

Disaster Recovery Planning Process

(Edited from three-part series written by Geoffrey H. Wold and published in Disaster Recovery Journal in 2007)

Most businesses depend heavily on technology and automated systems, and their disruption for even a few days could cause severe financial loss and threaten survival.

The continued operations of an organization depend on management's awareness of potential disasters, their ability to develop a plan to minimize disruptions of critical functions and the capability to recovery operations expediently and successfully.

A disaster recovery plan is a comprehensive statement of consistent actions to be taken before, during and after a disaster. The plan should be documented and tested to ensure the continuity of operations and availability of critical resources in the event of a disaster.

The primary objective of disaster recovery planning is to protect the organization in the event that all or part of its operations and/or computer services are rendered unusable. Preparedness is the key. The planning process should minimize the disruption of operations and ensure some level of organizational stability and an orderly recovery after a disaster.

Other objectives of disaster recovery planning include:

- Providing a sense of security
- Minimizing risk of delays
- Guaranteeing the reliability of standby systems
- Providing a standard for testing the plan.
- Minimizing decision-making during a disaster

The three-part diagram illustrates the planning process. The methodology is described below.

1. Obtain Top Management Commitment

Top management must support and be involved in the development of the disaster recovery planning process. Management should be responsible for coordinating the disaster recovery plan and ensuring its effectiveness within the organization.

Adequate time and resources must be committed to the development of an effective plan. Resources could include both financial considerations and the effort of all personnel involved.

2. Establish a planning committee

A planning committee should be appointed to oversee the development and implementation of the plan. The planning committee should include representatives from all functional areas of the organization. Key committee members should include the operations manager and the data processing manager. The committee also should define the scope of the plan.

3. Perform a risk assessment

The planning committee should prepare a risk analysis and business impact analysis that includes a range of possible disasters, including natural, technical and human threats.

Each functional area of the organization should be analyzed to determine the potential consequence and impact associated with several disaster scenarios. The risk assessment process should also evaluate the safety of critical documents and vital records.

Traditionally, fire has posed the greatest threat to an organization. Intentional human destruction, however, should also be considered. The plan should provide for the “worst case” situation: destruction of the main building.

It is important to assess the impacts and consequences resulting from loss of information and services. The planning committee should also analyze the costs related to minimizing the potential exposures.

4. Establish priorities for processing and operations

The critical needs of each department within the organization should be carefully evaluated in such areas as:

- Functional operations
- Key personnel
- Information
- Processing Systems
- Service
- Documentation
- Vital records
- Policies and procedures

Processing and operations should be analyzed to determine the maximum amount of time that the department and organization can operate without each critical system.

Critical needs are defined as the necessary procedures and equipment required to continue operations should a department, computer center, main facility or a combination of these be destroyed or become inaccessible.

A method of determining the critical needs of a department is to document all the functions performed by each department. Once the primary functions have been identified, the operations and processes should be ranked in order of priority: Essential, important and non-essential.

5. Determine Recovery Strategies

The most practical alternatives for processing in case of a disaster should be researched and evaluated. It is important to consider all aspects of the organization such as:

- Facilities
- Hardware
- Software
- Communications
- Data files
- Customer services
- User operations
- MIS
- End-user systems
- Other processing operations

Alternatives, dependent upon the evaluation of the computer function, may include:

- Hot sites
- Warm sites
- Cold sites
- Reciprocal agreements

- Two data centers
- Multiple computers
- Service centers
- Consortium arrangement
- Vendor supplied equipment
- Combinations of the above

Written agreements for the specific recovery alternatives selected should be prepared, including the following special considerations:

- Contract duration
- Termination conditions
- Testing
- Costs
- Special security procedures
- Notification of systems changes
- Hours of operation
- Specific hardware and other equipment required for processing
- Personnel requirements
- Circumstances constituting an emergency
- Process to negotiate extension of service
- Guarantee of compatibility
- Availability
- Non-mainframe resource requirements
- Priorities
- Other contractual issues

6. Perform Data Collection

Recommended data gathering materials and documentation includes:

- Backup position listing
- Critical telephone numbers
- Communications Inventory
- Distribution register
- Documentation inventory
- Equipment inventory
- Forms inventory
- Insurance Policy inventory
- Main computer hardware inventory
- Master call list
- Master vendor list
- Microcomputer hardware and software inventory
- Notification checklist
- Office supply inventory
- Off-site storage location inventory
- Software and data files backup/retention schedules
- Telephone inventory
- Temporary location specifications
- Other materials and documentation

It is extremely helpful to develop pre-formatted forms to facilitate the data gathering process.

