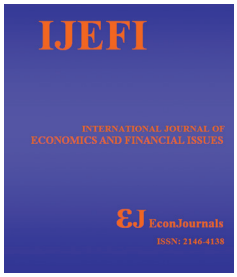


International Journal of Economics and Financial Issues

ISSN: 2146-4138

available at http: www.econjournals.com

International Journal of Economics and Financial Issues, 2015, 5(Special Issue) 128-134.

2nd AFAP INTERNATIONAL CONFERENCE ON ENTREPRENEURSHIP AND BUSINESS MANAGEMENT (AICEBM 2015), 10-11 January 2015, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia.

The Effect of Business Continuity Management Factors on Organizational Performance: A Conceptual Framework

Zahari Abu Bakar[1]*, Noorulsadiqin Azbiya Yaacob[2], Zulkifli Mohamed Udin[3]

[1]College of Business, Universiti Utara Malaysia, Sintok, Malaysia, [2]College of Business, Universiti Utara Malaysia, Sintok, Malaysia, [3]College of Business, Universiti Utara Malaysia, Sintok, Malaysia. *Email: zzzahari@gmail.com

ABSTRACT

This paper reviews the role played by business continuity management (BCM) factors in enhancing the organizational performance. The constructs of this paper are based on a comprehensive review of recent literature on BCM critical success factors, BCM standards and organizational performance. In this study, the organizational performance covers two specific areas of organizational results such as financial performance and non-financial performance. Financial performance which may encompass of revenue, profitability, cost saving, return on investment and other financial measures while the non-financial performance may includes effectiveness, efficiency, quality, quality of work life, innovation and productivity. A detailed literature review revealed the importance of effective BCM implementation in ensuring an organization's survivability and competitiveness. Therefore, the demand to protect the continuity of critical business services in the event of an unforeseen disaster or disruption has become more critical than ever. In Malaysia, among the widely adopted BCM related standards by both the private and public sectors are ISO 22301 and ISO 27001. These certified organizations are selected as the population of the study as they are deemed to possess considerably higher sense of commitment towards embracing BCM best practices to enhance their business resiliency. The international standard certification may also indicate the maturity of the organizations in practicing BCM. Previous study has proven that organizations with matured BCM processes had indicated substantial performance improvements. This paper also highlights the challenges encountered by the BCM professionals in developing and maintaining the BCM infrastructure and activities, which necessitate the support from the senior management. Among the challenges that may cause failure in BCM implementation are lack of financial support and the deployment of BCM initiatives on enterprise wide basis. In summary, this paper is expected to propose the conceptual framework for future researchers to investigate and provide the empirical evidence on the relationship that exist between the BCM factors and organizational performance.

Keywords: Business Continuity Management, Organizational Performance; Conceptual Framework
JEL Classifications: M000

1. INTRODUCTION

Present-day management thinking is driven by key business objectives such as service availability, prompt delivery and meeting customer's expectations. In order to survive, organizations must consistently deliver the right product, at the right time and at the right price to the end customers on a continual basis. Hence, so as to ensure the availability of service is maintained at all time, every organization must always be prepared and plan to a greater extent than they traditionally have, to counter all the potential threats.

According to Wong (2009), organizations that incorporate business continuity management (BCM) in their strategic management could gain a distinctive competency over their competitors in terms of operational resiliency which includes the speedy recovery of critical business functions at predefined period of time while minimizing the adverse impacts to their value and reputation. The readiness of an organization in responding to contingencies such as fire, avian flu pandemic, terrorism, killer tsunami waves, electricity power failure, earthquake, etc. is reliant on the involvement of its management in embracing the BCM (Low et al., 2010). Therefore, the consequence of not having a good BCM practices in place

may be threatening. According to the Gartner Group report in 2004, it was revealed that the average cost of service downtime worldwide was at USD 42,000 per hour (Vancoppenolle, 2007). A recent survey conducted by KPMG (2014) reported that the cost of downtime for the past 12 months is estimated to be over USD 100,000 for 36% of the organization, with almost 12% reporting losses at over USD 1 million while over 28% indicated that they "do not know" the total cost of the downtime. However, the downtime costs may vary significantly depending on the industries, size of business and the nature of disaster. Beside the direct monetary lost, the downtime may also affect corporate reputation, branding, customer loyalty, regulatory compliance and employee productivity.

