

Disaster Recovery Planning

❖ *DigitalSherlock.com | SafeHack.com*

❖ *Date: 2005/05/27*

❖ *Document Name: disaster_recovery_planning.pdf*

❖ *GNU Free Documentation License*

❖ *Version 1.00, 2005-05-27*

❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*

❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Help To



❖ **DRP Objectives**

- **Use BIA to create recovery strategy plan**
- **Disaster is defined as an interruption affecting user operation significantly**
- **Planning and development must occur before the disaster**
- **Deals with " OH MY GOODNESS THE SKY IS FALLING"**
- **DRP is when a man-made or natural event are Major**
- **DRP focus maintaining business operations in case of disaster**
- **DRP help to recover with minimum impact**
- **DRP address procedures during and after loss**
- **Minimize the risk from delays in providing services**
- **Provide sense of security**
- **Minimize the risk of delays to the business**
- **Provide a standard for testing the plan and**
- **Provide an organized way to make decisions if a disruptive event occurs**
- **Minimize decision making required by personnel during a disaster**
- **Reduce confusion and enhance the ability to deal with crisis**
- **Disaster recovery plans protect against the economic and intrinsic losses**
- **Availability Integrity and confidentiality needs to be considered**
- **Should be part of the security policy program**
- **Provides procedures for:**
 - **Emergency Responses**
 - **Extended backup operation**
 - **Postdisaster Recovery**
 - **Disaster and its ramifications right AFTER the disaster hit**
 - **Recover as quickly as possible**
- **DRP Involves**
 - **Data Processing Continuity Planning**
 - **Data Recovery Plan Maintenance**
 - **Testing of the Disaster Recovery Plan**
 - **Disaster Recovery Procedures**

❖ **Data Processing Continuity Planning**

- **Planning for disaster and creating plans to cope with it**

➤ **Reciprocal or Mutual Aid Agreements**

- **Arrangement with another company with similar hardware or software configurations**
- **Agreement by both parties, assumes sufficient capacity in time of need (Big Assumption)**
- **Should only be considered if no other options, or perfect partner (i.e. subsidiary)**
- **That it is free or of a low cost to both organizations**
- **Both companies share hardware & software**
- **It makes testing the recovery possible**
- **Issues to be addressed**
 - How long will the facility be available to the company in need ?
 - How much assistance will the staff supply in the means of integrating the two environment
 - How quickly can the company in need move into the facility ?
 - What are the issues pertaining to interoperability ?
 - How many of the resources will be available to the company in need ?
 - How will differences and conflicts be addressed ?
 - How does change control and configuration management take place ?
 - How often can drills and testing take place ?
- **Advantages**
 - Very little or no cost
 - If processing requirements are similar it may be workable
- **Disadvantages**
 - Highly unlikely the capacity will exist
 - Informal agreements
 - Severely limits responsiveness and support
 - It is unlikely that there will in fact be enough excess capacity
 - It must be tested frequently
 - Configuration management in the two sites is difficult
 - It is unlikely that a quick response will be available when required
 - Short term outages are all that can be handled
 - Mixed operations (between the two organizations) create security problems
 - There is little, or no technical, administrative and logistical support

➤ **Subscription Services**

- **Third party commercial services provide alternate backup and processing facilities**
- **The major distinction between types of backup sites is TIME and COST**
- **An alternate site strategy should best be determined by the results of a full BIA**
- **Hot Site Requires**
 - Requires
 - ◆ Fully configured facility with electrical power, (HVAC)
 - ◆ File and print servers and workstations
 - ◆ Applications are installed on the servers
 - ◆ Workstations are kept up to date
 - Allows walk in with a data restoration and begin full operations in short time
 - Advantages
 - ◆ 24/7 availability
 - ◆ Exclusivity of use
 - ◆ Immediately available
 - ◆ Supports short and long term outages

