Disaster Recovery and Business Continuity Planning:

Testing an Organization's Plans

By Yusufali F. Musaji, CISA, CGA, CISSP

With the recent attacks on America and threats of terrorism suspected everywhere and anytime, the realization that order and chaos are correlative—to know one is to know the other—has come to unfold with stark reality.

The question then is not if it will happen but when it will happen.

Failure to prepare for it can give an otherwise ideal model a theoretical name and spell disaster for those associated with the discharge of its responsibilities.

The attacks on America have brought home the realization of the horrors of disaster when it strikes. Even though the components of a perfect disaster recovery plan may exist, at the time of crisis they could be rendered useless in a matter of minutes.

As the experience dictates, putting the pieces together is not just technology but involves people and communication and the recognition that any problems here can be solved only through superior personal leadership skills combined with positive, strategic communication and in troubleshooting tough, touchy, sensitive corporate communications issues. In a disaster, organizations face serious internal and external problems involving: community relations and grassroots campaigns, corporate relations failures, reputation threats, crisis communication management, employee relationship building, ethics/integrity/compliance, litigation visibility management, management communication strategies, media relations strategy and analysis, public affairs/exposure management, and more. The situations often involve conflict, controversy, community action or activist opposition.

In the aftermath of 11 September 2001, as organizations began to build through the process of responding, reconstructing, restoring and recovering, they realized that classic recovery planning that focused on how to restore centralized data centers was far from adequate for contemporary businesses. These plans did not address the need for continuous operation of key business processes in distributed computing environment. The requirements for continuous operations in an e-business, web-speed world are more complex and challenging. Web-based and distributed computing have made business processes too complex and decentralized.

Business continuity and disaster recovery are so vital to business success that they no longer remain a concern of the IT department alone. It is no longer sufficient or practical to vest the responsibility exclusively in one group. Business continuity must become the shared responsibility of an organization's entire senior management, from the CEO to line-of-business executives in charge of crucial business processes. Although IT remains central to the business continuity formula, IT management alone cannot determine which processes are critical to the business and how much the company should pay to protect those resources.

Information technology has become embedded in the fabric of virtually every aspect of a business. Computing is no longer something done in the background. Instead, critical business data can be found across the enterprise—on desktop PCs and departmental local area networks, as well as in the data center. The same information technology driving new sources of competitive advantage also has created new expectations and vulnerabilities. Key business initiatives such as enterprise resource planning (ERP), supply chain management, customer relationship management and e-business have made continuous, ubiquitous access to information crucial to an organization. On the web, companies have the potential to deliver immediate satisfaction or dissatisfaction to millions of people. Within ERP and supply chain environments, organizations can reap the rewards of improved efficiencies, or feel the impact of a disruption anywhere within their integrated processes.

Serious business interruptions are now measured in minutes rather than hours. Because electronic transactions and communications take place so quickly, the amount of work and business lost in an hour far exceeds the toll of previous decades.

Figure 1: Keys to Recovery

- Commitment of all team members, including senior managers who, by definition, are significant players on the recovery team
- Team approach—cooperation
- Realization that an organization's survival after a disaster is dependent on many interdependent issues and departments
- Concerted effort and financial resources

More difficult to calculate are the intangible damages a company can suffer: lower morale and productivity, increased employee stress, diverted resources and a tainted public image. What was once considered a "minor" problem—a faulty hard drive or a software glitch—can cause the same level of loss as a power outage or a flooded data center if a critical business process is affected. Even successes can bring about a business disaster. As a result, protecting critical business processes, with all their complex interdependencies, has become as important as safeguarding data itself. The risks are great, especially when companies operate in the 24-hour, seven-day-a-week e-business global environment.

The events of 11 September have forced organizations to review their disaster recovery plans, especially in light of new technology. Organizations have realized that virtually all information technology components, including distributed open systems, large mainframes, desktop and mobile personal computers and work group servers must interact seamlessly to ensure accessibility to the information deemed critical to their business.

Disaster recovery efforts of the past were designed to provide backup options for centralized data centers. Disaster recovery efforts of the present multivendor, multiplatform environment require a plan designed for integrated business continuity.

