Disaster Recovery Plan to ISO 17799

Introduction

A disaster recovery plan attempts to run associated processes to transition smoothly in the event of a natural or human-caused disaster. To plan effectively, you need to first assess your mission-critical processes and associated processes before creating the full disaster recovery plan.

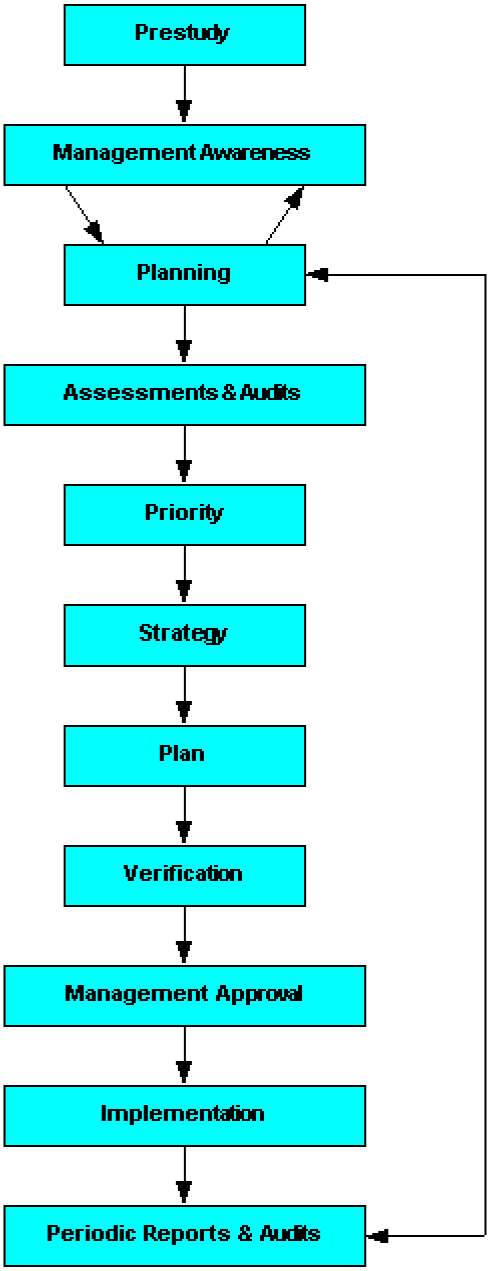
Performance Indicators for Disaster Recovery

Performance indicators provide the mechanism by which you can measure the success of your disaster recovery plan. Performance indicators for disaster recovery are somewhat different from those used to measure normal performances, because they are a combination of project status and test runs of infrastructure. Indicators of success include:

- Periodic reports from the implementation team to senior management.
- Representation of the planning team in the implementation team.
- Periodic tests to verify implementation of the disaster recovery plan and reports about gaps and risks.
- A review process that includes the deployment of new solutions.
- Analysis of the disaster recovery handling, effectiveness, and impact.

Process Flow for Disaster Recovery

The following diagram outlines your workflow for managing disaster recovery.



Management Awareness

Management Awareness is the first and most important step in creating a successful disaster recovery plan. To obtain the necessary resources and time required from your area, senior management has to understand and support the impacts and risks. Several key tasks are required to achieve management awareness.

Identify Possible Disaster Scenarios

First, identify the top ten disasters and analyze their impact. Your analysis should cover effects on communications, the impact on operations, and disruption on key operations. You should complete this pre-study in advance of the disaster recovery planning process, knowing that it will require additional verification during the planning process.

The following are examples of possible disasters: fire, storm, water, earthquake, chemical accidents, nuclear accidents, war, terrorist attacks and other crime, cold winter weather, extreme heat, airplane crash, and avalanche. The possibility of each scenario depends on factors such as geographical location and political stability.

Assess the impact of a disaster from both a financial and physical (infrastructure) perspective by asking the following questions:

- How much of the resources could be lost?
- What are the total costs?
- What efforts are required to rebuild?
- How long will it take to recover?
- What is the overall impact?
- How are people affected, what is the impact on them?

Build Management Awareness

Senior management needs to be involved in the disaster recovery planning process, and should be aware of the risks and potential impact. The first study on disaster recovery should include an estimate of possible costs and time to implement a disaster recovery strategy. Once management understands the financial, physical, and costs associated with a disaster, it is then able to build a strategy and ensure that this strategy is implemented across the organization.

