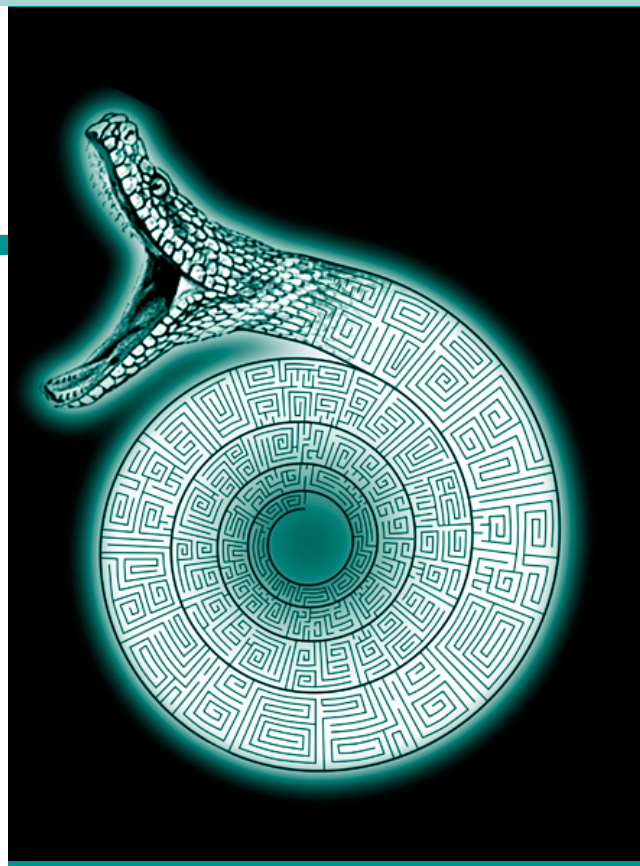
Disaster Recovery

and Business Continuity Step-by-Step

Version 2.0
October 2002



SANS PRESS

TABLE OF CONTENTS

A Survival Guide For Developing And Maintaining Business Continuity And Disaster Recovery Plan

An action plan for making sure your business operations and IT systems remain operational in the event of a disaster. A consensus of expert security practitioners.

Editor:
Mark T. Edmead, CISSP, SSCP, TICSA
MTE Software, Inc.

This document is the joint product of computer security professionals from corporations, government agencies, and educational institutions. These people recognize the importance of making sure business operations can continue to operate after a major disaster. They also understand that part of the process of developing and maintaining business continuity and disaster recovery plans involves an intimate understanding of critical business operations, processes and systems, and how their inoperability can affect the financial stability of the organization.

The SANS Institute enthusiastically applauds the work of these professionals and their willingness to share the lessons they have learned and the techniques they use to help develop and maintain business continuity and disaster recovery plans.

Michael Arata, CISSP
John C. A. Bambenek, EYT, Inc.
Arno Brok, CISA, P&O Nedlloyd
Richard Caasi, University of California, San Diego
Steve Davis, Principal, DavisLogic
Lee E. Defibaugh, CBCP, SRA International, Inc.
Rob Dodson, CISSP, USAR
Matthew Elias, Disaster Recovery Coordinator, Annuity Board of the Southern Baptist Convention
Stan Gatewood, CISSP, University Southern California
Ken Mac Garrigle, Department of Veterans Affairs
Danny Harris, Aon Corporation
Michael H. Huggins, CISSP/CTOC USN(ret), Independent Consultant
Ted Ipsen, CISSP, KPMG LLP
Murray E. Jennex, Ph.D, P.E. San Diego State University/Foundation for Knowledge Management
Gary Johnson, ISP, CISSP, Petro-Canada
Thomas J. Martin, CBCP, Booz-Allen-Hamilton
Andrea Morin, CPCB, Resourcigent
Michael D. Nickle, Verisign Consulting
Stephen Northcutt, The SANS Institute
Mayer Nudell, CSC, Specialized Consulting Services
Jim Orr, IT Security Manager, Raytheon Aircraft Company
Gal Shpantzer, Protection Consulting
Noel Taitt, Merck & Co. Inc
Louis C. Tinto, CISA, Corporate Audit, First Data Corporation

PREFACE

One of the great sources of productivity and effectiveness in the community of computer professionals is the willingness of active practitioners to take time from their busy schedules to share some of the lessons they have learned, and the techniques they have mastered. Most of the sharing takes place through online news groups, web postings, and presentations at technical conferences. Those who are able to take the time to scan the newsgroups, surf the web, and attend the meetings benefit immensely from this wealth of information.

SANS' Step-by-Step series raises information sharing to a new level in which experts share techniques they have found to be most effective. They integrate these techniques into a step-by-step plan and then subject the plan, in detail, to the close scrutiny of other experts. The process continues until consensus is reached. A large number of people spend a great deal of time making sure the information is pertinent, accurate, and timely.

We hope that you enjoy our Business Continuity/Disaster Recovery Planning: Step-by-Step Guide. We look forward to your suggestions for improvement.

