Enablers of Successful Business Continuity Management Process

Leong Lai Hoong, Govindan Marthandan

Graduate School of Management, Multimedia University, Cyberjaya, Selangor, Malaysia

Abstract: Business Continuity Management (BCM) is a management process to ensure the resilience of an organization in the face of a range of business disruptions. It considers the mitigation of risk in the business functions, put in place the process and procedure to recover the IT systems and business functions during any interruptions. BCM evolved from Disaster Recovery Planning (DRP) that commenced in the 1970s to recover electronic data processing capability during the mainframe era. In addition to technology recovery, BCM covers the recovery of people and business as a whole. It includes the full suite of recovery plans from reducing risks of business disruptions, response to disruptions and mobilise people to the secondary site to continue business. Service disruption is intolerable in the business environment especially in the financial industry, the lifeline industry in most countries if not all. The respective regulators have stringent guidelines to ensure the smooth operations in order to minimize systemic disruptions in the banking environment that ultimately impact the economy of the nation. Though with many strict regulations, coupled with availability of advance technology to recover business and technology services, there were still many banking interruptions that shocked the nation and caused severe inconveniences to the banking customers. The aim of this study is to identify the enablers of a successful BCM process. The first phase of this study involves the understanding of factors impacting the BCM process and develops a conceptual model for a successful BCM process. The methodological instruments employed include data collection through emailed questionnaires to the staff working in the BCM, IT, Operations, Risk departments of financial institutions. The data collected will be used to test the conceptual model and analysis will be drawn. The findings of this study provide useful information and could help bank managers implementing and maintaining BCM process in an effective manner. The main findings of this study is that technology components (IT availability and reliability, complexity and technology competence), perceived BC benefits, top management support, external pressure to adopt BC and business environment have positive effects on BCM implementation in the financial industry in Malaysia; but organizational compatibility and infrastructure readiness did not.

Key words: Business Continuity Management, BCM, Disaster Recovery Planning, DRP, IT Service Continuity Management, ITSCM, ITIL, IT Service Management, ITSCM, Business Process

INTRODUCTION

Business disruption refers to any untoward incident that interrupts the day-to-day business operations. It can be categorized as natural disaster (i.e. earthquake, typhoon and hurricane, etc) and man-made disasters (such as terrorist attack, IT service outages, social unrest, pandemic, etc). Business continuity management (BCM) is a management process and action plan to ensure the resilience of an organisation in the face of a range of business disruptions. The BCM process serves as the safety net for the organisation to resume business operations after a disaster. It covers organizing, planning, controlling and running the organisation before, during and after a disaster (Wold, 1997). BCM was described as a new and evolving discipline in the early 2000’s (Herbane, Elliott, & Swartz, 2002).

Disaster recovery planning (DRP) is an IT process started in the 1970’s in conjunction with the growth of the electronic data processing capability in an organisation (Finn, Guillot, & Taylor, 2006). It was during the era of the mainframe machines to facilitate the organisation in automating some human tasks (Colraine R., 1998). People are aware of the criticality of mainframe functions, data captured and information provided, therefore the development of DRP is to ensure that there are proper backup of data and able to restore when there is a loss of facility in the future. DRP focuses on recovery related to IT services. DRP evolved over the years and new buzz words emerged to complement the DRP function in the 1990’s, such as, Contingency Planning, IT service continuity management (OGC ‘s Authorized Authors, 2001), Crisis Management, Emergency Planning and BCM (Mainline Information System).

Literature Review:

In the face of pressures from the customers demanding for higher IT service level, the rampant terrorist threats and quick changes in weather that lead to natural disaster, the development of DRP is a priority and it

Corresponding Author: Leong Lai Hoong, Graduate School of Management, Multimedia University, Cyberjaya, Selangor, Malaysia
DRP is generally reactive to a disaster (Herbane, et al., 2007). DRP is critical to complete the recovery of businesses (Herbane, et al., 2002).

Business Continuity Management (BCM):

BCM and DRP have been studied extensively in the academic world and many guidelines have also been produced by the practitioners. Those studies can be grouped in few distinctive components of BCM that cover all types of interruptions: from small service disruptions to full blown disasters (Wood, 2006). These components are phases of BCM, recovery priority and strategy, types of BCM plans and BCM plans maintenance. The number of BCM phases recommended by researchers may differ from one to another depending on the subject matter being focused in their respective studies (Ketterer, Price, & McFadden, 2007; C. M.; Lawler & S. A.; Szygenda, 2007). The public non-governmental organisations and advocates also provide guidelines for implementing BCM processes, ranging from reactive processes like recovering an interruption, to proactive processes like reducing risk and preparing the people and business to face the disaster if it ever happens (BCI, 2010; BCM Institute, 2009; DRII, 2008).