Obtain Management Sign-Off and Funding

The senior management has to agree on the disaster recovery project, as well as provide financial and human resources for the project. The first step is the announcement of the disaster recovery project and kickoff of a planning group or steering committee, which should be led by a senior management person.

Disaster Recover Planning Process

In the disaster recovery planning stage, you should identify the mission-critical, important, and less-important processes, systems, and services and put in place plans to ensure these are protected against the effects of a disaster. Key elements of disaster recovery planning include the following:

Establish a Planning Group

Establish a planning team to manage the development and implementation of the disaster recovery strategy and plan. Key people from each sector, unit or operational area should be members of the team, responsible for all disaster recovery activities, planning, and providing regular monthly reports to senior management.

Perform Risk Assessments

In order to create the disaster recovery plan, your planning group needs to thoroughly understand the life style, available resources, networks, systems, and services. The disaster recovery planning team should prepare a risk analysis and an impact analysis that includes at least the top ten potential disasters. The risk analysis should include the worst-case scenario of completely damaged facilities and destroyed resources. It should address geographic situations, current design, lead-times of services, and existing service contracts. Each analysis should also include an estimate on the financial impacts of replacing damaged equipment, drafting additional resources, and setting up extra service contracts.

Establish Priorities

When you've analyzed the risks posed to your area from each disaster scenario, assign a priority level to each segment. Priorities should be based on the following levels:

- **Mission Critical**: Destruction that would cause an extreme disruption to life, cause major financial ramifications, or threaten the health and safety of the people. The targeted system or data requires significant effort to restore, or the restoration process is disruptive to the business or other systems.
- **Important**: Destruction that would cause a moderate disruption to life, cause minor financial ramifications, or provide problems with access to other systems. The targeted system requires a moderate effort to restore, or the restoration process is disruptive to the system.
- **Minor**: Destruction that would cause a minor disruption to life. The targeted systems can be easily restored.

Develop Recovery Strategy

Just as the analysis of the operations determine the priorities of the systems, the same analysis should be applied to the planning of the recovery. The site priorities and location of key services contribute to a fault-tolerant design, with resilience built into the infrastructure, and services and resources spread over a wide geography.

Develop a recovery strategy to cover the practicalities of dealing with a disaster. Such a strategy may be applicable to several scenarios; however, the plan should be assessed against each scenario to identify any actions specific to different disaster types. Your plan should address the following: people, facilities, services, communication, equipment, and maintenance.

Your recovery strategy should include the expected down time of services, action plans, and escalation procedures. Your plan should also determine thresholds, such as the minimum level at which the plan can operate, the systems that must have full functionality and the systems costs that can be minimized.

Prepare Documentation

It is important to keep your documentation up-to-date and have a complete list of all related officials, locations, devices, services, and contact names. The documentation should be part of the implementation process.

Your disaster recovery documentation should include:

- Complete inventory, including a prioritization of resources.
- Review process.
- Risk analysis based on the outcome of the assessments.
- Implementation plan to eliminate the risks and gaps.
- Disaster recovery plan containing action and escalation procedures.

Develop Verification Criteria and Procedures

Once you've created a draft of the plan, you should create a verification process to prove the disaster recover strategy and, if your strategy is already implemented, review and test the implementation.

It's important that you test and review the plan frequently. We recommend documenting the verification process and procedures, and designing a proof-of-concept-process. The verification process should include an experience cycle; disaster recovery is based on experience and each disaster has different rules.

Implementation

Now it's time to make some key decisions: How should your plan be implemented? Who are the related officials, and what are their roles? Leading up to the implementation of your plan, try to practice for disaster recovery using roundtable discussions, role playing, or disaster scenario training. Again, it's essential that your senior management approves the disaster recovery and implementation plans.

Backup Services

Backup services form a key part of disaster recovery, and you should review these services to make sure they meet the criteria for your disaster recovery plan. Backup is defined as the ability to recover from any failure or issue whether it is related to any part of the processes. A high availability is often the foundation for disaster recovery and can be sufficient to handle some minor or local disasters. Key tasks for planning backup services include the following:

Review and Implement Backup Services

Your disaster recovery plan should include a backup services strategy, which needs to be consistent throughout the whole organization. Backup scenarios are important to provide higher availability and access to main sites and/or access to existing parallel disaster recovery sites during a disaster.

All backup strategies depend upon networking. Disaster handling requires communication services, and the impact of a disaster could be greatly limited by having available communication services.