Business Continuity and Disaster Recovery Experience in Indian Banks

Shirshendu Maitra
Ph.D. Research Scholar,
JJT University
Jhunjhunu, Rajasthan, India

Dr. Meera Shanker
Associate Professor & Head (Management),
JDBIMS, SNDT Women's University,
Mumbai, Maharashtra, India

Pankaj K. Mudholkar
Ph.D. Research Scholar,
JJT University
Jhunjhunu, Rajasthan, India

Abstract- Advances in the banking sector have brought in an era of multi-product and multi-services being delivered using multiple yet integrated channels. The use of information and communication technology (ICT) is on the increase and encompasses nearly the entire gamut of banking operations. Rising competition and customer expectations have compelled top management to implement, and continuously upgrade, agile and scalable ICT practices and solutions. The enormity and range of banking services combined with the complexity of integrated and ICT-enabled delivery mechanisms require comprehensive partnerships to be forged between banks and providers of ICT solutions, especially with regard to Business Continuity Management (BCM). This paper presents the preliminary findings of a research study to identify the essential ingredients of successful BCM implementation based on experiences of banks in India.

The paper outlines the business continuity planning as a methodology that could be used by organizations in order to reduce the risks that occur both at the organizational level and in its outside environment. There are presented the main objectives and steps in business continuity planning process. In the end of the paper are presented some issues that organizations should take into consideration in the implementation of business continuity planning process projects.

Keywords-component: business continuity planning, business impact analysis, risk assessment, risk management, Disaster recovery planning

I. INTRODUCTION

Business interruptions can occur anywhere, anytime due to massive hurricanes, tsunamis, power outages, terrorist bombings etc. It is not possible to predict what may strike when. In today's world, it has become mandatory to prepare for such disaster scenarios always. Under this circumstance and 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'(BCP).

Most organizations, including banks, in Maharashtra nowadays depend on the information technology (IT) on their key business functions. In fact, IT is considered "a vital component for conducting business" (Jacques & Rossouw, 2004). Using simple logic, the value of the IT services for an organization can be known by understanding the impact on the business in case of failure in IT systems. Consequently, upon this understanding, organization management undertakes the right actions to ensure the continuity of information technology services (John R. Harrald, 1999).

According to Wing S. Chow (2000), IT is highly considered as a business continuity enabler in an organization due to high dependency on it. Hence, the process of enabling business continuity of IT services ensures the availability of IT services whether in normal or abnormal situations. IT business continuity is considered a

competitive advantage of a business especially in the e-business environment where the whole business is IT-dependent and data driven.

Disaster Recovery (DR) options can be visualized in a pyramid model. The least expensive, and most time consuming DR solutions would be found at the bottom levels of the pyramid. At these levels, 100% recovery of data lost in a disaster at the primary site is not possible. When proceeding to the top, each successive "tier" of the pyramid requires a greater investment in software, communications facilities, transportation equipment and System server and storage hardware. The return for this higher investment in services and equipment is the potential of a significantly shorter recovery time, with minimal loss of data, compared to the preceding tier. The top of our pyramid model would be reserved for those mission-critical applications with effectively zero data loss, as well as very rapid restoration of operations, following a disaster.

Business survival necessitates planning for every type of business disruption including but by no means limited to the categories of natural disasters; hardware and communications failures; internal or external sabotage or acts of terrorism; and the failures of supply chain and sales affiliate organizations. While such disruptions cannot be predicted, they can wreak havoc upon the business, with results ranging from insured losses of replaceable tangibles to uninsurable capital losses to customer dissatisfaction and possible desertion to complete insolvency.

A business continuity strategy, then, is a high-value but high-maintenance proposition. Business continuity embraces a broad spectrum of technologies: old and new, paper-based and electronic, manual and automated, individual and integrated.

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'.

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 boundary less 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. It is imperative that the costs of operation only increases by not having a proper BCP/DRP in place. 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.