The success of business recovery is measured by the speed of recovery and information available to resume business after a disaster (Herbane, Elliott, & Swartz, 2004). The disaster tolerance level of the business functions vary and the recovery measure are termed as recovery time objective (RTO) and recovery point objective (RPO) (Smith, 1995). RTO refers to the expected duration to recover its business function and RPO refers to the volume of data that could possibly loss. The longer the RTO means more time and effort needed to recover them before resuming business to the business as usual state. BCM covers all types of plans that document the process, procedure and other requirements for an organisation to survive a disaster. It is an anthology of plans that describe more specific details for disaster preparations and recovery work (T. Chang, 2008). They include information technology disaster recovery plan (C. M.; Lawler & S. A.; Szygenda, 2007), risk assessment and business impact analysis methodology (Garry Poole, n.d.; Simon, Stefan, & Gerald, 2008), incident management and response plans (T. Chang, 2008), crisis management plan (Mitroff, Shriwastava, & Udwadia, 1987), communication and emergency response plan (T. Chang, 2008) and human contingency plan (Ketterer, et al., 2007).

The BCM plan is not complete without testing, audit and maintenance. Frequent test and audit should be included as ongoing review, refresh and continuous improvement efforts to keep pace with the changes of business strategy and direction (Austin Finn, et al.; DRIII, 2008; Gibb & Buchanan, 2006).

Disaster Recovery Planning (DRP):

DRP is the process and procedures put in place to recover the technology infrastructure services that is critical to an organisation, in response to a natural or human-induced disaster. DRP includes activities that analyze the company vital business functions, recommend IT recovery strategies and document the roles and responsibilities of staff in executing the recovery tasks before, during and after a disaster (Petroni, 1999; Socka, 1998). It consists of many sub-plans, such as incident management plans, backup and recovery plan, IT systems and work area recovery plans. DRP is generally reactive to a disaster (Herbane, et al., 2004). DRP contains adequate detail for technical recovery, but it takes less interest on people and communication issues, like the some tasks the BCM process focused on (BCI, 2008; BCM Institute, 2009; DRIII, 2008).

In view of the exponential growth of e-Commerce systems that could not be shut down due to its 7x24 operational nature (Gerald, 2004), a proactive forward-looking plan is required in developing a system that is free from interruptions. As such, the core question for IT service continuity is how systems should be built in order to protect the business. In addition to the six stages of BCM life cycle, the physical and logical security for the business and IT environment is vital. A DR book (Jon Toigo, 1996) emphasized the benefits of using technology while designing the systems. It’s important that the earlier technology is considered, the more efficient and better cost proposition the system will provide for disaster recovery (C. M. Lawler & S. A. Szygenda, 2007). Technologies can be considered in the hardware utilization, software development, data and the network architecture and their backup systems (Jon Toigo, 1996). It was concurred that the recovery technology and strategy, need to be decided during the analysis and design stage of system development life cycle and be embedded in the project management methodology (George, 1998; Greg, 1999; Serrelis & Alexandris, 2007).
**IT Management And Organisation:**

Management of the IT infrastructure become serious issues as the IT service providers are facing tight constraints pertaining to human resources, budget and high investment in infrastructure cost. In addition, today's IT operating environments consists of a wide range of application services and infrastructure components which have evolved and expanded over time. This resulted to a complex network of servers and software components that can be costly and difficult to manage. It hinders the flexibility, challenge efficiency and effectiveness of IT (Mercury, 2004). Therefore, IT service providers' main focus is to improve the delivery of IT services, limit the outages of IT services and maximize the return on investment. This leads to the shift from technology-oriented to customer- and service-oriented IT management, which often known as IT Service Management (ITSM) (Brenner, Radisic, & Schollmeyer, 2002). And BCM, DRP and IT service continuity management are some of the critical processes in ITSM that ensure uninterrupted services delivered to the customers (OGC’s Authorized Authors, 2001).

A survey done in Hong Kong, concluded that five top critical factors for a successful DRP are: top management commitment, adequate financial support, appropriate backup site, off-site storage of backup and training of recovery personnel (Chow, 2000; C. M. Lawler & S. A. Szygenda, 2007). It was also recognized that if the right people can be contacted and be given the right information, they’ll have a substantial head start on recovery (Van Collie, 1990). However, Dirtadian recommended focusing on the resilience of critical assets which support key business processes, such as the building, equipment, technology, human resources and third party relationships instead of developing a set of finite scenario-specific plan (Dirtadian, 2008). The above researchers explained the critical components for recovery efforts: people (staff and management), facilities and location (for primary and backup sites), technology and assets.

