Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Disaster Recovery Plan Strategies and Processes

A Disaster Recovery Plan is designed to ensure the continuation of vital business processes in the event that a disaster occurs. This paper discusses the development, maintenance and testing of the Disaster Recovery Plan, as well as addressing employee education and management procedures to insure provable recovery capability.

Copyright SANS Institute
Author Retains Full Rights

AD
Take control of vulnerability threats Now!
Request a Free Trial
Secunia
Stay Secure

Disaster Recovery Plan Strategies and Processes
Written by: Bryan C. Martin
February 2002
Version 1.3

Introduction

This Disaster Recovery Plan is designed to ensure the continuation of vital business processes in the event that a disaster occurs. This plan will provide an effective solution that can be used to recover all vital business processes within the required time frame using vital records that are stored off-site. This Plan is just one of several plans that will provide procedures to handle emergency situations. These plans can be utilized individually but are designed to support one another. The first plan is the Crisis Management Plan. This plan allows the ability to handle high-level coordination activities surrounding any crisis situation. We will also discuss the development, maintenance and testing of the Disaster Recovery Plan. Lastly, we will discuss the culture and employee education on Disaster Recovery.

The term "disaster" is relative because disasters can occur in varying degrees. So, this Plan has considered this issue and incorporates management procedures as well as technical procedures to insure provable recovery capability.

The next key issue to be strongly considered within the strategy for disaster recovery is a recovery strategy for alternate processing (Hot-Site). This plan identifies discusses the Hot-Site and the alternatives if the primary location is not available to provide Disaster Recovery services for the various system environments.

The final issue to be addressed within the Disaster Recovery Strategy is to insure that every reasonable measure has been taken to identify and mitigate potential risks that exist within the processing environment. ***The most successful Disaster Recovery Strategy is one that will never be implemented; therefore, risk avoidance is a critical element in the disaster recovery process.***

A Disaster Recovery Management System can be defined as the on-going process of planning, developing, testing and implementing Disaster Recovery management procedures and processes to ensure the efficient and effective resumption of vital business functions in the event of an unscheduled interruption. With the growing dependence on I/S and the Business Process to support business growth and changes associated with their complexities, compounded with the complexities of changing technology, the following elements are key to implementing a comprehensive Disaster Recovery Program:

- Critical Application Assessment
- Back-Up Procedures
- Recovery Procedures
- Implementation Procedures
- Test Procedures
- Plan Maintenance

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Crisis Management Plan

This Crisis Management Plan is designed to ensure the continuation of vital business processes in the event that an emergency or crisis situation should occur. However, Executives and Senior Management can use the procedures in this plan. Should an emergency situation occur at any of the business locations, the plan should provide an effective method that can be used by management personnel to control all activities associated with a crisis situation in a pro-active manner and to lessen the potential negative impact with the media, the public and with shareholders. This plan should be updated annually and should always be readily available to authorized personnel.

This plan is designed as a companion document to the Business Resumption Plan. The Business Resumption Plan consists of two major parts, each a recovery plan. The first are the Disaster Recovery Plans for technology in the event that a disaster should strike data processing center(s). The second is the Business Recovery Plan that will address issues surrounding the business operation and business units should a disaster affect.

Scope and Objectives of the Crisis Management Plan

The plan should provide information for the pro-active handling of any crisis situation and should include detailed procedures for the following:

- Executives
- Legal
- Investor Relations
- Corporate Communications
- Corporate Administration
- Marketing and Sales
- Human Resources
- Technology management

The plan should also document the responsibilities, procedures, and checklists that will be used to manage and control the situation following an emergency or crisis occurrence.

The Crisis Management Plan has been developed to accomplish the following objectives:

- Prepare senior management personnel to respond effectively in a crisis situation;
- Manage the crisis in an organized and effective manner;
- Limit the magnitude or impact of any crisis situation to the various business units.

