Ref. RBI/2004-05/420
DBS.CO.IS Audit.No. 19/31.02.03/2004-05

April 15, 2005

To

All Chairmen / Managing Directors / Chief Executive Officers of all
Scheduled Commercial Banks

Dear Sir,

Operational Risk Management - Business Continuity Planning

In the backdrop of growing complexity of financial products and the increased leveraging of technology and its heightened sophistication, operational risks have assumed critical importance in recent times. The treatment of operational risks as a distinct risk category along with credit and market risks in the Basel II framework is a manifestation of the vital role played by operational risks in impacting risk profile of a bank. Operational risks can also have a systemic connotation in the event of contagion through channels like the payment system and undermine public confidence in the banking system.

2. Business Continuity planning is a key pre-requisite for minimising the adverse effects of one of the important areas of operational risk – business disruption and system failures. A recent study conducted by RBI revealed that some banks were still in the process of framing a business continuity plan (BCP). It is imperative that all banks have BCP's in place to be in readiness to tackle serious business disruptions.

3. The responsibility in respect of BCP rests with the Board of directors and the top management. The Board should provide top management clear guidance and direction in relation to BCP. The Board fulfils its responsibilities by approving policy on BCP, prioritizing critical business functions, allocating sufficient resources, reviewing BCP test results and ensuring maintenance and periodic updation of BCP. The BCP requirements enunciated in this circular should be considered as a minimum and the onus is on the Board and the top management for generating detailed components of BCP in the light of individual bank's

activities, systems and processes. The top management is responsible for executing such a BCP, if contingency arises. The top management should annually review the adequacy of the institution's business recovery, contingency plans and the test results and put up the same to the Board. The top management should also evaluate the adequacy of contingency planning and their periodic testing by service providers whenever critical operations are outsourced.

4. Aspects relating to controls to be put in place to address interruption risks arising as part of the overall IT operations risk were discussed in the Guidance Note on Risks and Controls in Computer and Telecommunication Systems which was circulated among all banks operating in India vide our letter DBS.CO.ITC.BC.10/31.09.001/98 dated February 4, 1998. Report of the Working Group for Information System Security for the Banking and Financial Sector, forwarded to banks in the year 2001, also contains recommendations pertaining to BCP.

5. Changing business processes (internally to the institution and externally among interdependent financial service providers) and new threat scenarios require maintenance of viable BCPs. An effective BCP should take into account the potential for wide-area disasters that impact an entire region and for the resulting loss or inaccessibility of staff. It should also consider and address interdependencies, both market-based and geographic, among financial system participants as well as infrastructure service providers. In most cases, recovery time objectives are now much shorter than they were even a few years ago.

6. It is, therefore, advised that banks may put in place a BCP including a robust information risk management system, if not already implemented, within a fixed time frame. They may implement such BCP and thoroughly test it to verify its full capability against the changing scenario and assumptions at frequent intervals, as per the policy. The plan may also be subjected to review annually.

7. The BCP methodology should include, *inter alia*,

- Identification of critical businesses, owned and shared resources with supporting functions (the BCP template shall include IT Continuity Plan template)

- Structured risk assessment based on comprehensive business impact analysis
- Formulating Recovery time objectives (RTO) based on Business Impact Analysis. It may also be periodically fine-tuned by benchmarking against industry best practices.
- Critical and tough assumptions in terms of disaster so that the framework would be exhaustive enough to address the most stressful situations
- Identification of the recovery point objective (RPO) for data loss for each of the critical systems and strategy to deal with such data loss
- Alternate procedures during the time systems are not available
- Clearly documented and tested processes for shifting to secondary/back-up systems and sites
- Risk management by implementing IS design and architecture to attain the bank's agreed RTOs and RPOs.
- Minimising immediate damage and losses
- Restoring critical business functions, including customer-facing systems and payment & settlement systems like cash disbursements, ATMs, Internet banking, call centres, etc.
- Establishing management succession and emergency powers
- Addressing HR issues and training aspects
- Providing for the safety and wellbeing of people in the branch or at the location at the time of the disaster
- Use of external resources/ support
- Having specific contingency plans for each outsourcing arrangement based on the degree of materiality of the outsourced activity to the bank's business
- Ensuring service providers for critical operations have BCPs in place and also periodically test the same
- Compatibility and co-ordination of contingency plans at both the bank and its service providers
- Action plans, practical manuals and testing procedures
- Independent audit and review of the BCP and test results
- Periodic updating to absorb changes in the institution or its service providers

8. The BCP should take into account the project management procedures, change management process, data centre process, backup and recovery

process. Based on a sound methodology, a development plan for the DRS / BCP may be initiated. The plan needs to be continuously evaluated and revised whenever the bank forays into new business tools and areas, either as part of a re-engineering process or for introducing new products and services. The relevant portion of the BCP adopted may also be disseminated to all concerned, including the customers, so that the awareness would enable them to react positively and in consonance with the BCP. The part of the plan kept in the public domain should normally be confined to information relating to the general readiness of the banks in this regard without any detailed specifics.

9. BCP involves cost implications. While banks may consider cost-effective strategies of BCP, the strategies considered should provide an adequate level of comfort and assurance in tackling serious disruptions. Moreover, the mitigating solution should be commensurate with the nature and complexity of their business operations.

10. Banks may also consider insurance as a risk mitigation strategy for externalizing risks to a third party so as to reduce financial exposure in the event of disruptions. However, diligence needs to be exercised in regard to the nature of insurance and the certainty of payments.

11. It is needless to emphasise that early compliance by all banks would reassure the public at large as well as the payment system entities on the resilience of the Indian banking system. A copy of the BCP approved by the Board may be forwarded for perusal to the General Manager, Reserve Bank of India, IS Audit Cell, Department of Banking Supervision, Central Office, 3rd Floor, Centre-I, World Trade Centre, Cuffe Parade, Colaba, Mumbai 400005. A soft copy of the BCP may be sent to cgmicdbsco@rbi.org.in by e-mail.

12. In addition, the bank should submit

    i. an annual statement at the end of each financial year describing the critical systems, their RTOs and the bank's strategy to achieve them, and

    ii. a quarterly statement, starting from June, 2005, reporting major failures during the period for critical systems, customer

segment/services impacted due to the failures and steps taken to avoid such failures in future.

Yours faithfully,

(P. Parthasarathi)
General Manager