2. PROBLEM STATEMENT

Peterson (2009) argued that one of the reasons many organizations fail to implement effective BCM is due to lack of financial support as great prudence in expenditures is exercised by many senior management and the board of directors. This may be due to there is no direct financial benefit or return of investment is seen from the BCM implementation. With all the expenditure associated with the preparation of essential BCM infrastructures and resources such as planning and consulting, setting up the hot-site data center and operation center and acquisition of additional hardware and software, it is crucial to present a solid business case in order to gain top management's buy in (Petroni, 1999). In order to successfully secure the funding, BCM professionals should work together with the business owners to estimate the potential loss due to service downtime, identify the likelihood of risks, define the optimum recovery objectives and choose the most cost effective solution and technology (Belaouras, 2009). Another challenge is deploying BCM in organizations which cut across several business units or implementing it on a corporate enterprise wide basis (Belaouras, 2009). These situations emphasize the importance of senior management support and directive to mandate the priority of BCM initiatives across all organization members.

In order to address the above challenges, understanding the potential benefits of BCM on the organizational performance is important to give a proper merit to the BCM efforts and draw attention and subsequently, obtaining full support from the senior management. Sawalha (2013) suggests that understanding the effects of BCM on organizational performance is significant since BCM is one of the primary driving factors for enhancing an organization's ability to withstand its resiliency, as well as survival under extreme internal and external pressures. The previous studies which focused on the strategic role of BCM argued that BCM could become a source of competitive advantage for organizations but these studies did not deliberated comprehensively on how BCM can contribute to organizational performance specifically (Herbane et al., 2004). In addition, Sawalha (2013) also highlighted that the role of BCM in enhancing organizational performance has rarely been deliberated or even addressed in the existing studies.

Notably, the major theoretical gaps in the present literature observed in this research lies in the insufficient studies which have investigated and established the relationships between BCM factors and organizational performance. Hence, the goal of this study is to extend the limited literature on the relationship that exists between BCM factors and organizational performance.

3. LITERATURE REVIEW

3.1. Organizational Performance and BCM

The current literature presents a number of studies that deliberate risk management and its relation to organizational performance. These studies have concluded that understanding the likelihood and impact of potential disaster events can enhance organizational performance (Alesi, 2008; Herbane et al., 2004; Herbane, 2010; Selden and Perks, 2007). On the same ground, Sawalha (2013) belief that, similar to risk management which is considered the roots of BCM, BCM could also play an important role that may contribute to the optimization of organizational performance. In this context, risk management is exercised by organization to minimize the adverse impacts of internal and external risks that may affect its activities and performance. Risk management also supports organizations in responding to uncontrollable market conditions to sustain consistent profitability, which eventually leads to optimized organizational performance (Jafari et al., 2011; Saleem, 2011).

A few of present literature which focus on the strategic role of BCM, posited that BCM can provide organizations with sources of competitive advantage, but these studies have not deliberated comprehensively on how BCM could influence the organizational performance specifically (Alesi, 2008; Herbane et al., 2004; Herbane, 2010; Selden and Perks, 2007). Additionally, Sawalha (2013) postulates that the relationship between BCM and organizational performance was found to be mainly underexplored by the researchers. He claims that his research is the first that examines the influence of BCM on the various elements of organizational performance, subsequently highlighting the value add and significance of BCM strategically. In his study on the Jordanian banking sector involving 11 out of 17 banks, one of the most important roles of BCM is to provide customers with uninterruptible and secured banking services at all time. This capability lays the foundations for preserving a positive corporate reputation, enhances the competitive advantage against the competitors, increase profitability, and subsequently improves the overall organizational performance. The qualitative study by Sawalha (2013) also reveals that BCM has a significant role in improving profitability. Based on the interviews, 100% of respondents asserted that BCM implementation ensure banking operations and critical business functions are preserved uninterrupted before, during and after an unexpected incident, hence making sure that banking transactions are carried out continuously by the customers (Sawalha, 2013). Besides the financial performance, his study also discovered that BCM also have positive effect on several non-financial performance indicators such as effectiveness, efficiency, quality, innovation, productivity and quality of work life.

