Disaster and contingency planning

Business, Accounting

Name: Course: Instructor: Date: Disaster and Contingency Planning Various disasters can negatively affect different parts of an organization. Examples of such disasters that can affect a business differently include calamities such as earthquakes, fires, volcanic eruptions, tornadoes, tsunamis, windstorms, terrorism, equipment malfunction and war. These disasters can occur at anytime which necessitates the need for disaster preparedness and contingency measures that will be effective against the effects of spontaneous disasters.

Disasters usually cause considerable damage to any organization. For instance, buildings, equipment and computer systems can be damaged resulting from disasters. Moreover, there is the possibility of grievous harm and death to people. In order to mitigate against disaster and its respective effects, it is important to develop a disaster recovery plan, which is advantageous in the avoidance and overcoming of disasters. Assessment Two Overview Melbourne Polytechnic of Business, Technology and Design utilize a complicated technical infrastructure to support the school’s objectives by supporting academic programs, student services and administrative operations.

Operations across the college are considerably dependent on the infrastructure and hence strategies must be structured that provide prevention against disasters, provide contingencies, and recovery if the disasters affect the systems in the college. The prevention strategies are described in order to lessen risk while the recovery options are described by outlining the structures and methods that will be followed in the event of a recovery scenario. 1.

Technology Infrastructure The college utilizes a technology infrastructure with which the campus is highly dependent on in order to carry out various operations. It is therefore important to formulate prevention strategies and disaster recovery options, which are essential and must be properly developed and recognized across the college. The prevention strategies identified are suitable for the reduction of risk while the recovery strategies are designed to describe the methods and structures that will be adhered to in the case of a recovery scenario. The college is obligated to the effort of the augmentation of dependability on technology infrastructure and the reduction of failure of components. There exist established processes for the backup of data and the storage of chief resources and information off site to make way for the reconstruction of systems in case of catastrophic events.

Moreover, critical business procedures have been identified which will require the necessity of continuum at the time of an extended system outage. The recovery strategies will focus on the ability of the institution to recover from catastrophic damage to a single or more of the institution’s major network and server hub locations – the Computer Center, Washington Hall and the Wayne Building Annex. The goal of the plans is to provide and facilitate recovery of every critical infrastructure service within the specified period of a disaster occurrence. Situations that incorporate fewer catastrophic losses will employ a subset of plans and recovery resources and will mostly take up less time.

2. Individual Microcomputer Data and Software The availability and security of restorable backups for the personal computers at the campus are the

responsibility of the personal users. Persons should store and backup their data and information on their computers. Various software tools are available for individual computer data and information backup. The Information Services and Configuration (ISC) building in the campus will be responsible for assisting and training students in the storage and back up of data. Moreover, the ISC technicians will offer access to a Backup Server for data and information.

Additionally, the staff and the campus faculty can sustain current backup of personal data documents and files on the Backup Server. For computers utilizing the Windows software, script packages are available for the allowance single-click backup initiations for applications such as My Documents, Desktop and other commonly altered resources to the server from the PC. For users of Macintosh, there is a commercially program for backup. Virtually, all computers at the Melbourne Polytechnic are endowed with forms of high-capacity backup devices such as DVD writers or CD writers. The availability of these high capacity devices permits customers to develop an offline duplicate of the data on their backup server swiftly and competently and for backup storage in a secure offsite location. 3. Prevention Strategies Prevention strategies for the prevention of disaster and the reduction of risk require to be implemented in the college in case of any catastrophic event.

The prevention strategies are based on the common types of risks that can affect the college. Network Path Redundancy The connections between the primary network router locations in the Computer Center and the Wayne

Building Annex are created with two different paths of same capacity. The backbone flows on each path. If any of the paths is disrupted in the event of a disaster, data can still be able to be transmitted on a different path and communication will not be disrupted. Equipment Component Redundancy All servers are set up with power supplies and Redundant Array of Independent Disks (RAID) disk systems. The RAID system authors every data segment to two locations on different disks. The Control Logic then permits the system to continue processing data without the exception of hard drive malfunction and hence vouches for the simple replacement of a malfunctioning drive. Data Center Redundancy The past telecommunications paraphernalia area in the Bruce Building Annex and the Network and Server Room in the Computer Center are based across each other in the college.