**Controls of IT Environment:**

There are a number of controls in the IT environments that indirectly supporting the BCM process. They are the regulators guidelines, industry best practices and the Service Level Agreement (SLA) signed between the customers and representatives from IT organisation (OGC’s Authorized Authors, 2001). The SLA sets the expectation of customers should an untoward incident occurs: when the IT system will be recovered (C. M. Lawler & S. A. Szygenda, 2007). Other BCM and IT service components included in SLA are BC strategy, roles and responsibilities, recovery location, plans and procedure to transfer business operations to the alternative location and the on-going maintenance programs (Smith, 1995). It is to ensure that customers are not ripped off their rights of using the IT services during the agreed service hours (Voas & Wilbanks, 2008).

From the process maturity perspective, it was recommended that the maturity level of BCM was used as a control for DR policy & plan adherence (Scott Ream, 2002a). Other control frameworks for the BCM and DRP are ITIL, COBIT and ISO/IEC 27002 (Shamsul, Mohammad, & Masarat, 2008). Besides, sine industry guidelines recommended by the popular institutes in US, UK and Asia regions are BCM Good Practices Guidelines by BCI (BCI, 2008), 10 Professional Practices by DRII (DRII, 2008) and BCM Body of Knowledge by BCM (BCMI, 2009).

**Technology-Organisation-Environment Framework:**

Technology-organisation-environment (TOE) framework has been used extensively to examine the contexts that affect the organisation adopting and implementing technological innovations (Tornatzky & Fleischer, 1990). According to Dogson, technology includes not only tangible artefacts but also the knowledge that enables it to be developed and used in many useful ways (Dodgson, 2000). Technology should deliver replicable functionality and it is clearly seen in new or improved processes, products and systems; that include the DRP and BCM processes. The TOE framework identifies three ways to explain an organisation decision-making behavior with respect to technological innovations: (i) Technological context includes both the internal and external technologies used by the firm, (ii) Organisational context refers to the descriptive characteristics of the organisation, including firm size and scope, complexity of firm managerial structure, quality and degree of its human resources and (iii) Environmental context refers to the industry the organisation is in and its dealings with trading partners, competitors and government. TOE framework has been used in studying the technology adoptions like EDI (C.L. Iacovou, I. Benbasat, & A.S. Dexter, 1995), open system (Chau & Tam, 1997; K.K.Y. Kuan & P.Y.K. Chau, 2001), website and web service (K Zhu, K Kraemer, & S Xu, 2005; Lippert; & Govindarajulu; 2006; TSH Teo, M Tan, & KB Wong, 1998), internet and e-business (Ifnedo, 2011; Oliveira & Martins, 2010), information system and enterprise system (J.Y.L. Thong, 1999; Ramdani, Kawalek, & Lorenzo, 2009), e-procurement (Teo Thompson S. H., Lin Sijie, & Lai Kee-hung, 2009), etc.

**MATERIALS AND METHODS**

There is limited model for a successful implementation of BCM and DRP. From past experiences, unplanned outages were still happening in the IT services in Malaysia and other parts of the world, in spite of...
many IT improvement initiatives have been undertaken and strong guidelines and controls are enforced in the industry. As one of the most vulnerable components in delivering uninterrupted services, the IT solution should target to provide uninterrupted services and have speedy recovery if there is a IT service failure (Seawright, Kristen, Bernhisel, & Charlotte, 2008). Although service recovery function is crucial in the IT environment, it does not fully influence overall satisfaction, quality and image, but the consistency in delivery of service does (Stephen, Deborah, & Tracy, 1996). Therefore, an optimum DRP and BCM process to ensure the resiliency of IT services and organisation is inevitable.

Problem Statement And Research Objectives:
With the close supervision and control of the central bank in Malaysia, Bank Negara Malaysia (BNM), there were still instances when major incidents rocked the investors’ confident in the local bourses, financial market and brought inconveniences and dissatisfaction to the bank customers and stakeholders (“Hong Leong Bank trying to fix computer glitch,” 2006; Internet Banking System Outages,” 2009; Sarif, 2008).

The objective of this research is to explore the enablers of BCM process in the financial institutions in Malaysia.

This study focuses on the critical processes in ITSM that ensures uninterrupted services are delivered to the customers (OGC’s Authorized Authors, 2001). The processes involved are BCM, DRP and IT service continuity management. TOE framework will be used following its effectiveness in understanding the organisation decision context for adopting IS innovation.

Technology Domain:
1) IT availability and reliability: DRP comprises of activities that ensure the recovery of the technology components underpinning the IT services supporting the business (OGC Official Site, 2008). It targets to maximize the availability duration of the IT components like network and telecommunications, hardware and software applications, desktop, IT security (David, 2008; Wiboonrat, 2008; Witty, 2008; Xu & Wang, 2008) and to ensure high reliability of IT services to the customers. Business profitability and shareholder loyalty are highly dependent on the availability, reliability, security and performance of IT services (Elephant, 2006). IT availability is especially critical due to increasing number of businesses moving towards 24x7, like the internet business environment (Xu & Wang, 2008). In summary, understanding all the possibility for system failure in order to maximise the availability and reliability are critical to ensure uninterrupted IT services.