3.2. BCM Factors

Based on literature, there are various critical success factors of BCM and for the purpose of this study, the critical success factors

are also referred as factors. The following Table 1 summarizes the previous studies on BCM factors by Järveläinen (2013); Chow and Ha (2009); Hoong (2011); Chow (2000); Herbane et al. (2004); Karim (2011).

Based on the above, this study will focus on examining the selected BCM critical success factors adapted from the previous studies. The selected BCM factors will be used as the independent variables in this study, which include: (1) Management support, (2) external requirements, (3) organization preparedness, and (4) embeddedness of continuity practices. These four factors are selected as their definitions and scopes able to represent all of the critical success factors from the past studies. Furthermore, these factors are important elements to ensure the successful implementation of BCM in an organization.

3.2.1. Management support

Several researchers posited that it is essential that business continuity program to be initiated, sponsored and authorized by senior management from the preliminary phase of its implementation (Arend, 1994; Chow, 2000; Yen et al., 2000). The senior management commitment in ensuring business functions and services operating at an acceptable condition under crisis situation and managing an organization's risk exposure to service disruptions are crucial elements of the overall corporate strategy (Laurent, 2007). In the context of BCM, it is a long-term commitment that necessitates a substantial financial investment by an organization (Cerullo and McDuffie, 1994; Chow, 2000). Hence, only strong engagement by the senior management can warrant the on-going provision of monetary support and other critical resources for developing and maintaining a BCM program.

Payne (1999) argued that lack of senior management commitment will ultimately results in poor executions, lack of corporate wide involvement and at the end, program failures. In a similar manner, a lack of senior management understanding also hinders the effectiveness of a BCM program implementation (Pitt and Goyal, 2004). Rohde and Haskett (1990) also posited that staff will normally undertake the BCM initiatives seriously if it is apparent that the management team has given a full commitment and support to the program. Without the sponsorship and visionary leadership from the management, most initiatives will not be effective and lesser chance for innovation and mobilization of potencies for organizational transformation (Attaran, 2003).

3.2.2. External requirement

Nowadays, BCM is no longer an optional task in large public and private sector organizations. The value preservation within an organization is increasingly become a matter of concern of external interested parties such as the legislators and regulators who consequently oblige organizations under their purview to comply with business continuity provisions. The regulatory requirements enforced by the government authorities and sometime even by the customers will motivate the management to further enhance the service continuity of their information technology and systems (Herbane et al., 2004).

Herbane et al. (2004) also argued that, while such external drivers have uplifted the importance of BCM to a greater level within the corporate governance agenda, they have also challenged the organizations to assess whether their actions should be merely to conform with the minimum requirements as outlined by the regulators or to take on a more strategic approach i.e., to exceed the minimum requirements with the intention of enhancing their BCM capabilities further. In some countries, health care and financial sectors are obliged to make sure that service continuity in their information system operations are in accordance to regulatory guidelines (Elliott et al., 2010).

3.2.3. Organization preparedness

Business resiliency is very much depending on the capability of an organization to avoid and swiftly recover from an untoward event. Herbane et al. (2004) posited that an organization which is able to quickly identify potential risks and subsequently escalate it to the crisis management team is said to be superior in organizational alertness.