Business continuity (BC) in IT has been of interest to many IT professionals. It is a very big subject and many studies have been conducted to address different aspects of it (Wing S. Chow, 2000). Some researches focused on the high level planning and management side of it which led to introducing processes inside the organizations such as business continuity management (BCM) and business continuity planning (BCP) processes. Others focused on the technical part of it which led to introducing technical business continuity solutions such as fault-tolerant systems and data replication solutions.

Business Continuity Planning (BCP) lifecycle is an iterative continuous process that involves business risk and impact analysis, preparation of required emergency procedures, testing and auditing recovery procedures, staff training and awareness of recovery procedures, and maintenance of the business continuity plan (Mick Savage, 2002). The purpose of the BCP is to keep organization business running. This is achieved by creating a plan that addresses how the recovery of key business functions will be in case of incident or a disaster.

II. LITERATURE REVIEW

Some preliminary works on BCP and DR in banking have been made through using data analysis. This literature review was also conducted to help put the research methodology in a better conceptual framework. In this regard the review focused on: the evolution and definition of DR; processes of BCP adoption; benefits, barriers and challenges to BCP adoption.

Information in literature highlighted common standard approaches and practices to develop BCP such as risk assessment and business impact analysis. However, literature review did not show a specific approach that addresses

decision making process based on considering key factors within BCP such as customer SLA or data security related factors.

Business Continuity (BC) in IT is the uninterrupted availability of IT resources that support key business functions. According to Business Continuity Institute (thebci.org) business continuity is a general term that includes disaster recovery. Both terms are used interchangeably in IT to refer to the ability to recover from a disaster or unexpected event. Most of the literature refers to the BC and DR as IT BC/DR for short. The interest in Business Continuity has gained significant momentum in the last few years, especially with the Y2K non-event, the increasing corporate dependence on computer systems and the growing levels of devastation associated with recent disasters.

The concept of business continuity has evolved almost with the begging of computer and communication industry since 1950's (Business Resilience). Unfortunately, it was not a major concern for organizations until September 11, 2001 (Mick Savage, 2002).

Michael and Sonia (2004) and also Nijaz (2006) agreed that business continuity is mostly focused on IT systems in a given organization. Business continuity has two major components: Business Continuity Management (BCM) and Business Continuity Planning (BCP).

Integrating business continuity in an organization involves introducing a management process dedicated to plan and operate business continuity tasks. This process is called business continuity management process (BCM). According to Michael and Sonia (2004), the focus of BCM has shifted from technology-focused (1970) to value-based (1990) as a strategic advantage to business.

In simple terms, Business Continuity Planning (BCP) is an iterative process that creates plans and procedures to be used in case of disasters. Mick (2002) emphasized that BCP should be absorbed in organization culture. The most common model of BCP lifecycle in literature has four major phases:

Phase I: Business & IT services Analysis: In this phase, all business processes and functions are identified and then analyzed through performing risk assessments and business impact analysis (covered later in this chapter). (Michael & Sonia, 2004). Business dependencies will be clear after completing his phase and can be visualized by Business modeling (Leon, 2006). The analysis phase identifies key requirement for the subsequent BCP phases.

Phase II: BC Solutions Planning & Design: Activities in this phase include defining scope and objectives of the plans, creating emergency procedures and design of recovery solutions and procedures. Estimation of costs and resources of developing the organization BCP takes place in this phase (Michael & Sonia, 2004).

Phase III: BC Solutions Testing & Implementation: According to Nijaz Bajgoric(2006), key activities in this phase include testing and deployment of plans and solutions and training of involved staff. Testing and implementation might take long time until the requirement is fulfilled.

Phase IV: Maintenance & Review of BCP: Regular review and enhancement as well as documentation are the key activities in this phase. This phase is to ensure up to date plans (Jacques & Rossouw, 2004).

Mick Savage (2002) sees that since IT is being important component in an organization, then BCP should include detailed specification about IT systems. Such specifications should contain IT systems documentation and preferably in graphical representation. In addition, business functions should be linked to IT systems using either business impact analysis (BIA) or business modeling which will be covered shortly in this chapter.

The challenge of having a close-to-perfect and valid-always BCP for IT is due to the fact that IT systems are dynamic in nature in terms of upgrades and re-configuration. (Mick Savage, 2002).