Hypothesis 1:
IT availability and reliability have positive influence on the BCM

2) Complexity: Disaster related behaviour and process is very complex due to its occurrence at different social times in the life of different community (Quarantelli, 1999). BCM is not simply a functional process, it is the capability, skills and integrity of the organisation to survive a disaster and resume business as soon as possible in order to minimize losses (Herbane, et al., 2004). BCM aims to setting up a backup plan and able to run the business during a disaster. Many perceive that there are insurmountable tasks to implement BCM process in addition to the day-to-day activities. From the technology aspect, a smooth and efficient IT service recovery includes successful recoveries of the hardware, software, data and network sequentially (Jon Toigo, 1996; Laura Diritadian, 2008 April; Serrelis & Alexandris, 2007). These explain the complexity of technology and business recovery that everyone fears for.

Hypothesis 2:
Complexity has negative influence on the BCM

3) Technology competence: Maintaining the DR testing are the major challenges for most organisations (Symantec research, 2009). One in four DR tests fails and nearly one third of the organisations do not include all critical IT environments in their DR test plan, some do not even have successful regular backups of the right IT environments. Use of technology like automation, workload management and cross-environment tools can close these fundamental gaps for DR implementation (Xiaoyun, et al., 2008). Data is expected to grow from 50% to 100% yearly (Arun Taneja, 2008), lead to the requirement of extensive management effort and high maintenance cost. Technology solution has been exploited to compress and optimize data in order to reduce data footprint, save data replication cost and shorten recovery time (Ciena Corporation). In summary, technology can shorten the recovery time and increase the success of the DRP and BCM.

Hypothesis 3:
Technology competence has positive influence on the BCM

Organisation Domain:
4) **Perceived Business Continuity benefits**: The main benefit of a recovery plan is to minimize potential losses when the organisation experiences an untoward situation. A short recovery time can increase the success of recovery (Petroni, 1999), bringing business back quickly to fulfill its responsibility for its stakeholders. Realizing the benefits of DRP, the annual surveys on IT issues had indicated the BCM and DRP matters were raised to the top ten IT issues for four consecutive years from 2004 to 2008 (Allison & DeBlois, 2008).

**Hypothesis 4:**
Perceived business continuity benefits have positive influence on the BCM

5) **Organisational compatibility**: Compatibility is defined as the degree to which an innovation is perceived as consistent with the existing values and past experiences of the organization or individual (Rogers, 1995). Some risk-related disciplines and corporate governance can complement the BCM process implementation (Technical Department of ENISA, 2008). Though BCM framework is not a pre-requisite for BCM process implementation, it is a deliverable of the BCM project, as guidance for future on-going BCM process maintenance. BCM was classified as a main concern of mostly private organisations (Khalid, et al., 2008), however, the organisation relationship and communication should reach out to the external community for successful BCM process. Effective communication integrates the inbound with outbound to promote resiliency is part of the best practices of BCM (Herbane, et al., 2004; Varolli Corporation, n.d). It’s an example of corporate governance and policy that are beyond the scope of BCM process but their readiness and compatibility will impact the successful of the BCM process.

**Hypothesis 5:**
Organisation compatibility has positive influence on the BCM

6) **Top management support**: Business continuity projects are getting higher visibility and is classified under enterprise corporate governance strategy (Herbane, et al., 2004). Keeping business operations running at acceptable levels under duress and managing a company's risk exposure to business interruptions are some critical components of the overall corporate strategy (William, 2007). Management’s responsibility include ensuring proper BCM implementation in order to protect the interests of shareholders, customers and employees (Socka, 1998). Prior researches also indicated that, most IT changes will be ineffective and little chance for process innovation and mobilization of forces for organisational transformation, if there is no visionary leadership and support from the top (Attaran, 2003).

**Hypothesis 6:**
Top management support has positive influence on the BCM

**Environment Domain:**

7) **External pressure to adopt BCM**: In some industry, there are regulatory requirements for the respective businesses in managing a healthy BCM and DRP programme. For financial institutions in Malaysia, Bank Negara Malaysia (BNM), the central bank has issued (i) The guideline for prudent management of IT environment (Bank Negara Malaysia, 2004) and (ii) the minimum guidelines on BCM (Bank Negara Malaysia, 2008). In the neighbouring country, Thailand had a similar guideline to ensure a satisfactory IT environment (Bank of Thailand, 2005).