Nonetheless, the components to integrated business continuity are the same: recovery options for facilities, technology, network infrastructure and human skills. However, the key to business continuity lies in understanding one's business and determining which processes are critical to staying in that business and identifying all the elements crucial to those processes—specialized skills and knowledge, physical facilities, training and employee satisfaction as well as information technology.

The goal for companies with no business tolerance for downtime is to achieve a state of business continuity, where critical systems and networks are available no matter what happens. This means thinking proactively; engineering availability, security and reliability into business processes from the outset—not retrofitting a disaster recovery plan to accommodate ongoing business requirements.

Importance of Testing

Finally, organizations must make an executive commitment to regularly test, validate and refresh their business continuity and disaster recovery programs to protect the organization against perhaps the greatest risk of all—complacency.

There are two main reasons why organizations do not test their disaster recovery plans regularly. The first is complacency, i.e., "I don't need to test because my technical staff are committed to their role and will resolve all the problems when a disaster occurs."

The second reason is that the exercise is seen as too costly and too difficult to perform, i.e., "I cannot test the plan because there is no suitable system available to use in the test and the vendor will not make such a system available to me." This often is the case with organizations that have subscribed to an external service such as a cold site and a supplier agreement for replacement equipment, or hot site solution.

Testing Methods

With good planning, a great deal of disaster recovery testing can be accomplished with modest expenditure. The current operational system often is quite satisfactory for testing low-level tasks, such as backup and restore procedures.

There are four classes of tests:

1. **Hypothetical**—The hypothetical test is an exercise, first, to verify the existence of all necessary procedures and actions specified within the recovery plan and, second, to prove the theory of those procedures. It is a theoretical check and should be conducted regularly. The exercise is generally a brief one, taking approximately two hours to conduct, and is designed to look at the worst case for equipment, ensuring the entire plan process is reviewed.
2. **Component**—A component is the smallest set of instructions within the recovery plan that enables specific processes to be performed. For example, the process "System Load/IPL" involves a series of commands to load the system. However, in a recovery situation this may differ from normal operational requirements. Certain functions may need to be enabled or disabled to suit the new environment. If this is not fully tested, incompatibility problems with other components are likely. Component testing is designed to verify the detail and accuracy of individual procedures within the recovery plan and can be used when no additional system can be made available for extended periods.

   Examples of component tests include backup procedures; offsite tape storage recovery; technology and network infrastructure assembly, recovery and restoration procedures; and security package startup procedures.
3. **Module**—A module is a combination of components. The ideal method of testing is for each component to be individually tested and proven before being included in a module (some of these components may be performed and verified during normal daily operational activities). The aim of module testing is to verify the validity and functionality of the recovery procedures when multiple components are combined. If one is able to test all modules, even if unable to perform a full test, then one can be confident that the business will survive a major disaster. It is when a series of components are combined without individual tests that difficulties occur.

   Examples of module tests include alternate site activation, system recovery, network recovery, application recovery, database recovery and run production processing.
4. **Full**—The full test verifies that each component within every module is workable and satisfies the strategy and recovery time objective (RTO) requirements detailed in the recovery plan. The test also verifies the interdependencies of various modules to ensure that progression from one module to another can be effected without problems or loss of data.

   There are two main objectives associated with a full test:
   - To confirm the total elapsed time to establish that the production environment meets the RTO
   - To prove the efficiency of the recovery plan to ensure a smooth flow from module to module

   To achieve the first objective, a computer system of similar capacity and speed must be available for the estimated RTO as stipulated in the plan. This is not critical to achieving the second objective.

Depending on the size and complexity of the computer facility, it may not be appropriate to conduct all testing phases. Some may wish to omit the module tests and go directly to a full test, or it may not be possible to conduct a full test, in which case as many module tests as practicable should be performed.

Timings always should be recorded during each test, except the hypothetical test, to verify the RTO required to fully restore the system. If the result is outside the RTO stipulated in the plan, the plan and/or the recovery method would have to be reviewed.

