Business Continuity Model: A Reality Check for Banks in India

Journal of Internet Banking and Commerce, August 2006, vol. 11, no.2
(http://www.arraydev.com/commerce/jibc/)

By
Prof. Sunil Rai, Joint Director, S. P. Jain Institute of Management & Research, Mumbai, India.
Dr. Lakshmi Mohan, Information Technology Management Faculty, School of Business, University at Albany, State University of New York

Email:
sunilrai@spjimr.ernet.in
l.mohan@albany.edu

Prof. Sunil Rai is the Joint Director in S. P. Jain Institute of Management & Research, Mumbai, India. His areas of interest are Business Continuity Management, IT Infrastructure & Security Management and People Issues in Knowkedge Driven Industries.

Dr. Lakshmi Mohan is a Faculty of Information Technology Management in the School of Business, University at Albany, State University of New York. Her current research interests are on impact of the Internet on business and Enterprise Systems, including CRM, SCM and ERP Systems. Her research publications include papers in prestigious journals such as MIS Quarterly, Decision Sciences, and Transportation Research.

Abstract

We have developed a framework to address the issues related to Business Continuity Management (BCM) and applied it to banks in India. The paper discusses the need for BCM in banks and presents a model to design, implement, operationalize and assess a business continuity plan. The proposed BCM model covers five components relating to the Organizational Soft issues, Processes, People, Technology and Facilities Management; and, defines a variety of metrics to measure the "Resilience" and "Vulnerability" of a bank in the event of business disruptions. The model has been applied to conduct a "reality check" of BCM implementation in 8 large and 14 medium/small banks in India. The value of the model lies in its ability to identify the gap areas for bank management to take corrective action.

1. THE NEED FOR BUSINESS CONTINUITY MANAGEMENT

Banks have formally been in existence for over 200 years. In the post-industrialization era, banks became the hub of economic activity. This was witnessed widely in the commercial sector or what may be termed as B2B (Business-to-Business). Banks also had a significant growth in the development of society at large by way of changes in attitude brought about by personal banking shifting assets from individuals to the public domain. Advancements in technology, particularly computerization and data communication, brought in an unprecedented dynamism to the banking business. There have been changes in the outlook of society from that of protectionism (saving assets for a rainy day) to that of entrepreneurial consumerism. Investments, which were treated as expenditures earlier, are now viewed

as the means to maximize wealth and attain higher levels of advancement. The trend has evolved in terms of generating funds from loans for housing and healthcare to education and, today, even for entertainment and leisure!

The banking industry is challenged to address the varied needs and expectations of diverse segments of society and business such as youth, working people and retired personnel. Businesses may range from small to medium to large, from process to discrete industry, from rural to urban, from national to global and so on. Each segment has unique demands for a customized range of products and services, combined with convenience, at low cost, "any time, anywhere".

This paper proposes a model to design, implement, assess, and upgrade a business continuity plan for banks. The key factors for a successful Business Continuity Management (BCM) implementation have been identified based on an analysis of experiences by major banks in India. In this context, the issue of BCM has been addressed in part by two other models: BCP - Business Continuity Planning, and DR - Disaster Recovery. However, we submit that the two put together do not provide the solution for BCM. They have helped a great deal in streamlining organizational processes and infrastructure to ensure continuity and were, perhaps, complete in a non-globalized, less competitive world. But, today, there are newer challenges in the form of higher degree of expectations in service levels, which transcend transactions and encompass issues dealing with emotive faith and trust.

2. RESEARCH METHODOLOGY

Published literature (particularly on the Internet) is replete with information on building rugged and reliable BCM infrastructure and solutions. These, however, are derived largely from the experiences of large banks and financial institutions in the U.S. and Europe [1]. Our research addresses the need to develop a model for successful BCM implementation for banks in India, with a special focus on small and medium banks who face challenges in both the financial and organizational fronts to create world class BCM infrastructure and solutions.

