CONTINGENCY PLANNING POLICY STATEMENT

According to the National Institute of Standards and Technology (NIST), the following statement means that "it is a set of management policies and procedures designed to maintain and restore business operations, possibly at an alternate location in the event of emergency, system failure or disaster".-2

This is one major component in the disaster recovery planning. In this, a plan is laid down keeping all the emergency situations in mind and preparation for any kind of disasters which may occur at any point of time. The policy statement is really talks about communication between management and those responsible for developing the plan. Keeping in view the driving goals of the project and the level of financial resources and other resources, the particular people who are involved and are to be responsible, this policy statement gives everything that the planners need to work out options in order to achieve the organization's goals. It also provides the scope to planners to interact with the management in case they need to re-assess the organization goals and resources from time to time. The importance of this step is not just for preparing the plan for the DR implementation but also at this step a major amount of cost is involved than the other phases of the DR implementation. Here are the key points that the policy statement should address:

What kind of disaster does the organization intend to cover?

What do the organizations need to accomplish?

How much time would it take in order to get things back to normal state?

Where does the responsibility of the plan and planners end?

How to take advantage of the crisis situation in order to improve your organization image with the stake holders?

What level of system should be covered in case of any crisis?

What is the maximum level of resources that the plan can command during the preparation, implementation, testing and maintenance?

The initial draft for this plan may set goals that turn out to be impossible under the resource constraints specified. But as the time passes we need re-evaluate the policy and adjust the goals and resources according the situations.

BUSINESS IMPACT ANALYSIS

The primary purpose of this step is to ensure that everything is protected without any loss of resources. This will also facilitate as to how quickly the business operation should have to return to full operations in case a disaster occurs. These are analyzed and identified on the basis of the worst-case scenario which may occur that assumes that the physical infrastructure supporting each respective business unit would be destroyed and all records, equipment, etc. are not accessible within 30 days.

The main objectives of the business impact analysis (BIA) are as follows:

Estimating on what scale on each business unit can be affected financially, considering the worst case scenarios

Estimating on what scale on the operations of each business unit can be affected considering the worse case scenarios.

Identifying and estimating the amount of personnel required for recovery operations.

Estimating the time frame required for each business unit, considering the worst case scenarios.

The key business processes that act as backbones to the organization's ability to carry out its business are identified and the requirements that drive these processes are also analyzed. The above processes can be identified and sorted in two different ways.

Outside-In Analysis: This analysis is conducted in consideration with external stake holders, outside suppliers and internal departments which depend on IT services. The outside-in analysis focuses on whole systems, at each layer taking into consideration, the current process or system as distinct from the users or other systems that depend on it and via versa. Depending on the overall complexity of your business and how it makes the ideal solution to divide things up in the context, we may end up with just a single layer or with many of them.

Inside-Out Analysis: The inside-out phase primarily focuses on resources that are required in each layer in order to provide the services that have been identified in the Outside-In phase which covers everything from the core system to the IT resources in the organizations. Then for each of the above we shall determine the impact of a disaster which may cause disruption or damage of the resource on the functioning of the system and its ability to deliver the services on which other layers depend on. Then we determine the maximum time wastage due to the disaster test we conducted on each of the services on the basis of what other layers are dependent on these services. We shall also include in the analysis any indirect effects which were caused by the disaster on these services.

"The BIA Report should be presented to the Steering Committee"

PREVENTIVE MEASURE

There has been a simple formula for determining the risk associated financially with a given type of disaster; $R=P\*C\*T where P is the probability that the disaster will occur, C is the hourly or daily cost of downtime in lost productivity, lost revenue, etc. and T is time outage. The primary purpose of this step is to reduce the time outage, which are also the main purposes of the DR plan. Since the risk and the other factor are directly proportional to the time outage associated, hence the reduction of time is the primary responsibility of this task. At the same time the reduction of the other two factors which is the probability of the occurrence of the disaster and the cost due to the downtime are equally important. So minimizing all the three factors would result in the least risk possible. Generally sources say that the cost of preventing a problem is far lower than the cost of fixing it after it occurs. Let us now look into how we can identify the above factors. Firstly the probability of disaster occurring is generally is the toughest one to say. Natural calamities come and strike without a sign. The only way to prevent them is to make the organization sites in safe places. Next is the computer malfunction or server crash, these can be prevented by regular maintenance, constant tracking through performance monitors, proper vigilance and good security. Secondly is the cost reduction, there should be maintenance in such a way that generally if by chance there has been any damage the system should be protected. We should not be in a position to replace and get a new one. Generally the cost associated in installing a new machine is always higher than the maintenance cost put on it. Even the cost of downtime can be reduced by reducing the organization's dependence on the system. Thirdly is the time outage, we need to have special ops teams which should act readily to any situational catastrophe. So by reducing all the above factors we can reduce the probability of risk on the organization.

