Disaster Recovery in the Business Enterprise

Michael Morfoot

Information Security Capstone Project 68-595

April 2009

Abstract

Disaster recovery plans are becoming a key part of a business's overall IT planning process to ensure the continuous availability of the business's critical infrastructure at all times. This thesis is a discussion of the process and procedures that an enterprise business may take. It will also provide some examples of why disaster recovery is important, who should be involved in the process, and how some of the processes and procedures can be implemented.

Table of Contents

Introduction	Page 4
Initiation Phase	Page 7
Risk Analysis Phase	Page 9
Creation and Implementation Phase	Page 17
Testing Phase	Page 27
Maintenance Phase	Page 31
Putting it all together	Page 32
Appendix A	Page 34
Appendix B	Page 35
Appendix C	Page 38
Appendix D	Page 47
Appendix E	Page 50
References	Page 53
Further Technical Details	Page 55

Introduction

Companies doing business today must be aware of the need for Disaster Recovery. There are endless possibilities in which a disaster can occur. Some of these possibilities are natural disasters, hackers, and disgruntled workers. There are many more causes of disasters, but regardless of the cause, the event must have a negative consequence on the business's ability to maintain their operations. All organizations should prepare for possible emergency situations, and should consider what type of back-up and preventive strategies would be appropriate for each aspect of their activities. [1] In this paper, I will discuss the various aspects regarding Information Technology Disaster Recovery (IT-DR). This includes the definition of Disaster Recovery, the reasons it is needed, and the process that should be followed. I will also expand upon these ideas using real world examples.

What is disaster recovery? Disaster recovery can be defined as the process, policies, and procedures relating to the preparation for recovery and continuation that needs to be taken for business continuity after a disaster occurs. It is also part of a larger process called Business Continuity Planning (BCP).

Why is Disaster Recovery needed? The answer to this question is that it always has been. What placed Disaster Recovery in the forefront was the New York twin tower disaster that occurred on September 11, 2001. After that event, there were many businesses that

suffered greatly as they had no disaster recovery plan and they could not recover quickly. The 9/11 disaster also had an effect on other businesses around the United States. One such example is Job Store Inc. This Denver based company was going strong as a staffing agency until 9/11. After 9/11, the economy got so bad that the owner Dorothy Grandbois, the owner, had to delay her retirement, restructure the company, and lay off 20 employees. [2]

As stated before, disaster recovery is a process. This process varies from business to business, but all of them seem to have the same common components. They are the initiation phase, the risk analysis phase, the creation and implementation phase, the testing phase, and the maintenance phase.

The first phase is the Initiation phase. This phase is where the scope of the plan is determined. It is also the phase where executive endorsement and approval is required, the planning teams are formed, and resource requirements, schedules and timetables are defined.

The second phase is the Risk Analysis phase. In this phase, there are 3 objectives. They are to identify the risks, analyze the vulnerabilities and prioritize them, and make recommendations for the next phase (Creation) based on the risks.

The third phase is the Creation and Implementation phase. This is where the plan is created by following a few simple rules. The first rule is that there must be authority at all steps in the plan. This means that there is a clear flow of authority during a catastrophe. The second rule is that the plan must have a clear set of processes and procedures that need to be

followed. The third rule is that the plan needs to be easily accessible at anytime in case of a disaster.

The fourth phase is the Testing phase. This phase requires that the process, procedures and policies are fully tested. This testing allows for plan effectiveness, auditing, and benchmarking. It also allows a run-through of the plan, allowing any discrepancies to found and corrected.

The final phase is that of Maintenance. The maintenance phase helps to keep the Disaster Recovery plan current. This is important as change is inevitable. If the plan becomes outdated, then its ability to be effective is greatly diminished.

Initiation phase

The initiation phase sets the tone for the entire project. There are many parts which make up this phase and each part is unique to each business, but there are a couple of parts which are universal. These universal parts are:

- **Establish scope and objectives**

  The scope and objectives of any DR plan must be identified. This includes the systems, applications and network environments that will be included within the review. At this point in time, management may already have a RTO (Recovery Time Objective) and RPO (Recovery Point in Objective) in mind. However, the risk analysis phase should not be stopped or skipped as a result of the Business/Sponsor thinking that they've already established a RTO/RPO. [3]

- **Obtain executive/management support**

  It is essential that the IT-Disaster Recovery organization has Executive Management support or sponsorship. But, just as essential, the Business must also have an Executive Sponsor for the initiative. This sponsor will be the individual who can assist with identifying and articulating the impact(s) if the system/application were unavailable.

- **Form the team and establish roles and responsibilities**

  Depending upon the organization, Disaster Recovery may be a department within the company or it may be a Disaster Recovery consulting firm that is engaged. Either way, their

responsibility is to assist and facilitate the creation of the Disaster Recovery plan. The DR Coordinator is the facilitator between the Business units defining their requirements and the Technical/Support teams design and delivery of an end product. If an outside consulting firm is creating the Disaster Recovery plan, then a project manager from within the company should be assigned.

- **Identify available resources**

Many companies have a formal resource allocation or demand management process that must be followed in order to have a resource assigned. Resources from all divisions, including IT, must be assigned in order to keep the project on track.

- **Create a schedule**

A schedule will need to be created and should include each one of the phases discussed within this paper. The schedule or project plan can often times be used as a repeatable process in the future. It should be noted that when creating a schedule during the initiation phase, the expectation should be set that after the requirements and initial design build have been produced, the project plan or schedule is subject to change, as new information may have come to light during these stages.

Risk Analysis Phase

This phase is when vulnerabilities are identified. A security assessment needs to be performed. The assessment is then analyzed and recommendations are made. A planned framework can then be developed. It is important to assess the organizations potential areas of exposure to identify the preparedness and preventive measures in place at any point in time. This is because one of the many goals of disaster recovery is to ensure the safety of personnel, customers, and assets during and after a disaster.