Organization preparedness is refers to familiarity with various recovery approaches and avoidance of risks, such as maintaining a business continuity plans, establishing crisis management teams and developing key personnel redundancy (Hägerfors et al., 2010; Ruighaver et al., 2012). The business continuity plans should be regularly updated, tested and improvised, even after occurrence of major incidents (Gibb and Buchanan, 2006). Herbane et al. (2004) added that the swiftness of recovery is the surface exposure

Table 1: Previous studies on BCM factors

Authors	BCM factors
Järveläinen (2013)	Management support, organizational alertness and preparedness, embeddedness of continuity practices and external requirements
Chow and Ha (2009)	Documentations, steering committee, testing, policy and goals, training, maintenance and staff involvement, minimum IT processing requirements, senior management commitment, prioritization of IS critical functions and backup system
Hoong (2011)	Planning (project management, maintenance), technology (IT availability, technology competency, infrastructure advantage), organization (business continuity benefits, top management commitment, organization readiness), environment (regulatory requirement, SLA, business environment) and individual (staff competency, roles and responsibility, stakeholder relationship)
Chow (2000)	Management support, adequate financial support, appropriate backup site, off-site storage of backup media and training
Herbane et al. (2004)	Speed of recovery (organization alertness and preparedness), configuration resilience, obligation (regulation and legislation) and embeddedness of BCM process
Karim (2011)	Strategic management, risk analysis, resources, training and awareness, documentation, information and life cycle management

BCM: Business continuity management, SLA: Service-level agreement

of a more profound capability in the form of organizational preparedness which includes readiness of alternative sites, well executed recovery plans and redundancy of critical resources. Organization preparedness is also enhanced if critical business functions or systems can be restored efficiently by one or several persons (Conlon and Smith, 2010).

3.2.4. Embeddedness of continuity practice

When an organization is well prepared, practices are incorporated into existing processes, staffs as well as senior management are highly committed, continuity practices are said to be embedded in the organization (Herbane et al., 2004). This embeddedness will contribute to positive business impacts in which the organization will become more robust, capable to minimize the potential risk of incidents and recover more speedily as compared to its rivals. In order to inculcate the embeddedness of BCM process, organization can employ a combination of ways to communicate its relevancy which includes awareness raising activities, training and constant communication personalized to meet the needs of various target groups. These actions also indicate the extent to which BCM is a one-off activity or it is embedded and on-going within the organization. One approach of embedding BCM in an organization is to adopt international standards or frameworks that systematically integrate it into the current critical processes (Järveläinen, 2013). Among the commonly adopted BCM related standards are ISO 22301, ISO 27001, BS 25999, NFPA 1600, NIST SP 800 and PASS.

3.3. BCM Standards

Numerous BCM best practices and standards are available (Kenny, 2006) but their contents are about the same. These models and standards offer the information as to how to implement BCM framework but they do not provide a mechanism to specify the extent to which an organization should deploy the BCM initiative. The following Table 2 presents a number of widely adopted standards.

Among these standards, the commonly adopted standards in the Asian region specifically in Malaysia are International Organization for Standardization's ISO 27001 and ISO 22301.

3.3.1. ISO 22301 - BCM system (BCMS)

The ISO 22301:2012, the world's first international standard for BCM has been established to assist organization minimizes the risk of business disruptions. The official title of this standard is "Societal Security - BCMS - Requirements". This new BCM standard was published on May 15, 2012 and will replace the current British Standard BS 25999 (St-Germain et al., 2012). The transition period will end by May 2014 when no new BS 25999 certification will be issued. As for the existing BS 25999 certified organizations, the required transition is relatively straightforward and can be conducted at a future surveillance audit visit up until May 31, 2014.

ISO 22301 utilizes BS 25999:2 as a foundation, a standard which has already gained wide acceptance outside United Kingdom (SunGard, 2012). On top of that, it was also developed along with feedbacks from the international communities and the existing business continuity practices outlined in other BCM standards, such as NFPA 1600, FINRA Rule 4370, NIST SP 800-34 and various national standards such as those in Australia/New Zealand, Canada, Japan and Singapore. Hence, ISO 22301 represents the latest milestone in the evolution of BCM best practices. According to Heng (2012), ISO 22301 should be viewed as a convergence of all BCM standards into an ISO requirement.