The following methodology was adopted to develop and evaluate a framework for conducting a reality check on BCM efforts of banks in India and identify gap areas that need to be strengthened.

First, a survey of published information about implementation of BCM practices and experiences (both successes and failures) was carried out in detail to ascertain the essential ingredients of a comprehensive BCM implementation in the financial sector, particularly, banks [2]. A detailed study of literature, including Reserve Bank of India (RBI) communications/directives, was also carried out to understand the regulatory provisions and state of BCM Implementations in banks in India [3].

Based on the literature survey, a theoretical model was developed with the aim of supporting the design and implementation of BCM initiatives in banking, in both the private and public sectors.

Primary research was undertaken next in selected public and private sector banks in Mumbai who have implemented BCP to evaluate the theoretical model as regards completeness and effectiveness. The study was carried out by interviewing corporate managers, bank unit heads and junior executives. Questionnaires were progressively evolved by testing on samples, spot observations and discussion with subject matter experts. The questionnaires were administered to various levels in the selected banks to identify factors that are critical for creating and implementing successful BCM. The learnings were clustered under five separate components: Organizational pertaining to Soft issues; Process; People; Technology; and Hard Organizational issues pertaining to Facilities [4].

A generic model addressing issues related to Organizational, Process, People, IT Infrastructure and Facilities was developed based on the results of the application of the theoretical model to selected banks in India. A set of metrics to track implementation status and monitor the performance of BCM was then created. The model and metrics were evaluated by Focus Group discussions employing the Delphi technique, with senior corporate managers from the selected banks and consultants from the top 5 consulting companies in India.

Finally, the generic model was evaluated for its applicability to selected banks in Mumbai.

3. THE BCM MODEL

The five components of the BCM model are briefly described on the following page:

Organizational

The bank must be clear in its vision and direction. The findings of the survey highlight the importance of clear articulation of the strategic objectives with respect to:

- The markets and geographies to be served.
- The scale, i.e. volumes, to be achieved each year.
- The diversity of portfolio of products and services to be offered in line with the demands of the segments being served.
- The multiplicity of channels to be deployed for delivering products and services.
- Innovative methods of differentiating products and services with a view to enhance value to customers in a cost-effective manner.
- The organization required to meet the above objectives.
- The infrastructure building blocks required to meet the objectives in terms of Information Technology, Communications, Security and Convenience.

Processes

This relates to processes for ensuring continuity of banking transactions, and not the rules and regulations (banking or legal) governing those operations. The following procedures need to be designed, communicated, practiced and reviewed periodically to ensure continuity.

- *Alternate processes* – Most banking processes are IT-enabled or automated. This necessitates a clear-cut scheme of alternate processes that can be resorted to in the event of a technical disruption [5]. Certain banks have a well-documented "Plan B".
- *Roles and Responsibilities*: Procedures to outline in clear terms who is to take responsibility of a particular role which may be at a higher level than, or different from, than his/her normal role in the event of the right person not being available for whatever reason.
- *Options to Customers* and the sequence in which they can resort to alternate processes, channels, outlets etc. ought to be communicated, and a sensitivity check made from time to time.
- *Alternate Channels of Delivery*: All stakeholders, internal and external, should be aware and comfortable to switch to alternate channels of delivery, for example, from Branch to ATM to Internet.
- *Alternate methods of communication to transact business or obtain information*: Paper-based, Internet-based, Voice-based or through third party such as call centers and media agencies (television, newspapers, etc.) for informing clients about alternative processes that have been put in place.
- *Support to Customers* through multiple methods of providing support to customers by way of self-service systems like AVR (Advanced Voice Recognition), Websites, assisted call center help, customer relationship executives and associate partners.

People

This is the most important and critical resource to ensure continuity of businesses on both the demand and supply side. We identify four categories of people who should be involved and be responsible to ensure business continuity. The "Soft Requirements" for these stakeholders to engage in a collaborative manner to ensure continuity are also outlined.