**Hypothesis 7:**
External pressures to adopt BCM has positive influence on the BCM

8) **Infrastructure Readiness**: The ability of recovery from a disaster depends very much on the environment and infrastructure. In its plan to build the multimedia super corridor (MSC), Malaysia has invested heavily in the infrastructure in Cyberjaya, a location in the state of Selangor, to support and encourage the investment in multimedia and technology organisations. Dual resources were put in place to ensure continuity and proper backup of essential utility. Such as, the availability of fibre-optic network that are supported by multiple service providers ("Cyberjaya – A Haven for ICT Industry ", 2009) and the electricity connections from two separate substations that provide 99.99% power utility service ("Cyberjaya," 2008). These are some examples of the readiness of environment that assist the achievement of swift recovery by minimizing utility outages.

**Hypothesis 8:**
Infrastructure readiness has positive influence on the BCM

9) **Business Environment**: In today’s outsourcing environment, the scope of work between buyers and sellers are guided and measured by a service level agreement (SLA) (Larson, 1998). An SLA should describe the commitments of both suppliers and buyers, the scope of services, their responsibilities and service performance targets. The SLA is also recommended to include recovery strategy, accountabilities and IT infrastructure that consist of recovery objective, procedure and performance measurement (Smith, 1995). Such as, availability,
reliability, serviceability, maintainability, security, response of service providers and user satisfaction (Larson, 1998; Wood, 2006). In order to achieve the stated metrics, the DRP is important to maintain the service level with the disaster recovery goals linking to the business expectation (Sun Microsystems, 2006). SLA becomes a business motivator for implementing DRP and BCM processes.

**Hypothesis 9:**
Business environment has positive influence on the BCM

**Disaster Recovery Planning (DRP):**

10) **IT project management framework:** DRP project is part of BCM lifecycle consists of program and project management component as the first stage of BCM activities (BCI, 2008; DRII, 2008; NFPA 1600-Standards for Disaster/Emergency Management and Business Continuity Program,” 2004). DR plans, the main project deliverable, is one of the IT components that should be developed using a life-cycle approach (Petroni, 1999) and adhere to the project management framework. This is in line with the system development life cycle (SDLC) which usually consist of three phases: systems analysis, design and implementation (Petroni, 1999). The SDLC and project management framework promote standardization and systematic approach for proper usage of technology during the initial system development stage.

11) **DR plan development:** DRP is a process to develop a plan that is reactive to an incident and focuses on the recovery of IT services and facilities (Herbane, et al., 2004). DR plan contains sufficient detail for the recovery of these technical components. Such as plans to recover network and telecommunications, hardware and software applications, desktop, IT security access respectively (Witty, 2008). In order to have an effective DR plan, planning for all critical resources are essential before a disaster strikes (Petroni, 1999).

12) **DR plan maintenance:** DR plan maintenance refers to the on-going evergreening of process and plans. Plan maintenance activities include frequent testing of DR plans for workability and efficiency; improving DR plans after audit feedbacks to ensure that plans are developed and aligned to the business requirements (BCI, 2008; DRII, 2008; NFPA 1600-Standards for Disaster/Emergency Management and Business Continuity Program,” 2004; Scott Ream, 2002a).

**Hypothesis 10:**
DRP has positive influence on the BCM

**Business Continuity Management (BCM):**

13) **BC framework:** BCM guidelines and framework have been well advocated by most researchers and practitioners. The BCM framework proposed by previous researchers were not exactly similar but they have the same objectives: recover critical business processes and minimize impacts to the organisations when a disaster strikes (Bank Negara Malaysia, 2008; Bank of Thailand, 2005; BCI, 2009; Cegiela, 2006; Emmanuelle, Damiano, Sandro, & Marco, 2007; Garry Poole, n.d.; George, 1998; Gibb & Buchanan, 2006; Herbane, et al., 2004; Jon Toigo, 1996; Khalil, Elmaghrawy, & Kumar, 2008; Loffness & Drapeau, 2007 June; Mainline Information System; Michael Wood, 2006 June; Scott Ream, 2002b; Simon, et al., 2008; Smith, 1995; Wing, 2002). Some of the common phases recommended in their BCM framework are: project and programme management, risk assessment and business impact analysis (BIA), recovery strategy selection, plans development that include DR or BC plans and all the supporting plans like crisis management plan, communication plan, technology component recovery plan and staff mobilization plan.

14) **BC Plan Development and Maintenance:** Herbane at el. recommended that the planning and BCM process was one of its four BCM process dimensions that distinguishes how an organisation deals with business interruptions (Herbane, et al., 2004). It was included in most of the researchers’ recommendation that various BC plans need to be documented, roles and responsibilities are communicated and accepted by the stakeholders, the plan must be tested at an agreed frequency. Pitt and Goyal concurred that the viability and effectiveness of BC plan is dependent on the regular review, audit and testing (Burling & Hyle, 1997; Pitt & Goyal, 2004; Quarantelli, 1985).

