A CYCLIC APPROACH TO BUSINESS CONTINUITY PLANNING

JACQUES BOTHA AND ROSSOUW VON SOLMS
Port Elizabeth Technikon, s9600426@petech.ac.za and rossouw@petech.ac.za

Key words: Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), Contingency Planning (CP)

Abstract: In a world where continuous operations are essential for business survival, action must be taken to ensure information and the business processes that use the information are continuously available. This usually involves the selection and implementation of a suitable Business Continuity Planning (BCP) methodology. Implementing a methodology is however not always a simple task. This especially holds true for small to medium sized organizations. Methodologies do not always specify how they are to be implemented. An implementation method that could be applied to virtually any BCP methodology would therefore be a welcome tool for organizations.

1. INTRODUCTION

The Information Technology (IT) industry has progressed considerably over the years, so much so that it now forms a vital component for conducting business (von Solms, 1999). The majority of organisations cannot do without their computer systems in this day and age. As these systems evolve, they also need to be protected against today's considerable amount of threats to the information they process, transmit and store (Halliday, Badendorst & von Solms, 1996). An IT failure or disaster could therefore have serious consequences for an organisation (IBM Global Services, 2000).

When the word disaster is mentioned events like earthquakes, fires and floods come to mind. However, system malfunctions and computer viruses can be regarded as disasters as well and are after all more common occurrences (Hawkins, Yen & Chou, 2000). Business Continuity Planning (BCP) involves developing a collection of procedures for the various

business units that will ensure the continuance of critical business processes while the data centre is recovering from the disaster (Wilson, 2000).

For organisations that fall into the category of small or medium, the development of a business continuity plan could prove difficult. Literature aimed at the development of a business continuity plan seldom concentrates on smaller organisations (Weems, 1999). Furthermore, through the study of various methodologies it is clear that the majority of literature seldom describes how these methodologies should be implemented.

The rest of this paper will therefore not only discuss a complete seven phase BCP methodology, but will also discuss an implementation method for this BCP methodology. The aforementioned implementation method will simplify the BCP process for organisations and will be applicable to any continuity planning methodology.

2. INFORMATION SECURITY AND BUSINESS CONTINUITY PLANNING

Information possessed by organisations is no longer only used by employees, but by customers and partners as well. These users expect continuous availability of and instantaneous access to organisational information (McAnally, DiMartini, Hakun, Lindman & Parker, 2000). Protecting their information is essential to ensure that the business has a competitive edge and maintains cash flow and commercial image (BS7799-1, 1999, p.1). In order to ensure that an organisation maintains its competitive edge, the information must be kept confidential, accurate and continuously available.

Although ensuring confidentiality and integrity is important, the availability component of information security is of greater importance with respect to BCP. Organisations nowadays are competing on a global scale and require high availability levels of information technology resources and services (Glorioso & Desautels, 1999). To completely define BCP one has to consider two aspects. Firstly, it should be ensured that an organisation could continue business as usual, or on an acceptable level in the wake of disaster. Secondly, IT should be restored to a state similar to that preceding the disaster (Glenn, 2002). To better understand these two components of BCP, the concepts Contingency Planning (CP) and Disaster Recovery Planning (DRP) have to be considered.

The aim of CP is to make provision for continuing business processes in a disaster situation while recovery is taking place (Glenn, 2002). It can be defined as the process of examining an organisation’s critical functions,

identifying the possible disaster scenarios and developing procedures to address these concerns (Rubin, 1999, p. 73). DRP was originally intended for operations established to minimise data centre downtime. Today DRP is seen as the active component of BCP and focuses mainly on the recovery of the IT department and all related functions (Hassim, 2000).

Keeping the above definitions in mind, BCP can be defined as a complete process of developing measures and procedures to ensure an organisation's disaster preparedness. This includes ensuring that the organisation would be able to respond effectively and efficiently to a disaster and that their critical business processes can continue as usual. (Business Contingency Preparedness, 2000). Although authors differ on the precise and clear distinction between the three processes, the inter-relationship of these processes, as defined in this paper, is depicted in figure 1. The smaller circles labelled A to I represent various business processes. These processes are all dependant on services and infrastructure provided by the IT Department, depicted by the innermost circle in the figure. Some of these processes are also dependant on others, as depicted by adjacent circles. The outermost circle represents a combination of the disaster recovery plan for the IT department and the contingency plans for these various business processes:

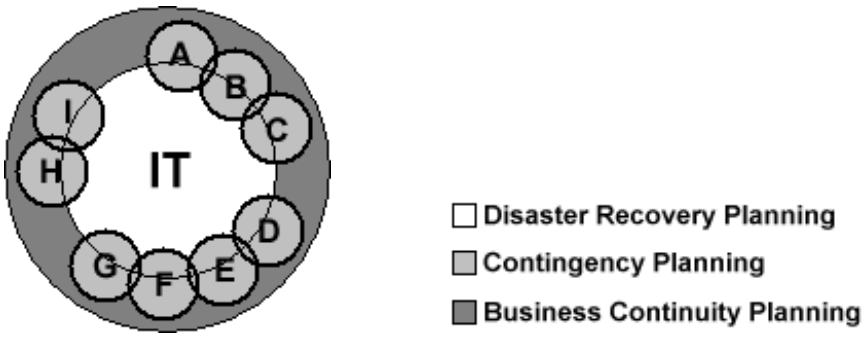

Figure 1: BCP, CP and DRP relationship

3. AN ASSESSMENT OF CURRENT BUSINESS CONTINUITY PLANNING METHODOLOGIES

In the majority of organisations the adoption of some continuity planning standards or a methodology is essential to ensure that the developed continuity plans are consistent and comprehensive. A traditional methodology would ensure that the plans for the various business functions are coordinated effectively (Heng, 1996). However, an abundance of methodologies are available today and they are all different to some extent.

This section will therefore focus on the characteristics and phases common to the majority of methodologies reviewed.

The majority of methodologies neglect to include a project planning step or phase. Such a phase is essential to ensure that the BCP project is initiated in the correct manner (Heng, 1996). Furthermore, a variety of methodologies tend to combine the processes of identifying recovery strategies and implementing them in a single phase. These two activities are both very important and to emphasise this they should preferably not be combined. A third noticeable characteristic is the lack of a testing segment in some of the methodologies. Without testing it is not possible to identify the flaws in the business continuity plan prior to use (BS7799-1, 1999). Employees would also not get a chance to exercise their portion of the plan beforehand (Morwood, 1998). A final phase that is ommitted from a a number of methodologies is a maintenance phase Once developed, the continuity plan needs to be regularly maintained. Without the presence of such a phase it cannot be ensured that organisational changes will be reflected in the plan as time passes (Devargas, 1999).

Another problem that became evident whilst studying various BCP methodologies is the lack of implementation information for these methodologies. Furthermore, even though some methodologies included a maintenance phase, these maintenance phases did not specify how to ensure that a plan is continually kept up to date and completely dynamic. Finally, while some methodologies incorporated both testing and training phases, they unfortunately did not specify how to ensure that employees are allways ready and aware of their BCP responsibilities. The next section will discuss a BCP methodology that solves some of the problems identified above.

4. A SEVEN-PHASED BUSINESS CONTINUITY PLANNING METHODOLOGY

As the requirements and characteristics of an effective methodology have been determined, a seven-phase methodology that will be used to explain the cyclic approach to methodology implementation will shortly be discussed in this section.

- **The project planning (PP) phase**: This phase incorporates all those activities required to ensure that the BCP project is properly planned. These activities include securing management support, high-level BCP education, holding a BCP orientation meeting and determining the project prospects.

- **The Business Impact Analysis (BIA) phase**: During the BIA phase critical business processes are identified and then analyzed. Once the analysis is complete, the impact that various disasters may have on business should become clear (Gordon, 2000).

- **The business continuity strategies (BCS) phase:** This phase entails the identification of various strategies that focus on ensuring business continuity and recovery. It requires the review of the various identified disaster scenarios to develop methods to deal with these situations (Wilson, 2000).

- **The continuity strategies implementation (CSI) phase**: For each of the strategies defined in the business continuity strategies phase, detailed functional plans must be developed with which to respond to the various scenarios.

- **The continuity training (CTR) phase**: Business continuity training must form part of the organization's training framework and should be allocated part of the training budget. The training should be carried out as soon as the plan is complete as well as when it undergoes significant changes (Morwood, 1998).

