Annex

Cyber Security Controls for ATM Switch Application Service Providers (ASPs)

1. Preventing access of unauthorised software

1.1. 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.

1.2. 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.

1.3. 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).

2. Environmental Controls

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

2.2. 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.

3. Network Management and Security

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

3.2. 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.

3.3. 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.

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

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

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

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

3.8. 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.

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

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

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

4. Secure Configuration

4.1. 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,

4.2. 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.

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

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

4.5. Ensure the software integrity of the ATM Switch related applications.

5. Application Security Life Cycle (ASLC)

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

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

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

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

5.5. 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.

5.6. 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 bank/RBI as and when requested.

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

5.8. 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.

6. Patch/Vulnerability and Change Management

6.1. 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.

6.2. 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.

6.3. 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.

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

6.5. 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.

6.6. 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.

7. User Access Control / Management

7.1. 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.)

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

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

7.4. 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.

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

7.6. Monitor any abnormal change in pattern of logon.

7.7. 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.

7.8. Trivial and/or default passwords shall not be used.

8. Data Leak prevention strategy

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

8.2. 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.

9. Audit Logs

9.1. 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.

9.2. 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.

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

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

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

10. Incident Response and Management

10.1. 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 bank, during response.

10.2. 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.

10.3. 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 bank about any cyber security incident occurring in respect of the bank on timely basis to early mitigate the risk as well as to meet extant regulatory requirements.

11. Advanced Real-time Threat Defence and Management

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

11.2. 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.

12. Vulnerability assessment and Penetration Test

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

12.2. 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.

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

13. Forensics

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

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

14.1. 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.

15. Compliance with various standards

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

****