The Procedure for Incorporating a Disaster Recovery Scheme in a Corporate Setting

Disaster Recovery is a procedural act of preparing an organization for any disruptions or activities that might cause an alteration or shift from the daily routine and achievements. Most daily operations are faced with the risk of engaging in calamities, more so in Information Technology fields or such related fields (Luftman & Zadeh, 2011). This is a challenge that is inevitable as there exist a direct relationship between improving technological advancements and improvised threats. In order to maintain a business running and realizing unaltered profit margins, a perfect recovery plan must be implemented to counter any disasters that might be encountered.

At initial level, a perfect implementation process to be used is one that considers all prevalent situations of the current system and its augmentation to the environment. Proper processes must be followed, with a powerful study prior to implementation to ensure the system is working and is not prone to failures(Peslak, 2012). The business organization should consider implementing the system in a sort-of sub organization to determine its working environment and the output each environment is subjected to.

Testing of the system is fundamental to determining the kind of hardship endurance the project can withstand, and also providing for vulnerability footing. Each testing of the system must be handled with utmost care to evade instances of future calamities.

Another aspect to be handled is training of the end users of the system. Each level of user is to be handled and tested on different levels to allow for different levels of management of the system(Peslak, 2012). The specific levels that are in question are DR/BC team, middle managers, department heads, and employees in the company, suppliers as well as other users who might be interested in the company's operations.

System Testing

The most significant stage of determining the success of any system is done during system testing. Basically, black box testing is used in this stage, where the system should be leased out to a third party in order to assess the functionality. This leasing is done after in-house testing by issuing random commands expected to be performed by the system in the larger working environment of the company (Luftman & Zadeh, 2011). Extreme values should be used to determine output nature and behavior, as well as the amount of data capacity that can be

handled within a given scope of duration. Technically, any system must meet the criteria of output required by a particular business premise or organization, and in any sense, the targeted group of clients (Peslak, 2012). In any case of breakdown or calamity such as fire accidents, the system must be able to withstand normal calamities. The main aspect of a perfectly working system entails ability to auto save any worked documents and back them up in a secure server somewhere, preferably a cloud server.

Testing of a system should be systematic and non-biased to determine the kind of errors that might be in existence within the system and the various codes that might have been used. In other instances, a program that could have been used might be inapplicable to the situation of the company and its business needs. Daily events must be captured and updated with the system, ensuring that it meets all the required needs (Peng et al., 2011). Additionally, system testing ensures consistency among the various modules that have been worked on by different teams. An accurate testing reduces incidences of data loss in future in incidences of accidents such as malware attacks and accidental erasure.

Training

The next step before unleashing the system for full implementation is training. All the targeted group of users must be made aware of the new changes and the way and manner in which they shall be able to work with the system. Different levels of access are achieved through the use of different layers of users within the framework to ensure security of the system as well. The work of Disaster Recovery and Business Continuity Team is to ensure that the system is constantly updated, and as such, they must be trained to handle specific errors that will be encountered during the course of operation (Peslak, 2012). Such work for the DR/CB team shall entail work on the mechanisms of ensuring that correct tools of data management that ensure auto backup are in place. It is irrefutable to argue that training is utterly essential in any business organization.

Software Transformation and training

Transformation from traditional-based software or system to a totally new system translates to a kind of attitude creation and ignorance. Without proper attention to accurate training skills, any organization might be incapacitated to handle any emergent issues in future. Middle managers play a major role in maintaining the functionality of a business organization. Any new changes in the organization affect them directly, as they are answerable to all functional units of the organization in general (Peng et al., 2011). Delegation of responsibilities is key to ensuring continuity and smooth running of an organization.

As such, their training on the system should entail details of assigning users to the system, and

managing owner accounts to the various departments (Peng et al., 2011). This shall ensure accurate tracking of all records and responsibility to each transaction of a business organization, and be able to crack down all defaulters in case of any calamity or downfall. The log of events is also essential in managing security threats and risks from the corporate outer networks.

It is necessary to conduct a thorough training to ensure all users are familiar with the kind of product they will be using and outline the specific reasons of necessity to using that kind of system.Department heads function as major building blocks in running the organization since they are in close contact with the employees(Snedaker, 2013). Therefore, in terms of training, a management of the employees is due responsibility of each departmental head to maintain an accurate record of all services offered(Peng et al., 2011). They should as well be able to manage any changes within the organization, besides handling suppliers' goods and other responses from the outer world.

Implementation

To begin with, the implementation process takes on several measures. All the system requirements must have been met prior to the implementation process. In fact, this stage comes after successful testing and debugging, to remove all errors and dysfunctional units of the block of codes in use within the system. A careful study must have been conducted to determine the working environment of the full system, and additionally include a clearly defined procedure for maintaining and upgrading the system in later stages while the system is already in use (Whitman, Mattord & Green, 2013). Training must have been successfully completed and after all considerations made, implementation strategies come in.

Implementation considers disasters to be encountered during working of the system and business organization. This is a mode of eradicating possible flaws within the system and ensuring that all units agree and work efficiently. Prior to an occurrence of any calamity, a business organization should have in place a system of backing up its data in a secure storage cloud server, and ensure all administrators have access to auto recovery mechanisms from the storage cloud server (Whitman, Mattord & Green, 2013). To ensure such unfortunate incidences are prevented, preventive measures are to be used. These could range from protecting against hackers, to using heavy metallic ware to protect against theft and malice of the organization's information and system ware. Specific surveillance cameras could be used to monitor all activities by people within and around the premises. Additionally, antispyware materials are to be used.

System Updates

Despite any challenges that might be encountered, a recovery plan entails accurate methods of

maintaining an up to date system that ensures productivity round the clock. Events of system failure should not be a reason for under-productivity. In essence, this should be a time of realizing continuous supply and growth to consumers (Snedaker, 2013). Such can be achieved by having an objective that runs the business. Recovery modes are to be used during such times, and these could include a storage based on the cloud server which is then retrieved. Customers and suppliers with the knowledge of the new system should be able to access the resources online from different work stations(Whitman, Mattord & Green, 2013). A VPN of networks set to enable employees work from other stations in case of an event within the premises is an essential part of the integration process to be used within the business corporation. Events of hacking the IT system should at no time lower productivity. Secure encryption modes could be used to channel information round the business platform enabling continuous productivity.

The response team should be a vibrant team that must be able to cross-examine the system of the business on daily basis to ensure that flaws are identified and proper debugging measures are taken (Snedaker, 2013). Team is a composition of analysts and a programmer who make sure that all departments have a report of the functioning of persons under their jurisdiction. Moreover, the response team manages the situation in all times of calamities and accidents, responding efficiently to the cases and providing appropriate solutions to ensure the business does not close down(Whitman, Mattord & Green, 2013). Network administrators are a part of this Emergency response team. The team provides all-time response to system attacks such as malware attacks and hacking. Prompt actions to combat these events are a feature of the ERT which completes security actions and restoration of the particular system disaster.

Post-events actions to be taken are quite critical to the path the business is going to take. Cases of phobia to particular incidences are always notable under all institutions (Snedaker, 2013). These entail a listing of possible control actions that need to be undertaken to avert such scenarios and events.