

AN ANALYSIS OF BUSINESS CONTINUITY RISKS AND RELATED BUSINESS CONTINUITY PLANS AT COMPANIES IN SOUTH AFRICA

I. NEL AND B. MARX

ABSTRACT

This study investigated the different business continuity risks organisations face and the existence of business continuity plans to address and manage these risks. The study found that although the majority of organisations are aware of the business continuity risks that they are faced with, not all fully understand the impact thereof on their organisations, and accordingly do not have effective and adequate business continuity plans in place to address and manage these risks. Also, not all organisations are placing enough emphasis on the establishment of a business continuity culture within their organisations to support their business continuity philosophy and plan.

Keywords: Business continuity, Business continuity risks, Business continuity plan, Business continuity culture, Business impact analysis

1. INTRODUCTION

To prevent the disruption of an organisation's daily operations and to ensure the survival of an organisation in the event of a catastrophe, organisations must reconsider the importance of creating awareness and being prepared for the unexpected. No organisation can be certain that it will never encounter a disaster or crisis. The disaster or crisis may perhaps not take the form of a natural disaster or a terrorist attack, but a power disruption, software failure or labour strike could also cause significant damage to an organisation (Altman, 2006:46; Dalton, 2010:23; Clas, 2008:45; Green & Mark, 2009; Reuid, 2005:26). Most organisations currently do not prioritise business continuity as part of their critical business processes. The reason for this is, firstly, due to the great deal of work that needs to be done around this matter. Secondly, most organisations do not have staff with enough experience to perform this function. And, lastly, many organisations naively believe that they are already prepared for any disaster (Green & Mark, 2009). Some organisations defer or ignore the development and implementation of a business continuity process due to financial pressures or other seemingly more important problems (Doughty, 2002). It is only when an organisation has been struck by a disaster that it realises the benefits of having business continuity processes in place (Bakshi & Rafeq, 2005). There are still organisations that do not have any plans or strategies in place to effectively address the impact of business continuity risks on their organisation. Disaster or crisis events will cause significant disruptions to these organisations' critical business operations and could even put the survival of the organisation at risk (Young, 2010; Clas, 2008:45; Fluss, 2008:12; Altman, 2006:46; Sarrel, 2007:152).

Risk management has become an important process within the governance of an organisation, with a broad risk focus on financial, operational and business risks. The modern corporate environment requires an integrated risk management process that consists of an all-inclusive risk approach (Marx, 2008:85; Reuvid, 2005:20). The shift in focus of risk management from financial risks only to incorporate business risk, which includes the risk of business continuity, has led to business continuity becoming more prominent in today's business world (PricewaterhouseCoopers, 2009:32). Another factor that has increased the importance of business continuity relates to the fact that Information Technology (hereafter IT) has become an integral part of organisations' day-to-day business processes (Green & Mark, 2009; Wagner, 2007:41). The rapid changes and developments of information technology within organisations, and the increased reliance placed by organisations on their information systems, also increasingly exposes organisations to business continuity risks (Wessels 2006:131; Curtin, Hayman and Hussein, 2005:168). The latest King Code of Governance for South Africa 2009 (hereafter King III) emphasises that IT should form an integral part of the company's risk management process, and specifically recommends that IT risk management should include disaster recovery planning to address the risk of business continuity (Institute of Directors Southern Africa (hereafter IOD), 2009:40; PricewaterhouseCoopers, 2009:35).

This study found evidence that business continuity risks are a prominent factor in modern organisations, but that currently not all organisations fully understand the impact of these risks on their organisations and therefore still do not have business continuity plans in place. The study also revealed that there is still room for improvement in the way organisations in South Africa currently address their business continuity risks. The research is of importance to companies within South Africa, as limited research has been done to date on business continuity practices in South Africa. The present study, then, could contribute significantly to the existing body of knowledge.

The remainder of this paper is structured as follows: the next sections will discuss the objective, scope and limitations of the study; thereafter the theoretical background of the study will be discussed as well as the methodology that was applied and the empirical findings and interpretations. The recommendations drawn from the study and areas identified for future research possibilities will then be provided. The conclusion of the study will be presented in the last section.