There are 2 categories of disaster prevention. They are procedural prevention and physical prevention. Procedural prevention includes the activities performed on a daily, monthly, or annual basis that relate to security and recovery. The objective is to define the activities necessary to prevent various types of disasters and to ensure that they are performed regularly. Some of these activities may include:

- **Briefing of all personnel on security and disaster processes and procedures**

  Policies and processes should be kept in a repository or where all users have access to them. It is best practice to review procedures on an annual basis with all participants that have a role in the DR process. Additionally, each team should have their own specific set of procedures that they will follow. Often times, this is called an Incident Response or Crisis Communication Response document.

- **Backups of data, programs, and software on tape or disk**

All critical data, programs and software should be backed up onto a form of media. Tape backup has been the traditional method for performing these backups, but, most recently, there has been a change in direction toward disk. This can be attributed to numerous risks associated with tape media including: bad media, poor tape handling processes and reliability of tape. Over the years disk has become more economical and easier to cost justify compared with tape media.

- **Rotation, Retention and Transportation of backup's offsite**

Standard procedures should be implemented which clearly state the rotation, retention and transportation process for backups. Rotation refers to the act of swapping media so that you have multiple backups on multiple media. The rotation method will depend upon the retention period required. The retention period is the time that the media needs to be kept in case of a disaster. Normally, the media is reused after its retention period. It should also be transported off-site to a secure location. All three of these components are critical to the success of a Disaster Recovery event. Many products also have best practice standards available that should be reviewed when evaluating a product. Additionally, there must be a procedure implemented which states the backups that will be taken to the Recovery Site. This is now an important factor because often times the retention period is dictated by legal, compliance or audit regulations and all of the backups retained are not necessarily needed when recovering a system.

- **Performing preventive maintenance procedures on various equipment**

Preventative maintenance on equipment should be performed routinely. This not only includes the physical aspects of the equipment but also upgrades, releases and patches.

- **Developing and implementing emergency procedures for threats**

As previously stated, there are numerous risks and threats that each organization is exposed to. Some are based on natural occurrences or location, and others are based on the type of business that is established. Procedures should be developed and implemented to address the most probable threats and disasters that can occur. This is directly associated with an Incident Response plan as well.

- **Testing of the emergency procedures**

Testing of emergency procedures is best practice within the Disaster Recovery and Business Continuity industry. Often times, testing can be required from an audit and regulatory perspective as well. There are various forms of testing that can be performed depending upon the plan that has been established. Some of those include table top exercises, testing within a duplicated environment but one that is separate from production, and failing production systems over to disaster systems.

Physical prevention and preparedness for a disaster include special requirements for building construction, as well as the safety and protection of assets, records and personnel. Some of the points that need to be addressed are:

- **Computer area**

The computer area should be evaluated for both structural deficiencies as well as man-made risks. This can include implementing standards such as preventing food and water from being allowed within the computer area.

- **Computer room floor**

Most facilities now have regulations that must be followed regarding depth and space below a computer room floor. It should provide enough capacity for wiring, cabling, electrical and the like. Additionally, it is best practice to have the computer room floor be constructed so that if there is a small amount of standing water, the equipment is not affected.

- **Furniture and equipment**

Furniture placement and misuse can sometimes be attributed to disaster recovery events. A common example would be furniture and equipment not being installed properly and damage resulting from equipment falling.

- **Fire and water detection**

Fire and water detection systems within a data center environment are considered best practice. These systems will provide notification to an Operator or designated individual of an issue. Furthermore, fire suppressant systems are also highly recommended.

- **Records**

Record maintenance and storage should be addressed as a part of any disaster recovery solution. Just as with tape or disk backups, critical records should be evaluated and process implemented for rotation and retention of critical records off-site.

- **Temperature Control**

Air and heating systems are essential and must be maintained in order to support a stable environment. An environment that is too hot or cold will not only prevent equipment from performing at its optimal rate but can also damage components, media, and data.

- **Electrical supply systems**

Electrical supply systems should be built with redundancy. This can include installation of UPS, batteries, and generators. Power loss is a common threat across the globe and should be accounted for within any disaster recovery plan. Furthermore, one should evaluate the electrical feeds that come into the facility and identify whether the power is coming from separate sub-stations.

- **Security Systems**

Physical Security systems should be established within a data center environment. This will assist with keeping unauthorized personnel from entering the computer area. This will also prevent individuals who have the intent to perform harm within the environment as well as individuals who are unaware of precautions that should be taken in this type of environment. [4]

In order to address the preparedness of the organization, a Disaster Prevention Checklist may be used. The checklist is designed to assist the user in identifying and addressing the key security and control issues which affect disaster prevention and recovery planning. In the risk assessment process the probability of a disaster occurring should be determined. A disaster could be classified as natural, technical, or human.

Once a risk assessment is formed that identifies the major risks that a company could be exposed to, a Business Impact Analysis (BIA) should be conducted. A Business Impact Analysis is a tool used to identify the impact that a disaster would have on a Business unit. There are several common components that are typically included within a BIA. They are:

- **Financial Impact**

  The Financial Impact is often defined as potential loss or harm to monetary expenditures and receipts. This is any potential monetary loss that a company could exhibit such as profit loss, interest loss, fees, fines, penalties, portfolio management, fee income, or financial liabilities. The organization should determine how they will calculate financial impact. This can be derived from gross revenue loss, profit loss, fines/penalties, etc. A standard should be established in order to ensure that all users completing a BIA are being consistent.

- **Legal Impact**

  Legal impact is often defined as the requirement to comply or adhere to laws, ordinances, statutes, SLA's, and contract agreements. Examples include purchasing or vendor

agreements, customer SLA agreements, real estate/leasing contracts, and government laws and regulations (e.g. PCI, HIPAA, SOX).

- **Customer Service Impact**

Customer Service is often defined as the services provided to any customer (both internal and external) in an effort to support their need or business. Customer Service refers to activities performed before, during and after a customer purchase or provided service. This can include internal and external customers or employees. External examples include performing customer sales, and looking up customer information. Internal examples include performing or processing employee information requests such as benefit adjustments, insurance claims and other internal data (like email and payroll records).