**Conceptual Framework:**

BCM and DRP development are important parts of the organisations today. Past researchers have extensively studied the various component of the BCM process. However, it has not gone beyond the aspect of BCM phases for a complete view of what impacts the successful implementation of BCM. From the discussion above, it’s obvious that the various components: the process, people and tools contribute heavily to the DRP and BCM processes. Therefore, they are pulled together in this study to explain the implementation success and performance of the DRP and BCM processes. The conceptual model in Figure 1 below includes a set of three antecedent dimensions developed, as discussed in the section 3 above.
Research Methodology:

1) Measurement development: In the conceptual model, there were a total of 9 independent variables that were grouped into 3 dimensions following the TOE framework. There is 1 mediating variable (DRP) and 2 dependent variables, business continuity framework and business continuity plan. The items for all the 12 variables were adapted from previous studies using TOE framework (S.-J. F. Chang, Patel, & Withers, 2007; Chau & Tam, 1997; Hamann, Schappert, Iyengar, van Kessel, & Claassen, 2008; Lin; & Lin, 2008; Lingeswara; & Tammineedi;, 2010; Wang, Wang, & Yang, 2010) and surveys published in trade journals and public guidelines (Aligning COBIT, ITIL and ISO 17799 for Business Benefits, 2005; Bank Negara Malaysia, 2008; BCI, 2008; Scott Ream, 2002b).

A five-point Likert-type scale was employed for all the items of the constructs; 1 being “strongly disagree”, 5 being “strongly agree” with 3 being the middle point. The survey participants based their responses on their experiences and perceptions while answering the questionnaire.

2) Sampling strategy: An expert sampling method was used, as this study requires the respondents to have some knowledge about BCM, DRP and general IT subjects. The population are all the individuals working in the functions of BCM, IT, risk management and operations department of the financial institutions in Malaysia. There are 73 banks and 59 insurance institutions (Bank Negara Malaysia, 2010) at the time the survey is conducted.

3) Data collection: There are three phases in data collection, the first and second phase data collected were used to validate and improve the survey instrument. During the final phase of data collection, questionnaire survey is conducted using emails with a reminder sent two weeks after the initial invite to participate in survey. 316 questionnaires were sent, 218 respondents replied and the achieved response rate was 69%. After screening the replies for completeness of survey, there were only 208 responses were useable. It was above 200 units of samples, therefore Structural Equation Modelling (SEM) could be used for this research (Kline, 2005).

Results:
The evaluation and analysis was conducted using Statistical Package for Social Sciences (SPSS 19.0) and Analysis of Moment Structure (AMOS 19.0) analytical software, due to its user friendliness.

1) Respondents profile: Of the 208 survey respondents, 60% of the total respondents were from the middle management category: 22% were team leads or junior managers and 17% were at senior levels who make decision in their respective area of responsibility. There were 52.4% of the respondents have 5 or more years of BCM and DRP experience. In addition, 86% of respondents have been in the work force for more than 10 years. It is obvious that the respondents have a good knowledge of BCM and DRP, and well adapted to the work environment and are appropriate in participating in this survey.

2) Instrument validation and measurement model development. Three tests were performed on the final data to validate the instrument and develop a measurement model. Cronbach’s Alpha is used to assess the degree of density of the scale. Coefficient greater than 0.7 indicates strong reliability; coefficient range between 0.6 to 0.7 are modest and deemed to be the lower limit of acceptability for exploratory research (Hair, Black, Babin, & Anderson, 2010). Factor analysis was performed for convergent test with factor loading greater than 0.7 demonstrates an acceptable level of correlation between two items. The exploratory factor analysis is then performed using principal component approach with threshold value 0.3 and varimax rotation. Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy was obtained for discriminant test. KMO greater equal than 0.6 was mediocre and greater than 0.7 demonstrates sufficient internal consistency and adequate convergence between two concepts. The result for all the above tests were tabled as following table. They were within the acceptable range and a valid measurement model was produced for the next level of analysis.
Table 1: Result of reliability test and factor analysis