2. OBJECTIVES, SCOPE AND LIMITATIONS

The objective of the paper is twofold: firstly, to provide a brief overview of the different business continuity risks that an organisation can encounter and the concept and principles of an effective business continuity plan to address and manage these risks; and, secondly, to provide evidence on the current

business continuity risks and practices at organisations in South Africa. To achieve this objective a literature review was performed through which the critical types of business continuity risks and the process of identifying, assessing and analysing these risks were investigated as well as the business continuity plans and cultures that should support this process. This review is supported by empirical evidence obtained from questionnaires completed by the big four accountancy service firms in South Africa.

This study has the limitation that it is confined to the clients of the big four accountancy service firms in South Africa, and the findings might not necessarily be representative of the business continuity risks and practices at all organisations within South Africa. The sample size might also make it difficult to generalise the findings to all South African businesses. However, the big four firms' clients represent the majority of publicly traded companies as well as private companies within South Africa and therefore should be representative of the majority of organisations in South Africa.

3. THEORETICAL BACKGROUND

3.1. The concept of business continuity

The concept of business continuity relates to activities or procedures implemented at an organisation to limit the impact of a disaster or crisis on the critical business processes or functions of the organisation, ensuring that the organisation can effectively continue with business as usual (http://en.wikipedia.org/wiki/Business_continuity; Altman, 2006:48; Muthukrishnan, 2005; Toigo, 2003:3; Wylder 2004:153).

Most organisations are reliant on only a few key factors to ensure the survival of their business. It is these factors that must be identified and considered during the business continuity process. The first two key factors include the organisation's physical assets and its systems, which allow the business operations to be performed and the customer to be delivered the required end product. In cases where the organisation's assets or systems are not available or not functioning effectively, this will negatively impact the operations of the organisation, the customer's confidence and, ultimately, the organisation's profit and continuity. The last key factor that is of the utmost importance to the organisation is its human resources. These are essential to the business, as they monitor and control the organisation's assets and systems. Business continuity is not a process that organisations must consider only when they have reached a certain size. The process is essential for small, medium and large organisations. Any organisation, small or large, is dependent on its key business factors for survival (Curtin, et al. 2005:167).

3.2. Identifying, assessing and analysing business continuity risks

The first important step an organisation must take in the direction of business continuity is to be aware of and understand the business continuity risks that it could be faced with. The nature of the organisation and its location and business processes will all have an impact on the different business continuity risks that the organisation could experience. Once an organisation has identified its risks it will be possible to assess these risks and also determine the impact these risks could have on the organisation's business operations (Bakshi & Rafeq, 2005; Chantico Publishing Company, 1991; Devlin & Arnold, 2007; Doughty, 2001; Federal Financial Institutions Examination Council (hereafter FFIEC), 2008; Muthukrishnan, 2005; Rash, 2008; Reuvid, 2005; Wallace & Webber, 2004).

The concept of business continuity risk can be explained by dividing it into four components: threats, resources, modifying factors and consequences. The threat component relates to the range of events that could lead to significant consequences. The resource component consists of the assets, people or profits that could be affected by the threats, while the modifying factors relate to the internal and external factors that will influence the possibility of the threat taking place and the significance of the impact of the threat. Lastly, the consequence component explains the effect the threat will have on the relevant resources involved (Charlette, 1996:373; Doughty, 2001:3, FFIEC, 2008; Wallace & Webber, 2004:29).

There are various different types of risks that could have an impact on the organisation's business continuity. These can be divided into the following five categories (FFIEC, 2008; Devlin and Arnold, 2007:9; Chantico Publishing Company, 1991:109; Rash, 2008:30):

- Malicious activities
- Natural disasters;
- Technical disasters;
- Non-physical damage crises; and
- Political disasters.

The first category of business continuity risks relates to malicious activities caused by the intentional actions of internal or external parties, with the main purpose of obtaining financial gain or revenge (Bakshi and Rafeq, 2005; Devlin and Arnold, 2007:114; FFIEC, 2008; Marx, 2008:9). The second category relates to natural disasters, which are caused by acts of nature (Amadeo, 2010; Devlin and Arnold, 2007:17; Hargreaves, 2010; Schwerdtfeger, 2010:1; Tseng, 2010). Thirdly, technical disaster is of great concern to many of today's modern businesses, which are heavily reliant on their information systems for their survival (Clas, 2008:45; Dalton, 2010:23; Green & Mark, 2009; Miller & Wenham, 1991:31; Ross, 2008:1; Wagner,

2007:41). The fourth category refers to the non-physical damages to the organisation's brand generally caused by negative publicity or a shift in the market (AM-Online, 2010; Devlin and Arnold, 2007:10; Halvorson, 2010). The last category of business continuity risks relates to the disruption and financial impact of a strike on an organisation's operations (Chantico Publishing Company, 1991:109; Flak, 2010).