Setting Objectives

Each test is designed around a worst-case scenario for equipment as this will ensure the entire plan is examined for all possible disastrous situations. For staffing, base tests are designed around best-case scenarios to ensure that all participants are involved and all available expertise is on hand to understand and resolve each issue in the process of building a complete plan. Appropriate personnel should note any weaknesses or opportunities to improve the plan for action.

Once confident that the recovery plan is effective, other scenarios for staffing can be tested, e.g., worst-case scenarios, to verify the procedures are complete and can be performed by less technical personnel.

Only when every requirement associated with each component has been documented and verified can the recovery plan be said to be complete and functional.

It is important that all aspects of the test are properly examined before a commitment is made to invoke the test. Because it is a test, some considerations will be necessary which perhaps would not be valid in a real disaster. For example, a test may require agreement with business units to prevent any impact to production, require all change control to be frozen for a period or require discussions with the building superintendent to ensure no power/air conditioning maintenance is planned. This may result in the test being rescheduled or conducted over a weekend. The last thing management or participants of the test want is for the test to be cancelled because a simple item has been overlooked. It then would be a waste of time, commitment and money.

Test objectives should include:

- Recovery of systems at the standby site, and establishment of an environment to enable full accommodation of the nominated applications
- A fully documented set of procedures to obtain and utilize offsite tapes to restore the system and critical applications to the agreed recovery point, as set out in the recovery plan
- Recovery of system/application/network/database data from the offsite/backup tapes
- Detailed documentation on how to restore the production data as stipulated in the recovery plan, to the agreed recovery point (e.g., start of day)
- Fully documented procedures for establishing communication lines/equipment to enable full availability and usage by appropriate areas (e.g., business units, data entry, users, etc.)
- Established communication lines/equipment as set out in the plan
- Examination of the designated alternative site and confirmation of all components are as noted in the plan

Defining the Boundaries

Test boundaries are needed to satisfy the disaster recovery strategy, methodology and processes. The management team also must consider future test criteria to ensure a realistic and obtainable progression to meet the end objectives. Opportunities to test actual recovery procedures should be taken wherever possible, e.g., a purchase of new/additional equipment, vendor agreements (use of hot site, loan of system at site or cold site). Management also must determine whether or not to include internal (auditors/management) or external (data security services) observers or a combination of both.

Scenario

The scenario is the description of a disaster and explains the various criteria associated with such a disaster. For example, the scenario should outline what caused the disaster and the level of damage sustained to the equipment and facilities, and whether or not anything can be salvaged from the wreckage. The purpose is not to get bogged down in great detail but to explain to all participants what is or is not available, what tools can or cannot be used, what the object of the exercise is, the time the disaster occurred and the planned recovery point.

[*Author's note:* The object of testing is to have a fully validated recovery plan. Testing should purposely not be made difficult during the initial phases. Complicated testing programs that previously have not been verified will only delay this objective and waste resources.]

Test Criteria

Not all tests will require all personnel to attend. The test "criteria advise all participants, including observers as appropriate, where they are to be located and the time/day the exercise will take place. The role of the observer is to give an unbiased view and to comment on areas of success or concern to assist in future testing.

Assumptions

Assumptions will need to be made. They allow a test to achieve the results without being bound by other elements of the recovery plan, which may not yet have been verified. Assumptions allow prerequisites of a particular component/module to be established outside the test boundaries. Examples include:

- All technical information documented in the plan, including appendices, are complete and accurate.
- All purchases (equipment/furniture, etc.) can be made in the RTO required.
- Tapes and other equipment recalled from offsite are valid and useable.

Test Prerequisites

Before any test is attempted, the recovery plan must be verified as being fully documented in all sections, including all appendices and attachments referenced to each process. Each of the participating teams in a test must be aware of how their role relates to other teams, when and how they are expected to perform their tasks, and what tools are permissible. It is the responsibility of each team leader to keep a log of proceedings for later discussion and action to prepare better for future tests.

Briefing Session

No matter whether it is a hypothetical, component, module or full test, a briefing session for the teams is necessary. The boundaries of the test are explained and the opportunity to discuss any technical uncertainties is provided.