<table>
<thead>
<tr>
<th>Independent Variables</th>
<th>Cronbach's Alpha</th>
<th>KMO</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT availability &amp; reliability</td>
<td>0.910</td>
<td>0.845</td>
</tr>
<tr>
<td>Complexity</td>
<td>0.874</td>
<td>0.600</td>
</tr>
<tr>
<td>Technology competence</td>
<td>0.950</td>
<td>0.916</td>
</tr>
<tr>
<td>Perceived BC benefits</td>
<td>0.845</td>
<td>0.600</td>
</tr>
<tr>
<td>Organizational Compatibility</td>
<td>0.914</td>
<td>0.758</td>
</tr>
<tr>
<td>Top Management Support</td>
<td>0.909</td>
<td>0.757</td>
</tr>
<tr>
<td>External pressure to adopt BC</td>
<td>0.910</td>
<td>0.758</td>
</tr>
<tr>
<td>Infrastructure readiness</td>
<td>0.822</td>
<td>0.696</td>
</tr>
<tr>
<td>Business environment</td>
<td>0.870</td>
<td>0.600</td>
</tr>
<tr>
<td>DR Planning</td>
<td>0.935</td>
<td>0.941</td>
</tr>
<tr>
<td>BC framework</td>
<td>0.923</td>
<td>0.902</td>
</tr>
</tbody>
</table>

3) Confirmatory Factor Analysis (CFA). CFA was run on the measurement model. Goodness-of-fit (GOF) tests are used to collect evidence for fitnes of model. GOF acceptable thresholds and result were summarised in row 1 to 6 of the following table. All the indices were within the recommended thresholds.

Table 2: Result of GOF test for measurement and structural model

<table>
<thead>
<tr>
<th>Row</th>
<th>Thresholds</th>
<th>CMIN</th>
<th>DF</th>
<th>P</th>
<th>CMIN/DF</th>
<th>CFI</th>
<th>TLI</th>
<th>RMSEA</th>
<th>RMR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Technology</td>
<td>66.351</td>
<td>41</td>
<td>0.007</td>
<td>1.618</td>
<td>0.986</td>
<td>0.981</td>
<td>0.055</td>
<td>0.032</td>
</tr>
<tr>
<td>2</td>
<td>Organisation</td>
<td>23.136</td>
<td>17</td>
<td>0.145</td>
<td>1.361</td>
<td>0.994</td>
<td>0.990</td>
<td>0.042</td>
<td>0.014</td>
</tr>
<tr>
<td>3</td>
<td>Environment</td>
<td>10.047</td>
<td>17</td>
<td>0.902</td>
<td>0.591</td>
<td>1.000</td>
<td>1.000</td>
<td>0.000</td>
<td>0.014</td>
</tr>
<tr>
<td>4</td>
<td>DR Planning</td>
<td>14.765</td>
<td>14</td>
<td>0.394</td>
<td>1.055</td>
<td>0.999</td>
<td>0.999</td>
<td>0.016</td>
<td>0.009</td>
</tr>
<tr>
<td>5</td>
<td>BC Management</td>
<td>34.923</td>
<td>34</td>
<td>0.424</td>
<td>1.027</td>
<td>0.999</td>
<td>0.999</td>
<td>0.011</td>
<td>0.020</td>
</tr>
<tr>
<td>6</td>
<td>Measurement Model</td>
<td>926.154</td>
<td>836</td>
<td>0.016</td>
<td>1.108</td>
<td>0.987</td>
<td>0.985</td>
<td>0.023</td>
<td>0.024</td>
</tr>
<tr>
<td>7</td>
<td>Structural Model</td>
<td>953.353</td>
<td>855</td>
<td>0.010</td>
<td>1.115</td>
<td>0.986</td>
<td>0.984</td>
<td>0.024</td>
<td>0.029</td>
</tr>
</tbody>
</table>

The measurement model was transformed to a structural model and CFA was performed again. The result was listed on row 7 of the table above. All the indices were within recommended thresholds. Therefore sufficient evidences gathered for accepting the structural model.

4) Hypothesis test. Hypotheses were tested on the accepted structural model. The following hypothesis table was extracted from the standardized and unstandardized regression weight table of the AMOS reports. p-value less than 0.05 indicates significance of hypothesis. As a result, there were evidence for acceptance of 9 of 11 hypotheses. The 2 hypotheses not accepted are infrastructure readiness (E2) and organisational compatibility (O2).