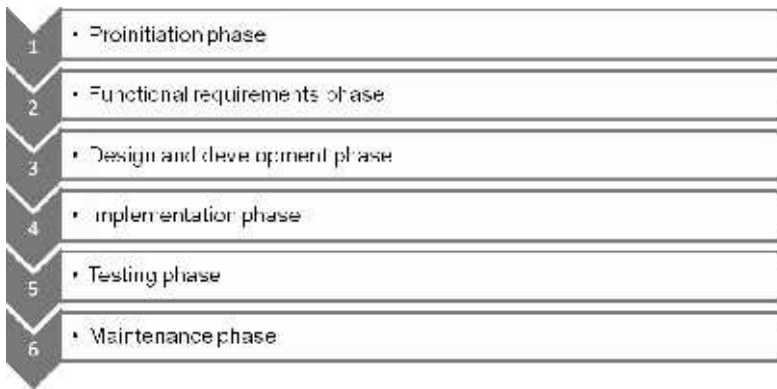
Performing a risk assessment on the possible business continuity risk faced by an organisation will entail an evaluation of internal and external factors that are inherent to the organisation's nature, business processes and geographic location. These factors will all influence the possibility of the occurrence of business continuity risks at the organisation (Bakshi & Rafeq, 2005; Devlin & Arnold, 2007:26; FFIEC, 2008; Muthukrishnan, 2005; Reuvid 2005:28). The next essential step that follows the risk assessment process is referred to as the business impact analysis (hereafter BIA). The BIA consists of three phases. During the first phase of the analysis the organisation must determine the critical business functions and processes of the organisation. It is these critical functions and processes that require priority within the business continuity plan. During the second phase the recovery time objective (hereafter RTO) and recovery point objective (hereafter RPO) of each critical function and process must be determined so as to highlight the maximum allowable downtime and acceptable level of data loss a system will be able to tolerate. In the last phase the organisation must evaluate the resources necessary to support and maintain each critical function or process in the event of a disaster or crisis (Bank for International Settlements, 2006:1-4; Doughty, 2001:116-129; FFIEC, 2008; FR Technologies, n.d; Muthukrishnan, 2005; Reuvid, 2005:54; Sayana, 2005; Toigo, 2003:42).

3.3. The concept and principles of a business continuity plan

As is evident from the previous section, it is essential for organisations to identify, assess and analyse their business continuity risks. But the process of business continuity does not end here, as it is essential that the organisation implement policies and procedures to address business continuity risks. These policies and procedures can be addressed through an effective and adequate business continuity plan that will ensure that the organisation is prepared for the event of a disruption or disaster, and also to ensure that business continuity measures are maintained and managed within the organisation. If its actions and procedures are not captured in a formal document such as a business continuity plan, the organisation will not be able to survive a catastrophic event and could be faced with significant financial losses. Organisations therefore need to be aware of the steps they need to follow when developing and implementing a business continuity plan (Bank for International Settlements, 2006:1; Curtin, et al., 2005:165; Information Systems Audit and Control Association (hereafter ISACA), 2005:3; Muthukrishnan, 2005).

The figure below indicates the different steps or phases the organisation must consider when looking at a business continuity plan:

Figure 3.1.: Business continuity plan methodology



Source: Doughty (2002); Chantico Publishing Company (1991:26)

The figure illustrates that the development of a business continuity plan consists of six phases. The first phase is the framework of the plan, which includes the objectives and goals of such a plan. During this phase it is essential that the organisation selects the business continuity team that will be responsible for the development of the plan. It is important that members from all the critical business functions as well as executive management form an integral part of such a team (Curtin, et al., 2005:170; Doughty, 2002; Sarrel, 2007:152; Wylder, 2004: 157-160).

The second phase consists of the functional requirements of the business continuity plan. It is during this phase that business continuity risks must be identified, assessed and analysed (as discussed in section 3.2) to ensure that the correct functional areas are addressed in the plan.

Phase three refers to the design and development of the plan, during which the recovery strategy must be determined. The RTO (as discussed in section 3.2) of each critical business function is an essential element that must be considered during phase three. Organisations can decide to develop the plan internally, develop it externally, or combine the two (Doughty, 2002; Chantico Publishing Company, 1991:187).