As banking operations rely greatly on critical transaction data, continuous availability of information and fast recovery from system failures may spell differences between success and failure of the financial sector. Uninterrupted service of such IT system constituent as networks, servers, storages, and integrated systems is crucial. Zero downtime is an ultimate goal, although it is practically unachievable. At times, at IT system is subject to planned or unplanned service disruptions.

IT contingency planning, business continuity planning, and disaster recovery planning are required to ensure proper handling of the disaster and to promptly resume normal operations (Elrod R.,2005).

Some recommended disaster recovery measures from Rudolph, C. G (1990) include

i. Worst-case scenario planning for a disaster

ii. Initiating strategies for recovering critical business data or processes

iii. Implementing technologies to support the recovery of automated functions and systems

iv. Training involved operators on operational and contingency processes for handling with all unexpected incidents.

Young-Fai Lee & John R. Harrald (1999) stated that “preventive measures are more important than recovery measures.” Pre-planned procedures for system recovery represent significant part of IT contingency planning, particularly for

companies whose critical business functions rely mostly on data communication. Proper IT contingency planning is thus key to optimizing operations and investment.

Geary W. Sikich (2003) investigated that once any disruption occurs, the organization must know how to handle the situation immediately. This is called incident handling or crisis management. After the incident has been taken into control, the other business continuity processes will do what is necessary to continue delivery of products and services to the intended parties within the acceptable and already agreed 'Service Level Agreement' (SLA). The final step will be to recover the damages or losses and restore the operation into its original status.

In the area of improving the responsiveness to network /system alerts in IT operations, Hanemann, A.(2005) presented a service fault management framework, which identified the relevant components and their interactions between them to provide a service-quality-based fault management. Hanemann, A.(2005) also presented a framework to automatically determine the impact of resource failures with respect to services and service level agreements by monitoring the service quality from inside and outside the service provider and also by incorporating information about the current and expected future service usage.

The research in (Michael Pit & Sonia Goyal, 2004) aims at addressing the issues with respect to the service orientation in the IT management industry. The developed approach aims to build a repository of all information needed that is required for business-oriented service management. None of the previously mentioned however makes use of BCP concept to deal with the service oriented fault correlation and service impact analysis as we do in this work.

For the activities in BCP, (Nijaz Bajgoric, 2006) made clear that BCP and plans did not mark the end of business continuity activities. They are the pivot between planning and the ongoing management of increased resilience from and response to business interruptions.

According to Maria Cirino (2007) many people equate BCP with IT disaster recovery planning. BCP should contain a detailed specification of system and network infrastructure. Such documentation should make it clear which key business processes and functional activities are dependent on each of the systems. In fact, the purpose of BCP not only documents backup and recovery procedures along with details of any off-site storage arrangements for data/media in response to significant premises-based incident (power outage, fire, flood, etc.), but also provides the full understanding of the key business processes/activities/systems to react service-based incident (e.g. email, venue facilities, network services, etc.).

Charles Cresson Wood (2002) reviewed the development phases for BCP and highlighted that BCP had evolved from simple reactive disaster recovery planning, to crisis management principally driven by information technology, and finally to a more proactive comprehensive approach. The use of BCP in aiding service impact analysis for fault management is therefore cited as the effective way to help organization for better IT service management. ITIL subdivides service support into the areas of incident management, problem management, change management, release management and configuration management. Service delivery is subdivided into the areas of service level management, financial management, IT service continuity management, capacity management and availability management. Detailed description of these processes is not included here. One can refer to (Russel Smith, 1995) for details.

On the other hand, although IT service continuity management process in (Robert Hester, 2009) is part of the service delivery set the process primarily considers continuity plans development and those IT assets and configurations that support the key business processes rather than the activities in service-oriented fault correlation and business service impact analysis. Today, business services are supported by IT services and sub-services which in turn depending on the underlying IT resources. There are not only situations where an IT service is available or not, but it can be available with a low quality. Although software tools with respective management modules are available in the market for ITSM, solutions for managing IT services, customers and operational processes are not sufficiently developed nor integrated with other management applications following IT services daily processes (Mick Savage, 2002). To provide agile response to service event which is derived from resource event, we propose to adopt BCP processes to structure the correlation matrices for service impact analysis in IT service management. By making use of the structured process in BCP development, the IT operation management can realize the linking properties amongst business services, IT services, IT sub-services and IT resources. This knowledge framework acts as the supplementary process for fault management in the existing ITIL processes.