Depending on the complexity of the test, additional briefing sessions may be required—one to outline the general boundaries, another to discuss any technical queries and perhaps one to brief senior management on the test's objectives. The size of the exercise and number of staff involved will determine the time between the briefing session(s) and the test. However, this time period must provide sufficient opportunity for personnel to prepare adequately, particularly the technical staff. It is recommended that the final briefing be held no more than two days prior to a test date to ensure all activities are fresh in the minds of the participants and the test is not impacted through misunderstandings or tardiness. An agenda could be:

- Team objectives
- Scenario of the disaster
- Time of the test
- Location of each team
- Restrictions on specific teams
- Assumptions of the test
- Prerequisites for each team

Checklists

Checklists provide the minimum preparation for all test types. Checklists are directly related to specific modules of the recovery plan and all sections relevant to a particular test must be verified as complete before a test date is set.

As these checklists follow the various modules associated with the recovery plan, only those parts applicable to the forthcoming test are compulsory prerequisites for that test. However it is recommended that all sections of the checklist be completed as soon as possible.

The following checklists show the detail required:

1. Documentation Checks

Maintaining currency of the documentation contained within the recovery plan is essential to the success of not only tests, but more importantly, to safeguard the recovery of critical business activities in the event of a real disaster. There are a number of important documents which need to be monitored, maintained and issued for testing and emergency situations, and they fall into two main groups:

■ General

- Prepare and maintain an annual test schedule.
- Regularly advise all teams of the test schedule.
- Maintain business impact information if applicable.
- Maintain documented test procedures.
- Maintain a floor plan of each team's location during tests.
- Maintain a supply of special forms (e.g., security, authorizations, checklists).

■ Plan

Review the recovery plan to ensure the following are maintained and current:

- Team objectives and responsibilities
- Team procedures
- Team actions
- All low-level procedures (components)
  - Operations procedures
  - Operations schedule
  - Application runbooks
  - Disaster recovery fallback runbooks
  - Network configuration diagrams
  - Escalation procedures
  - Contact list
  - Security logs/registers
  - Alternative site manual
  - System configuration
  - Storage requirements
  - Change control activities
  - Sequence of application recovery
- Critical applications
- Simultaneous updates of master and team recovery plans
- Test high-level flowchart (road map) master

2. System Module Checks

This is the first of the modules required to establish a system after a disaster. It covers the items necessary for staff to proceed once the hardware is installed and progresses to the point where application and/or database recovery can commence.

3. Network/Communications Module Checks

The first section, offsite tapes, forms a critical component of system recovery. An additional checklist under this heading also should be located in the applications/database module.

■ Offsite tapes

- Is there a regular review of backup procedures?
- Are critical files/records (e.g., backups) stored offsite on a daily basis?
- Are these tapes sent offsite immediately after creation?
- Is there a list of tapes required for each recovery step? Offsite?
- Can the tapes be retrieved from the offsite location in the required RTO?
- Are there any authorizations or passwords required to collect these tapes (e.g., can the designated person collect them?)?
- Is the process of getting tapes documented in the plan?
- Have people tested the process of obtaining tapes from the offsite location? How often? Without warning?