Phase four focuses on the implementation of the plan, which must consist of a prevention plan, an emergency response plan as well as a business resumption plan (Doughty, 2002; Devlin and Arnold, 2007:43).

Phase five represents the testing phase, which is one of the most critical phases in the development of a business continuity plan. Organisations must determine the roles and responsibilities of the people involved in this phase and also decide on the most effective testing method to be used (Doughty, 2002; FFIEC, 2008; Lengyel, 2006; Snow, 2008:26; Wallace and Webber, 2004:129; Wylder, 2004:166; Zawada, 2009).

The last phase refers to the maintenance phase during which the post-implementation review of such a plan must be conducted on an ongoing basis to ensure that the required updates and changes to the plan are monitored and implemented. This ensures the constant readiness of the organisation's business continuity plan (Doughty, 2002).

3.4. Business continuity culture within an organisation

An organisation may have all the procedures and plans in place to address its business continuity risks, but if it does not have a business continuity culture, the success of all the measures that are in place may be placed in jeopardy. It is therefore essential that the management of business continuity within the organisation provides a sound environment and framework in which business continuity measures will be supported in order to ensure the effective functioning of the organisation's business continuity plan (Reuvid, 2005:53).

The figure below indicates the elements necessary to build a culture that supports the organisation's business continuity philosophy and business continuity plan.

Figure 3.2.: Elements for developing a business continuity culture



Source: Doughty (2001:27)

Implementing a sound business continuity culture that will support the organisation's business continuity philosophy consist of six elements. The first element refers to the commitment, support and involvement of an organisation's executive management within this process. Secondly, organisations must identify the major stakeholders of the business continuity process to ensure their active participation in this process. Thirdly, it is emphasised that the formation of a business continuity plan team is critical to the success of the business continuity plan and the importance of implementing a business continuity policy. The second last element concerns the shared vision and trust of the business continuity policy among all employees of the organisation. The last important element that will ensure that a sound business continuity culture is created refers to the importance of the communication of this policy among employees and business continuity team members. This can be achieved through the implementation of education programmes that will emphasise the importance of the concept as well as the determination of every employee's role and responsibility in this process (Doughty, 2001:28-32; Doughty, 2002; FFIEC, 2008; Wylder, 2004:167).

4. METHODOLOGY

The literature study provided the foundation for the aspects that were tested empirically through questionnaires sent to the big four audit firms, as discussed below.

4.1. Population

According to Wikipedia (2010), the largest international accountancy professional service firms are KPMG, Deloitte Touche Tohmatsu, Ernst & Young and PricewaterhouseCoopers. An internet search of literature on professional service firms in the field of accountancy provided further support for this view (Answers.com, 2010; QFINANCE, 2010; The Free Dictionary, 2010). One can therefore conclude that these firms' client base represents a wide range of national and international organisations, and accordingly these firms in South Africa were selected as the population for the testing conducted in the empirical study. The head of auditing as well as the head of the technical division of each firm were asked to complete questionnaires relating to business continuity practices at their clients.

4.2. Questionnaire design and testing

The questions in the questionnaire were based on the information obtained from the literature study as well as discussions held with academics, experts from industry and audit practitioners. The questionnaire was designed to ensure that respondents could easily complete the questions. The questions also made provision for open-ended sections where respondents could provide comments. The participants were able to complete the questionnaire either electronically or manually.

Before the questionnaire was sent out it was tested by a selected group of people consisting of academics and audit practitioners. Through testing the questionnaire it was ensured that the questions were set out logically and that the questionnaire was easy to complete.

4.3. Response rate for the questionnaire

For the questionnaires a 100% response rate was achieved. All of the questionnaires were completed and received back.

Table 4.1.: Response rate of questionnaires

	Questionnaire to Big Four audit firms	
	Number	Percentage
No response	0	0%
Completed and usable questionnaire	8	100%
Total percentage of questionnaires sent out	8	100%

5. RESEARCH FINDINGS AND INTERPRETATIONS

The objective and findings of each question of the questionnaire are explained and discussed below:

5.1. Business continuity risks and the impact on organisations

i) Objective of the questions

The objective of the questions in Table 5.1 was to determine the different types of business continuity risks that are applicable to organisations in South Africa and to establish the different impacts that these risks have on the organisations.

