Cisco − Disaster Recovery: Best Practices White Paper

Table of Contents

Disaster Recovery: Best Practices White Paper

Introduction

A disaster recovery plan covers both the hardware and software required to run critical business applications and the 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 business processes and associated applications before creating the full disaster recovery plan.

This best−practice document outlines the steps you need to take to implement a successful disaster recovery plan. We'll look at the following critical steps for best−practice disaster recovery: Management Awareness, Disaster Recovery Planning, Resiliency and Backup Services, and Vendor Support Services.

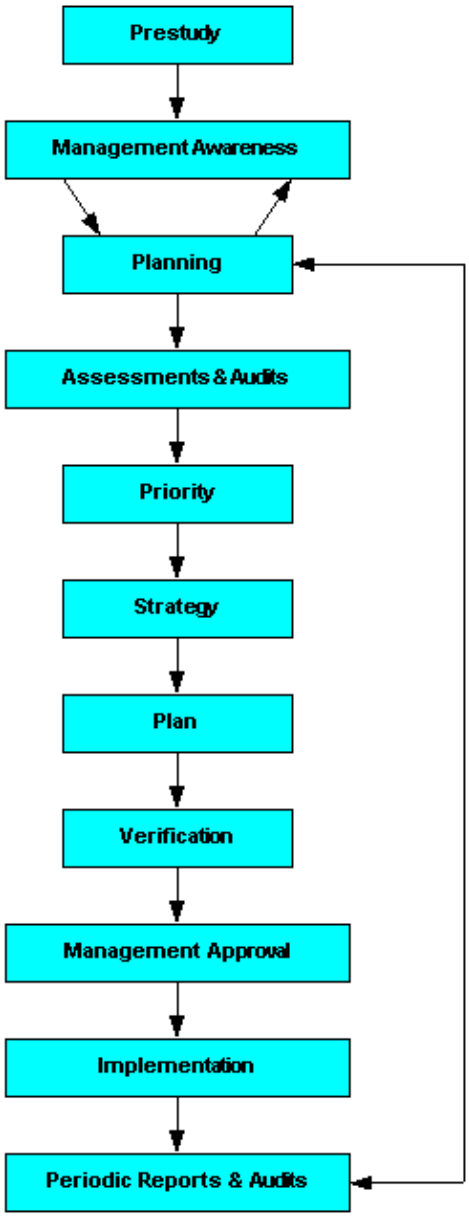
Performance Indicators for Disaster Recovery

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

- Periodic reports from the planning group to senior management.
- Representation of the network design team on the disaster recovery planning 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 on the business (after a disaster occurs).

High−Level 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 each area of your organization, senior management has to understand and support the business 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 on your business. Your analysis should cover effects on communications with suppliers and customers, the impact on operations, and disruption on key

business processes. 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 (loss of key staff), and avalanche. The possibility of each scenario depends on factors such as geographical location and political stability.

Note: Most disasters are caused by fire and we therefore recommend you start with fire as your first case study.

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

- How much of the organization's 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 impact on the overall organization?
- How are customers affected, what is the impact on them?
- How much will it affect the share price and market confidence?

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 on the organization. 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 business 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 in your network 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.
- Perform risk assessments and audits.
- Establish priorities for your network and applications.
- Develop recovery strategies.
- Prepare an up−to−date inventory and documentation of the plan.
- Develop verification criteria and procedures.
- Implement the plan.

Establish a Planning Group

Establish a planning group to manage the development and implementation of the disaster recovery strategy and plan. Key people from each business 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 and Audits

In order to create the disaster recovery plan, your planning group needs to thoroughly understand the business and its processes, technology, networks, systems, and services. The disaster recovery planning group should prepare a risk analysis and business 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 for Your Network and Applications

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

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

Develop Resiliency Design and Recovery Strategy

Just as the analysis of the business processes determine the priorities of the network, applications, and systems, the same analysis should be applied to your network design. The site priorities and location of key services contribute to a fault−tolerant design, with resilience built into the network 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, network services, communication equipment, applications, clients and servers, support and maintenance contracts, additional vendor services, lead−time of Telco services, and environmental situations.

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 can the business operate, the systems that must have full functionality (all staff must have access), and the systems that can be minimized.