The requirements stipulated in ISO 22301 are quite generic and aims to be applicable to all organizations regardless of size, type and nature of business. However, the extent of applicability of these requirements is very much depends on the operating environment and complexity of an organization (Heng, 2012). Similar to BS 25999, the purpose of this standard is to plan, establish, implement, operate, monitor, maintain, review and continuously enhance the documented BCMS. As posited by

Table 2: BCM standards

Document	Title	Comments
PAS56	Publicly available specification – BCM	It is a standard that was published by the British Standards Institution in 2003 which then, largely succeeded by BS 25999. The intention of PAS 56 is to be adopted by organizations to enhance their performance in BCM, whether starting out the BCM plan for the first time or refining their existing BCM plan next to best practice
BS 25999 (Part 1 and 2)	BSI BCM	The standard was launched by British Standard Institute in 2006 and 2007 which is considered as excellent reference for BCM. The standard has 2 parts namely, code of practice and specification for BCM
NFPA 1600	Standard on Disaster and Emergency Management and Business Continuity Programs	It was created by National Fire Protection Association (U.S) in 1995 which is used as blueprint for any organization in dealing with emergency and BCM
NIST 800-34	Contingency Planning Guide for Information Technology Systems	It was first published in June 2002 by National Institute of Standards and Technology (U.S.) which provides instructions, recommendations, and considerations for government IT contingency planning
ISO 27001	The Information Security Standard and ISMS	It was released in October 2005 to replace the old BS7799-2 standard. It is a specification for an ISMS
ISO 22301	Societal security - BCMS - Requirements	Newly introduced BCM standard in 2012 which provides a framework to plan, establish, implement, operate, monitor, maintain, review, and continuously enhance a BCMS

Source: (Peterson, 2009), BCMS: Business continuity management system

Heng (2012), the main objectives of the BCMS are to protect against, minimize the likelihood of occurrence of, prepare for, respond to and recover from a disruptive situation when it arises.

3.3.2. ISO 27001 – Information security management system (ISMS)

ISO 27001 is a global information system security standard that assists organizations in establishing a comprehensive ISMS (Rosso, 2011). It was established in October 2005, essentially to replace the old BS7799-2 standard. The standard offers a model for establishing, deploying, operating, monitoring, maintaining, evaluating and enhancing an ISMS (Gillies, 2011). Similarly as the BS25999 standard, the ISO 27001:2005 version of the standard introduced in 2005 heavily utilized the Plan-Do-Check-Act model in structuring the related processes.

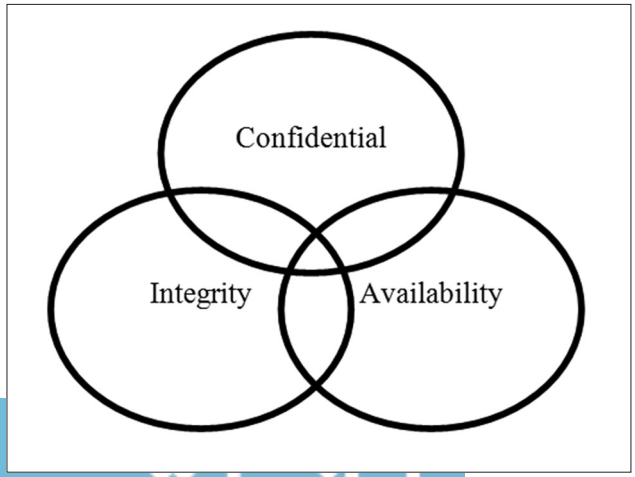
An important element involved in the implementation of ISO 27001 standard is to assess the risk of information assets scoped within the system against three fundamental information security requirements. The risk assessment process involves evaluation of potential risks that would compromise an information asset's confidentiality, integrity and availability (frequently abbreviated as CIA) (Lomas, 2010). Figure 1 illustrates the CIA concept.