ii) Findings

Table 5.1: Business continuity risks and the impact on organisations

	Total	Number		Percentage	
		Yes	No	Yes	No
Are you of the opinion that the following business continuity risks are applicable to your audit clients?					
Natural disasters (i.e. flood, fire, earthquake, etc.)?	8	7	1	87.5%	12.5%
Technical disasters (i.e. power outages, loss of e Commerce capabilities, loss of internet or email access, etc.)?	8	8	0	100%	0%
Non physical damages (i.e. negative publicity, market shift, brand issues, financial or cash problems, etc.)?	8	8	0	100%	0%
Political events (i.e. strike of employees)?	7	7	0	100%	0%
Malicious activities (i.e. fraud, sabotage or vandalism activities, terrorist attacks, etc.)?	8	6	2	75%	25%
Have any of your audit clients experienced the following due to business continuity risks?					
Loss of strategic data or information?	8	4	4	50%	50%
Loss of human resources?	8	3	5	37.5%	62.5%
Loss of capital resources?	8	3	5	37.5%	62.5%
Loss of market share?	8	3	5	37.5%	62.5%
Disruption to business processes?	7	5	2	71.43%	28.57%
Financial losses?	8	6	2	75%	25%

Source: Questionnaire (own calculation)

Key interpretations based on the above findings:

In the literature review it was pointed out that the different business continuity risks can be divided into the following categories: natural disasters, technical disasters, non-physical damages, political events and malicious activities. From the findings above it is evident that all of these categories of business continuity risks are applicable to organisations in South Africa, as 100% of organisations are exposed to technical disasters, non-physical damages and political events, while 87.5% of organisations are faced with natural disasters and 75% with malicious activities.

The above findings also revealed that South Africa organisations have been impacted by business continuity risks as follows: 75% of organisations have suffered from financial losses, 71.43% were exposed to disruption to business processes, 50% experienced the loss of strategic data or information and 37.5% of organisations were impacted by loss of human resources, capital

resources and market share. Therefore, the findings indicate that most organisations are faced with financial losses and disruptions to business processes due to business continuity risks.

These findings emphasise the fact that business continuity risks are relevant to organisations in South Africa, and that there is a need to constantly assess and manage these risks.

5.2. Identification and addressing of business continuity risks by organisations

i) Objective of the questions

The objective of the questions in Table 5.2 was to determine the organisation's awareness of the business continuity risks that it is faced with, its understanding of the impact of these risks, and whether sufficient and effective procedures and actions are in place to address business continuity risks. A further objective of the question was to establish whether organisations have a business continuity culture that supports their business continuity philosophy.

ii) Findings

Table 5.2: Identification and addressing of business continuity risks by organisations

	Total	Number			Percentage		
		To what extent			To what extent		
Are you of the opinion that your audit clients:		Large	Lesser	None	Large	Lesser	None
Are aware of the business continuity risks faced by their organisation?	8	5	3	0	62.5%	37.5%	0%
Understand the impact of business continuity risks on their organisation?	8	4	4	0	50%	50%	0%
Have sufficient and effective actions and procedures in place to address their business continuity risks (i.e. business continuity plan)?	8	4	4	0	50%	50%	0%
Executive management is involved with their organisation's business continuity planning?	8	5	3	0	62.5%	37.5%	0%
The board of directors is committed to their organisation's business continuity planning?	8	5	3	0	62.5%	37.5%	0%
There is a business continuity culture that supports their business continuity philosophy?	8	0	8	0	0%	100%	0%

Source: Questionnaire (own calculation)

Key interpretations based on the above findings:

From the literature study it is evident that the first essential tool in the development of a business continuity plan is to perform a risk assessment through which the organisation can identify and analyse the possibility of the different types of business continuity risks that could impact the organisation. Through the risk assessment process the organisation will become fully aware of the types of risks applicable to it. From the findings it is encouraging to see that 62.5% of South African organisations are to a large extent aware of the business continuity risks that could affect their business continuity, but it is worrying that 37.5% of organisations are aware of these risks only to a lesser extent. This is worrying due to the fact that the first step in business continuity planning is an awareness of the organisation's business continuity risks. If organisations are aware of their business continuity risks, effective measures and actions can be implemented to address them.

The risk impact analysis as discussed in the literature study highlighted the fact that organisations are required to determine their critical business functions, establish the maximum downtime that can be endured by these critical functions and also evaluate the resources required to recover or resume any critical function or process. The process will assist the organisation to determine the impact of business continuity risks on its survival. The findings indicated that 50% of South Africa organisations to a large extent understand the impact of business continuity risks on their organisations, but it is concerning that the other 50% of organisation understand the impact of business continuity risks only to a lesser extent. For organisations to address business continuity risks effectively, they must fully understand the impact of these risks on the organisation.