Table 3: Hypotheses test result

<table>
<thead>
<tr>
<th>Variables</th>
<th>B</th>
<th>Beta</th>
<th>p</th>
<th>Hypothesis</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR &lt;--- T1 IT availability &amp; reliability</td>
<td>0.211</td>
<td>0.210</td>
<td>***</td>
<td>Supported</td>
</tr>
<tr>
<td>DR &lt;--- T2 Complexity</td>
<td>0.120</td>
<td>0.170</td>
<td>0.006</td>
<td>Supported</td>
</tr>
<tr>
<td>DR &lt;--- T3 Technology competence</td>
<td>0.110</td>
<td>0.123</td>
<td>0.038</td>
<td>Supported</td>
</tr>
<tr>
<td>DR &lt;--- O1 Perceived BC benefits</td>
<td>0.207</td>
<td>0.176</td>
<td>0.006</td>
<td>Supported</td>
</tr>
<tr>
<td>DR &lt;--- O2 Organisation compatibility</td>
<td>0.038</td>
<td>0.034</td>
<td>0.521</td>
<td>Not supported</td>
</tr>
<tr>
<td>DR &lt;--- O3 Top management support</td>
<td>0.230</td>
<td>0.225</td>
<td>***</td>
<td>Supported</td>
</tr>
<tr>
<td>DR &lt;--- E1 External pressure to adopt BC</td>
<td>0.145</td>
<td>0.199</td>
<td>0.003</td>
<td>Supported</td>
</tr>
<tr>
<td>DR &lt;--- E2 Infrastructure readiness</td>
<td>0.049</td>
<td>0.047</td>
<td>0.436</td>
<td>Not supported</td>
</tr>
<tr>
<td>DR &lt;--- E3 Business environment</td>
<td>0.179</td>
<td>0.148</td>
<td>0.008</td>
<td>Supported</td>
</tr>
<tr>
<td>BC1 &lt;--- DR DR Planning to BC Framework</td>
<td>0.642</td>
<td>0.638</td>
<td>***</td>
<td>Supported</td>
</tr>
<tr>
<td>BC2 &lt;--- DR DR Planning to BC Plan</td>
<td>0.443</td>
<td>0.511</td>
<td>***</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Discussion:
From the hypothesis result, there are evidences supporting 7 enablers for BCM process. They are the IT availability and reliability, complexity, technology competence, perceived BC benefits, top management support, business environment and external pressure to adopt BC. The results were in line with prior studies. Organisation compatibility and infrastructure readiness are not the enablers for BCM process. These results have mixed findings as compared to prior studies. In this study, organisation compatibility refers to the level of compatibility of BCM process to the existing corporate governance and framework, organisation values and practices. For example, if the organisation has an existing framework for communication, staff learning and...
development policy, then BCM can ride on it for a smoother process implementation. Prior BCM literatures discussed the various stages required for a full suite of BCM; namely, BCM program management, risk assessment and business impact analysis, recovery strategy selection, BC plan development, maintenance and audit (BCI, 2010; Gibb & Buchanan, 2006). BCM framework is one of the recommended deliverables but it’s not a pre-requisite for a BCM process implementation, neither nor other governance and policy. Therefore, organisation compatibility is not a critical factor for BCM process. Similarly infrastructure readiness was not an enabler for BCM process. In this study, it refers to the physical infrastructure where the business is located (S.-J. F. Chang, et al., 2007) and focuses on possible advantages gain for investing in the right physical infrastructure. This study disagrees with few literatures but agrees with one (Lingeswara & Tammineedi, 2010). Physical location and its infrastructure is one of the critical resources that facilitate execution of business activities and any threats associated are required to be analyzed during a site risk assessment (“Disaster Preparation Beats Disaster Recovery,” 1992). A central team like business continuity function can coordinate the risk assessment, analyze results and deploy risk mitigation measures (Lingeswara & Tammineedi, 2010). However, mitigated risk may still leave residual risk that can cause disaster and trigger the business continuity plan. Therefore, infrastructure readiness may not be an enabler for BCM process.

Conclusion:

This study has some important contributions for the practitioners, the managers and academic world. Generally, this instrument has passed various reliability and validity tests and they could be used in future studies. Since the behavior to adopt or implement an innovation is a significant step to organisational effectiveness, a better understanding of its dimensions will improve the overall organisational performance. Through the understanding of the enablers, organisations will gain a higher return-on-investment for BCM process implementation due to the right focus is put in the influencing factors. In addition, the managers can review their BCM process and shift their attention to the enablers for better process performance.

Every study will have some areas that could not be addressed. The key limitations of this study are: (1) In view that most people have tight schedule, the survey respondents’ attitudes and right level of time spent in answering the questionnaires may impact the quality of the survey and final result of the study. (2) This study focused on only one industry, the financial services industry in a developing country, Malaysia. The results may not be able to generalize to other industries and other regions.

In future researches, it is recommended to extend this study and model to explore the value BCM brings to the organisation and its importance on the business strategy map. This study explores the practitioners’ view of BCM on their respective organisations; a holistic view may be obtainable if the survey audience can be extended to cover the view of customers, vendors and competitors.

REFERENCES

Austin Finn, James Guillot, & Taylor, J. Essentials of Disaster Recovery Planning.


Sun Microsystem, 2006. Linking disaster recovery time objectives to business requirements.

Symantec research, 2009. Disaster Recovery Pressures Rise Due to Cost of Downtime and More Stringent RTOs.