RECOVERY STRATERGIES

The primary task of this step is to determine how we have to achieve the disaster recovery goals for each of the systems and system components that were identified in the Business Impact Analysis. It is here that we do the core work of balancing costs and benefits of the available approaches. This step is not just about selecting specific vendors, determining exact costs, or developing detailed procedures, but the main purpose in this stage is to select the types of solution that you will use and to determine the scales of the costs involved. There are a set of consideration we need to follow while going through this phase. Firstly, we need to consider exactly what type of disasters may occur and classify them into different types based on the effectiveness Secondly; we need to consider solutions of differing range of coverage i.e. we need to determine solutions which can protect on the site failures as such a solution can also protect the system and its components. Lastly we need to consider are the characteristics of infrastructure, human and data aspects of recovery. Each of the above three factors should be considered separately and we should determine what type of solution and the cost associated for the solution. Out of the above three factors Infrastructure recovery is the simplest. The best feature of infrastructure is that it can be replaced easily. People are considered more difficult factors. Every personnel in the company are associated with particular skills and accordingly they are assigned roles. So if a recovery strategy is needed to be implemented on these people, suppose if a personnel has been fired or he quits then finding another personnel of the same skill set and roles is always an additional cost ,since we need to play better salaries. Thirdly it is the data; this cannot be replaced at any cost. Once a data is lost cannot be recovered at any cost. What we need to determine is to what extent of data we can lose and identify which is the critical data and we need to protect it accordingly. Once this is done, we have to note the recovery strategies for each system on the Master System Information form.

DEVELOP THE CONTINGENCY PLAN

This step is the apex or the peak activity of all your work. The main outcome of this phase is the documented plan and the complete implementation of the infrastructure in order to implement the plan. This documented plan includes each and every information of assumptions, constraints and specific procedure needed to be implemented. The implementation phase contains all the purchasing and setup of all the hardware and implementation at the sites, communication services etc. This phase itself is run by a team, just like a team which handles projects. Team which consists of different expertise with fixed timelines and deadlines. According to the NIST guide the following are some aspects or steps which needed to be followed during the plan.

1. Introduction: Here the main task is to document the goals and scope of the plan, along with any requirements that must be taken into account whenever the plan is updated.

2. Operational Overview: The purpose of this section is to provide a concise picture of the plan's overall approach. It contains essentially two types of information: (1) a high-level overview of the systems being protected and the recovery strategies employed and (2) a description of the recovery teams and their roles.

3. Notification/Activation Phase: According to the NIST guide this phase" defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities like notifying recovery personnel, assessing system damage and implementation of the plan. At the completion of this phase, recovery staff will be prepared to perform contingency measures to restore system functions on a temporary basis".

4. Recovery Phase: This section of the plan is one that documents in detail the solutions to be used to recover each system and the procedures required to carry out the recovery and restore operational activities.

5. Reconstitution Phase: This is the last of the three sections of the plan. As per the NIST guide this phase is where the "recovery activities are terminated and normal operations are transferred back to the organization's facility. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new facility to support system processing requirements".

6. Appendices: The appendices contains any information that (a) is necessary as reference material during recovery, (b) may be necessary during any revision of the plan, or (c) documents legal agreements.

PLANNING TESTING TRAINING AND EXERCICES

In this fast moving modern information technology world, with the change in time and things, many hardware components are replaced, software's are upgraded, networks are reconfigured, data sizes grow. All the above factors play a major impact on the performance of the disaster recovery systems. Testing and exercising goals are established and alternative testing strategies are evaluated from time to time. Each and every procedure required for testing should be properly documented from time to time. Initially the testing should be done in sections and should be conducted after the office hours. Below are some types of testing:

Check List Testing

Simulation Testing

Parallel Testing

Full Interruption Testing

Although these systems were fully tested when first installed, but the system is dynamic in nature, so proper training should be given to personnel from time to time. We need to conduct exercises from time to time to check the status and under different condition with the help from all the personnel in the organization. Once the plan has been properly tested and documented it should be approved by the top management to start off. The management would take all the responsibility of preparation of policies, procedure, responsibilities and tasks associated with it. It should make sure that they review the contingency plan at least annually and re-assess and approve it. At the same it should be responsible in making limitations and constraints. Proper implementation of the above all factors will lead to a smooth start up and helps the DR plan successful.

PLAN MAINTAINENCE

After developing a disaster recovery plan, it is equally important to ensure that the plan accurately runs accordingly to the current requirements and systems. There are three places, at which the plan can be reviewed firstly, during testing annually or semiannually, and secondly when changes are made in either the IT systems being protected or in the business processes they support. The first of the above two falls in the responsibility of the top management in the disaster recovery planning and so has to be done on a regular basis. The last requires that consideration of the impact of the changes on the disaster recovery plan to be introduced as a standard consideration in procedures that are outside the scope of direct concern of those responsible for the DR plan.

SUMMARY

The world is fast changing and organizations need to be prepared for natural or manmade disasters that could disrupt business processes. Customers and millions of dollars could potentially be lost and never be recovered if business processes are disrupted. The Business Continuity Plan helps resume the business processes and the Disaster Recovery Plan helps resume the IT systems. The core objective of a Disaster Recovery Plan is to restore the operability of systems that support mission-critical and critical business processes to normal operation as quickly as possible. Business continuity planning integrates the business resumption plan, occupant emergency plan, incident management plan, continuity of operations plan, and disaster recovery plan. Personnel from each major business unit should be included as members of the team and part of all disaster recovery planning activities. These people need to understand the business processes, technology behind those processes, networks, and systems in order to create the disaster recovery plan. Applications and systems are identified by the team that is mission-critical and critical to the organization. There would be a specialist disaster recovery team which will be responsible for training, implementing, and maintaining the plan. They will possess unique skills, knowledge, and abilities that should be updated in the plan. A Disaster Recovery Plan that is well developed, trained on, and maintained, will minimize loss and ensure continuity of critical business processes in the event of disaster.