The literature study also pointed out that organisations must develop and implement actions and procedures in the form of a business continuity plan to manage their business continuity risks effectively and ensure the survival of the organisation in the event of a catastrophe. The above findings revealed that 50% of South Africa organisations do to a large extent have business continuity plans in place, while the other 50% of organisations have business continuity actions and procedures in place only to a lesser extent. The above findings indicate a point of concern: the findings displayed in Table 5.1 reveal that organisations are faced with all five categories of business continuity risks which cause financial losses and disruptions to business processes. Taking these findings, which indicate that organisations are currently exposed to business continuity risks, into account, it is concerning that 50% of organisations have effective and adequate actions and procedures in place to address these risks only to a lesser extent. The above findings, which reveal that only 50% of organisations to a large extent fully understand the impact of these risks on them, could indicate why organisations do not currently realise the importance of a business continuity plan.

The above findings also revealed that 62.5% of South Africa organisations' managements are to a large extent involved in and committed to the organisation's business continuity planning. Management is designated to include executive management as well as the board (which includes non-executive directors as well). Although management is involved in and committed to this process, the findings also indicated something of concern: none of these organisations have a business continuity culture. As discussed in the literature study, a business continuity culture is essential to support an organisation's business continuity philosophy and to ensure the success of the organisation's business continuity process. These findings therefore indicate that current organisations do have the involvement and commitment of management to the business continuity process, but lack the existence of a business continuity culture that supports this philosophy. Without a sound business continuity culture within an organisation the business continuity plan might not be effectively implemented and functioning.

5.3 Improvement in addressing business continuity risks by organisations

i) Objective of the questions

The objective of the question in Table 5.3 was to determine if there is any room for improvement in the way organisations in South Africa address business continuity risks.

ii) Findings

Table 5.3: Improvement in addressing business continuity risks by organisations

	Total	Number		Percentage	
		Yes	No	Yes	No
Are you of the opinion that there is room for improvement in the manner in which the following parties address business continuity risks:					
The organisation (audit clients)?	8	8	0	100%	0%

Source: Questionnaire (own calculation)

Key interpretations based on the above findings:

The above findings revealed that there is a need at South Africa organisations (100%) to improve the way in which organisations address business continuity risks. These findings are supported by the findings in Table 5.2, which revealed that 50% of organisations currently do not fully understand the

impact of business continuity risks on them and that 50% of organisations still do not have a business continuity plan in place. Table 5.2 also revealed that 100% of organisations also do not have a sound business continuity culture that supports their business continuity philosophy. These findings all strongly suggest that there is still room for improvement in the way organisations in South Africa address their business continuity risks.

5.4. Summative findings on the empirical study:

The findings of the empirical study discussed in sections 5.1 to 5.3 indicate that organisations in South Africa are faced with business continuity risks, which include natural disasters, technical disasters, non-physical damages, political events and malicious activities, and that most of these organisations have suffered business disruptions and financial losses as a result of these business continuity risks. Although most of the organisations in South Africa are aware of the different business continuity risks they are faced with, the findings indicated that organisations do not always understand the impact of these risks and also do not have sufficient and effective business continuity plans in place to address these risks.

The findings also indicated that South African organisations in general do not have a sound business continuity culture established within the organisation that supports its business continuity plan, although the management of these organisations is committed to and involved in the business continuity process. Lastly, the findings indicated that there is still room for improvement in the way organisations in South Africa currently address business continuity risks within their organisations.

6. RECOMMENDATIONS AND AREAS FOR FUTURE RESEARCH

Given the results of the study, it is recommended that organisations in South Africa, as well as globally, give careful consideration to business continuity risks, which have become a prominent factor within modern organisations. It is also essential for organisations to identify, assess and address these risks in order to ensure their survival in the case of a crisis or disaster. It is further recommended that organisations address these risks through the implementation of an effective business continuity plan and a sound business continuity culture within the organisation that will support its business continuity philosophy.

The study focused on larger organisations which form part of the client base of the big four audit firms. It is accordingly recommended that an analysis similar to this one be performed on smaller organisations to investigate the different business continuity risks applicable to these companies and the policies and procedures in place to address these risks.