Both spaces are furnished with a complete set of environmental protections for the data centers. Storage host and virtual server resources are situated in both centers. These will permit critical virtual resources to be merged to one of the bases if one is destroyed. Moreover, it permits for the resources of the Data Backup Server to be situated in a guarded space and at the same time being physically segregated from the servers involved in backing up. Power Safety The equipment in the Wayne Building Annex and the Computer Center are guarded by system generators. The generators are beneficial since a power outage lasting for a maximum of 72 hours does not affect operations. The network facilities and the switches of network interfaces in the administrative and academic departmental buildings are protected by separate Uninterruptible Power Supply (UPS) systems, which provide 60-120

minutes of power in case of a power malfunction or a considerable dilapidation of incoming power.

A Silicon UPS unit, which provides power for several hours, protects the servers that are non-critical in the data centers. Additionally, the APC Unit is responsible for sending emails to network services employees in order to alert them of power loss and restorations. In the event of a loss of power that stays for more than five hours, the ISC technicians is expected to utilize the accessible UPS time to insure that restricted shutdown processes are commenced and to observe automatic shutdown processes to ensure that they are functioning normally.

In case of a massive outage, vital processes that rely on desktop printers and computers require relocation in order to be unaffected by the power malfunction. The printers and computers are linked to surge protection power strips to inhibit damage because of occasional power surges. Laptops will go through a normal shutdown in case of a power failure. 4. Recovery Options Determination of Restoration Site The restoration site is one of the most vital stages for the recovery processes.

Usually, the restoration site is provided for the facilities recovered in case of a catastrophic event. In case of a disaster, if the central site is not available for the restoration of service, then an alternate location will be provided. The alternative sites include the Wayne Building Annex if the Computer Center is damaged, the Computer Center if the Wayne Building Annex is damaged, the ISC Building offices in the Third Floor and the space at the Center for Rural Development in the college. Moreover, the equipment that will be salvaged

from the event will be transferred by the appropriate and selected personnel to the alternative location.

Establishment of Security Control, Network and Communication Services The recovery work will be bent on the establishment of security control and basic network as well as voice communication applications. The restoration of these services and functions will aid in the restoration of basic security protocols in case of a security breach, augment communication and know the current recovery operations that are underway and the recovery and reconstruction of network services to facilitate various network services such as intranet communication and the use of internet services. Additionally, the establishment of the services will be advantageous for the provisional operations environment. Restoration of Network Connectivity The restoration of network connectivity is also a viable recovery option. This is attributed to the objective of restoring network connectivity in areas that were deemed inaccessible resulting from the implication of the disaster. The people responsible for the restoration of the network connectivity such as the recovery task team will focus on restoring the connectivity to locations that were made inaccessible by the catastrophe. Additionally, the recovery process in terms of network restoration will ensure that emergency orders are put across for materials required for the accomplishment of compulsory merging, testing and certification of communication and network systems.

Setting up of Provisional Work Spaces Setting up temporary workspaces is also another option for recovery. This is because of the unavailability of former workspaces in case of the destructive event. It would be appropriate

to create temporary work bases, which will assist in the continuance of essential services until the period whereby the communications infrastructure will have been reinstated throughout the college. The recovery task team provided with such a task will be accountable for the relocation of personal computers and other equipment to the provisional workspaces. Assessment Three Introduction Martin College of Business, Technology and Design is an Australian college which offers Certificate and Diploma level qualifications in the areas of Business, Marketing, Graphic Design, Management, Events, Tourism and Information Technology. Over the years, Information Technology (IT) services have become important for the performance of educational objectives of the college.

