It service continuity management

Business, Management

If the company is not ready to strike disaster the outcomes range from prolonged system downtime and also loss of revenue to the companies which may lead to going out of business completely The solution to hit such an event is a business continuity strategy. The business continuity strategy is a set of policies and procedures which are intended to react to and recover from a disaster. Glen Kunene noted that the solution to recover effectively from a disaster is to execute a plan when the disaster occurs.

Disaster recovery plan is a set of simple, effective guiding principles and procedures to be followed by all people in the organisation. The disaster recovery plan (DRP) is the main component of a business continuity strategy. Steps in disaster recovery plan: There are four steps in disaster recovery plan. Those steps are as follows: Risk analysis: The first step in the disaster recovery plan is the risk analysis. Risk analysis of computer system includes the analysing the possible risk that menace the system. Anything that can cause a system outage is a risk the risk may be man made risk or natural disasters.

Risk analysis includes the determining the most likely occurrence of disaster, rating the risk and analysing impact of risk. Estimation of budget: After analysing the risks, cost should be estimated to reduce the potential occurrence of risk and to hold back from risk. It is the process of listing all possible risks to data of organisation with its solution and estimation of cost for the solution. Disaster recovery budgets vary from company to company. The organisation will decide which risks can afford to tolerate and which risk is serious impact.

Development of plan: After estimating the cost to recover from the disaster, Data Recovery procedures (DRP) will begin to shape by business unit of the company. The DRP procedures are detailed plan or script in written form. This also includes the establishing the disaster recovery team and assignment of specific responsibilities to each member in the team to recover the risk. The plan should include the process to deal with the loss of various databases, servers, communications links, etc. and data recovery process. The scripts should also include: priority of recovery i.

e. what threat need to recover first and procedures to communicate with initial respondents. Testing: Data recovery planning (DRP) procedures need to be tested frequently after once set. If there is change in businessenvironment, there will be a change in DRP procedures also. So, there is need to reexamine the plan periodically. The changes in the budget, hardware, software in network of organisation should enter and add into the plan and also employees to be trained on recovery procedures. Recovery team members should know their roles.

Testing process includes the testing of the system which will use in recovery process regularly and to validate the work of all members in team. The one of the output from the business continuity life cycle is recovery plan. This plan is detailed instructions and procedures to recover or continue the business, operations of the systems and services. The main goal of the recovery plan is to uphold the service continuity of the business or organisation. The various disaster recovery options are: Do nothing: It is nothing but simply waiting until services will re-establish

Manual system: it is the option of adopting the manual process until the It service start again. Reciprocal arrangement: This is the option of making an arrangement or agreement with another company to share the facilities in the case of disaster. Gradual recovery: In this recovery option, organizations will not use the business processes which are supported by IT services for long period. Warm start: In this recovery option, organizations will use the facilities of technical support and system management to recover the IT services with in the period of 72 hours.

Hot start: This option provides the immediate recovery from the disaster. This provides the immediate restoration of IT services but it is expensive one to implement. This option is used for critical services that cannot be loss for even for short duration also. ITSCM: In present days, Organisations are mostly depended on IT services to support their business practices and to provide services to their customers. The dependency on IT services is increasing day by day and this also demanding that services need to be protected from comprehensive inaccessibility.

ITSCM is a critical procedure that will maintain and protect services of organisation and it also contributes to the endurance and continuance of an organisation. The organisation can’t get profits and returns on investment (ROI) unless there is an implementation of effective ITSCM. ITIL Service Continuity management is more than just Disaster Recovery Planning. IT Service Continuity Management prepares the organisation to face the worst case scenario, by giving a capability of how to recover from disaster.

It not only gives the capability of just recover from the disaster, if possible it also gives the capability to prevent the disaster occurrence in the first case itself. ITSCM investigates, develops and implements recovery options when an interruption to service reaches a pre-defined point. Defining the pre-conditions that constitute a disaster is part of the ITSCM process. Such definitions form an integral part of any Service Level Agreement relating to the provision of services.

ITSCM addresses the most costly risks that could cause a sudden and serious impact, such that they could immediately threaten the Continuity of the business. These typically include things like: • damage, loss or denial of access to key Infrastructure services •failureor non-performance of critical service providers, distributors or other third party services that interpret business continuity • corruption or loss of key information • disrupt, extortion or commercial mishandling of key business information • Deliberate illegal attack on critical information systems.

IT service continuity management (ITSCM) offers a proactive mechanism to assure that IT services can be recovered and provisioned based upon the established business continuity management timeframes. ITSCM focuses on the IT services required to support the organizations critical lines of business. For example, in a CRM system the customer data is a critical entity to be protected and recovered immediately after a disaster. Here not only the recovery of customer data but also the details about supporting IT infrastructure and services such as active directory, telecommunications, networks, service desk and the technical support are important

ITIL's approach to service continuity and disaster recovery Following are the steps to an ITIL compliant Service Continuity Plan ITIL prescribes the following five steps to the ITSCM planning process: 1. Prioritizing the businesses to be recovered by conducting a Business Impact Analysis (BIA) 2. Risk Analysis by assessing each IT Service including the assets, threats, vulnerabilities and related countermeasures that might be taken 3. Response Analysis by way of evaluating the recovery options Plan 4.

Development of the actual production of a Service Continuity Plan which contains details of detection of an event and the protocols to be followed 5. Plan Testing and Renewal to prepare an actual simulation of a crisis or disaster event and to assess the response effectiveness and the revision of the plan based on the issues arising during the simulation exercise The above process needs a thorough understanding of the impact of the crisis event on the operations of the business and the system capability to conduct business with or without IT.