- *Employees*: The knowledge, commitment and motivation of employees at all levels in the bank are paramount to ensure business continuity [4]. It is essential that all employees perform their designated functions correctly, efficiently and effectively. Banks have an excellent record in operationalizing the concept of "job rotation" better than any other kind of business that the authors have been involved with. This ensures that employees possess an acceptable level of knowledge of related functions along with their primary function, where they are expected to be experts [5]. Our survey, however, highlighted variances in realization of some softer aspects, particularly at the operating level. These are:
  - *Empowerment*: To take decisions not only pertaining to authorization and limits, but also in dealing with situations supposedly outside the realm of authority to meet the contingency [6]. This can however be authorized ex-post facto.
  - *Commitment*: To fulfill customer's requirements and not just completion of a task
  - *Motivation*: This is an important factor wherein each employee perceives himself/herself to be the owner of the business, and runs it as if he/she has a personal stake in its successes.
- *Customers*: They are the very reasons for which the business exists and, hence, are the most important link for business continuity. The following aspects are essential for effective engagement of customers while transacting business.
  - *Awareness*: The bank must make the customers aware about the products and services in terms of offerings, limitations, regulations etc. This is the task of every employee who interacts with the customer for whatever duration and for whatever purpose [7].
  - *Esteem*: Customers should be made to feel important and worthy, irrespective of the value or importance of the transaction. Operational responsiveness is only one part of the story. It has to be complemented with visibly evident disposition of the employees in terms of courtesy and care.
  - *Trust*: Sustained performance, cordial treatment and ethical and upright disposition ensure high level of trust, which translates into tolerance on part of the customers in the event of business discontinuity [8].
- *Business Partners*: The terms "Vendors", "Suppliers" and "Contractors" are passé in present times. The correct term for representing all those who contribute

towards the success of your business is “business partners”. They may be involved in facilities management, supplying provisions and consumables, maintaining IT Infrastructure or bandwidth. Irrespective, they are all more than equal partners in the business. Their performance and commitment, including a high degree of ownership, are the mainstays of supporting the business during unforeseen disruptions [9]. The following elements have to be considered in this regard:

- *Service Level Agreements (SLAs)*: Well-defined and justified terms and conditions that form the SLAs are the backbone of a fruitful relationship with business partners.
- *Empathy*: Banks need to be alive to the concerns, both operational and commercial, of their business partners to harness above-par performance and extra efforts needed during unexpected contingencies.
- *Sense of Belonging*: Business partners must feel a sense of belonging to the banks, which can be created by non-discriminatory treatment to them on the same lines as the bank’s own employee in terms of working space, usage of common facilities, and other related factors.

- *External Stakeholders*: These comprise the government (central, state and municipal), regulatory bodies, professional associations, and media. An excellent working relationship in an atmosphere of trust with these stakeholders may also be crucial to find the requisite support for continuing your business as regards operational logistics and image. The following are essential to maintain relationships with these stakeholders:
  - Continued good performance
  - Transparency and honesty of purpose
  - Regular interaction with them on professional and social forums
  - Regular engagement in symbiotic relationship, such as specialized service in terms of dedicated outlets etc.

Technology

There have been significant advances in the usage of technology in the banking sector in general. Our survey does indicate that there are higher levels of maturity and excellence achieved in the selected banks, who have invested heavily in installing near world class IT infrastructure [10]. Broadly the technology usage in banks can be grouped as follows:

- Banking Applications at Service Points:
  Core Banking System, Internet Banking, Phone Banking, and Mobile Banking
- Electronic Banking:
  ATM’s, Smart Cards, Credit Cards, Debit Cards, and Prepaid Cards
- Back Office Processing and Administration:
  Intra Branch end of the day (EOD) transactions, Intranet, Mail Messaging Systems, Online Help, and Magnetic Ink Character Recognition (MICR) Processing
- Inter Branch Transaction handling:
  Real-Time Gross Settlement (RTGS), and Electronic Funds Transfer (EFT)
- Data Communications:
  Intra Branch Network and Inter Bank Network
- Data Center Management:
  Main Data Center and Disaster Recovery Site (Servers, Storage, Backup Systems, Switches, Systems Software, Application Software)
- Security:
  User Level Security - Access Permissions, Authorizations, Application Security - Transactional & Inter Application Security, Systems Security – System – Administration Level & Perimeter Security, and Physical Security - Access Control, System Logs, Fire and Damage Control
- Technical Support:
  Help Desk, Documentation, Performance Monitoring, and Upgrades

Facilities Management

The facilities include physical space, amenities, communication and transportation. It was observed during the survey that, on more than 80% occasions, the discontinuities were on account of non-technical disruptions such as absence of key personnel, sudden increase of loading and other infrastructure-related disruptions, for example, power failure, public network links outage, traffic congestion etc [7]. This is true even in medium to large banks whose IT Infrastructure and automation standards are near world class. Still they face problems due to scale and scope of their products and services offerings. Better Facility Management is therefore, a key issue to be dealt with by banks. Six components have been identified under this head:

- Physical Space:

Front Offices, Office Spaces, Data Centers, Secured Spaces (Vaults), Engineering Maintenance Spaces, etc [7]
- Office Equipment
- Amenities:
  Catering Services, Aesthetics & Comfort, and Entertainment & Information [11]
- Power Supply:
  Captive Power Generators and Uninterrupted Power Supply [7]
- Communication:
  Telephone, Wireless Links, Media, and Calling trees [11]
- Transportation:
  To commute personnel and equipment to alternate sites in the event of disaster [11]

4. THE BUSINESS CONTINUITY REALITY CHECK

We have developed metrics to measure the business continuity parameters for each of the five components of the BCM Model outlined in Section 3: Soft Organizational Issues, Processes, People, Technology and Facilities. For each component, specific measures were defined to capture the relevant issues at four different levels:

A. *Corporate Planning / Policy Level* – This is to ascertain the policy decisions taken by Bank's top management as regards degree of preparedness from the business continuity perspective. The top management sets the performance expectations in terms of quality of service to be rendered, including response time standards for various transactions (personal banking, loans, etc.) On the technology front, these get translated into Recovery Time Objective (RTO), Recovery Point Objective (RPO), etc.
B. *Tactical / Organizational level* – This deals with the organization structure and processes implemented in the bank in accordance with the policy guidelines. This also includes the alternate organization, processes and infrastructure together with outsourced arrangements to cater for emergency situations which cause interruptions to business.
C. *Tools / Methods* – The IT Infrastructure and operating instructions that are pressed into action once discontinuity is declared, including instructions to switch over to "contingent mode" in terms of alternate facilities, movement of people and modus operandi to transact business, and reverting back to normal operations once the contingency is over.
D. *Up gradation / Review / Testing Mechanism* – The prevalent culture and processes adopted by the bank to review and/or test the BCM organization and effectiveness, and upgrade the same on a regular basis or as and when necessary.

The table below shows the number of metrics for each Component and Level. Details each metric are available with the lead author of this paper.

Component Level	Organizational (Soft)	Process	People	Technology	Facilities
1. Corporate Planning / Policy Level	9	14	2	10	3
2. Tactical / Organizational Level	7	6	8	12	4
3. Tools / Methods	3	1	5	3	3
4. Up-gradation / Review / Testing Mechanism	2	4	3	3	5

Each of these metrics was assessed by respondents in the selected banks according to four criteria to measure Effectiveness:

- *Strength / Preparedness*, (shortened as P), of the bank in addressing the issue specified in the metric on a scale of 0 to 5
  0 - Very Low; 1 – Low; 2 – Moderate; 3 – Satisfactory; 4 – High; 5 - Very High
- *Threats / Challenges*, (shortened as R), both internal and external, faced by the bank in meeting the requirements of the metric
  0 – Negligible; 1 - Very Low; 2 – Low; 3 – Moderate; 4 – High; 5 - Very High
- *Vulnerability*, (shortened as V), of the bank in terms of the Probability of Occurrence of the threat or challenge in the bank on a scale of 0 to 1: 0 – Negligible and 1 – Near Certain
- *Up-gradation Factor*, (shortened as T), does the bank upgrade/test/review the state of preparedness on a regular and systematic basis on a scale of 0 to 1: Somewhat & Occasional to Highly Organized and Regular

Application of the Metrics

The metrics were administered to 8 large and 14 small and medium banks in Mumbai at three management levels: Top Management, Middle Management and Functional Management. The data was normalized to smoothen stray responses due to incomplete knowledge or not understanding the genesis of the parameter in question. The responses were analyzed to understand the prevailing status in each bank with emphasis on seriousness and completeness of the BCM implementation as well as its effectiveness. The gap areas were then identified along with the degree to which they need to be addressed by bank management in order to keep their BCM current and effective.

The following steps outline the analysis of the data obtained in the surveys to compare Strengths / Preparedness against Vulnerability:

Step 1: Calculate "Resilience Indicator" (RI) as shown below: RI(F) = P(F) * T(F) where, RI is the Resilience Indicator F is the Parameter or Metric in question P is the Preparedness T is the Up-gradation Factor

Step 2: Calculate "Vulnerability Indicator" (VI) as shown below: VI(F) = R(F) * V(F) where, VI is the Vulnerability Indicator F is the Parameter or Metric in question R is the Threat / Challenge V is the Vulnerability

These Indicators were then compared for Large and Small banks to evaluate their relative positioning on each parameter.

5. DATA ANALYSIS AND FINDINGS

The scores for P, R, V and T (defined above) were calculated for the metrics relating to each of the five components for Large banks as compared to Small banks. The Resiliency and Vulnerability Indicators were then determined, again for each of the five components for Large banks vs. Small banks. The key findings are summarized in this section.

- Small banks are more Vulnerable than Large Banks on all the factors except "Organization" as can be seen from the table below:

Component	Average of Resilience (RI)		Average of Vulnerability (VI)	
	Large	Small	Large	Small
Organization	3.23	2.47	1.34	1.46
Procedure	3.36	2.67	0.65	2.61
People	3.54	2.51	0.64	2.85
Technology	3.40	3.92	0.55	3.31
Facilities	2.43	4.06	0.26	3.37
Overall	**3.24**	**3.12**	**0.71**	**2.71**

Interestingly, the Resilience of Small banks is higher than Large banks with regard to "Facilities" and, to a lesser extent, "Technology".

On the whole, Large banks are less vulnerable (0.71 score) than Small banks (2.71 score), which is logical given that Large banks have the funds to invest in organization, infrastructure and technology to establish reliable and rugged processes to counter any eventuality.

- The Average Vulnerability Indicator (VI) for each of the three components - Organizational, Facilities and Technology – is shown below for Large and Small banks:

Bank	Average of Vulnerability (VI)		
	Organization	Facilities	Technology
Large	1.34	0.26	0.55
Small	1.46	3.37	3.31

Large banks are more vulnerable to discontinuity on account of Organizational issues as compared to Facilities and Technology. Small banks are more

vulnerable with respect to Facilities and Technology. The Organizational issues are far more complex in Large banks owing to size, hierarchy, expanse and diversity making them more vulnerable. It is often said that it is difficult to make “elephants dance”. The Small banks, on the other hand, are unable to put in place world-class facilities and technology as it involves sizable investment that cannot be met within their operating budgets.