- **Reputation/Brand Image Impact**

Reputation and Brand Image are often defined as how a company is perceived by customers, media, outside organizations and employees. Reputation can be associated with the company's achievements, attainments, integrity, trustworthiness, reliability, customer focus, etc.

Confronting the Process

The business impact analysis (BIA) is designed to ensure a thorough understanding of the vital business functions and systems within an organization. [5] For very large organizations, the BIA process can become very overwhelming and it is suggested that the process be divided into

several sections. The first section would most likely include Security and Authentication Systems. The second section would include Enterprise Wide applications. Any subsequent sections should be determined based on the type and focus of the business. Depending on the type and focus of the business, more sections could be added. A couple of examples could include HIPAA or PCI sections.

The BIA should have inherent logic built within it that helps identify an overall impact based on all components. Additionally, Executive Management should establish an "all encompassing" threshold or "line in the sand", which states that if "x" impact is reached, then the Application/System is critical, less-critical or non-critical. To expand upon this concept, a grading system needs to be designed so that the common components can be evaluated depending on the "importance" to the company. An executive decision will need to be made regarding the importance of each component. For example, the financial component may be deemed more important to the company than the reputation component. The management would then fill out a "scorecard" and that would be added up. The total would then fall into a certain range which would determine the strategy (explained in the next section) used in the Disaster Recovery process. Upon completion of the BIA process, one should be able to identify the applications/systems that are critical to the business.

Creation and Implementation Phase

The Creation and Implementation phase is divided into two parts. The first part deals with the solution design and creation. The goal is to identify the correct disaster recovery solution that meets the criteria from the risk analysis phase. A few strategies that can be used for in-house computer departments are:

- **Mirrored or Replicated Sites**

  Mirrored or replicated environments reference the transfer of data or information from one system to another. This can be implemented for backup data (data libraries), equipment configurations, and software. Mirrored or replicated sites are usually implemented when an RTO or RPO can not be met with an alternate solution such as a hot site or warm site.

- **Hot sites**

  Hot sites refer to a facility that has the infrastructure established such as electricity and cabling. Typically there are key components or equipment that have been installed and are ready to be used. However, the data/information is not at the facility yet.

- **Warm sites**

  Warm sites refer to a facility that is partially built from an infrastructure or equipment perspective. This type of solution would require some time and effort but not nearly the amount of time involved in establishing a cold site.

- **Cold sites**

  Cold sites refer to facilities that do not typically have all necessary equipment or infrastructure in place. This type of solution would require time and effort at the time of disaster to get up and running.

Many IT Recovery departments select between 2 and 4 of these strategies and assign them a Tier Recovery Category that is then associated with a Recovery Time Objective (RTO). For example:

Tier 1 - Mirrored Recovery Plan provides dedicated electronic storage for mirroring data at predetermined intervals along with a dedicated server(s) and network environment. The Recovery Time Objective for this system is one day.

Tier 2 - Hot Site (Core Systems) Recovery Plan provides the computer(s), telecommunications, and environmental infrastructure required to recover critical business functions or information systems. This plan is implemented when backups and additional provisioning, software or customization is performed. The Recovery Time Objective for these systems is between 2–7 days.

Tier 3 - Warm Site (Supporting Systems) Recovery Plan provides a processing site which is equipped with some hardware, and communications interfaces, electrical and environmental conditioning which is only capable of providing backup after additional

provisioning, software or customization is performed. The Recovery Time Objective for these systems is between 8–14 days.

Tier 4 - Cold Site (Alternate/Permanent Systems) Recovery Plan provides an alternate facility that already has in place the environmental infrastructure required to recover critical business functions or information systems, but does not have any pre-installed computer hardware, telecommunications equipment, or communication lines. These must be provisioned at time of disaster by the organization or a third party recovery provider. The Cold Site is planned using an alternate company site or permanent site. The Recovery Time Objective for these systems exceeds 15 days.

Many of these solutions can be created at a 3rd party recovery provider site. Mobile Recovery Units are also very common. A company would establish written or verbal agreements with the Vendor to provide comparably capable equipment within a certain timeframe. Although this strategy does not require much in-house involvement, there are a few disadvantages. Some of these disadvantages are shipping delays, high costs, testing difficulties, and outdated equipment. Additionally, these agreements are often in the form of contracts, which may come at a high cost to the Business. Some of these concerns, such as outdated equipment, can be addresses through proper budgeting and contractual guarantees from the provider. A cost benefit analysis should always be performed in an effort to determine the most fiscally responsible strategy over several years. Some of these concerns,

such as outdated equipment, can be addressed through proper budgeting and contractual guarantees from the provider.

The second part of this phase deals with the implementation and execution of the disaster recovery plan. During this part, the plan can be tested to ensure its effectiveness. Problems can be identified and the plan can then be modified.

During the creation and implementation phase, additional requirements will need to be flushed out. Most often, the following departments will need to be involved in order to secure an accurate IT-Disaster Recovery plan:

- Operations (includes Media and Tape Operations)

  The operations department will manage and support hardware requests, production jobs and media management activities during the recovery. They will coordinate the shipment of Disaster Recovery software, tapes and recovery instructions to the recovery site.

- Network

  The network department will establish data network communications and connectivity between the company site, contracted recovery site and third party service companies. They will support restoration of the data center, servers and desktop computers.

- Database Architecture

The Database Architecture department will recover the systems databases and applications of the affected servers.

- SAN Administration

  The SAN administration department will setup and maintain the storage architecture. They will assist in the recovery of data in the event of a disaster.

- System Administration

  The system administration department will recover and maintain the operating systems.

- IT-Compliance/Audit/Security

  The compliance, audit and security departments will maintain proper network and system security infrastructures to protect the company. They will administer the reinstatement of system ID's and access as needed to support continuation of critical business and recovery activities.

- IT-Applications

  The application department will recover and validate the recovery of the affected application(s).