James C. Barnes in his book titled "A guide to Business Continuity Planning" has succeeded in providing us a much-needed tool, with which we can confidently face many of the day-to-day challenges of business contingency. With this book, he has taken an important step in removing much of the guesswork and frustration from the business continuity implementation project (James C. Barnes, 2003).

In Business Continuity and Disaster Recovery Planning for IT Professionals by Susan Snedaker (June 21, 2007) it is reminded of importance of creating and maintaining a BC/DR plan. The purpose of this book is to cover many important elements of BC/DR .It provides a framework within which we can develop an effective BC/DR plan for the

company. It targeted at small and medium-sized businesses, though it can be easily used in larger companies. The book adheres to industry standards and practices though it does not deal in detail, comprehensive and exhaustive look at BC/DR. But for a fast and effective framework that can be used in a small sized company, this book is an ideal guide.

In the article (Gary Donlon, 2004) it is mentioned that without the flow of electronic information, government comes to a standstill. When a state's data systems and communication networks are damaged and its processes disrupted, the problem can be serious and the impact far-reaching. The consequences can be much more than an inconvenience. Serious disruptions to a state's IT systems may lead to public distrust, chaos and fear. It can mean a loss of vital digital records and legal documents, loss of productivity and accountability and a loss of revenue and commerce too.

According to Montri Wiboonrat, Kitti Kosavisutte (2008) disasters that shut down a bank's mission critical applications for any length of time could have devastating direct and indirect costs to the state and its economy that make considering a disaster recovery and business continuity plan essential. The bank's Chief Information Officers (CIOs) have an obligation to ensure that bank IT services continue in the state of an emergency. The good news is that there are simple steps that CIOs can follow to prepare for before, during and after an IT crisis strikes. The book also suggested that Disaster recovery and business continuity planning provides a framework of interim measures to recover IT services following an emergency or system disruption.

Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or execution of agreements with an outsourced entity. IT systems are vulnerable to a variety of disruptions, ranging from minor short term to major term.

In (Peter H. Gregory CISA CISSP, Philip Jan Rothstein, 2007) IT Disaster Recovery Planning for Dummies by Peter H. Gregory he combines a common and time-proven methodology that can be helpful for the organization during disaster. The authors' goal is simple: to help and prepare people, system and processes for an organized response. How the system can be made more resilient meaning people will need to put less effort is described here.

Wing S. Chow (2000) said that as important as all constituents within the organization understanding their role in time of crisis is senior management's support of the continuity program. And the best way to win that support is to present business continuity as a business issue. Threats Addressed As the word continuity implies, today's emphasis is ensuring and safeguarding continuous business operations against a litany of potential threats originating from one of three categories: nature, technology, and man-made events. Nature has certainly exhibited its fury; Hurricane Katrina and the recent Southern California fires are two recent and devastating examples. Technology disruptions occur most frequently, ranging from power outages to hardware and software breakdowns to e-mail failure. And recent history has given rise to an array of diverse manmade disruptions - from the horror of the September 11th attacks to workplace violence to executive ethical misconduct. Clearly against these odds, mitigation and response has taken precedent over recovery. A holistic approach to continuity planning is both necessary and vital to ensure enterprise-wide success. In its absence, the impact of business "downtime" can be significant and enduring, including loss of revenue, customers, reputation, and market share, as well as employee attrition, market value, and much more.