1. Confidentiality refers to the property that information is not disclosed or made accessible to unauthorized parties
2. Integrity refers to the property of safeguarding the completeness and accuracy of information assets
3. Availability refers to information assets should be readily accessible and useable upon demand by an authorized party.

In the context of BCM, ISO 27001 classified the business continuity requirement as part of the "availability" component. The BCM control statements are outlined in Clause 14 i.e., BCM with the objectives to respond to disruption on business processes and to safeguard critical business functions from the effects of major disruptions of information system services and to ensure timely recovery.

The adoption of ISO 27001 standards shall benefits organizations in several ways. Besides tighten up the information security system, the standards may help to streamline the internal processes, eliminate redundancies, prevent costly litigation and enhance the competitive advantage. The ISO 27001 standard necessitates continuous security management, which means that after obtaining the initial certification, organizations should constantly monitor, review and improvise as necessary to remain in compliance. The surveillance audit will be conducted annually while the recertification audit will be conducted once every 3 years (Rosso, 2011). ISO 27001 certification can be an essential market differentiator for an organization which may attract and retain customers with the enhanced information system security. It is a recognition that the organization is actively managing its information security based on the internationally established standards.

Figure 1: Confidentiality, integrity and availability concept



4. RESEARCH FRAMEWORK AND HYPOTHESIS

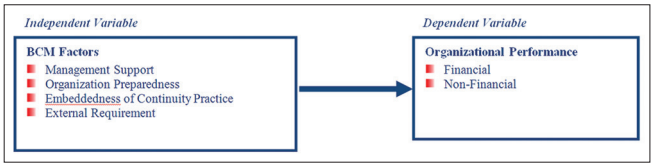
This paper attempts to fill the theoretical and practical gaps by proposing a conceptual framework for future research to provide empirical evidence on the relationships that exist between BCM factors and organizational performance. Figure 2 depicts the conceptual framework which represents the main variables of this study.

The relationship between BCM factors and organizational performance is based on the resource based view theory that proposes the performance of an organization is influenced by internal resources. An organization achieves better performance than its competitors by effectively utilizes its internal resources. However, in order to foster distinctive capabilities, the resources must be rare, valuable, non-imitable, non-transferable and non-substitutable (Barney, 1991).

The relationship between BCM factors and organizational performance is also explained by the crisis management theory that highlighted the importance of organization readiness in responding to unexpected crisis events that may hinder or impede normal business operations, thus threatening the achievement of organizational objectives (Pearson and Clair, 1998). Jafari et al. (2011) postulates that when a company is capable to avoid the adverse impacts of external risks and respond to the environmental changes, it will be less vulnerable to financial consequences of market disparity. In other words, when an organization manages its risks effectively, it will successfully adapt to changes in market conditions and profit variation will be minimized. The high level hypotheses statements are as follows:

H1: The extent of BCM factors significantly effect the financial performance.

Figure 2: Conceptual framework



H2: The extent of BCM factors significantly effect the non-financial performance.

In order to test the research framework and hypotheses, samples will be selected from organizations which have obtained the ISO 22301 and/or ISO 27001 accreditation from Standards and Industrial Research Institute of Malaysia. This population is selected as organisations which have obtained the certification of internationally recognized standards are deemed to possess considerably higher sense of commitment towards ensuring the business resiliency by enhancing their capability and competency. This could also be seen as an indication of the organization's maturity in practising BCM. In the research conducted by Sawalha (2013), he found that organizations with matured BCM processes had indicated substantial performance improvements. Furthermore, these organizations represent various industries such as financial institution, telecommunications, ICT, utility providers, services, industrial, education, transportation and government agencies from both public and private sectors.

