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
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)