Crisis Management Plan activities are initiated by a situation or crisis alert procedure. After discovery of an incident, the Crisis Management Team will perform an assessment of the situation and determine if there is a need to declare an emergency or crisis and activate the Crisis Management Plan. When the plan is activated, assigned management personnel will be alerted and directed to activate their procedures.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Disaster Definition

A "disaster" is any event that can cause a significant disruption in operational and/or computer processing capabilities for a period of time, which affects the operations of the business.

The purpose of defining a crisis or a discontinuity is to establish a documented description of what constitutes a crisis or a discontinuity. The intent is to minimize the decision-making process when an event occurs.

An outage (crisis/discontinuity) may exist when:

a. A service providing support to a critical business function fails.
b. It is determined the service cannot be restored before the point it becomes vital to the business.

Disaster Recovery Scenario

The disaster recovery scenario that will be specifically addressed, within the scope of this plan, is the loss of access to the computer center and the data processing capabilities of those systems and the network connectivity. Although loss of access to the facility may be more probable, this Disaster Recovery Plan will only address recovery of the critical systems and essential communications.

This scenario also assumes that all equipment in the computer room is not salvageable and that all critical telecommunications capability has been lost.

In the event of a declared Disaster, key personnel will take immediate action to alert the Disaster Recovery Center. Restoration of the Critical Coverage will be provided after a Disaster is declared and after turnover of the disaster recovery backup site. It will include, without limitation, the following:

1. Delivery of the Authorized User Data and Software archived in off-site storage to the Disaster Recovery Center
2. Connecting Network lines to the Disaster Recovery Center
3. Operating the Critical Applications on the Configuration at the Disaster Recovery Center
4. Provide Critical Coverage at the Disaster Recovery Center
5. Provide workspace and required equipment.

Recovery Strategy

The recovery strategy that will be discussed as part of this Disaster Recovery Plan will be to relocate critical Information Systems processing to an alternate computer-processing center. The processes will be recovered at the Disaster Recovery Services provider name and location of the Hot-Site. The Disaster Recovery Services provider name is responsible for ensuring that the system configurations and the associated network requirements are accurate and technically feasible at all times. Therefore, yearly testing will be a part of the alternate processing strategy.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Also, the associated network connectivity will be recovered, within the disaster recovery scenario, using the alternate processing strategy.

Recovery Phases

Recovery activities will be conducted in a phased approach. The emphasis will be to recover the critical applications effectively and efficiently. Critical applications will be recovered over a period of time after data center activation.

Phase I
Move operations to the Disaster Recovery Backup Site and the Emergency Operations Center. This activity will begin with activation of the Disaster Recovery Plan. There is a period of up to 24 hours allowed for organization and the turnover of the disaster recovery backup site.

Phase II
To recover critical business functions, restoration of the critical applications and critical network connectivity. The goal here is to recover the systems and network so that our customers can continue business.

Phase III
Return data processing activities to the primary facilities or another computer facility.

The following conditions, if met, will constitute a successful recovery effort:

- Restore critical applications to the most current date available on backup tapes stored off-site. Updating the systems and databases will take place as the recovery effort progresses.
- It is understood that, due to the emergency or disaster, response times will probably be slower than normal production situations.

The Plan provides recovery procedures to be used at the present data center site after repairs have been made or at the Disaster Recovery Backup Site and the Emergency Operations Center. It also provides recovery procedures for the restoration of critical applications using either data recovered from the damaged data center or from the backup data stored off-site.

Scope and Objectives of the Plan

The Disaster Recovery Plan provides a state of readiness allowing prompt personnel response after a disaster has occurred. This, in turn, provides for a more effective and efficient recovery effort. The Disaster Recovery Plan should be developed to accomplish the following objectives:

1. Limit the magnitude of any loss by minimizing the duration of a critical application service interruption.
2. Assess damage, repair the damage, and activate the repaired computer center.
3. Recover data and information imperative to the operation of critical application's.
4. Manage the recovery operation in an organized and effective manner.
5. Prepare technology personnel to respond effectively in disaster recovery situations.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Every business has the responsibility to respond to any short or long term disruption of services. By developing, documenting, implementing and testing this Disaster Recovery Plan, businesses will be able to restore the availability of critical applications in a timely and organized manner following a disaster occurrence. In order to accomplish these objectives, the technology area will depend on support from senior management, end users and staff departments.