5. CONCLUSION

At present, the global business atmosphere and conditions are becoming more turbulent and sometime unpredictable. Such situation, as well as the fast technology advancements and social dynamics affect almost everyone including all organizations around the planet (Mitroff, 2004; Pollard and Hotho, 2006). Hence, organizations desiring to stay competitive and successful must be well protected, through heightened resiliency so that it could remain profitably in the event of any fatal business disruption. Organizations from both the private and public sectors have to be more prepared to counter any undesirable crisis and ensure that the interruptions to their business operations are kept at a very minimal possible. Any critical operational failure may cause a degradation of service quality and even a monetary loss if the duration or degree of business interruption is extensive (Yiu and Tse, 1995).

This paper aims to further establish the importance of BCM as a strategic management tool which must be employed by organizations to minimize the operational risk and its impact to critical business functions. The paper also proposes the conceptual framework for future research to provide empirical evidence on the relationship that exist between the BCM factors and organizational performance. The researchers hope that the outcome of the research will assist the managers, business and BCM professionals to justify further investment and effort in improving the BCM knowledge, processes and infrastructure. In addition, this study could provide better understanding to the decision makers on the significant role of BCM in relation to the organizational performance and encourage their participation at the strategic level.

REFERENCES

Alesi, P. (2008), Building enterprise-wide resilience by integrating business continuity capability into day-to-day business culture and technology. Journal of Business Continuity and Emergency Planning, 2, 214-220.

Arend, M. (1994), Time to dust off your contingency plan. ABA Banking Journal, 86(2), 56-67.

Attaran, M. (2003), Information technology and business-process redesign. Business Process Management Journal, 9(4), 440-458.

Barney, J.B. (1991), Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99-120.

Belaouras, S. (2009), State of business continuity preparedness. Disaster Recovery Journal, 22(1). Available from: http://www.drj.com/index.php?option=com_content&task=view&id=2206&Itemid=676.

Cerullo, M.J., McDuffie, R.S. (1994), Planning for disaster. CPA Journal, 64(6), 34-39.

Chow, W.S. (2000), Success factors for IS disaster recovery planning in Hong Kong. Information Management and Computer Security, 8(2), 80-87.

Chow, W.S., Ha, W.O. (2009), Determinants of the critical success factor of disaster recovery planning for information systems. Information Management and Computer Security, 17(3), 248-275.

Conlon, R., Smith, R.V. (2010), The role of the board and the CEO in ensuring business continuity. Financial Executive, 26(9), 52-55.

Elliott, D., Swartz, E., Herbane, B. (2010), Business Continuity Management: A Crisis Management Approach. 2nd ed. New York, USA: Routledge.

Gibb, F., Buchanan, S. (2006), A framework for business continuity management. International Journal of Information Management, 26(2), 128-141.

Gillies, A. (2011), Improving the quality of information security management systems with ISO27000. The TQM Journal, 23(4), 367-376.

Hägerfors, A., Samuelsson, S., Lindström, J. (2010), Business continuity planning methodology. Disaster Prevention and Management, 19(2), 243-255.

Heng, G.M. (2012), Business Continuity Management Specialist Series: A Manager's Guide to ISO 22301 Standard for Business Continuity Management System. 1st ed. Singapore: GMH Pte Ltd.

Herbane, B. (2010), The evolution of business continuity management: A historical review of practices and drivers. Business History, 52(6), 978-1002.

Herbane, B., Elliott, D., Swartz, E.M. (2004), Business continuity management: Time for a strategic role? Long Range Planning, 37(5), 435-457.

Hoong, L.L. (2011), Factors Influencing the Success of the Disaster Recovery Planning Process : A Conceptual Paper. In: Research and Innovation in Information Systems (ICRIIS), 2011 International Conference.

Jafari, M., Chadegani, A., Biglari, V. (2011), Effective risk management and company's performance: investment in innovations and intellectual capital using behavioural and practical approach. International Research Journal of Finance and Economics, 3(15), 780-786.