Within the design and execution phases, there are 2 sets of Core Deliverables that should be developed. They are Functional and System Components. Below are examples of each:

Functional DR Plan Components

- **Hardware Recovery Plan**

A hardware recovery plan includes the hardware components that are necessary in a recovery. This typically includes the footprint, space and equipment specifications. Instructions needed to install or establish the equipment are included in this component.

- **OS/Software Recovery Plan**

An OS or software recovery plan includes the Operating System and necessary software that is necessary in a recovery. Often IT departments back up their OS and software onto a server. It should be determined how you will access that OS/Software if that server is a part of the disaster. These servers are often referred to as NIM servers. There are products available (i.e. Sysback) that assist in recovering the OS and file systems. Instructions need to be established that include how to install, load, set up or configure these pieces.

- **Database Recovery Plan**

A database recovery plan includes instructions on how to recover the database and archive logs if necessary.

- **Storage Recovery Plan**

A storage recovery plan includes how to establish and set up the SAN or Storage Area Network. Systems that contain test and production data can often be separated so that only production data is restored onto the SAN at time of disaster. The RAID level should also be

pre-determined and documented within the recovery plan. Another consideration is the speed of the disks and what is required during a disaster. Often times, companies will accept lower speed disk drives during a disaster because it is more cost effective.

- **Application/Data Recovery Plan**

An application and data recovery plan includes instructions on how to restore the application data, how to "sync" the data from one system up to another system in the event that the backups were taken at different times, and test cases for validating that the correct and most current data was restored.

- **Change Management**

Technology and our environments are constantly changing. Often times this can lead to invalid disaster recovery plans, contracts, instructions, etc. It is crucial to ensure that the team managing the disaster recovery plans is involved in the change management process. This includes applications, database, network, hardware, etc...

- **Management of Dependencies/Interfaces**

As noted above, environments are constantly changing and being enhanced. Users are always looking for a better way to access and control their data. In an effort to prevent duplicity of data across systems, often times systems interface and depend upon one another. For example, rather than maintain an employee database within the company's payroll system and another employee database within the user id management system, (which would be a duplication of employee data), the employee database becomes its own

entity, and the payroll and user id systems interface with the employee database. Maintaining an understanding and properly documenting those interfaces is critical to a DR plan.

- **Contracts**

Often times, companies establish contracts with third party vendors for software, equipment, and services during a disaster. Because environments change greatly (see change management), it is imperative that any contracts are also kept up-to-date.

- **Testing**

Testing procedures and plans are necessary to ensure that all components have been recovered successfully and are working harmoniously. Testing must be performed for the periods before, during, and after the implementation of the plan. To perform a test before the implementation, a thorough and structured walk-through should be performed to identify any foreseeable issues that may arise. Testing during the plan's implementation allows for any issues to be found and corrected during the process and testing after the implementation allows the business to verify any issues with the completed plan.

System Components

- **Network Architecture**

Network Architecture, whether it is wide-area network, local-area network, or tiny-area network is a critical component within any DR plan.

- **DNS**

Organizations utilize DNS (Domain Name System) to translate names into IP addresses and direct traffic to the appropriate system. Depending upon the size of recovery or organization, you may be able to modify a systems host table rather than recovering DNS.

- **Third Party Vendors**

Third Party Vendor plans should be established in the event that a) your company has a disaster, or b) their company has a disaster. Depending upon the vendor and various regulations, the vendor may require dedicated hardware, infrastructure or may require that the equipment be owned and maintained by them. These details should be determined prior to a disaster event and documented.

- **Backup and Vaulting Process**

The backup and vaulting process is crucial as an organization will not have any data to recover if performed properly. Recovery Point Objectives are based off of the backup and vaulting process. An RPO is the point in time that you want to recover your data. In laymen's terms, "how much data can you afford to lose"? This is very different from an RTO, which is "how long will it take to recover the system". The business owners should be able to identify how much data they can lose and this is often determined on how or if they can re-enter the data that would be lost.

- **Authentication/Login**

Authenticating to a system or logging into a system is often times maintained on a separate system. Active Directory is currently a major initiative across organizations now and falls into this category. The IT team can recover the critical systems, but if the users can't access the data because they can't log in, then your disaster recovery plan has failed.

- **Firewalls & IDS**

Firewalls are often critical components, as they maintain a level of security within your disaster environment. If the security is required in production, then most often it is required in a long term disaster scenario. This should be reviewed with the IT-Security and IT-Compliance departments.

All of the documentation should come together to formulate an overall Disaster Recovery Plan. Depending upon the organization and the infrastructure established, these components may vary from company to company. However, once the core components are identified, one should realize that if one component is out of place or invalid, it can affect the entire Recovery Plan and impact the organizations ability to recover the system.

Testing Phase

The reason this phase is necessary is due to the fact that a disaster recovery plan is only good when it is implemented correctly. A false sense of security may occur as the plan is drafted, but not actually tested to verify whether it works or not. There are a few major points that need to be addressed during this phase.

- Effectiveness

  For the plan to be effective, the goal it must accomplish is for the business to continue with little to no disruptions.

- Auditing

  Auditing from time to time shows that the business is keeping their disaster recovery plan in workable order.

- Benchmarking

  Benchmarking calls for collecting data so that it can be analyzed and used to evaluate the plan's effectiveness. The data collected may include time, cost or resources.

- Dry Run

  Completing a dry run allows for the team members to actually see how their roles would be implemented and how the processes and procedures will work.

Testing procedures vary depending upon the organization. There are many different formats business's can take. Some of these formats are checklist testing, structured walk-through testing, simulation testing, and full interruption testing.

Checklist testing is a techniques that business's use to identify key components of the disaster recovery plan and make sure that they are current and available. Examples of key components might be emergency phone numbers, supplies at the backup site and copies of the recovery plans.

Structured walk-through testing is a verbal walk-through of the specific steps of the process as documented in the plan. The purpose of this testing is to identify the plan's weaknesses and its effectiveness. It has been recommended to use both the checklist test and the structured walk-through test so that any modifications to the plan can be determined before performing more extensive testing.

