not be given.

2.3. Instructions on storage of payment system data, as applicable to PSOs, shall apply.

2.4. All refunds shall be made to original method of payment unless specifically agreed by the customer to credit an alternate mode.