- **The continuity testing (CTE) phase**: Testing is used to determine whether all the individual contingency plans are adequately written to ensure continuity of business processes and the recovery of the data centre. Furthermore, testing will help to determine whether the plans can be implemented timeously (United States General Accounting Office, 1998).

- **The continuity plan maintenance (CPM) phase**: It is imperative that a business continuity plan is reviewed regularly and updated if required. This is done to ensure that the plan stays effective and up to date (BS7799-1, 1999)

As a detailed methodology has been outlined and described, the next logical step would be implementing it. Methodology implementation methods are however not often included as part of the methodology package. For this reason, the cyclic approach to methodology implementation was developed to address this problem.

5. A CYCLIC APPROACH TO METHODOLOGY IMPLEMENTATION

As have been mentioned earlier, three problems concerning methodologies were identified. They are, the lack of implementation methods for BCP methodologies, the lack of dynamic plan maintenance procedures, and the lack of continuous BCP education and involvement for employees. The rest of this paper will however only concentrate on addressing the problem of methodology implementation. This will be done through a thorough discussion of the cyclic approach.

The concept of a cyclic approach will be introduced by means of an example. The idea behind this approach could be compared to building an outer city wall as have been done in medieval times. Building such a wall would obviously not be a simple task. If, for example, it was decided that the wall should be twenty feet high, building a twenty foot section along one part of the city at a time would be impractical and would offer no protection until the whole wall has been completed. However, if the wall were to be built in phases, it would provide much better protection.

During the first phase, the wall could be built five feet high around the city. This would, for example, serve to keep out small predators threatening the livestock. The next phase would involve continuing the building process until the wall is ten feet high. At this height, the wall would succeed in keeping out the small predators as well as protecting against threats the five-foot wall did not cater for. Further improvements would include raising the wall to a height of fifteen feet and finally twenty feet. The twenty-foot wall will keep out the majority, if not all, of the anticipated threats. Each phase therefore builds on the previous by adding functionality to that which already existed.

The merits of such a phased approach are obvious. If the project is relatively large, but the workforce and funding are limited, it is advantageous to complete the project in various steps. This will ensure that no single part is neglected due to time, funding or workforce related constraints. An identical approach could be used towards the proposed BCP methodology implementation. It aims at dividing a methodology into four separate sections. Each section, or cycle as it is called in this approach, will have a different disaster recovery/business continuity related goal. It can be applied to any BCP related methodology.

To illustrate the workings of the cyclic approach, the seven-phase BCP methodology discussed in the previous section will be used as a sample

methodology. The following sub sections will discuss how this methodology has been split up to accommodate the cyclic approach, which is depicted in figure 2. The four cycles, in order, are the backup cycle, disaster recovery cycle, contingency planning cycle and business continuity planning cycle.