Prepare Up−to−Date Inventory and Documentation of the Plan

It is important to keep your inventory up−to−date and have a complete list of all locations, devices, vendors, used services, and contact names. The inventory and documentation should be part of the design and implementation process of all solutions.

Your disaster recovery documentation should include:

- Complete inventory, including a prioritization of resources.
- Review process structure assessments, audits, and reports.
- Gap and risk analysis based on the outcome of the assessments and audits.
- Implementation plan to eliminate the risks and gaps.
- Disaster recovery plan containing action and escalation procedures.
- Training material.

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. You may want to call on experts to develop and prove the concept, and product vendors to design and verify the plan.

Implementation

Now it's time to make some key decisions: How should your plan be implemented? Who are the critical staff members, 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.

Resiliency and Backup Services

Resiliency and 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. Cisco defines network resiliency as the ability to recover from any network failure or issue whether it is related to a disaster, link, hardware, design, or network services. A high availability network design is often the foundation for disaster recovery and can be sufficient to handle some minor or local disasters. Key tasks for resiliency planning and backup services include the following:

- Assess the resiliency of your network, identify gaps and risks.
- Review your current backup services.
- Implement network resiliency and backup services.

Assess Network Resiliency

We recommend you assess the resiliency of your network keeping in mind the following three levels of availability: reliable networks, high−availability networks, and nonstop network environments. Doing so helps prioritize risks, set requirements for higher levels of availability, and identify the mission−critical elements of your network.

Be sure to evaluate the following areas of your network:

- Network links
    - ♦ Carrier diversity
    - ♦ Local loop diversity
    - ♦ Facilities resiliency
    - ♦ Building wiring resiliency
- Hardware resiliency
    - ♦ Power, security and disaster
    - ♦ Redundant hardware
    - ♦ Mean time before replacement (MTTR)
    - ♦ Network path availability
- Network design
    - ♦ Layer 2 WAN design
    - ♦ Layer 2 LAN design
    - ♦ Layer 3 IP design
- Network services resiliency
    - ♦ DNS resiliency
    - ♦ DHCP resiliency
    - ♦ Other services resiliency

Review and Implement Backup Services

Your disaster recovery plan should include a backup services strategy, which needs to be consistent throughout the whole organization. For example, Frame Relay services could use ISDN as a backup service. 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 system and application backup strategies depend upon network connections. Disaster handling requires communication services, and the impact of a disaster could be greatly limited by having available communication services.

The following table shows possible backup services (across the top row) for a primary connection (down the left column). Based on your location, some of the services may not be available, or may only be available with limited bandwidth. An **X** represents a possible backup services solution; an **O** represents a limited backup services solution; and a blank box represents an option that is not sufficient as a backup service solution.

	IP Services	PLC (E1, T1, fractional)	ISDN	Frame Relay	ATM	POTS	SDH / SMDS	VSAT	Communication by Light	Microwav
IP Services	X	X	X	X	X	X	X	X	X	X
PLC (E1, T1, fractional)	X	X	X	X	X		O	O	O	O
ISDN	X	X	X	X	X	O		O	O	O
Frame Relay	X	X	X	X	X					

ATM	X	X	X	X	X			O	O	O
POTS	X	X	X			X		X		X
SDH /SMDS	X	O			X		X	X	O	O
VSAT	X	X	X	X	X	X		X	O	O
Communication by Light	X	X	X	X	X	O		X	X	O
Microwave	X	X	X	X	X	O		X	O	X
X.25	O		X	X		X		X	O	O
xDSL	X	X	X	X		X		O	O	O
GSM 9.6 kbps			X			X		X		

A backup service (marked with an X) should offer 60 percent of the bandwidth requirements of the primary service. The backup service must be compatible, and in some cases additional interfaces for routers, switches, adapters, and protocols are required.

Vendor Support Services

Having support services from your major vendors in place adds a strong value to disaster recovery planing. For example, specific managed hot standby sites or on−site services with rapid response times can significantly ease disaster recovery. Key questions regarding vendor support include:

- Are support contracts in place?
- Has the disaster recovery plan been reviewed by the vendors, and are the vendors included in the escalation processes?
- Does the vendor have sufficient resources to support the disaster recovery?

Most vendors have experience handling disaster situations and can offer additional support. Cisco offers a wide range of Service & Support Solutions (registered customers only) and can assist with limiting downtime in the case of an unexpected outage.

Related Information

- **Technical Support − Cisco Systems**