Today all banking businesses rely on electronic commerce services. Since banking business services are involving with security, reliability, availability, online-real time, and accuracy of information, electronic commercial service needs rapid resumption to normal productions no matter what critical disaster levels is (Mick Savage, 2002). The business continuity plans propose for maintaining, resuming, and recovering the business not only the recovery of the service systems and data, but also the provision of guidance and examination procedures to assist, evaluate financial services, and provide risk management processes. This will ensure the availability of critical financial services (Leon Erlanger, 2006)

III. OBJECTIVE

A disaster recovery plan should interface with the overall business continuity management plan, be clear and concise, focus on the key activities required to recover the critical IT services, be tested reviewed and updated on a regular basis, have an owner, and enable the recovery objectives to be met.

The objectives of the study are:

1. To identify external factors that influence decision making process during the BCP lifecycle in banking organizations in Maharashtra.
2. To identify internal factors that influence decision making process during the BCP lifecycle in banking organizations in Maharashtra.
3. Employ the above factors in an assessment model that can be used throughout the whole BCP lifecycle.
4. As per the recovery time objectives, how long can the banks continue to function without the critical IT services (how quickly it will recover the service from the 'decision to invoke'). Resuming critical operations within a specified

time after a disaster is also of high importance; otherwise in today's world of competition customers may move to other Bank for their service.

5. The recovery point objective, from what time in the processing cycle it is going to be recovered the data (how much data the organization is prepared to lose or have to re-enter from an alternate source). There are several options, these are:

- zero data loss, recovery to the point of failure;
- start of the current business day (SoD);
- end of the previous business day (EoD);
- period end, the weekly or monthly backup.

6. Minimizing financial loss in case of banking industry by having proper DRP/BCP .Financial loss will arise out of non-functioning of important banking operations. To minimize or mitigate it is also required on bank's behalf to assure clients, customers, community, suppliers, employees and share holders and stakeholders that their interests are protected and always maintaining a positive public image of the organization will also help in the long run.

IV. PROBLEM STATEMENT

Since decision making process throughout BCP lifecycle is affected by internal and external qualitative factors to the organization, this research attempts to answer the following questions:

1. What are the external factors that influence decision making process during the BCP lifecycle?
2. What are the internal factors that influence decision making process during the BCP lifecycle?
3. How can these factors be employed to present an assessment model for decision making process in banking organizations in Maharashtra?

V. RESEARCH METHODOLOGY

The research is based on collecting qualitative data extracted from a survey which is then formulated into another quantitative survey. The explanation of both surveys and the research propositions and methodology is going to be presented.

In order to appreciate the current trends in IT disaster recovery planning activities in Indian banks , a mail-out survey was distributed to 2 private and 2 nationalized banks in India.

Surveys were mailed to IT professionals in banks who were involved in IT BC/DR process ,CEOs and bank managers. The questions were derived specifically for the purposes of this study. A cover letter explained the purpose of the survey and included directions for its completion. Among these directions was the request to have the individual in charge of information technology complete the survey. Along with the cover letter and the survey, a self-addressed, business return envelope was included for returning the survey.

Alternatively, a web-based version of the survey was also available. The cover letter provided the web address of the survey and included an authentication code for activating the survey. Later analysis indicated that there were no significant differences in responses between paper-based surveys and web-based surveys.

A. Target Populations–

This research is exploratory research in nature since it attempts to find out the qualitative factors such as effectiveness, efficiency and other attributes on the corporate performance reference to banking sector in Maharashtra. Hence, it is targeting IT professionals in banks who were involved in handling e-business. Those people are aware of the risk and responses of using e-businesses, several security issues of using e-business facilities in banks. To go further step and measure, in real life, the research is also targeting the customers of the banks who are using these facilities.

B. Sample Size-

The survey includes approximately four banks (both private and private sectors).I'll include approximately 25 IT banking professionals and 25 IT experts from different organizations.

C. Sources for the data used-

The study is based on both primary and secondary data.

D. *Primary Data-*

Survey questionnaire was administered to empirically assess the level of adoption and strategy taken by the banks for the BCP/DR in Maharashtra. A survey questionnaire will be completed by the banks' IT employees' respective banks, IT experts of different IT organizations.

E. *Secondary Data-*

The secondary data obtained through the Net, books and related journals. The four banks' strategies with regard the BCP and DR will be retrieved from these banks' annual reports, websites, and referred journals. These annual reports were obtained from the banks' themselves through their Web sites.