- ◆ Annual testing available
 - Disadvantages
 - ◆ Most expensive
 - ◆ Requires constant maintenance of hardware, software, data and applications
 - ◆ Service provider may oversell processing capabilities
 - ◆ Security of hot site, primary site security must be duplicated
- **Warm Site**
 - Cross between hot and cold sites
 - Facility with electrical power, Heating Ventilation and Air Conditioning (HVAC)
 - File and print servers may not have workstations, software may not be installed
 - External communications should be installed
 - Advantages
 - ◆ Cost - much less than hot
 - ◆ Location - since less control required sites can be more flexible
 - ◆ Resources - resource drain is much lower than hot site
 - ◆ Availability for longer time frames because of the reduced costs
 - ◆ Practical for proprietary hardware or software use
 - Disadvantages
 - ◆ Not immediately available
 - ◆ Operational testing not usually available
- **Cold Site**
 - Least ready of all three, but most common
 - Facility with electrical power, Heating Ventilation and Air Conditioning (HVAC)
 - Ready for equipment but no computer hardware on site.
 - Communications links may or may not be ready
 - Advantages
 - ◆ Cost - much less than hot and worm site
 - ◆ Availability for longer time frames because of the reduced costs
 - ◆ Practical for proprietary hardware or software use
 - Disadvantages
 - ◆ Not immediately available
 - ◆ Operational testing not usually available
 - ◆ Not considered adequate because of length of time for recovery
 - ◆ False sense of security
- **Redundant site**
 - Equipped and configured exactly like the original site before a disaster.
 - This fallback would be the least risky of the 4 choices.
 - A hot site would be next least risky
- **Multiple Processing Centers**
 - **Processing spread over multiple centers, creating distributed redundancy.**
 - Can be in-house or through reciprocal agreement.
 - **Cost is contained, but same issues as Mutual Aid Agreements (reciprocal agreement)**
- **Service Bureaus**
 - **Contract with service bureau to provide all alternate backup processing.**
 - **Advantage - quick response**
 - **Disadvantage - cost, resource contention during disaster**
- **Transaction Redundancy Implementations**
 - **Electronic Vaulting-**
 - Transfer each on-line transaction or change to an off site location

- Batch process through communication lines to a server
- **Remote journaling-**
 - Mirroring transaction processing over high-speed to an alternate site
 - Backing up transaction logs to an off-site facility
 - Performs updates to a backup copy of the database
 - A communications line is used to transmit live data as it occurs.
- **Shadowing-**
 - Uses live processing of remote journaling,
 - Creates redundancy by duplicating the database sets to multiple servers.
- **HSM Hierarchical Storage Management**
 - HSM system dynamically manages the storage and recovery
 - The functionality happens in the background (transparent to users)
 - Files are copied to storage media that vary in speed and cost
 - Optical disks
 - Magnetic disks
 - Tapes
- **Other alternatives**
 - **Stockpiling**
 - In-house or external supply of hardware replacements
 - Vendors resupply hardware or internal stockpiling of critical components.
 - Subscription service with vendor for overnight shipping
 - May be OK for Warm site but not Hot site
 - **Rolling mobile backup sites**
 - Mobile homes or trucks with power and HVAC
 - Considered Cold Site variation.
 - **Prefabricated Buildings**
 - Use of prefabricated (mobile homes).
 - Very cold site.

❖ **Data Recovery Plan Maintenance**

- **Keeping plans up to date**
- **Disaster Recovery Plans often get out of date**
- **Changes in technical infrastructure and company structure**
- **Plan maintenance must be employed from the outset**
- **Audit procedures should report regularly on the plan**
- **Version control on all plan copies**

❖ **Testing of the Disaster Recovery Plan**

- **Objectives**
 - **Testing must be conducted in an orderly manner**
 - **Testing must be conducted on a regular basis**
 - **Testing must be conducted in a standardized fashion**
 - **No recovery ability exists until it is tested**
 - **Testing verifies the accuracy of the recovery procedures**
 - **Testing prepares and trains personnel to execute during emergency**
 - **Proven feasibility of recovery process**
 - **Ongoing verification of the backup facilities**

- **Verified adequacy of the team procedure**
- **Identification of deficiencies in the existing procedures**
- **Demonstration of the ability to actually recover**
- **Provides a mechanism for maintaining and updating the plan**
- **It is essential that the test does not disrupt work**
- **It is essential that Tests are conducted using the actual written test plans**
- **It is essential That a long term testing schedule be developed**
- **The test should start small and enlarge as things progress**
- **The test identify weaknesses that need to be corrected**
- **Testing verifies the processing capability of the alternate backup site**
- **DRP and BCP should be tested at least EVERY Year**