■ System

- Is there a listing of tapes to be used in the recovery of the system and all subsystems?
- Is this documented and is a copy offsite and in the plan?
- Do professionals know and understand the sequence of restoring the system?
- Is this documented in the plan?
- Have these procedures been tested/proven?
- Has this process been performed before—alone or assisting others?
- Are backup copies current (e.g., PTFs, fixes/patches, upgrade level, etc.)?
- Does one know the RTO to restore the system to recovery point as stated in the plan?
- Can the operating system be restored and is this documented in the plan?
- Can each subsystem be restored and is this documented in the plan?
- Does staff know what time and day it has to recover to (e.g., start of current day, end of previous day, midday, etc.)? Is this in the plan?
- Do recovery procedures reflect the correct backup tapes to be used (e.g., if recovering to SOD, the backup tapes will probably have the previous day's date)?
- Is recovery point known (e.g., SOD, EOD checkpoint recovery)? Is this documented in the plan?
- Can one recover the databases to the SOD? Is this in the plan?
- Can one forward recover the databases to the point of failure? Is this documented in the plan?
- Can one verify the integrity and currency of the databases?
- Who is to perform this task and is it documented in the plan?
- Does this person need to formally authorize this fact?
- Can one IPL the system and is it fully documented in the plan?
- Are these procedures accurate, i.e., can the appropriate manager use them to load the system?
- Are there any processes that are not included in the recovery plan? Why not?
- Has the vendor/supplier/maintainer checked and verified all procedures?
- Are there documented and verified procedures to:
  - Initialize disk drives
  - Restore system (reload)
  - Reboot from standalone backup
  - Perform restarts
  - Restore other libraries
  - Initialize catalogues
  - System startup
  - Application restore
  - Database restore
  - Set unit addresses
  - Perform restarts

4. Cold Site Checks

- Does everyone know the location of the recovery site?
- Have all those who will be located there visited the site?
- Has access to/from the location been checked?
- Is the equipment stated/contracted to be onsite actually there?
- Have people tested the equipment to verify it as fully functional?
- Are there procedures to invoke a DRP at this site?
- Does the site have a security system and do the appropriate persons know how to program/use it?
- Are all the cables, phones, power, telex, modems, etc., of the agreed type and quantity to meet recovery needs?
- Are the air conditioners, lights, phones and power functional?
- Is there sufficient floor/office space to meet needs?
- Have people checked the access for entry/exit of equipment and staff?
- Is there a diagram showing the network/system configuration and floor plan?
- Is there an emergency evacuation procedure of the site?
- Does the fire fighting equipment meet the required standards and has it been checked recently?
- Is all this documented in a site manual?
- Is there a copy of the site manual available?
- Does the site satisfy all recovery communications/network equipment needs?
- Is anyone else situated at this location?
- If so, are they totally isolated from your equipment/communications (e.g., cable moves, security risk, physical risk)?
- Is a method in place to check regularly the readiness of the facility?
- Are all critical consumables (special forms) located in controlled conditions and at multiple locations?

5. Third Party Hot Site Checks

- What peripheral equipment is required to meet disaster needs as stated in the recovery plan?
- What system size/capacity is required to run in disaster mode?
- Is the hot site equipment (e.g., system, peripherals, communications) compatible to the existing production site?
- What is the maximum RTO acceptable before one must commence the recovery process?
- Does the site have tape library facilities?
- Do professionals regularly review the site to check all these items?
- What will the status of the system be on occupation of the hot site (e.g., powered up/down, operating system, configured)?
- If powered up, what levels of release, patches, PTFs etc.?
- What procedures are in place to ensure the hot site system remains current?
- Have any tests been performed on this system at this site?
- Are there any special software licensing requirements when running at a second location under recovery mode?

6. Own Warm/Hot Site Checks

- Is there a DRP machine at this location?
- Is the system a development or second production machine?
- Is the system large enough to allow the DRP system and all its requirements to be loaded (e.g., CPU/disk capacity, tape/cart drives, speed to meet user satisfaction)?
- Do staff know which files/libraries should be removed from the DRP system to provide sufficient space?
- Does the organization wish to keep the data on the DRP machine and restore it after a test or actual disaster?
- If not, is there a plan to clear/prepare this system for testing and the actual disaster?

- Are there procedures to perform this clear (backup and delete)?
- Are there clean-up procedures for the DRP machine at the completion of the test, to enable return to normal processing?

Analyzing the Test

While testing is in itself beneficial, an effective recovery plan can be achieved only by constructive analysis of each test and its results through a postmortem. This also maintains the momentum gained from the test, which is critical in the process of building a workable plan. Many staff see disaster recovery as an additional workload. However, over time, through constructive and regular involvement, staff develop a greater commitment.

Debriefing Session

If the company has a dedicated DRP team or coordinator assigned permanently, this team or coordinator would have the responsibility of conducting the briefing and debriefing sessions. If not, then the responsibility lies with the command team leader.