VI. RESULTS

The results of the analysis were organized so that a series of benchmarks could be established (see Table 1). As mentioned in previous sections, these benchmarks relate to IT disaster recovery planning activities, not parts of actual plans. They are grouped according to the seven categories of activities, and are summarized on the following table. The third column on the table indicates the percent of banks which perform each process.

I 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.

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

Table 1 : Levels of BCP practices

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

VII. CONCLUSION

As per the survey the following factors critical to implement reliable BCM structure and practices .Establish and nurture partnerships with agencies that work in a collaborative mode in supporting banking operations with technology.

a) The customers and partners hold an esteem value about the bank and that is not only a catalyst for progress, but also provides strong support during the phase when the bank is attempting to recover from a disaster.

b) A wider customer base served with a variety of products and supported on multiple delivery channels ensures higher degree of continuity, both in terms of operations and preparedness of a bank in dealing with disruptions in services.

c) Most banks consider state-of-the-art technology as critical to growth and efficient delivery of service. Some large banks also do not want to give up manual processing which they consider as the last resort in effecting transactions during a major discontinuity.

With regard to the current status of BCM practice, the following are important:

a) Banks have put together reliable IT Infrastructures to support their operations. These are built using high-end platforms and proprietary solutions. Certain banks also have custom-built solutions developed by in-house teams using open-source software to attain vendor independence.

b) All banks that have achieved high degree of computerization have modern central data centers with distant DR Sites. The DR site utilization percentage was, however, found to vary significantly. Only a few banks are more regular with putting the actual load on DR Sites frequently.

c) The composition of teams managing IT in banks is mostly a judicious mix of Banking and Systems professionals to foster a rich blend of knowledge of banking processes and technology.

d) The advanced practices of server and storage consolidations to optimize data storage and processing have been implemented in the banks studied.

e) Security at both database and systems levels has been implemented in most banks using complex and comprehensive third-party solutions.

f) The Network and Systems Administration are carried out using remote control solutions ensuring greater reliability and efficiency.

Most banks have built sufficient redundancy in their information and communication technology components to ensure a high degree of reliability.

REFERENCES

[1] Agatino Grillo (2003). "Information Systems Auditing of Business Continuity Plans". Upgrade. Vol 4. No 6. pp:12-16.