➤ **Creating the Test Document**

- **Test document should include:**
- **Test scenarios**
- **Reasons for the test**
- **Objectives of the test**
- **Type of tests**
- **Testing schedule**
- **Duration of the test**
- **Specific test steps**
- **Who will be the participants**
- **The task assignments of the test**
- **Resources and services required**
- **Test must not disrupt normal business functions**
- **Testing should start with easy areas to build skills and confidence**
- **Purpose is to find weaknesses, update and retest**

➤ **5 Disaster Recovery Plan Types**

- **Checklist**
 - Preliminary step to real test, distribute plan for review by business unit managers
 - Copies of plan are distributed to management for review
- **Structured walk through**
 - Business unit management meets to review the plan
 - Each step is walked through and marked as performed
 - The goal is to ensure we can recover on paper successfully.
- **Simulation**
 - All support personnel meet in a practice execution session
 - Enacts recovery procedures but no alternate processing
 - All of the operational and support personnel expected to perform during an ACTUAL emergency meet in a practice session.
- **Parallel**
 - Critical systems are run at an alternate site
 - The production processing of the business does not stop.
 - Primary processing does not stop.
 - Most common type of recovery plan testing.
 - The test runs at the same time
- **Full-interruption**

- Normal production shut down, with real disaster recovery processes
- Plan is implemented as if it were a disaster
- Scary and can cause its own disaster, but best way to test completely
- A disaster is replicated even to the point where it ceases normal production operations.
- **The test SHOULD NOT disrupt normal business.**

❖ **Disaster Recovery Procedures**

➤ **Recovery team**

- **Implement the recovery procedures**
- **Get critical business functions operating at the alternate site**
- **Implement the recovery procedures in a disaster**
- **Get critical functions operating at backup site**
- **Retrieval of materials from off-site storage, backups, workstations**
- **Installs critical systems and applications**

➤ **Salvage Team**

- **Return the primary site to normal processing conditions**
- **Authority to declare when the site is resumptive or not**
- **Separate from recovery team**
- **Returns the primary site to normal operating conditions**
- **Safely clean, repair, salvage the primary processing facility**

➤ **Normal Operations Team**

- **Full procedures on how to return from the alternate site to the primary site**
- **Emergency is not over until all operations are back in full production**
- **Task of Recovery Team, or another separate team**
- **Returning production from the alternate site to the primary site**
- **Disaster is not over until all operations have returned to their normal location and function.**

➤ **Other recover issues-**

- **Interfacing with external groups**
 - **Municipal Emergency Groups, fire, police, ambulances, EMS.**
 - **Escalation and interaction should be included in the plan**
- **Fraud and crime**
 - **Fraudsters try to capitalize on the disaster**
 - **Vandalism and looting may occur**
- **Financial Disbursement**
 - **Expense disbursement**
 - **Signed and authorized checks will be needed**
- **Media relations**
 - **Define Methods of Dealing with Media**
 - **Important to have a well trained spokesperson.**
 - **Credible, trained, informed, spokesperson**
 - **Establish a unified organization response**
 - **Report your own bad news**
 - **Tell the story, quickly, easily and honestly**
 - **Maintain a mailing list for larger audiences**
 - **Identify emergency press conference sites in advance**
 - **Record events as the crisis evolves**

- Review and update the crisis communications plans and documents on a regular basis
- Consider follow-up communications to allow for fair and impartial reporting of the event
- **Employee Relations**
 - Inherent responsibility to employees and their families
 - Salaries must continue
 - Insurance must be adequate

➤ **End-User Disaster Contingency Planning**

- **It is important to provide functioning environment to End-Users after the disaster**
- **Who will notify users of the disasters ?**
- **Who will tell the users where to go when the disaster hit ?**
- **A TREE structure of managers can be developed**
- **The person at the TOP of the TREE Call Two managers**
- **The Two managers call THREE managers**
- **The THREE managers call THREE others until all managers are notified**
- **Each manager will notify peoples he is responsible for until everyone is notified**
- **One or two peoples must in charge of coordination**
 - Directing the users to new facility
 - Making sure they have necessary resources to complete their tasks
 - Being a liaison between the different groups