Simulation testing is a technique used that simulates a disaster during non-business hours. This is to ensure that it does not conflict with normal business operations. For this testing, it may not be practical or economical to accomplish all tasks in the plan. These tasks may include major equipment moves and extensive travel. Simulation testing should identify:

- Purpose
- Objectives

- Types of tests
- Timing
- Scheduling
- Duration
- Participants
- Assignments
- Constraints
- Assumptions
- Test steps

The testing should also adequately test the hardware, the software, personnel, data and voice communication, procedures, supplies, documentation, transportation, utilities and alternate site processing.

Parallel testing requires the recovery team to take historical transactions and process them against the backup files to determine whether the team can obtain identical results. An important step is to make sure to compare the reports at the alternate site with the actual reports for verification.

Full-Interruption testing is the activation of the total recovery plan. It can be expensive and disruptive to normal business operations and should be approached with caution. This test is an extremely thorough test as the primary site is shut down and the recovery plan is implemented. [4]

Maintenance Phase

The maintenance phase is where the changes take place that are needed when modifying the disaster recovery plan. The plan is tweaked in order to better streamline the processes and procedures in the event of any issues that may arise. Over time, businesses change directions, needs, personnel, technologies, applications, and reporting timelines. Due to these factors, the disaster recovery plan must also change to reflect them. Change controls are a very important part of this phase. It is considered good business practice to adhere to a strict change control procedure. Changes need to be well-documented and stored in secure locations. There are numerous products within the industry that will track changes made within the infrastructure and provide reporting capabilities for review (LDRPS, Remedy). These tools are very effective if you find the change management process is not being adhered to. The disaster recovery plans should be considered "living" documents. It should be kept up-to-date to ensure its effectiveness. [6]

Putting It All Together

Now that I have presented the many various concepts regarding disaster recovery, I will explain how to put them together using the documents presented in the appendixes. Of course, the first step is the initiation phase. As explained earlier, this phase is where the scope is determined, teams are formed, requirements are identified and schedules and timetables are formed.

The Risk Analysis phase is next. It's during this phase that the form on Appendix A is used. This is a risk assessment form. It is used to determine the impact and severity of risks to the business that may occur. Appendix A uses 4 categories. They are the likelihood of the event, the impact on staff/property, impact on the business, and insurance coverage of the risk. The first category, likelihood of event, has 3 event ratings that it can be given. They are 0 (no event), 1 (rare event), 2 (occasional event), and 3 (frequent event). The next two categories use the rating type of impact. The impact rating types are 0 (no impact), 1 (limited impact), 2 (substantial impact), and 3 (full impact). The last category uses the rating type of coverage. The coverage types are 0 (no coverage), 1 (limited coverage), 2 (substantial coverage), and 3 (full coverage). After this form is filled out, it can be used to identify the more dangerous risks to the business.

After Appendix A is complete, Appendix B can then be started. Appendix B is the business impact analysis questionnaire. The questions on this form get very specific as they assist in telling the impact a disaster will have for each business unit and their applications and

systems. Since the BIA can be fairly long, it may be broken down into smaller sections. Appendix C and Appendix D can be combined into Appendix B, but some organizations like to get more granular and separate the applications impact from the systems impact. Appendix C contains questions regarding the applications assessment and Appendix D contains questions regarding the systems assessment.

Now that all the forms have been filled out and the disasters and impacts identified, the third phase (creation and implementation) begins. Using the knowledge gained from the assessments, the teams can more accurately create and design the disaster recovery plan.

For the testing phase, Appendix E can be used as a guide. This form gives great examples of questions that should be answered in order to better evaluate the plan. It can also be used for the next phase, maintenance.

The final phase is maintenance. This is the phase where changes to the disaster recovery plan are made. This should be done on an annual basis in order to keep the plan's processes and procedures current. It should also be evaluated quarterly in case any changes do occur. All the changes should be made and documented. A "maintenance" log should be filled out so that the changes are recorded. This log should also document who made the changes and why they were made.

Appendix A

RISK IDENTIFICATION AND RATINGS

Risks	Likelihood of Event 0 = No Event 1 = Rare Event 2 = Occasional Event 3 = Frequent Event	Impact on Staff/Property 0 = No Impact 1 = Limited Impact 2 = Substantial Impact 3 = Major Impact	Impact on Business 0 = No Impact 1 = Limited Impact 2 = Substantial Impact 3 = Major Impact	Insurance Coverage of Risk 0 = No Coverage 1 = Limited Coverage 2 = Substantial Coverage 3 = Full Coverage
Bomb				
Civil Disorder				
Prolonged IS Failure				
Single-Points-of-Failure				
Dam Failure				
Drought				
Earthquake				
Electrical Failure (Bldg)				
Electrical Storms				
Fire				
Flood/Flash Floods				
HAZMAT – Fixed Facility				
HAZMAT -				
Human Error				
Hurricane/Tropical				
Labor Dispute/Strike				
Landslide				
Power Failure (Area)				
Radiological -- Facility				
Radiological – Transp.				
Telecom Failure				
Tornado				
Transp. - Air/Rail				
Water Leaks				
Wildfire				
Wind				
Winter Storm (Severe)				

[7]

Appendix B

BUSINESS IMPACT ANALYSIS QUESTIONNAIRE

Respondent Information

Prepared By: _____ Date: _____

Department:_____

Process Name: _____

Interview Participant(s): _____

Systems Support Liaison: _____

BIA Questions

Process Description: _____

_____

1. Please list the computer applications systems upon which this business process is reliant:

Supporting Applications	Platform (Desktop, Server, Internet)

2. Frequency of Process activity/performance

   ❒ Continuous ❒ Daily ❒ Weekly ❒ Monthly ❒ Quarterly ❒ Yearly

   ❒ Other (Describe)_____

3. Identify periods when performing this Process or accessing this data is especially critical.

   ❒ Daily ❒ Weekly ❒ Monthly ❒ Quarterly ❒ Yearly

4. Are there any periods of high volume? ❒ Yes ❒ No If yes, please identify.

   _____

   _____

5. Outage Tolerance (i.e. 24 hours, 2 days, 1 week, etc.) _____

6. Importance of Process (circle only one) **1** **2** **3** **4**

1 = Mission critical, absolutely essential for Company to remain operational (24 Hrs or less)