Resulting from the reliance on technology in the attainment of the college's objectives, the Information Technology Department is tasked with the mandate of formulating a disaster recovery strategy that will be efficient in the prevention of disasters and recovery of the affected assets from the disasters. A Disaster Recovery Plan (DRP) is designed to ensure the continuation of important college operations and practices in the event that a disaster happens. The plan provides effective solutions, which can be utilized in the recovery of every important process or operation in the campus within the needed period while utilizing important records that are backed up off site. A comprehensive Disaster Recovery Plan summarizes the outcomes of a comprehensive risk analysis which is usually conducted for every It service. It offers the general procedures that will be used in case of a disaster in order for the restoration of functions related to Information Technology and the provision of recommendations that will be sued for the

security of the technology infrastructure. Objectives The main objective of the Disaster Recovery Plan is to assist in ensuring that there is business continuity through the provision of the ability for successful recovery of computer services in case of a catastrophic event. The main goals of the Plan in terms of an emergency incorporate the detailing of a broad action to take in case of the event, lessening misunderstanding, inaccuracy and expense to the campus and the implementation of fast and full service recovery. The derivative objectives of the plan include the reduction of risks, provision of protection regarding the college assets and the surety of continued feasibility of the plan (Gregory, 57).

Scope The scope of the plan lies mainly on the address of the Information Technology Department in the college on system recovery due to the consideration of the systems that are important for the continuity of business in the campus. Additionally, the plan does not intend on providing specific recovery instructions for each system given the uncertain effect of a given event or disaster. Alternately, the plan will summarize a broad recovery process that will lead to the development of specific responses to an event or a disaster. The IT Department is expected to recover network systems in the data centers, Wayne Building Annex and the Computer Center in the college. The network in the campus comprises: Critical business applications such as Oracle Financial and Human Resources Management Systems and PeopleSoft Campus Solutions (student administration system) E-mail File servers that support every business operation Gateway to other host sites and applications E-commerce processing Wireless networks Campus Phone System The personnel responsible for the development and sustenance of

the Plan are the Campus Network Coordinating Committee. Explicit responsibility for the guaranteeing that the Plan is sustained and tested is vested in the Information Technology Department under the Associate Vice President of the IT Department. Business Impact Analysis The Business Impact Analysis is finished in order to determine the Critical Time Frame in which the functionality and aptitudes of the application system require to be available after the interruption of a service in order to lessen the operational loss associated with control and the latent loss associated with revenue.

Moreover, the Business Impact Analysis helps in the identification of unconventional manual procedures that may be utilized in case of service interruption. Hence, the objectives of the analysis comprise the education of the sure on the need for the Plan, the identification of Critical Time Frames for every application, the identification of manual procedures for minimal impact associated with interruption in service and the identification of the least Critical Time Frame for each. Determination of Business Impact Analysis The purpose of the Business Impact Analysis is to verify the maximum period that each functioning department can be without the system’s functionality in the event that the department does not incur material or operational interference due to a disaster. The period will be denoted as the Critical Time Frame. The Critical Time Frame is defined as the gone period between the interruption points to the point at which the system is required to become functional. Recovery procedures within the Plan are placed around the most critical application, which possesses the least Critical Time Frame to the application that holds the longest Critical Time Frame.

The application or system with the least Critical Time Frame is the Server Room in the ISC Building.

Since each application possesses a variable period, the Plan bears the period on the application with the least period. Thus, the Plan possesses a Critical Time Frame of two days as a whole. In order to determine the Critical Time Frame allowable, the following departments were interviewed: The IT Department, Admission, Counseling, Human Resources, Accounting and Finance, Health Center and the Library departments. The outcome from the interview with the functioning departments indicates the effect of the power outage or disruption while assuming a worst-case scenario.

The effect of each application by the operational department indicates the departments' dependency on computer support and shows the Critical Time Frame that the department can be without the functionality of the applications. Application System Impact Statements and the outcome of the Business Impact Analysis are used in the classification of each application in the essential, delayed or suspended categories. If an application is deemed essential, then it means that its loss would influence the ability of the college to continue being solvent irrespective of financial loss or convey a grave loss of functional control. On the other hand, an application is deemed delayed whereby the function can withhold without the support of computer processing for a period while the application deemed suspended indicates the suspension or discontinuance of computer support for various business functions (Rothstein, 67-98).