Disaster Recovery Plan activities are initiated by a situation or disaster alert procedure. After discovery of an incident, technology management will be informed of a potential disaster at the computer center. The Recovery Management Team will perform an assessment of the situation and determine if there is a need to declare a disaster and activate the Disaster Recovery Plan. When the Plan is activated, assigned recovery personnel will be alerted and directed to activate their recovery procedures.

Recovery Objectives

This section will define those applications and customers that are critical to the business and the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) for this Disaster Recovery Plan. The Recovery Time Objective is the length of time a business can be without data processing availability and the Recovery Point Objective (RPO) is how old the data will be once the systems are recovered.

The following applications and customers have been defined as critical and require restoration within the Recovery Time Objective (RTO) following a disaster declaration in order to support the restoration of the vital business functions. These applications and the supporting systems will be recovered within the Disaster Recovery Scenario using the alternate processing strategy. The list of Critical Applications and Critical Customers and the Recovery Time and Point Objectives should be reviewed and updated by management on an annual basis.

Development of a Disaster Recovery Plan

A. Plan Scope and Objectives
B. Business Recovery Organization (BRO) and Responsibilities (Recovery Team Concept)
C. Major Plan Components - format and structure
D. Scenario to Execute Plan
E. Escalation, Notification and Plan Activation
F. Vital Records and Off-Site Storage Program
G. Personnel Control Program
H. Data Loss Limitations
I. Plan Administration (general)

Maintenance of the Plan

The purpose of this section is to define the activity necessary to maintain the Disaster Recovery (DR) Plan for the mainframe and mid-range environments. DR Plan maintenance is of utmost importance to ensure currency of what is to be recovered and procedures governing the recovery. This means keeping the test plan and implementation plan current and in sync with business changes. All changes to the business and in the mainframe and mid-range environments must be considered for inclusion in and for updating of the Disaster Recovery Plan.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The Disaster Recovery Plan may require updates if problems or changes include some or any of the following:

- Mainframe and Mid-Range Disaster Recovery Test results
- New critical applications or critical customers
- Increased application complexity
- New equipment acquisitions
- Changes to:
- Hardware
- Software
- Network
- Applications
- Data

A formal review of a Disaster Recovery Plan should be conducted yearly, and a quarterly Disaster Recovery Readiness Assessment Audit should be conducted as well. The purpose of the reviews and the audits is to identify any changes to ensure that these and any other updates identified since the previous review have been captured.

Items to be reviewed for Plan update should include:

- Personnel changes
- Mission changes
- Priority changes
- New Business Organizations
- Mainframe and Mid-range Disaster Recovery Test procedures and results
- Backup procedures
- Recovery procedures
- Relocation / Migration Plan
- Software (operating system, utilities, application programs)
- Hardware (mainframe, mid-range and peripherals)
- Communications Network Facilities

Particular attention should be paid to the review of the recovery equipment configurations to ensure that the business has the required equipment to restore the business functionality as quickly and smoothly as possible.

These reviews will require the time and attention of all Plan holders and team members, especially those that have hardware and network responsibilities.

The proper maintenance of the Plan will be the responsibility of ALL holders of the Plan. It will be their responsibility to incorporate all approved revisions into their assigned copy to ensure that the Plan manual is maintained as a viable and readied Action Plan. All removed pages are to be properly disposed; they should be placed in the classified materials bins throughout the office or shredded. It is the responsibility of all Plan holders to protect Confidential material and dispose of it in a proper manner.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Disaster Recovery Testing Overview