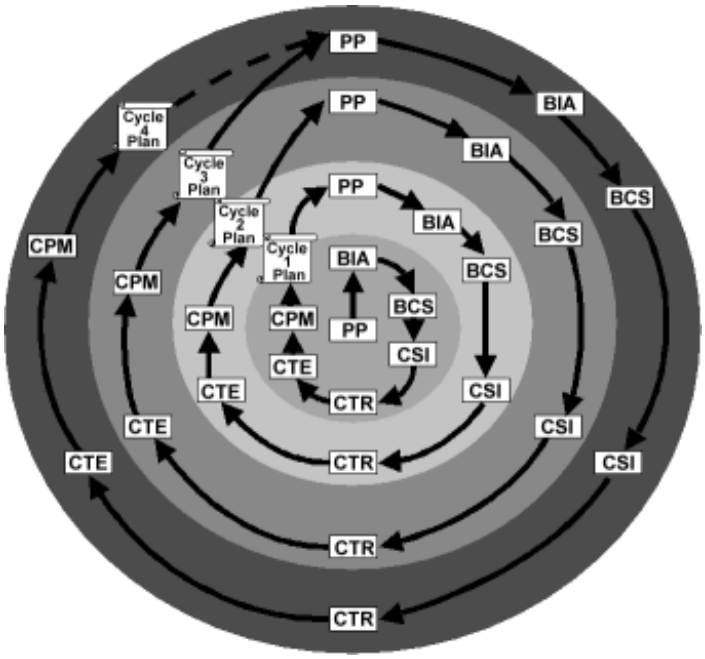

Figure 2: A cyclic approach to BCP

The backup cycle: If an organization has no access to their data after a disaster, it is virtually impossible to recover. Having an effective backup plan in place lays the foundation for further recovery efforts (Koski, K, 2001). For this reason the backup cycle has been chosen to initiate the implementation a BCP methodology. Although ensuring data backup and availability is the main purpose of this cycle, activities belonging to other methodology phases also need to be included. As this is the first cycle, it is essential that all project planning activities are carried out. Following the project planning is the performance of all BIA activities. As the organizational data is mostly identified during the BIA phase, all of the analysis activities need to be performed during this first cycle. Once the data is listed, it should be ensured that it is safe and out of harms way. This is achieved through regular backup and offsite storage of data.

Identification of the required teams to perform all backup cycle activities will be done during the strategies implementation phase. All that is left is training, testing and maintenance for this cycle. Training is fully carried out

and will include both introductory and detailed awareness training. The topic for training should however only concentrate on backup cycle activities.

Cycle testing should only include procedures to verify the efficiency of the backup plans. This will include attempting to determine whether all necessary data is backed up and whether it can be easily retrieved and restored. After testing, plan maintenance should commence. Maintenance should be carried out in full irrespective of whether the continuity plan is merely a backup plan or a fully functional business continuity plan.

The disaster recovery cycle: The main objective of this cycle is ensuring that IT can recover following a disaster. As for the first cycle, project planning activities should once again be included as part of this cycle. It is imperative that management commitment is obtained before the second cycle commences. Employees and plan participants must furthermore be introduced to disaster recovery cycle concepts and schedules and milestones must be identified for the rest of the cycle. Having completed the project planning for the second cycle, it is time for the BIA again. All processes and supporting resources should already be identified and prioritized at this point. This eliminates the need for a complete BIA. A brief review should therefore be sufficient to identify any changes in existing processes or the addition of new processes.

During the continuity strategies phase one usually identifies various recovery alternatives by assessing the recovery timeframes for the most critical business processes. This, along with the emergency response procedures and the recovery procedures written during the strategy implementation phase, must be completed. Furthermore, the teams responsible for the recovery efforts must be identified. To bring this cycle to a close, training testing and maintenance has to take place.

The contingency planning cycle: The contingency planning cycle aims at ensuring the continuity of all critical business processes while IT is recovering. As have been the case in preceding cycles, planning is an essential activity that includes steps identical to the disaster recovery cycle. Management must support all decisions and a meeting to discuss this cycle with project participants must take place. Also, a BIA review should once again prove sufficient for this cycle. The difference between this cycle and the preceding one comes into play during the continuity strategies and strategy implementation phases. The user holding strategies, part of the continuity strategies phase, directly supports business continuity and is therefore included in this cycle.

Strategy implementation phase steps, such as process continuity procedures and team identification, will also form part of this cycle. Training, once again, will involve informing employees about business process continuity and other issues regarding the contingency planning cycle. Following the training, the testing phase as in the previous cycles, will concentrate not only assessing the effectiveness of plans for this cycle, but also those developed during the preceding cycles. Maintenance should be completed soon after testing to ensure that the entire plan stays up to date.

The continuity planning cycle: At this stage of the BCP project, the business continuity plan could be said to be nearing completion. This cycle will concentrate on business continuity as a whole, i.e. on both recovery and business process continuation. It mainly contains the various steps that could not be directly attributed to just continuity or recovery, but rather apply to all these previously established goals or related goals. The project planning section of this cycle is once again identical to the previous two cycles. As for preceding cycles, management is required to commit to decisions subject to the current cycle. A final orientation meeting is required to discuss cycle prospects and schedules.

A review of business processes is required to ensure information is correct and to record any new processes and related information added since the review done in the previous cycle. Progressing to the continuity strategies phase, activities that need to be completed are the insurance cover review, public relations preparation and emergency resources identification. Finally, before training, testing and maintenance commences, the remaining group of teams responsible for activities during this cycle need to be identified. Training, testing and maintenance is conducted in the same fashion as before.

6. CONCLUSION

Information and IT have become a vital part of conducting business in our technologically advanced world. Undeniably a business can practically not do without these two components for extended periods of time. Employees, shareholders and customers have come to expect that information should be available around the clock. Even a minor disaster or disruption could cause irreversible damage to an organization and it’s public image.