Application/Department1-2 Days3-5 Days6-10 Days11-14 DaysCategoryOracle HRMDMDCT EssentialOracle AccountingMNMDMNMNSuspendedHealth Ctr/ClinixMNMDMNMNSuspendedServer RoomCTMDMNMNEssentialCounselingMNMNMNMNSuspendedAdmissionMDCT EssentialLibraryMDCT EssentialLegend: MN= Minimum Impact, MD= Moderate Impact, CT= Critical Impact Recovery Team Responsibilities The Recovery Management is answerable for the management of recovery while ensuring that restoration takes place within the planned Critical Time Frame and aids in the solution of problems that require action from the management. The Recovery Management team comprises the Senior Recovery Manager and the Recovery Manager. The team commences its recovery duties if alerted by the Senior Recovery Manager in the occurrence of a disaster.

All other recovery teams answer to the Recovery Management Team directly. The Recovery Management Team is mandated with specific actions in the pre-disaster period and the post-disaster period. In the pre-disaster period, the Senior Recovery Manager is responsible for the approval of the end Disaster Recovery Plan.

He or she is also responsible for ensuring that the Disaster Recovery Plan is maintained. The Senior Recovery Manager is also responsible for ensuring that the Disaster Recovery Plan is conducted and is responsible for the authorization of testing of the Disaster Recovery Plan. After the disaster, the Senior Recovery Manager is responsible for the declaration of the occurrence

of the disaster and hence the activation of the Disaster Recovery Plan. He or she is also involved in the determination of the Plan strategy that is supposed to be implemented. The Senior Recovery Manager is also responsible for determining the alternate members of the recovery team and other support members in the recovery process. The Senior Recovery Manager manages and monitors the overall recovery process. He or she also is also in charge of advising the management of the institution or department on the status of the efforts of disaster recovery. The Senior Recovery Manager is also responsible for the coordination of press and media releases within the Public Information Office.

Moreover, the Senior Recovery Manger is responsible for the constitution and formation of damage assessment and salvage team who will be responsible for the assessment of the damage caused by the disaster and the process of recovery and restoration after the disaster (Hiatt, 89). The Recovery Manager also possesses the mandate to act in the pre-disaster and post-disaster periods in the institution. In the pre-disaster, the Recovery Manager is responsible for the maintenance and updating of the Plan with respect to the scheduled time. The Recovery Manager is also responsible for the distribution of the Disaster Recovery Plan to the tem members who are part of the recovery team (Maiwald and Sieglein, 123-126).

The Recovery Manager is also mandated with the appointment of members of the recovery team as well as alternates to the team members if present. The Recovery Manager is also tasked with the coordination of the testing of the Disaster Recovery Plan. The Recovery Manager is also responsible for the

training and equipping of members of the Disaster Recovery Team regarding the Disaster Recovery Plan (Maiwald, 134-137). At the time of post-disaster, the Recovery Manager is mandated to assist in the assessment of the extent of damage and destruction to the facilities in the college. The Recovery Manager is also tasked with the provision of data processing services to the organization after the event. The Recovery Manager is also required to provide the initial notification of declaration regarding the disaster to the members of the recovery team as well as the alternates. The Recovery Manager is also responsible for the coordination of every recovery team in order to ensure clear specification of work roles in the recovery processes and job criteria in the process of restoration.

Moreover, the Recovery Manager is supposed to notify all teams of the systems, application and network software to ask for off-site backup systems, documentation, manuals and equipment. The Senior Recovery Manager is supposed o report to the Senior Recovery Manager on the recovery effort status as well as every process and event in the recovery event. Works Cited Gregory, Peter H. It Disaster Recovery Planning for Dummies. Hoboken: Wiley, 2008.

Print. Hiatt, Charlotte J. A Primer for Disaster Recovery Planning in an It Environment. Hershey: Idea Group Pub, 2000. Print. Maiwald, Eric, and William Sieglein. Security Planning & Disaster Recovery.

New York: McGraw-Hill/Osborne, 2002. Print. Rothstein, Philip J. Disaster Recovery Testing: Exercising Your Contingency Plan. Brookfield: Rothstein Associates, 2007. Print.