7. CONCLUSION

The study investigated the different business continuity risks that organisations in South Africa could be faced with and the concept and principles of a business continuity plan to address these risks. It was found that there are various business continuity risks that could have an impact on organisations and that effective and adequate procedures should be implemented through a business continuity plan to ensure the survival of an organisation during a catastrophic event. These plans must also be supported by a business continuity culture.

It was found that business continuity risks are a factor in South Africa organisations, although from the findings it was evident that organisations might not fully understand the impact of these risks on their business and therefore do not have a proper business continuity plan in place to address such risks. The study further revealed that there could still be room for improvement in the way organisations in South Africa currently address their business continuity risks.

The study supports the findings of the literature that it is essential for the survival of an organisation that it identify, analyse and address its business continuity risks through a business continuity plan. This will ensure not only profitable and continuous business operations, but also the long-term survival of the organisation.

8. BIBLIOGRAPHY

Altman, W. 2006. When it all comes raining down. IEE Engineering Management, February/March: 46-48.

Amedeo, K. 2010. Economic Impact of Iceland Volcano. Available from: <http://useconomy.about.com/b/2010/04/19/economic-impact-of-iceland-volcano.htm> (Accessed on 27 June 2010).

AM-Online. 2010. Toyota brand image falls in YouGov index. Available from: <http://www.am-online.com/news/story/Toyota-brand-image-falls-in-YouGov-index/42901> (Accessed on 24 June 2010).

Answers.com. 2009. The world leading Q & A site. Available from: <http://www.answers.com/topic/big-four>. (Accessed on 01 September 2010).

Bakshi, S. & Rafeq, A. 2005. The Asian Tsunami: A Wake-up Call for Traditional Disaster Recovery Planning. Information Systems Control Journal, Volume 3. Available from: <http://www.isaca.org/Journal/Post-Issues/2005/Volume-3>. (Accessed on 2 November 2009).

Bank for International Settlements. 2006. The Joint Forum. High-level principles for business continuity. Basel. Switzerland. Press & Communications. ISBN 9291317225.

Chantico Publishing Company Inc. 1991. Disaster Recovery Handbook. 1st edition. Blue Ridge Summit, Pa. TAB Professional and Reference Books. ISBN 0830676635.

Charlette, RN. 1996. The Mechanic of managing IT risk. Journal of Information Technology, Volume 11: 373-378.

Clas, E. 2008. Business Continuity Plans Key to Being Prepared for Disaster. Best Practices. Professional Safety, September: 45-48.

Curtin, T., Hayman, D. & Hussein, N. 2005. Managing a crisis: A practical guide. Houndsmill, Basingstoke, Hampshire. Palgrave Macmillan. ISBN 1403943222.

Dalton, C. 2010. The brink of the abyss and back again! Kaseya Special Focus, March: 23-24.

Devlin, S. & Arnold, RL. 2007. Crisis management planning and execution. Boca Raton, FL. Auerbach Publications. ISBN 0849322448.

Doughty, K. 2001. Business Continuity planning: protecting your organization's life. Boca Raton. Auerbach. ISBN 0849309077.

Doughty, K. 2002. Business Continuity: A Business Survival Strategy. Information Systems Control Journal, Volume 1. Available from: <http://www.isaca.org/Journal/Post-Issues/2002/Volume-1>. (Accessed on 2 November 2009).

Federal Financial Institutions Examination Council. (FFIEC). 2008. Business Continuity Planning. IT Examination Handbook. Available from: <http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bcp> (Accessed on 12 November 2009).

Flak, A. 2010. Transnet strike halts rail and port operations. Mail & Guardian, 10 May: Online. Available from: <http://www.mg.co.za/article/2010-05-12-transnet-strike-halts-rail-and-port-operations>. (Accessed on 14 June 2010)

Fluss, D. 2008. A Disaster Waiting to Happen? Business continuity and disaster recovery are often overlooked. Customer Relationship Management, November: 12.

FR Technologies n.d. Business Continuity and Disaster Recovery. Available from: <http://www.fr-tech.net/bcp-dr.php#bcp-life-cycle-dets> (Accessed on 12 November 2009).

Green, RP. & Mark, R. 2009. An Executive Primer on Business Continuity Planning and Related IT Considerations. The CPA Technology Advisor, September. Available from:

<http://license.icopyright.net/user/viewFreeUse.act?fuid=NTc2NDEyNA%3D%3D> (Accessed on 12 November 2009).

Halvorson, B. 2010. Toyota Recall Already Denting Residuals, Resale Values. Available from: http://www.thecarcnrxction.com/marty-blog/1042406_toyota-recall-already-denting-resid (Accessed on 24 June 2010).