The purpose of this Test Plan Document is to specifically identify and document the task plan and procedures to be implemented in a testing environment. This Test Plan includes test parameters, objectives, measurement criteria, test methodology, task plan charts and time lines to validate the effectiveness of the current Disaster Recovery Plan. The Disaster Recovery Plan will be tested to ensure that the business has the ability to continue the critical business processes in the event of a disaster. It is very important that the Recovery procedures are executable and accurate. Another benefit of testing the plan is to train the personnel who will be responsible for executing the Disaster Recovery Plan. The important issue is not that the test succeeded without problems, but, that the test results and problems encountered are reviewed and used to update or revise the current Disaster Recovery Plan procedures. Testing can be accomplished by executing the disaster implementation plan or it may be desirable to execute a subset of the plan. When performing a Disaster Recovery Test, it is very important to use only that information which is recalled from the off-site storage facility. This is to ensure the following:

1. Simulate the conditions of an ACTUAL Disaster Recovery situation.
2. Completeness of the disaster recovery information stored at the Records Retention Site.
3. Ensure the ability to recover the intended functions.

This test plan includes the following areas:

1. Schedule
    a. Planning Sessions
    b. Pre-Test Technical Review
    c. Debriefing
2. Introduction
    a. Preface
    b. Scope
    c. Recovery Site
    d. Primary Test Objectives
    e. Secondary Test Objectives
    f. Exclusion (if applicable)
    g. Test Assumptions, Dependencies and Success Criteria
3. Test Teams
    a. ChoicePoint Participants
    b. IBM Participants (as applicable)
4. Pre-Test Planning
    a. Activities
    b. Issues
    c. Concerns
5. Test Timeline
    a. Planned start and stop time of test and tasks.
    b. Actual start and stop time of test and tasks (to be completed during the test)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

6. Critical Test Checkpoints
    a. Activity
    b. Recommendation
    c. Responsible party
7. Test Problem Log
    a. Document any problems encountered prior to the test.
    b. Record any deviations from Test Plan.

Post Test Review

The purpose of this Post Test Review document is to identify any problem areas and any recommendations for improvement to the plan. The Post Test Review document includes the following areas:

1. Highlights
    a. Overall Test Results
    b. Test Dates
    c. Disaster Recovery Back-up Site
    d. Local Access Suite
    e. Test Participants
2. Test Objectives
    a. Primary Test Objectives
    b. Secondary Test Objectives
    c. Exclusions (if applicable)
3. Timeline
    a. Planned task, start and end times and duration
    b. Actual task, start and end times
4. Problems Encountered During the Test
    a. Problem Log
        1. Actual Problem
        2. Assigned to
        3. Target Date for Resolution
        4. Status
        5. Resolution
        6. DR Process or Technical
    b. Problem Summary
5. Follow Up to Pre-Test Problems
6. Follow Up to Suggestions for Improvement/Recommendations from Last Year's Test
7. Detailed Summary and Observations
8. Recommendations for Next Year's Test

Establishing the Continuity Culture

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Documenting the Disaster Recovery Plan is one element of developing a strategy. The plan's success, however, depends upon:

- Implementation of the recommendations made, across the entire business.
- A program of training of those directly involved in the execution of the plan
- An education and awareness program to ensure enterprise-wide understanding and adoption of the plan, covering internal and external stakeholders, i.e. employees, customers, suppliers and shareholders

It is essential to commit to implementing all recommendations and strategies identified in the Disaster Recovery Plan, otherwise investment made in its preparation will be redundant. Similarly training and awareness must be embarked upon to ensure that the entire organization is confident and competent concerning the plan. All parties must appreciate the importance of Disaster Recovery Plan to the operation's survival and their role in this process.

This awareness should extend to those external stakeholders and third parties upon whom the organization depends/has influence in both normal and crisis operations.
Implementation of the plan in this manner and all those associated with the organization can have confidence in its ability to manage in a crisis, and the continuity culture will have started.

Actions:

- Select the Emergency Management/ BCM/ Crisis and Recovery Teams.
- Implement relevant training programs for each team dependent upon task, including crisis communications/ media training as appropriate. This process is ongoing, as team members will change.
- Establish and equip emergency and crisis centers.
- Establish internal and external contractual arrangements/ service level agreements.
- Implement back-up and off-site storage arrangements.
- Distribute plan documentation as appropriate.
- Conduct internal and external awareness programs. These programs can be built into employee and supplier induction processes and customer marketing programs.