2 = Significant impact on the Company; Process will become critical soon (2-7days)

3 = Some Impact on the Company; Process could become critical later (8-14 days)

4 = Process has little or no impact on the Company (15 days or more)

7. Describe the impact on business if this function/process cannot be performed

HIGH=$100,000

MEDIUM=$50,000 TO $99,999

LOW=UP TO $49,999

Monetary Impact (PER DAY)	% Loss of Public Image/Customer Confidence	Obligations	Recovery Expenses	Effect Public & Employee Safety/Health
☐ High ☐ Medium ☐ Low	☐ High **(15+)** ☐ Medium **(10-14)** ☐ Low **(0-9)**	☐ Contractual ☐ Regulatory ☐ Legal ☐ Labor	☐ Yes ☐ No	☐ Yes ☐ No

8. Indicate estimated actual losses per Outage Periods

Outage Periods	Monetary Impact	Loss of Public Image/Customer Confidence	Obligations	Recovery Expenses	Effect Public & Employee Safety/Health
24 HOURS					
2-7 DAYS					
8-14 DAYS					
15 DAYS (+)					

9. Do you have documented alternate or manual processing or recovery capability? _____

- ♦ If yes:
  - Are your associates trained to perform alternate processing?_____
  - How long would it take to implement? _____
  - Would an increase in staffing be necessary to maintain a minimum workflow? _____
  - How long can this alternate procedure be used?_____

- ♦ If no, why not?

_____

_____

_____

10. Identify other Departments/processes that send or receive items/information relating to this process:

Receive Item/Information From: ***Send Item/Information To:***

Item/Information	**From**	**Item/Information**	**To**

_____

_____

_____

11. List any Legal/Regulatory ties to this process: _____

_____

_____

_____

_____

12. Other special considerations/comments:_____

_____

_____

_____

_____

[8]

Appendix C

Applications Assessment

Respondent Information: Please complete one questionnaire for **each** application.

Application Name: _____

Application Type: **Real Time** ☐ **Batch** ☐ **Both** ☐

Name of Responder: _____

Title of Responder: _____

Supervisor of Responder: _____

Phone Number:

Scope: Your Company Business Continuity Project

The purpose of the Applications Assessment Questionnaire is to determine the criticality to the company of a computer based application and the losses which may be incurred if this application was not available for a period of time. This questionnaire is designed to collect the information necessary to support the development of alternative processing strategies, solutions, and IS Recovery Plans

NOTE – Special Instructions:

1. If the Application is "real-time", complete all questions under General Information and Section 1. Real-Time Environment (Online) Questions.
2. If the Application is "batch", complete all questions under General Information and Section 2. Batch Environment Questions.
3. If the Application is BOTH "real-time" and "batch", answer ALL questions in this questionnaire.

General Information

List all Business Users of this application:

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

General Information (continued)

If this is a vendor software package, what release is installed in production?

_____

What is the Service Level Agreement (SLA) for this application?

_____

Has this application been recovered at an off-site location as a test or in support of production?

☐ Yes ☐ No

If yes, what took place? _____

How long did it take? _____

Has a recovery plan been developed for this application? ☐ Yes ☐ No

If yes: When was the last time it was reviewed? _____

When was the last time it was updated? _____

When was the last time it was tested? _____

Are multiple staff members trained in using this plan? ☐ Yes ☐ No

Is there existing documentation for this application? ☐ Yes ☐ No

If yes, is it up to date? ☐ Yes ☐ No

Does the documentation conform to Corporate Standards? ☐ Yes ☐ No

Are there Operational Recovery Procedures for daily outages? ☐ Yes ☐ No

Is there an offsite copy of all application documentation? ☐ Yes ☐ No

Where is the location? _____

Are there known legal liabilities associated with this application? ☐ Yes ☐ No

If yes, what are they? _____

Has this application been audited in the last 3 years? ☐ Yes ☐ No

If yes, by Internal Audit? ☐ Yes ☐ No When?

By government regulators? ☐ Yes ☐ No When?

General Information (continued)

Answer the following about the source code for this application:

What is the library name the source code is stored in? _____

Where is the source code stored? _____

How often is the source code backed up? _____

What is the media being used for the backup? (i.e., Tape, Disk) _____

Where is the backup stored? _____

Who is responsible for the backup? _____

Complete Only the Applicable Sections

Real-Time Environment (Online)

What is the production hardware/platform and operating system? _____

What is the physical location of hardware/platform? _____

What is the run-time environment? (i.e., Java, Oracle) _____

Application Security Control:

At what level is the security access granted? (i.e., application, network sign-in) _____

Who is responsible for granting security rights to the application? (i.e., security, application team, user) _____

Database Information:

Database Name	Database Type (DB2, Oracle, etc)	Location

Are transaction logs being utilized? ☐ Yes ☐ No

If yes, please explain? _____

Real-Time Environment (Online) (continued)

Complete this section only for databases that are unique to or updated by this application

Database Backup and Recovery Information

Are full database backups being performed? ☐ Yes ☐ No

If no, Are incremental backups (logs) being utilized? ☐ Yes ☐ No

When was last full DB backup performed? _____

Will forward recovery be performed on lost databases? ☐ Yes ☐ No

List any specialized utilities being used to assist with backups/recovery? (i..e., BMC software, etc.)

_____

Can application processing continue during the backup process? ☐ Yes ☐ No

Are the backup procedures documented? ☐ Yes ☐ No

Are the recovery procedures documented? ☐ Yes ☐ No

Are they in a recovery plan? ☐ Yes ☐ No

What is the backup schedule? ☐ Daily ☐ Weekly ☐ Monthly

Other: _____

If Tapes are being used:

Are there multiple copies of the backup tape(s)? ☐ Yes ☐ No

Where is the Primary tape(s) stored? _____

Where are the Secondary tape(s) stored? _____

What is the vaulting rotation schedule? ☐ Daily ☐ Weekly ☐ Monthly

Other: _____

Real-Time Environment (Online) (continued)

Where is the off-site vault located?