Hargreaves, S. 2010. BP's \$70 billion whipping. CNNMoney, 2 June. Available from:

http://money.cnn.com/2010/06/01/news/companies/BP_analysts/index.htm?postversio (Accessed on 14 June 2010).

Information Systems Audit and Control Association. (ISACA). 2005. IS Auditing Guideline Business Continuity Plan Review from IT Perspective. Document G32: 1-8.

Institute of Directors Southern Africa. 2009. King Code of Governance for South Africa. Johannesburg.

Lengyel, R. 2006. Testing Methodology for Business Continuity Plan Testing. Brains for Business, May: 1-4.

Marx, B. 2008. An analysis of the development, status and functioning of audit committees at large listed companies in South Africa. Thesis submitted in fulfillment of the requirements for the degree doctor commerce in auditing in the faculty of economic and financial sciences. University of Johannesburg. September.

Miller, J. & Wenham, MA. 1991. Planning to recover from the loss of computer facilities: Trends in South Africa over the last five years. South Africa Journal of Accounting Research , 5(2): 31-50.

Muthukrishnan, R. 2005. The Auditor's Role in Reviewing Business Continuity Planning. Information Systems Control Journal, Volume 4. Available from: <http://www.isaca.org/Journal/Post-Issues/2005/Volume-4>. (Accessed on 2 November 2009).

PricewaterhouseCoopers. 2009. King's counsel Understanding and unlocking the benefits of sound corporate governance. Executive guide to King III. PricewaterhouseCoopers. South Africa.

QFINANCE. 2010. Definition of big four. Available from:

<http://www.qfinance.com/dictionary/big-four>. (Accessed on 1 September 2010).

- Rash, W. 2008. 10 Things you should know about business continuity. eWeek, 7 January: 30.
- Reuvid, J. 2005. Managing business risk: a practical guide to protecting your business. 2nd edition. London: Sterling, Va. Kogan Page. ISBN 074944288X.
- Ross, SJ. 2008. IS Security Matters: Managing Information Crises. Information Systems Control Journal, Volume 4: 1-2.
- Sarrel, MD. 2007. Your Disaster Recovery Plan. PC Journal, January: 152.
- Sayana, SA. 2005. Auditing Business Continuity. Information Systems Control Journal, Volume 1. Available from: <http://www.isaca.org/Journal/Post-Issues/2005/Volume-1>. (Accessed on 2 November 2009).
- Schwerdtfeger, M. 2010. The economic impact of Iceland's volcanic eruption. TD Economics, 20 April: 1-2.
- Snow, C. 2008. Can't stop, won't stop Disarm malicious hackers and storms with a recovery plan. Government technology, September: 26.
- The Free dictionary. 2010. Big Four. Available from: <http://financial-dictionary.thefreedictionary.com/Big+Four>. (Accessed on 1 September 2010).
- Toigo, W. 2003. Disaster recovery planning: preparing for the unthinkable. 3rd edition. Upper Saddle River, NJ. Prentice Hall PTR. ISBN 0130462829.
- Tseng, N. 2010. BP after the spill: Bankrupt, bought, or business as usual? CNNMoney, 7 June. Available from: http://money.cnn.com/2010/06/04/news/companies/gulf_coast_BP_bankruptcy_odds (Accessed on 14 June 2010).
- Wagner, KL. 2007. Technical Storm. JPM, May/June: 41-44.
- Wallace, M. & Webber, L. 2004. The disaster recovery handbook: a step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets. New York. American Management Association. ISBN 0814472400.
- Wessels, PL. 2006. The South African business environment in which accountants function and the role of information technology in that environment. Meditari Accountancy Research, 14(2): 131-149.
- Wikipedia. 2010. Available from: <http://en.wikipedia.org/wiki>. (Accessed on 16 November 2009).
- Wylder, J. 2004. Strategic information security. Boca Raton, Fla. Auerbach

Publications. ISBN 0849320410.

Young, K. 2010. Continuity in a Virtual World. Available from: http://www.isaca.org/Content/ContentGroups/InfoBytes/20001/Continuity_in_a_Virtual (Accessed on 31 March 2010).

Zawada, B. 2009. Business Continuity Plan Testing: considerations and Best Practices. Available from: http://www.isaca.org/Content/ContentGroups/InfoBytes/20032/Business_Co ntinuity_Plan (Accessed on 3 November 2009).