7. Organize and document a written plan

An outline of the plan's contents should be prepared to guide the development of the detailed procedures. Top management should review and approve the proposed plan. The outline can ultimately be used for the table of contents after final revision. Other benefits of this approach are that it:

- Helps to organize the detailed procedures
- Identifies all major steps before the writing begins
- Identifies redundant procedures that only need to be written once.
- Provides a road map for developing the procedures

A standard format should be developed to facilitate the writing of detailed procedures and the documentation of other information to be included in the plan. This will help ensure that the disaster plan follows a consistent format and allows for ongoing maintenance of the plan. Standardization is especially important if more than one person is involved in writing the procedures.

The plan should be thoroughly developed, including all detailed procedures to be used before, during and after a disaster. It may not be practical to develop detailed procedures until backup alternatives have been defined.

The procedures should include methods for maintaining and updating the plan to reflect any significant internal, external or systems changes. The procedures should allow for a regular review of the plan by key personnel within the organization.

The disaster recovery plan should be structured using a team approach. Specific responsibilities should be assigned to the appropriate team for each functional area of the company.

There should be teams responsible for administrative functions, facilities, logistics, user support, computer backup, restoration and other important areas in the organization.

The structure of the contingency organization may not be the same as the existing organization chart. The contingency organization is usually structures with teams responsible for major functional areas such as:

- Administrative functions
- Facilities
- Logistics
- User support
- Computer backup
- Restoration
- Other important areas

The management team is especially important because it coordinates the recovery process. The team should assess the disaster, activate the recovery plan, and contact team managers.

The management team also oversees, documents and monitors the recovery process. Management team members should be the final decision-makers in setting priorities, policies and procedures.

Each team has specific responsibilities that must be completed to ensure successful execution of the plan. The teams should have an assigned manager and an alternate in case the team manager is not available. Other team members should also have specific assignments where possible.

8. Develop testing criteria and procedures

It is essential that the plan be thoroughly tested and evaluated on a regular basis (at least annually). Procedures to test the plan should be documented. The tests will provide the organization with the assurance that all necessary steps are included in the plan. Other reasons for testing include:

- Determining the feasibility and compatibility of backup facilities and procedures
- Identifying areas in the plan that need modification
- Providing training to the team managers and team members
- Demonstrating the ability of the organization to recover
- Providing motivation for maintaining and updating the disaster recovery plan

9. Test the Plan

After testing procedures have been completed, an initial test of the plan should be performed by conducting a structured walk-through test. The test will provide additional information regarding any further steps that may need to be included, changes in procedures that are not effective, and other appropriate adjustments. The plan should be updated to correct any problems identified during the test. Initially, testing of the plan should be done in sections and after normal business hours to minimize disruptions to the overall operations of the organization.

Types of tests include:

- Checklist tests
- Simulation tests
- Parallel tests
- Full interruption tests

10. Approve the plan

Once the disaster recovery plan has been written and tested, the plan should be approved by top management. It is top management's ultimate responsibility that the organization has a documented and tested plan.

Management is responsible for:

- Establishing policies, procedures and responsibilities for comprehensive contingency planning.
- Reviewing and approving the contingency plan annually, documenting such reviews in writing

If the organization receives information processing from a service bureau, management must also:

- Evaluate the adequacy of contingency plans for its service bureau
- Ensure that its contingency plan is compatible with its service bureau's plan

Conclusion

Disaster recovery planning involves more than off-site storage or backup processing. Organizations should also develop written, comprehensive disaster recovery plans that address all the critical operations and functions of the business. The plan should include documented and tested procedures, which, if followed, will ensure the ongoing availability of critical resources and continuity of operations.

The probability of a disaster occurring in an organization is highly uncertain. A disaster plan, however, is similar to liability insurance: it provides a certain level of comfort in knowing that if a major catastrophe occurs, it will not result in financial disaster. Insurance alone is not adequate because it may not compensate for the incalculable loss of business during the interruption or the business that never returns.

Other reasons to develop a comprehensive disaster recovery plan include:

- Minimizing potential economic loss.
- Decreasing potential exposures
- Reducing the probability of occurrence
- Reducing disruptions to operations
- Ensuring organizational stability
- Providing an orderly recovery
- Minimizing insurance premiums
- Reducing reliance on certain key individuals
- Protecting the assets of the organization
- Ensuring the safety of personnel and customers
- Minimizing decision-making during a disastrous event
- Minimizing legal liability

Geoffrey H. Wold is the National Director of Information Systems and Technology Consulting for the CPA/Consulting firm of McGladrey & Pullen. He has written four books on disaster recovery planning.

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.