© SANS Institute 2002, Author retains full rights.

Disaster Recovery Education for Employees:

Prepare Your Employees for Data Backup:
You'll need to educate your employees about where to store their files (in a specific directory on their PC that is backed up or on the central server) so that all files are included in the backup.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

You'll also want to avoid data loss and downtime by installing anti-virus software and teaching your employees how viruses are spread and

Prepare your Employees for Disaster Recovery:
Involving employees in the disaster recovery effort will also help ensure that recovery procedures are well planned and executed based on your business' need to provide as seamless a recovery as possible. Find out typical processes and turnaround times that your customers have come to expect and plan how you will prioritize recovery efforts. Make sure all employees know whom to contact in an emergency, and outline what they can do to remain productive during the recovery period. If you're using a service, identify who in the company will contact the service to initiate recovery efforts. Make sure you have the contact information off-site in case of a fire, flood, or other act of nature.

Disaster Recovery Statistics:

- Only 15% of midrange data centers would be able to recover more than 30% of their applications in any time frame.
- Just 3.8% could recover their applications within the same day.
- Only 2.5% could recover within four hours.

The eight R's of a successful recovery plan

- Reason for planning
- Recognition
- Reaction
- Recovery
- Restoration
- Return To Normal
- Rest and Relax
- Re-evaluate and Re-document

Conclusion

Every day, businesses are confronted with disasters of varying degrees. Those that have adequately developed, maintained, and exercised their contingency plans will survive. Yet many corporate executives continue to take the uninhibited operations of their companies for granted. They remain complacent, assuming that the power will always be available, the telephone system will not fail, there will be no fire or earthquake--everything will always be normal. Very few executives plan for their own, much less their organization's mortality; however, if a business is to survive, organizational "strategic" and "tactical" battle planning is essential. The final corporate contingency plan is the lifeblood of corporate survival. However, it is only as good as the foundation upon which it was built. The foundation is, of course, the concept. This document is the means by which a particular mission, program, or policy directive is translated into a fundamental organizational and operational methodology. Once the concept is developed through a logical building block approach, and is sanctioned by both management and the operating elements, construction of the contingency plan may commence. A fundamental premise of successful contingency planning is that plans are developed by those who must

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

actually carry them out in the event of an actual disaster. The role of the Corporate Contingency Planner is to strategically, and relentlessly, manage the process. And, in doing so, he or she must rely on both internal and external assistance. In addition to in-house assistance, there are a multitude of disaster assistance organizations and services available to assist the contingency planner. Preparing a corporate contingency plan is a non-trivial undertaking. However, corporate leaders must recognize the vulnerabilities they invite by not adequately planning for survival. Disaster planning is truly a vital part of the overall business plan.

References:

1. Wold, Geoffrey H. "Disaster Recovery Planning Process"
   http://www.drj.com/new2dr/w2_004.htm

2. The Business Continuity Institute
   http://www.thebci.org/frametrial.html

3. Boroski, Doran. "Protect processes as well as investments in disaster recovery plans"
   http://www.computerworld.com/storyba/0,4125,NAV47_STO68345,00.html

4. DRI International "Business Continuity Management Survey Examines How The Events of 9/11 Shape the Business Continuity Industry"
   http://www.dr.org/fallnews.pdf

5. Wrobel, Len "Components of a Successful LAN Disaster Recovery Plan"
   http://www.disaster-resource.com/content_page/nuggets.shtml

6. Radeke, Michelle "Prepare for Effective Data Backup and Recovery"
   http://www.workz.com/content/543.asp

7. Hussong, Jr. William A. "So You're The Company's New Contingency Planner"
   http://www.drj.com/new2dr/w3_001.htm

8. Disaster Recovery Planning: Strategies for Protecting Critical Information Assets
   By: Jon William Toigo

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**