Capacity management: capacity flashcard

Capacity Management: Capacity management ensures the delivery of existing and future IT infrastructure requirements of business in right time and in the efficient manner.

It involves sub-processes namely, Business Capacity Management, Service Capacity Management and Resource Capacity Management Continuity management: Continuity Management is the process is responsible for ensuring the business continuity strategy of an organisation when disaster happens. It includes business impact analysis, risk assessment, business continuity strategy. Financial Management: The financial management provides cost-effective stewardship of IT assets and resources that are used in providing IT services. Service Support: The process of Service Support of ITIL frame work is very important in creating dynamic IT system and applications and it enables organizations to provide IT services effectively. The procedure of service support provides satisfied customers to organization.

There are 6 Service Support disciplines included in ITIL frame work. Those are: Configuration Management, Incident Management, Problem Management, Change Management, Service/Help Desk and Release Management. 1. Help Desk: Help desk provides help to client request and problems. It is tracking procedure. This is responsible for any projected changes in distributing information to company which has impact on company operations and procedures.

2. Incident Management: This is responsible for restoration of services tracking incident. This is first reactive process to be taken when incident

occurs. It includes the necessary procedures to be followed to restore the services of company. 3. Problem Management: Problem Management plays a significant role in receiving and investigating data.

This mainly focuses on distinguishing the causes of service issues. This identifies the corrective work to prevent repetition of events. 4. Configuration Management: – It is the processes that reports individual infrastructure. This process closely works with the Change Management process.

5. Change Management: It is responsible to manage any change in IT framework. This process assess the risks due to changes, recognizes the dependencies and other changes which will create impact on system and applications. 6. Release Management- It concentrates on large scale changes in the IT environment.

This includes installing the latest database management system and managing extensive changes to company’s application. It manages large amount of changes in production operating environment. Disaster recovery planning: In information technology sector, the disaster recovery is an action to be taken when there is occurrence of unplanned outages. The disaster recovery plan helps to minimize the adverse effects of those unexpected outages. Disaster recovery involves the process of designing the steps to get back the running processes when they were lost during a certain period of time.

In IT industry, disasters may occur from events like hacker attacks, computer viruses, and power failures, natural disasters such as flood, fire, earth quake,

attrition and mistakes in system administration. Importance of Disaster Recovery: For any organization especially IT organization, data is a critical component to be protected by all means and in all times. The unexpected Disasters may damage the continuity of the data entry and access into the system. So, the data should be recovered immediately to continue the further business process of an organization after disasters.

An organization that can recover the data to resume the operations within a less time after a disaster can be said as having an efficiently operating system. The Disaster recovery Plan is one such tool in starting up the recovery operations to regain the lost data connectivity in an organization. ITIL framework has this component of disaster recovery plan for the purpose of business continuity management. Dana Turner notifies that disaster recovery plan is supposed to come with the following elements:• Making do with whatever is left after disaster • Buying time to: o Recover from the initial impact; o Restore basic operations; o Resume normal operations; and o Replace damaged equipment & facilities; and • Redundancy management for critical people, places and things.

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 business environment, 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.