Järveläinen, J. (2013), IT incidents and business impacts: Validating a framework for continuity management in information systems. International Journal of Information Management, 33, 764-774.

Karim, A.J. (2011), Business disaster preparedness: An empirical study for measuring the factors of business continuity to face business disaster. International Journal of Business and Social Science, 2(18), 183-192.

Kenny, J. (2006), Strategy and the learning organization: a maturity model for the formation of strategy. The Learning Organization, 13(4), 353-368.

KPMG. (2014), The 2013-2014 Continuity Insights and KPMG LLP Global Business Continuity Management (BCM) Program Benchmarking Study.

Laurent, W. (2007), Business Continuity Dashboards. DM Review, 17(6), 30-40.

Lomas, E. (2010), Information governance: Information security and

access within a UK context. Records Management Journal, 20(2), 182-198.
Low, S.P., Liu, J., Sio, S. (2010), Business continuity management in large construction companies in Singapore. Disaster Prevention and Management, 19(2), 219-232.
Mitroff, I.I. (2004), Think like a sociopath, act like a saint. Journal of Business Strategy, 25(5), 42-53.
Payne, C.F. (1999), Contingency plan exercises. Disaster Prevention and Management, 8(2), 111-117.
Pearson, C.M., Clair, J.A. (1998), Reframing crisis management. The Academy of Management Review, 23(1), 59-76.
Peterson, C.A. (2009), Business Continuity Management and Guidelines. 2009 Information Security Curriculum Development Conference on - InfoSecCD '09. p114. doi:10.1145/1940976.1940999.
Petroni, A. (1999), Managing information systems' contingencies in banks: a case study. Disaster Prevention and Management, 8(2), 101-110.
Pitt, M., Goyal, S. (2004), Business continuity planning as a facilities management tool. Facilities, 22(3/4), 87-99.
Pollard, D., Hotho, S. (2006), Crises, scenarios and the strategic management process. Management Decision, 44(6), 721-736.
Rohde, R., Haskett, J. (1990), Disaster recovery planning for academic computing centers. Communications of the ACM, 33(6), 652-657.
Rosso, A. (2011), ISO 27001 primer. Collector, 77(1), 31-35.
Ruighaver, A.B., Ahmad, A., Hadgkiss, J. (2012), Incident response teams – Challenges in supporting the organisational security function. Computers and Security, 31(5), 643-652.
Saleem, S. (2011), Do effective risk management affect organizational performance. European Journal of Business and Management, 3(3), 258-268.
Sawalha, I.H.S. (2013), Organisational performance and business continuity management: a theoretical perspective and a case study. Journal of Business Continuity and Emergency Planning, 6(4), 360-373. Available from: http://www.ncbi.nlm.nih.gov/pubmed/23835428.
Selden, S., Perks, S. (2007), How a structured BIA aligned business continuity management with Gallaher 's strategic objectives. Journal of Business Continuity and Emergency Planning, 1(4), 348-355.
St-Germain, R., Aliu, F., Lachapelle, E., Dewez, P. (2012), Whitepaper: Societal Security Business Continuity Management System. Professional Evaluation and Certification Board.
SunGard. (2012), ISO 22301 : A Framework for Business Process Definition, ISO.
Vancoppenolle, G. (2007), In: Hiles, A., editor. The Definitive Handbook of Business Continuity Management. 2nd ed. England: John Wiley and Sons Ltd.
Wong, W.N.Z. (2009), The strategic skills of business continuity managers: putting business continuity management into corporate long-term planning. Journal of Business Continuity and Emergency Planning, 4, 62-68.
Yen, D.C., Chou, D.C., Hawkins, S.M. (2000), Disaster recovery planning: a strategy for data security. Information Management and Computer Security, 8, 222-230.
Yiu, K., Tse, Y.Y. (1995), A model for disaster recovery planning. IS Audit and Control Journal, 5, 45-51.