Introduction

Business interruptions can occur anywhere, anytime. Massive hurricanes, tsunamis, power outages, terrorist bombings and more have made recent headlines. It is impossible to predict what may strike when. In today's 24x7x365 world, it has become mandatory to prepare for such disaster scenarios. With the ever increasing dependence on banks for both electronic and traditional banking services, it has become almost mandatory for the banking industry to plan for 'Business Continuity'.

Relevance of BCP for Banks

It may sound cliché to mention that much of the commercial activity that we see today is dependent on banks. Banks, in turn, have turned to increasingly complex technology and business models to deliver the services expected in this age of boundaryless commerce. Sophisticated and interconnected Automated Teller Machine (ATM) networks, Tele-banking, Core Banking Solutions and Internet Banking Solutions for seamless customer access are but some of technologies currently deployed. Add to this, the ever expanding branch network to provide banking services in semi-urban and rural areas in India. With this background in mind, it is indeed worrying to imagine a scenario where a disaster may render a bank inoperative for an extended period of time.

The floods in Mumbai brought to fore one such concern for banks. Bank ATM terminals are typically located on the ground floor of premises with the backup power generator being located in the basement. The unprecedented floods of July 2005 made all such ATMs non-functional. In such crisis situations, lack of access to financial resources could have severe repercussions. Without these resources, organizations and individuals would find it daunting to take measures to recover from the disaster. This would compound the already difficult situation being faced and could lead to anarchy and situations like run on banks.

Some of the other factors that might negatively affect your bank's revenue stream and brand image include:

* Senior Director, Enterprise Risk Services, Deloitte Touche Tohmatsu India Pvt. Ltd, Mumbai. The author gratefully acknowledges the assistance provided by Keith Prabhu and Anita Pai Ramchandani. The views presented in this document are the personal views/opinions of the authors and not of the organization they represent and are informative in nature only. It is not intended to be relied upon, nor be used as a substitute for, specific professional advice.
The only thing harder than planning for an emergency is explaining why you didn’t.

Plan ahead: It wasn’t raining when Noah built the ark!

Anonymous

BCP Related Regulatory Requirements

The World Trade Center attacks on September 11, 2001 brought about never-before-imagined catastrophes which completely changed the perception of BCP preparedness. Consequently, the Federal Reserve, Securities and Exchange Commission, Office of Comptroller of the Currency and the New York State Banking Department released a white paper ¹ in April 2003 which identified three business continuity objectives as having special importance for all financial institutions:

- Rapid recovery and timely resumption of critical operations following a wide-scale disruption
- The ability to recover and continue operations following the loss or inaccessibility of staff in at least one major operating location
- A high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible

The need, therefore, was felt for continuous availability of operations as an absolute necessity for customer satisfaction and brand protection in case of banking and other financial institutions.

In keeping with the theme of continuous availability of banking operations, the Basel Committee on Banking Supervision (BCBS) released a publication ² which provided that all banks should have in place contingency and continuity plans to ensure that they could continue to operate on an on-going basis and limit losses in the event of a severe business disruption. The group recommended that:

- Banks should identify critical business processes, including dependencies on third parties or external vendors, and identify alternative mechanisms for resumes service in the event of an outage
- Attention should be paid to the restoration of physical or electronic records; care should be taken so that back-up facilities are at an adequate distance from the impacted operations to minimize the risk that back-up facilities are unavailable
- Banks should periodically review their disaster recovery and business continuity plans so that they are consistent with current operations
- These plans should be tested periodically to ensure that the bank would be able to execute the plans during a severe business disruption

On account of growing number of high-profile operational loss events worldwide, Operational Risk Management (ORM) was identified as an integral part of the risk management activity. The Basel II Framework ³ identified broad types of operational risk events having the potential to result in substantial losses which included continuity risk events such as damage to physical assets, business disruption and system failures, loss on account of external fraud such as computer hacking, etc.
The importance of BCP was reemphasized by the Basel Committee by the release of a publication on “High Level Principles of Business Continuity” ⁶. This publication was the effort of the Joint Forum consisting of BCBS, the International Organization of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS). This publication provided seven guiding principles for effective BCM and reiterated that BCM is a significant component of ORM and its purpose is to minimize the operational, financial, legal, reputational and other material consequences arising from a disruption.

The Reserve Bank of India (RBI) had recognised the importance of BCP way back in 1998 when it released a guidance note ⁶ for management of banks to evaluate the adequacy of controls in relation to risks related to computer and telecommunication systems including interruption risks. This was followed by the release of a report on “Information Systems Audit Policy” including “Information Systems Security Guidelines” ⁴ by the RBI in 2001 which provided indicative standards and procedures for Audit of Information Systems including BCP as a component.

The RBI in its Guidance note on “Management of Operational Risk” ⁶ has stressed the need to establish a disaster recovery and BCP for technology related risks as a part of ORM framework. The RBI, in its circular on “Operational Risk Management : Business Continuity Planning” ⁵ clearly states that the responsibility for effective BCP rests with the Board of Directors and the top management and has listed a set of minimum requirements for effective BCM by banks. The circular also required banks to disclose information relating to major failures of critical systems customer segment/services impacted due to the failures and steps taken to avoid such failures in future. The RBI, in its guidelines on “Outsourcing of Financial Services by Banks” in 2005, has mandated banks to ensure that the service provider has a BCP and the same is regularly tested and maintained.