The format is to discuss the results and findings of the test with a view to improving the recovery plan for future exercises. From these discussions, a set of objectives is developed for later inclusion into the report. An agenda could be:

- Overall performance
- Team performance
- Observations
- Areas of concern
- Next test (type and time)
- Test report

Each team leader has the responsibility of maintaining a log of events during each test. The information gathered from these logs, in addition to the postmortem report by the test manager, is used to produce a test report. Any areas of improvement are noted for action, assigned to an appropriate team member and given a realistic completion date. A typical format could be:

- Executive summary
- Objective results
- Performance
- Overall
  - – Teams
  - – List of actions

In conclusion, the methodology described will provide a good basis for creating tests to prove the accuracy and validity of the disaster recovery plan. Testing is essential if a plan is to keep pace with changes in technology and company objectives. Nonetheless, always remember that no test is considered a failure, as any information gained through an exercise such as this can only be of benefit, even if the objectives are not met.

In addition to the availability of test capacity necessary not to disrupt ongoing operations and simultaneously allow the ability to test and validate the recovery efforts, organizations must ensure sufficient latent capacity will be available immediately to assure rapid failover and recovery. To achieve this objective, organizations must house failover equipment in strategic locations away from the main production equipment and provide further redundancies, such as sourcing electrical supplies from different power grids and ensuring redundant network capacity dedicated to business continuity.

The ability to understand the integration of IT with business strategy and define the risks and impacts of a disaster to critical IT infrastructure is crucial to achieving this objective. So is an understanding of e-business dependencies and business critical requirements.

Organizations must establish and maintain relationships with vendors to assure quick delivery of replacement PCs, network hardware, desks, chairs, telephones, etc., in the event of a facility-wide disaster. All these activities require formal capital management systems that allow best practices, extensive experiences and up-to-the-minute procedures to be shared across a seamless interface to additional services and support across the organization. To make all these a reality, organizations have to invest in the human resources to acquire, train and retain skilled personnel who can and will manage the complex interdependencies and specialized elements of business continuity.

Self-audit

Those who do not learn from history will repeat history. Therefore, this simple self-audit should help assess one's readiness for business continuity and disaster preparedness.

1. Can you identify your critical business activities that satisfy your customers' expectations and support your overall business operations?
   Yes No

2. Can you identify the critical business information needed for these activities to succeed?
   Yes No

3. Do you have information on the frequency, impact and causes of downtime?
   Yes No

4. Does this information allow you to identify and rank your most vulnerable business activities?
   Yes No

5. Are your legacy systems and IT resources adequately protected against hacker intrusion and viruses?
   Yes No

6. Have you developed a checklist, by functional area, of what your organization will need to continue business effectively in the case of a disruption or emergency?
   Yes No

7. Have you and your IT colleagues been successful in placing business continuity on the board agenda?
   Yes No

8. Have you worked with your IT colleagues to develop an approved business continuity plan that accounts for all aspects of business continuity and recovery?
   Yes No

9. Is your business continuity plan regularly tested?
   Yes No

10. Do you have a change control process in place to keep your continuity plan current with process, organizational and technology changes?
    Yes No

11. Are you confident that if a disaster were to strike this very minute, your organization could recover quickly and smoothly to prevent damage to your business?
    Yes No

Yusufali F. Musaji, CISA, CGA, CISSP
is the founder, director and president of Ali's N Y Consulting, Inc., an IT and financial consulting firm specializing in computer consulting. Yusufali's experience embraces the full spectrum of financial, operational and IT disciplines required of state-of-the-art organizations. His functional and technical areas of expertise include financial system development and implementation and computer security. He is widely published in IT, financial and security journals regarding IT/user relationships, and he has developed numerous business continuity and disaster recovery plans. His book, *Auditing and Security, AS/400, NT, UNIX, Networks and Disaster Recovery Plans* was published by John Wiley in January 2001. His upcoming book, *Auditing the Implementation and Operation of ERP Systems,* will be published by John Wiley in early 2002.