_____

How long does it take to recover the databases from tape?

Database Name	**Time**
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

If Disk is being used:

What is the method being utilized? (I.e., disk mirroring, etc.)

_____

Where is the backup hardware located?

_____

Printing Requirements

Printer Type	Location
_____	_____
_____	_____
_____	_____

Identify any special forms that are needed and special print instructions:

Forms	Instructions
_____	_____
_____	_____
_____	_____

Real-Time Environment (Online) (continued)

Dependencies:

What are the internal dependencies? (i.e., applications, databases, etc.)

_____

_____

_____

_____

_____

What are the External Dependencies? (i.e., Vendor Services)

_____

_____

_____

_____

_____

Batch Environment

Identify all batch job names and when they execute:

Batch Job Names	Execution Cycle
Sample: JOB XYZ	*Daily*

What is the production hardware/platform and operating system?

What is the physical location of hardware/platform?

What is the run-time environment? (i.e., Java)

Dependencies:

What are the internal dependencies? (i.e., other jobs or applications)

What are the External Dependencies? (i.e., Vendor Services)

Batch Environment (continued)

Application Security Controls:

Who is responsible for granting security rights to the application? (i.e., IS, Security, application team, user) _____

When production problems are encountered or recovery of the application/data is required:

What type of ID is required? (i.e., administrator, productions ID, fire call ID) _____

Database Information:

Database Name	Database Type (DB2, Oracle, etc)	Location

Are transaction logs being utilized? ☐ Yes ☐ No

If yes, please explain? _____

List all critical files that are backup up:

File Name *Sample: ABC File*	When **Daily**	Media Tape

If Tapes are being used:

Are there multiple copies of the backup tape(s)? ☐ Yes ☐ No

Where is the Primary tape(s) stored? _____

Where are the Secondary tape(s) stored? _____

What is the vaulting rotation schedule? ☐ Daily ☐ Weekly ☐ Monthly

Other: _____

Where is the off-site vault located?

_____

If Disk is being used:

What is the method being utilized? (I.e., disk mirroring, etc.)

_____

Batch Environment (continued)

Where is the hardware located?

_____

Backup of flat files or directories:

What utility is being used to perform this function (i.e., Copy, BMC Utilities, etc.)?

_____

Batch Printing Requirements

Provide the information for printers being utilized by this business process:

Printer Type	Location	LAN Printer	RTO
_____	_____	☐	_____
_____	_____	☐	_____
_____	_____	☐	_____
_____	_____	☐	_____
_____	_____	☐	_____

Provide the information for any pre-printed forms that are being used for any group (LAN) printers for this business process:

Form	Print Instructions	Location of Instructions	Copy of Forms Stored Off-site
_____	☐	_____	☐
_____	☐	_____	☐
_____	☐	_____	☐
_____	☐	_____	☐
_____	☐	_____	☐

[9]

Appendix D

Systems Assessment

Respondent Information: Please complete one questionnaire for **each** platform/server for each Company location.

Platform Server Name (Mainframe, Unix, Win/NT): _____

Server Location: _____

Name of Responder: _____

Title of Responder: _____

Supervisor of Responder: _____

Phone Number:

Scope: Your Company Business Continuity/Disaster Recovery Project

The purpose of the Systems Assessment Questionnaire is to determine the criticality to the company of a computer, hardware/Servers and the losses that may be incurred if this system was not available for a period of time. This questionnaire is designed to collect the IS information necessary to support the development of strategies, solutions and recovery plans.

It is designed to collect all information required to identify, inventory and categorize all platforms/hardware. Please **single focus** on one platform/server per questionnaire. This will be the rule even if other platforms/servers are an exact duplicate.

General Information

What is the operating system and release level installed on this server? _____

What is the Service Level Agreement (SLA) with Your Company Customers for this server? _____

What executive software resides on this server? (i.e., hardware/system monitors. Java, Oracle)

_____

_____

Is this hardware on a UPS system? ☐ Yes ☐ No

Where is the computer room located for this hardware? _____

List all additional attached hardware (i.e., disk drives, tape drives, etc).

Hardware Type	Hardware Name
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

General Information (continued)

Server Security Control:

At what level is the security access granted? (i.e., server, network sign-in, administrator) _____

What applications run on this server?

_____

_____

_____

_____

_____

_____

What databases reside on this server?

_____

_____

_____

_____

_____

_____

_____

Has this server been recovered at an **off-site location?** ☐ Yes ☐ No

Has this server been recovered **as a test or in a production site**? ☐ Yes ☐ No

If yes: Explain what took place? _____

How long did it take? _____

Has a recovery plan been developed for this server? ☐ Yes ☐ No

If yes: When was the last time it was reviewed? _____

When was the last time it was updated? _____

When was the last time it was tested? _____

Are multiple staff members trained in using this plan? ☐ Yes ☐ No

Server Backup and Recovery Information

Who is responsible for the backup of the server? (i.e., Group or person)_____

Can application or database processing continue during the backup process? ☐ Yes ☐ No

Are the backup procedures documented? ☐ Yes ☐ No

If yes, where? _____

List any specialized utilities being used to assist with backups/recovery? (i.e., BMC software, etc.):

_____

_____

In order to restore, are there any dependencies requirements? (i.e., SMS servers or Firecall ID, etc.)

_____

_____

Are full server backups being utilized? ☐ Yes ☐ No

If yes, what is the backup schedule? ☐ Daily ☐ Weekly ☐ Monthly Other: _____

If no, explain the process being used, data being backed up, and the backup schedules? _____

If tapes are being used:

What is the vaulting rotation schedule? ☐ Daily ☐ Weekly ☐ Monthly Other: _____

Are there multiple copies of the backup tape(s)? ☐ Yes ☐ No

Where are the Primary tape(s) stored? _____

Where are the Secondary tape(s) stored? _____

What is the vaulting rotation schedule? ☐ Daily ☐ Weekly ☐ Monthly Other: _____

Where is the off-site vault located? _____

If disk is being used, what is the backup method (i.e. disk mirroring)?_____

Where is the off-site location? _____

Other Information

Single-Points-of-Failure

Are there any single-points-of-failure (i.e., technology or human) that needs to be explained?

