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. 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 the 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'.

![Costs of DRP/BCP](image)

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. From Fig 1. 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.

**Background of the Study**

As mentioned above, in banking organizations whether small or big, decision making process during the phases of BCP depends on certain factors that are analyzed and
studied well by IT professionals. The variables that are of importance to this research can be categorized as follows:

• Organization external qualitative factors that influence decision making process in BCP.
• Organization internal qualitative factors that influence decision making process in BCP.

Qualitative factors affecting decision making inside the BCP have not been a major focus for researchers since every organization is unique and the decision making process is largely organization-dependent. According to Nijaz Bajgoric (2006), the development of business continuity planning (BCP) concentrates mostly on large organizations and seldom on smaller ones and not addressing the differences between them. This could be due to the fact that BCP is a non-revenue project and small or medium organizations do not consider this as a priority.

Leon Erlanger (2006) suggested an advanced business modeling that can be used to assess risks and hence business continuity by analyzing the business and mapping it to processes. This model, though very useful, addresses only internal factors and elements and can be used in the Business Impact Analysis (BIA) step within the BCP lifecycle.