भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2012-13/547
DIT.CO(Policy)No. 2636/ 09.63.025/2012-13 June 26, 2013

The Chairmen/Chief Executive Officers,
All Scheduled Commercial Banks (excluding RRBs)

Dear Sir/Madam,

Business Continuity Planning (BCP), Vulnerability Assessment and Penetration Tests (VAPT) and Information Security

Please refer paragraph 102 of the Monetary Policy Statement 2013-14 wherein we have emphasised the importance of securing the Information Systems (IS) of banks. In order for banks to secure their ISs, ensure their continuity, and check their robustness, it is expected that banks put in place appropriate business continuity plans (BCPs) and test them periodically. These ISs should also be subjected to vulnerability assessment and penetration testing (VAPT).

2. Formulation of consolidated BCP documents by banks covering critical aspects of people, process and technology is important in view of the increased contribution of 24x7 electronic banking channels. The documents should cover policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes, at an agreed level and limit the impact of the any disaster on people, processes and infrastructure (including IT); or to minimise the operational, financial, legal, reputational and other material consequences arising from such a disaster. In order to test their internal IT systems to handle unforeseen disruptions, it is important for the banks to conduct Disaster Recovery (DR) Drills on a regular basis. It is also important that these arrangements are subject to periodic testing.

3. Further, considering that cyber attacks could threaten the confidentiality, integrity and availability of data and the systems, it is imperative for the banks to conduct VAPT periodically to prevent any such attacks. There is a need to prepare documents detailing these activities, update the same regularly and ensure that gaps identified from the tests are plugged in a timely manner. This should form part of the Information Security assurance function undertaken by banks.

4. Reserve Bank has been emphasising to banks on the importance of putting appropriate IT and IS governance structures to enable, interalia, better control and security. The policies governing security of ISs may be discussed and approved at the Board level and updated from time-to-time. A certificate confirming the same

may be forwarded to us for our record. This aspect may be subjected to scrutiny at a later date during the Annual Financial Inspection of banks.

5. The information regarding the conduct of DR drills and VAPT is received by the Reserve Bank on a quarterly basis and this may be continued.

6. The critical components of Business Continuity Management Framework as enunciated in the report of Working Group on information security, electronic banking, technology risk management, and cyber frauds (Chairman: Shri G Gopalakrishna) can serve as reference material for banks while finalising their policies.

7. Please acknowledge the receipt of the letter.

Yours faithfully

(A. S. Ramasastri)
CGM-in-charge