- The Average Resilience (RI) for Facilities Management issues for Large and Small banks were calculated to be 2.43 and 4.06 respectively. Large organizations are, hence, less resilient with regard to Facilities management as compared to Organization and Technology. The lesser resilience of Large banks in managing facilities is largely due to their size and expanse (all over the country). Small banks, on the other hand, have mostly state-level operations, and have facilities which are fairly compact, and can, hence, be managed easily. Large banks have strong organizational structures, adequately manned departments as well as well-documented and well-communicated procedures as compared to their smaller counterparts.

6. THE WAY AHEAD

The application of the model to banks in India has given insights into the gaps that exist in otherwise seemingly comprehensive BCM implementations. The BCM organization and practice needs to be monitored regularly to ensure its relevance under contemporary conditions. The model serves as a “barometer” to do a reality check and apply corrections where necessary. The trends in banks in India suggest the following conclusions:

- Issues related to Facilities and Technology are better poised to handle business disruptions because of advances in Technology and Maturity of banking practices.

- More management attention will have to be focused on softer issues of service delivery such as trust of customers, image in the industry, and participation of all stakeholders as owners.

BIBLIOGRAPHY

1. Vicky Kubitscheck, AEGON UK and Chair - Insurance internal audit group (UK), Business discontinuity – a risk too far, Volume 9 Number 3 2001 pp. 33-38, ISSN 0965-7967
2. Dave Shore, Web-based solutions can ensure business continuity, Published: 5/20/02, http://techrepublic.com.com/5100-10878_11-1048802.html?tag=search
3. M. R. Srinivasan, Chief General Manager-in-Charge, Internet Banking in India – Guidelines to All Scheduled Commercial Banks, DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01, June 14, 2001
4. Ron Bleiberg, SmartAdvice: Planning Ahead Means A Disaster Needn't Wipe Out Your Business, Aug. 22, 2005, http://www.fileon.com/press/articles/disaster-neednt-wipe-out-business.html
5. Excerpts from interviews with Mr. Ravi Trivedy, Partner, KPMG and Mr. V. Girish, Banking, Financial Services & Insurance, Consultant, April 15, 2006
6. Jon Oltsik, Hot spots: So much can go wrong with disaster recovery. What can you do to ensure all goes well?, Published: Jun 2004, http://storagemagazine.techtarget.com/magItem/1,291266,sid35_gci969972,00.html
7. Hal Hunt, Lesson of Hurricane Hugo: Plan Recovery, 08/05/04 6:00 AM PT, Part of the ECT News Network, http://www.crmbuyer.com/story/35561.html
8. Excerpts from the interviews with Mr. S. S. Purohit, DGM, SBI Zonal Office (West), Mumbai on 28th December 2005, 24th January 2006 and 16th March 2006.
9. Dave Shore, Sept. 11 teaches real lessons in disaster recovery and business continuity planning, Published: 5/17/02, http://techrepublic.com.com/5100-10878_11-1048799.html?tag=search#
   Marc Staimer, Data determines the right disaster recovery, Issue: Jan 2005, http://storageMagazine.techtarget.com/magItem/1,291266,sid35_gci1042972,00.html
10. Security 2002: Rethinking Risk, Published: September 16, 2002, http://www.cioinsight.com/article2/0,1540,537635,00.asp

ACKNOWLEDGEMENTS

Authors are thankful to the following professionals for their support and guidance:

1. Senior Management of target banks
   Mr. Ajit Rath, Mr. B. T. Pillai, Ms. Bhavana Ugrankar, Mr. Dinesh Pandey, Mr. G Subrahmanyam, Mr. Kalyan Sundaram, Ms. Naina Panse, Mr. Suren Shetty, Mr. T. Prabhakar
2. Academicians and Researchers
   Dr. M. L. Shrikant, Dr. Suranjan Das, Prof. Suresh Lalwani, Ms. Priti Miranda, Ms. Dipali Manjrekar, Ms. Lakshmi Narayan, Mr. Rajesh S., Mr. Bharat Mishra