To ensure that an organization could recover after a disaster, a complete business continuity plan should be in place. A complete BCP methodology should preferably be followed to ensure that such a plan is effective in protecting an organization.

A large number of methodologies are available, but it is rarely specified how each should be implemented. Smaller companies in specific have to implement a methodology differently than larger organizations. For this reason a method simplifying the implementation process was developed. As elaborated upon here above, this method or approach involved methodology execution in four cycles. Each cycle concentrated on a specific BCP goal and each goal was completed and tested before the next was attempted.

Further study will be aimed the identification of methods to ensure that a business continuity plan is continually and dynamically maintained. This will guarantee that the plan stays up to date and thereby effectively cater for disasters at any time. This study will also concentrate on activities that will ensure that human involvement in BCP is maximized and by so doing increase employees' BCP awareness and readiness.

References

BS7799-1. (1999). Information security management – Part 1: Code of practice for information security management. London: British Standards Institution

Business Contingency Preparedness (2000). Glossary of Contingency Terms. [Online]Available: http://www.businesscontingency.com/glossary/html/glossary.htm (2002, May 11)

Devargas, M. (1999). Survival is Not Compulsory: An Introduction to Business Continuity Planning. Computers & Security, 18 (1), 35-46

Glenn, J. (2002). What Is Business Continuity Planning? How Does It Differ From Disaster Recovery Planning? Disaster Recovery Journal [online]. [Cited May 11, 2002] Available from Internet URL http://www.drj.com/articles/win02/1501-14p.html

Glorioso, R. M. & Desautels, R. E. (1999). Disaster Recovery or Disaster Tolerance: The choice is yours. Disaster Recovery Journal [online]. [Cited November 21, 2000] Available from Internet URL http://www.drj.com/articles/spr99/glor.htm

Gordon, C. (2000). How to Cost Justify a Business Continuation Plan to Management. Disaster Recovery Journal [online]. [Cited March 7, 2002] Available from Internet URL http://www.drj.com/articles/spring00/1302-05.html

Halliday, S., Badenhorst, K. & von Solms, R. (1996). A business approach to effective information technology risk analysis and management. Information Management and Computer Security, 4(1), pp. 19-31

Hassim, M. (2000). To plan or not to plan? [Online]. Available: http://www.accountancysa.org.za/archives/1999nov/features/plan.htm [2002, May 11].

Hawkins, S. M., Yen, D. C. & Chou, D. C. (2000). Disaster recovery planning: a strategy for data security. Information Management and Computer Security, 8(5), pp. 222-229

Heng, G. M. (1996). Developing a suitable business continuity planning methodology. Information Management & Computer Security, 4 (2), 11-13

IBM Global Services. (2000). Managing information technology in a new age [online]. [Cited October 18, 2000] Available from Internet URL http://www.ibm.com/services/whitepapers/gsw1178f.html

Koski, K. (2001). Backup and Offsite Vaulting [Online]. Available: http://w3.arcusds.com/Backup%20White%20Paper.pdf [2000, November 21]

McAnally, P., DiMartini, B., Hakun, J., Lindman, G. & Parker, R. (2000). Real time data availability solutions: Does your business have a need for speed? Disaster Resource Guide [Online]. Available from Internet URL http://www.disaster-resource.com/cgi-bin/article_search.cgi?id='22'

Morwood, G. (1998). Business continuity: awareness and training programmes.Information Management & Computer Security, 6 (1), 28-32

Rubin, H. (1999). Bracing for Zero Day. IT Pro. May/June, pp.73-76

United States General Accounting Office. (1998). Year 2000 Computing Crisis: Business Continuity and Contingency Planning [Online]. Available: http://www.gao.gov/special.pubs/ai10119.pdf [2000, October 23].

von Solms, R (1999). Information security management: why standards are important. Information Management and Computer Security, 7(1), pp. 50-57

Weems, T. L. (1999) Business Continuity Planning-for the rest of us. Disaster Recovery Journal [online]. [Cited October 23, 2000] Available from Internet URL http://www.drj.com/articles/fall99/weem.htm

Wilson, B. (2000). Business Continuity Planning: A Necessity In The New E-Commerce Era. Disaster Recovery Journal [online]. [Cited October 21, 2000] Available from Internet URL http://www.drj.com/articles/fal00/1304-02.htm