[2] Aidan Berry and E. Jarvis (1993). "Accounting for decision making: resource constraints and decisions which are mutually exclusive". Accounting in a Business Context . Chapman & Hall: pp:401.
[3] Carol V. Brown, Daniel W. DeHayes, Jeffery A. Hoffer, E. Wainright Martin, William C. Perkins. "Managing IT in an E-world". Managing Information Technology . Person Prentice Hall: pp 1.
[4] Charles O. Omekwu (2006). "African clustuer and libraries: the information technology challenge". The Electronic Library. Vol 24. No 2. pp 243-264.
[5] Charles Cresson Wood (2002), Information Security Policies Made Easy, Information Shield Inc.,pp: 202-210
9. Gary Donlon (2004). "IT Service Continuity: Know the unknowns". Service talk. Issue No 66. pp:38-39.
[6] Geary W. Sikich(2003), Business Continuity: Maintaining Resilience in Uncertain Times, Pennwell Books,pp:234-240
[7] H. Frank Cervone (2006). "Managing digital libraries: the view from 30,000 feet. Disaster recovery and continuity planning for digital library systems". OCLC Systems & Services. Vol. 22 No. 3. 173-178.
[8] Jacques Botha & Rossouw Von Solms (2004). "A cyclic approach to business continuity planning". Information Management & Computer Security. Vol 12 ,pp:328-337.
[9] James C. Barnes (2003), A guide to Business Continuity Planning, John Willey & Sons, ISBN:13-978-0-8144-1613-6,pp 125-132
[10] John William Toigo(2002), "Disaster Recovery Planning:Preparing for the Unthinkable", 3rd Edition, Prentice Hall,pp:19-54
[11] Joshua Weinberger (2004). "Averting Customer Data Loss". Customer Relationship Management. Vol 3, p 16.
[12] Kakoli Bandyopadhyay & Peter P. Mykytyn & Kathleen Mykytyn (1999). "A frame work for integrated risk management in information technology". Management Decision. Vol 37 No 5. pp: 437-444.
[13] Leon Erlanger (2006). "In case of emergency activate business continuity plan". InfoWorld. pp:27-31.
[14] Dr. Manik Dey(2011),Business Continuity Planning (BCP) methodology –Essential for every business,ISBN:978-1612-84-119-9
[15] Maria Cirino(2007), The Art of Comprehensive Vulnerability Management (Black Book Series), Larstan Publishing,pp: 156-162
[16] Michael Pit & Sonia Goyal (2004). "Business continuity planning as a facilities management tool". Facilities. Vol 22 No 3/4. pp:87-99.
[17] Mick Savage (2002). "Business continuity planning". Work Study. Vol 51 No 5. pp:254-261
[18] Montri Wiboonrat, Kitti Kosavisutte(2008), Optimization Strategy for Disaster Recovery :ISBN 978-1-4244-2330-9
[19] Nijaz Bajgoric(2006). "Information technologies for business continuity: an implementation framework". Information Management & Computer Security. Vol 14 No.5. pp:450-466
[20] Peter H. Gregory CISA CISSP, Philip Jan Rothstein (2007), IT Disaster Recovery Planning For Dummies: ISBN: 978-0-470-03973-1
[21] Rentsch, T(1982), Object Oriented Programming"; SIGPLAN Notices; Vol.17 ; pp:51
[22] Rick A. Myer, Christian Conte & Sarah E. Peterson (2007). "Human impact issues for crisis management in organizations". Disaster Prevention and Management. Vol 16. pp:761-770
[23] Rudolph C.G(1990), "Business Continuation Planning/ Disaster Recovery: A Marking Perspective." HBS, Pp 25-28.
[24] Russell Smith (1995). "Business continuity planning and service level agreements". Information Management & Computer Security. Vol 3 . pp:17-19
[25] Samuel Certo and Trevis Certo (2006). " Making Decisions". Modern Management (10th ed). Prentice Hal: pp:161
[26] Samuel Certo and Trevis Certo (2006). "Strategic Planning". Modern Management (10th ed). Prentice Hal: p:180
[27] Scott, D. (2002), Best Practices and Trends in Business Continuity Planning, Gartner Symposium ITxpo 2002, Gartner, Inc.,pp: 230-235
[28] Sharman Lichtenstein (1996). "Factors in the selection of risk assessment method". Information Management & Computer Security. Vol 4 No. 4. 20-25
[29] Sharon Halliday, Karin Badenhorst & Rossouw Von Solms (1996). "A business approach to effective information technology risk analysis and management". Management & Computer Security. Vol 4 ,pp: 19-31
[30] Stewart H.C. Wan & Yuk-Hee Chan (2008). " Improving service management in campus IT operations". Campus-Wide Information Systems. Vol.25 No. 1. pp:30-49
[31] Stewart Wan (2009). "Service impact analysis using business continuity planning process." Campus-Wide Information Systems. Vol 26. No. 1. pp:20-42
[32] Susan Snedaker(2007), Business Continuity & Disaster Recovery for IT Professionals. Publisher: Syngress. ISBN-10: 1-59749-172-34, pp:34-40
[33] ThuyUyen H. Nguyen (2008). "Information technology adoption in SMEs: an integrated framework". International Journal of Entrepreneurial Behavior & Research. Vol 15 pp:162-186
[34] Tillal Eldabi, Zahir Irani, Ray Paul & Peter E. Love (2002). "Quantitiative and qualitative decision-making methods in simulation modeling". Management Decision. Vol 40 pp:64-73
[35] Wing S. Chow (2000). "Success factors for IS disaster recovery planning in Hong Kong". Information Management & Computer Security. Vol 8 No. 2. pp:80-86.
[36] Young-Fai Lee & John R. Harrald (1999). "Critical issue for business area impact analysis in business crisis management analytical capacity". Disaster Prevention and Management. Vol 8 No 3. pp:184-189