The RBI has made conscious efforts on an on-going basis to encourage banks to have an effective BCP plan in place and has reiterated this vide several circulars. Predominantly, the message from these circulars in relation to BCP is as follows:

- Boards of directors are required to approve a BCP policy; allocate sufficient resources and provide clear guidance and direction in this regard to top management
- Banks may provide for a comprehensive BCP rather than having only disaster recovery arrangements
- Banks should focus on keeping the ‘Disaster Recovery’ site current and to test it comprehensively

Thus, the growing importance for continuity of banking operations in the face of disasters without much interruption is being recognized by banking regulatory authorities globally.

State of BCP in Indian Banking Industry

As we have seen, Indian banks have had a mandate to develop, implement and maintain a BCP for many years. The sheer nature of banking business requires a robust plan to provide resilience and effectively deal with disasters, impacting the continuity of transacting its business. However, the emphasis, more often than not, has been on Information Technology Disaster Recovery Plan (DRP) and not so much on people and processes. Additionally, the terminology of DRP and BCP are used interchangeably stressing importance only on recovery of data and critical applications. The RBI circulars also focus more on the technology aspect. The overall understanding of BCP, therefore, generally revolves around technology recovery and the most important component - the human factor- more often than not is missed out. In the wake of the recent disasters such as bomb blasts in Delhi, floods in Bihar and Orissa, the need for an effective BCM is paramount.

The RBI has in recent times taken significant measures to modernize the Payment and Settlement System by intensifying IT usage. Additionally, the RBI has established three state-of-the-art data centers and successfully migrated many of its systems to the new data centers including critical payment applications such as Real Time Gross Settlement (RTGS) and the Negotiated Dealing System (NDS), etc. The systems have been designed in such a way so as to provide for a high level of uninterrupted availability. The RBI also conducts periodical Disaster Recovery (DR) drills regularly involving all participating members.

Interestingly, the “Mid-Term Review of Annual Policy Statement 2007-08” ⁹ concluded that the level of preparedness by participating banks in periodic drills conducted by RBI in respect of critical inter-bank systems to facilitate banking services and ensure continuity is inadequate. The RBI recognizes that there is a further need to strengthen efforts in respect to BCM for banks. The concept of effective BCM is still evolving in the Indian banks and there are conscious efforts by the banks to move from the traditional concept of disaster recovery to a holistic approach to BCM.

There have been several definitions and interpretations of what a BCP should really cover. It would, therefore, be worthwhile to have a brief overview of what a comprehensive BCP entails.
BCP Demystified

Business Continuity Management (BCM) is defined by the Business Continuity Institute (BCI), UK as a “holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities”.

BCM is the preparedness of an organization to ensure continuity, resumption and recovery of critical business processes at an agreed level and limit the impact of the disaster on people, processes and infrastructure.

BCP, therefore, is not merely making arrangements for recovery of IT infrastructure, but a comprehensive plan that includes people, processes and non-IT infrastructure such as workspace as well.

This involves the key phases of:
- Analysis of the current state
- Development of a BCP
- Implementation of BCP

Another key aspect, often overlooked in a BCM program, involves continuous testing and maintenance of BCP without which the plan would soon become obsolete.

The Business Continuity Institute, United Kingdom (BCI) has also defined a BCM lifecycle that includes six subject areas as depicted in Fig. 4.

It conducts an internationally recognized Certification Scheme for BCI practitioners. The skills required for
obtaining certification and ultimately professional membership of the BCI are assessed in six subject areas which form the BCM life cycle. With a view to raise the awareness of BCM within the banking community, the College of Agriculture Banking of the RBI organized a BCI-recognized BCM training in August, 2008 for the bankers. For more information about BCI training and certifications, please visit www.thebci.org

Conclusion

The importance of a good BCP cannot be emphasized enough. There are seven steps that you should take into account while implementing a BCP.

- **Process** (not a project): BCP does not stop at insurance, or documentation of a plan on paper. Ongoing updation and pre-defined business continuity teams are some of the elements of a successful BCP.
- **Holistic approach**: BCM evolves beyond the information technology realm and should cover people, processes and infrastructure.
- **Focus**: The plan should focus on critical business processes and their dependencies.
- **BCP governance**: Commitment, control and guidance from management, clearly documented roles and responsibilities and formal governance process ensures that the BCP is updated regularly.
- **Resilience**: The recovery procedure should not compromise on the control environment at the recovery location.
- **Involvement of business partners**: All critical business partners should be considered at the time of plan preparation including testing.
- **Media management**: It is important to maintain corporate image during a disaster. A media management strategy enables the organization respond to media coverage proactively / systematically.

Given the increasing threats due to terrorism and natural catastrophes and ever growing dependence on banks in every sphere of life, implementation of BCP by Indian banks is no longer a matter of choice.

References:

1. Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, April 7, 2003
6. RBI Information Systems Audit Policy for the banking and financial sector, October, 2001
7. RBI Guidance Note on Management of Operational Risk, October 2005
8. RBI circular Ref. RBI/2004-05/420 DBS.CO.IS Audit. No. 19/31.02.03/2004-05 on 'Operational Risk Management; Business Continuity Planning'
9. RBI - Mid-Term Review of Annual Policy Statement for the Year 2007-08