☐ Yes ☐ No

If yes, please explain? _____

[10]

Appendix E

Testing the disaster recovery plan

In successful contingency planning, it is important to test and evaluate the plan regularly. Data processing operations are volatile in nature, resulting in frequent changes to equipment, programs, and documentation. These actions make it critical to consider the plan as a changing document. Use these checklists as your conduct your test and decide what areas should be tested.

Conducting a recovery test

Item	Yes	No	Applicable	Not Applicable	Comments
Select the purpose of the test. What aspects of the plan are being evaluated?					
Describe the objectives of the test. How will you measure successful achievement of the objectives?					
Meet with management and explain the test and objectives. Gain their agreement and support.					
Have management announce the test and the expected completion time.					
Collect test results at the end of the test period.					
Evaluate results. Was recovery successful? Why or why not?					
Determine the implications of the test results. Does successful recovery in a simple case imply successful recovery for all critical jobs in the tolerable outage period?					
Make recommendations for changes. Call for responses by a given date.					
Notify other areas of results. Include users and auditors.					
Change the disaster recovery plan manual as necessary.					

Areas to be tested

Item	Yes	No	Applicable	Not Applicable	Comments
Recovery of individual application systems by using files and documentation stored off-site.					
Reloading of system tapes and performing an IPL by using files and documentation stored off-site.					
Ability to process on a different computer.					
Ability of management to determine priority of systems with limited processing.					
Ability to recover and process successfully without key people.					
Ability of the plan to clarify areas of responsibility and the chain of command.					
Effectiveness of security measures and security bypass procedures during the recovery period.					
Ability to accomplish emergency evacuation and basic first-aid responses.					
Ability of users of real-time systems to cope with a temporary loss of on-line information.					
Ability of users to continue day-to-day operations without applications or jobs that are considered noncritical.					
Ability to contact the key people or their designated alternates quickly.					
Ability of data entry personnel to provide the input to critical systems by using alternate sites and different input media.					
Availability of peripheral equipment and processing, such as printers and scanners.					
Availability of support equipment, such as					

air conditioners and dehumidifiers.					
Availability of support: supplies, transportation, communication.					
Distribution of output produced at the recovery site.					
Availability of important forms and paper stock.					
Ability to adapt plan to lesser disasters.					

[11]

References

[1] "The Disaster Recovery Guide - Getting Started." The Disaster Recovery Planning Guide: A-Z Business Continuity Plans. 05 Apr. 2009 < http://www.disaster-recovery-guide.com/backup.htm>.

[2] "Recovery slow for many after 9/11 - Denver Business Journal:." Bizjournals | National Business News. 05 Apr. 2009 <http://www.bizjournals.com/denver/stories/2002/09/02/story1.html>.

[3] "What is the difference between RPO and RTO (from a backup perspective)?" Data storage technology and management resources - SearchStorage.com. 12 Apr. 2009 <http://searchstorage.techtarget.com/generic/0,295582,sid5_gci1212112,00.html>.

[4] Wold, Geoffrey H., and Robert F. Shriver. Disaster Proof Your Business A Planning Manual for Protecting a Company's Computer, Communications & Records Systems and Facilities. Chicago: Probus Professional Pub, 1991.

[5] Devlin, Edward S. Crisis Management Planning and Execution. Boca Raton: AUERBACH, 2006.

[6] "Security Series: Disaster Recovery Tactics that Ensure Business Continuity (Part 1 of 6)." Network Security Articles for Windows Server 2003, 2008 & Vista. 05 Apr. 2009 <http://www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part1.html>.

[7] Harris, Norm, and Tracy Cowan. Risk Assessment. Digital image. 14 Jan. 2004. Harris Recovery Solutions Inc. 13 Mar. 2009.

[8] Harris, Norm, and Tracy Cowan. Business Impact Analysis Questionnaire. Digital image. 14 Jan. 2004. Harris Recovery Solutions Inc. 13 Mar. 2009.

[9] Harris, Norm, and Tracy Cowan. Applications Assessment. Digital image. 14 Jan. 2004. Harris Recovery Solutions Inc. 13 Mar. 2009.

[10] Harris, Norm, and Tracy Cowan. Systems Assessment. Digital image. 14 Jan. 2004. Harris Recovery Solutions Inc. 13 Mar. 2009.

[11] "Help -." IBM Support & downloads - United States. 15 Apr. 2009 <http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzarm/rzarmtestdisarecplan.htm&tocNode=toc%3Arzahg%2Fi5os%2F17%2F0%2F5%2F28%2F10%2F>.

Further Technical Resources

"How Important is a Disaster Recovery/Business Continuity Plan to your Corporation?" Toolbox for IT - Knowledge Sharing Communities. 05 Apr. 2009 <http://it.toolbox.com/blogs/cio-it-strategy/how-important-is-a-disaster-recoverybusiness-continuity-plan-to-your-corporation-28542>.

"Disaster Recovery Dos & Don'ts: How to plan for worst-case scenarios." Network Management: Covering today's Network topics. 05 Apr. 2009 <http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci835644,00.html>.

"Get a secure grip on continuity planning." Network Management: Covering today's Network topics. 05 Apr. 2009 <http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci831131,00.html>.

Business Contingency Preparedness - Disaster Mitigation and Contingency Planning. 05 Apr. 2009 <http://www.businesscontingency.com>.

Myers, Kenneth N. Total contingency planning for disasters managing risk ... minimizing loss ... ensuring business continuity. New York: Wiley, 1993.

Ulmer, Robert R. (Ray), Timothy L. Sellnow, and Matthew Wayne Seeger. Effective Crisis Communication Moving From Crisis to Opportunity. Minneapolis: Sage Publications, Inc, 2006.