RESERVE BANK OF INDIA
www.rbi.org.in

DPSS.CO.OD. No. 1325/06.11.001/2019-20 January10,2020

To

All Authorised Payment Systems Operators and Entities

Madam/Dear Sir

System Audit of Payment Systems operated under the Payment and Settlement Systems (PSS) Act, 2007 - Review of Scope and Coverage

Please refer to Reserve Bank of India (RBI) circulars DPSS.AD.No./1206/ 02.27.005/2009-2010 dated December 7, 2009, DPSS CO.OSD. No. 1444/ 06.11.001/2010-2011 dated December 27, 2010, DPSS.CO.OSD.No. 2374/ 06.11.001/2010-2011 dated April 15, 2011 and DPSS.CO. OSD. No. 2764 /06.11.001/ 2010-2011 dated June 14, 2011 on submission of System Audit Report (SAR).

2. The scope of SAR has been reViewed and enhanced in order to ensure standardisation along with the need to encompass all relevant areas of information system processes and applications to be covered as part of the audit.

3. Entities shall note to take necessary action in this regard and submit SAR for the current financial year, i.e. 2019-20, and onwards as per the scope, coverage and periodicity detailed in the Annexure.

4. Please acknowledge receipt of this letter and confirm compliance.

Yours faithfully

(Rajani Prasad)
General Manager (Officer in Charge)

Encl.: Annexure

भुगतान और निपटान प्रणाली विभाग, केंद्रीय कार्यालय, 14 वी मंजिल, केंद्रीय कार्यालय भवन,शहीद भगत सिंह मार्ग, फोर्ट, मुम्बई - 400001
Tel. (91 22) 2260 1000, Fax: (91-22) 2265 9566, -e mail . cgmd ••° e rbi.org.in
Depanment of Paymenl and Seltlemenl Systems, Cenmal Ofl ce, 14* Floor, Cenmal Office Building, Shahid Bhagal Singh Road. Fort. Mumba -40000

Enclosure to letter DPSS.CO.OD.No.1325/06.11001/2019-20 dated January 10, 2020

Annexure

System Audit of Authorised Payment System Operators- Scope and Coverage

1. 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 1** June of that year. Entities, which follow a calendar year annual closing, are advised to submit their system audit reports by 1 t March of the following year.
2. There should not be any conflict of interest for auditor, 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.
3. 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 (KRls) 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. lt 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 deîetion.

vi. Physical and Environmental Security — Assessment of the physicaT 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. lt 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).

Vîii. 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 groMh 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.

xî. 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 îdentify 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.

xîu. 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 App(ication 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 and provided by the entity to its customers from malicious attacks.

4. The auditors need to check open observations and compliance noted in the previous system audit so as to ensure sustained compliance.
5. 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.
6. 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 recei\ling closure acceptance from the auditor.