INTRODUCTION

Sometimes it takes a drastic and catastrophic event to force us to re-examine our way of doing things. This is the case with the terrorist attacks of September 11th, 2001. The images of this event will stay in our minds forever. Not only did these attacks take human life, but they also had a profound, direct effect on over 400 businesses that had assets in the World Trade Center. My good friend lives and works near the WTC; a few days after the attack, he called me to ask if I had room on my Web server for his company's Web site. While his company was not located in the WTC itself, their offices were a few blocks away. Their building lost power, telephone, water, and Internet connectivity.

As we momentarily set aside the sorrowful human element, we must look anew at our organizations' business continuity and disaster recovery posture. We perform more thorough business impact assessments to determine our truly critical assets and review our procedures for prevention, response, and recovery. The disaster of September 11th put business continuity and disaster recovery plans through the ultimate test. Some organizations were prepared, and they will survive. Those organizations that were not prepared for the worst have had a much more daunting task to perform. How can you be prepared for a disaster or a disruption to your business? What can you do to prevent this from happening to you? As the saying goes, "Plan for the worst, and hope for the best." In this guide, we present two complementary methodologies that can be implemented to help minimize the effects of a disastrous event: the Business Continuity Plan (BCP) and the Disaster Recovery Plan (DRP).

While you might hear these two terms used interchangeably, they actually address two different concerns. The Business Continuity Plan addresses an organization's ability to continue functioning when normal operations are disrupted. In essence, it addresses the continuity of the critical business functions. The BCP might include other plans such as: disaster recovery, end-user recovery, contingency, emergency response, and crisis management plans. A BCP, by definition, is an all-encompassing "umbrella" term covering both disaster recovery planning and business resumption planning. A DRP, on the other hand, is a document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals. Specifically, the DRP is used for the advanced preparation and planning necessary to minimize the impact of damage caused by the disaster, and helps to ensure that an organization's critical information systems remain available during the disaster.

A year has passed since the September 11, 2001 attacks. The question to ask is: "what have we learned?" Right after September 11th many companies initially began to look at their own BCP/DRP procedures to determine if they were vulnerable to the effects of a disaster. Unfortunately, as time went by, the business continuity efforts began to lose focus. Other priorities emerged. The need for developing or maintaining a BCP/DRP document was no longer a paramount concern. That is, until the next disaster occurs.

The business continuity/disaster recovery plans are living documents that will change as your business needs change. Hopefully, you will never have to put these plans into place. By developing and implementing these plans, however, you will at least be prepared in the event of a disaster to resume business operations as quickly and efectively as possible, thus increasing the likelihood of business survival.

Mark T. Edmead, CISSP, SSCP, TICSA
October 2002

Benefits of a Business Continuity/ Disaster Recovery Plan

There are many benefits to developing and implementing a business continuity/disaster recovery plan. Here are just a few:

- Allows your organization to avoid certain risks or mitigate the impact of unavoidable disasters by
  - Minimizing potential economic loss
  - Decreasing potential exposures
  - Reducing the probability of occurrence
  - Improving the ability to recover business operations
- Helps minimize disruption of mission critical functions – and recover operations quickly and successfully – in the event of a crisis by
  - Reducing disruptions to operations
  - Ensuring organizational stability
- Assists in identifying critical and sensitive systems
- Provides for a pre-planned recovery by minimizing decision making time
- Eliminates confusion and reduces the chance of human error due to stress reactions
- Protects your organization's assets and employees
- Minimizes potential legal liability
- Reduces reliance on certain key individuals and functions
- Provides training materials for new employees
- Reduces insurance premiums
- Satisfies regulatory requirements, if and where applicable

REMARKABLE STATISTICS

The best way to understand the importance of having an effective plan is to look at the various statistics for those companies that experienced a disaster event and did not have a BCP/DRP plan in place.

- According to a Gartner study, two out of five companies that experience a disaster will go out of business in five years.
- A 3M study done in 1995 showed that in the course of "normal business operations", 30% of computer users spend one week per year reconstructing lost data.
- According to a case study article published by the Association for Information Management Professionals (ARMA) and published in the magazine InfoPro, most businesses experience 2 hours of downtime per week. The table below summarizes some of the other survey statistics.

CAUSE OF INTERRUPTION	% OF US COMPANIES THAT HAD BUSINESS OPERATIONS INTERRUPTED
Power Outages	72.2%
Computer hardware problems	52.2%
Software problems	43.1%
Human error	34.4%
Telecommunications failure	46%

TOP BUSINESS CONTINUITY PLANNING MISTAKES

A well-developed and executed BCP/DRP plan is the first step, but it does not end there. Regardless of the effort put into its development, the BCP/DRP plan will undoubtedly require modification as omissions and errors found during development and testing must be addressed. The development of the BCP/DRP takes a lot of time and planning. Here are some common planning mistakes to avoid:

1. **Blindly relying on BCP** — Many organizations believe that just having the BCP is enough. The BCP is only marginally useful without adequate updating, testing, and training.
2. **Limiting scope** — An incomplete BCP plan will not address all of the corporate needs for recovery. The BCP plan needs to cover business processes, systems recovery, back office functions, and the replacement of key personnel, if needed.
3. **Lack of prioritization** — There is a need to prioritize the key business processes. The risk is to prioritize less-than-critical processes instead of the ones crucial for business survival.
4. **Lack of plan updates** — The BCP should be updated periodically, especially when there are significant system or business process changes.
5. **Lack of ownership** — Someone with the power to lead, influence, prioritize, and organize the BCP is instrumental to the success of the program
6. **Lack of communications** — There is a need for clear and precise communication with employees, contract employees, vendors, business partners, and clients.
7. **Lack of security controls** — During the recovery process, security controls can be disregarded, resulting in a greater risk of exposure.
8. **Lack of Public Relations planning** — Companies often fail to consider customer, public and investor relations and the need to communicate the effective means being implemented to get the organization back on track.
9. **Inadequate insurance** — Some companies lack adequate insurance coverage, and fail to support the filing of insurance claims which result in delayed or reduced settlements.
10. **Inadequate evaluation of vendor suppliers** — Many companies poorly evaluate recovery products (hot site, cold site, and planning software), relying on vendor-supplied information. This often leads to a solution that may not adequately address a company's needs.
11. **Lack of business support** – Business continuity and disaster recovery is not just an IT issue. All functional business process groups need to be involved in the risk and business impact analysis stages.

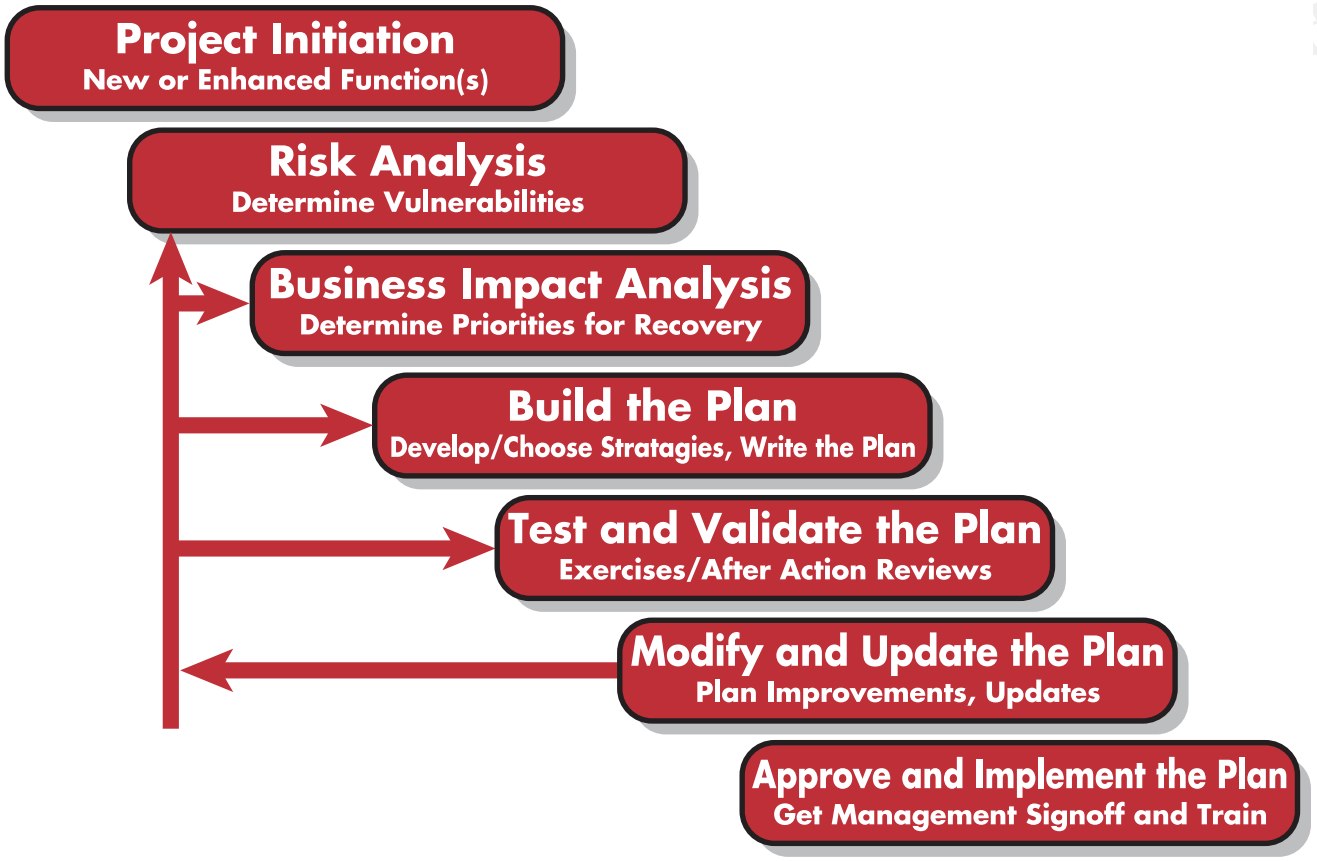
STAGES IN AN INCIDENT

In the world of incident handling, a disaster is considered to be an incident of the highest magnitude. This list is a good guide to understanding the stages of an incident, and the steps to take:

1. **Preparation**
   a. Establish a good security policy
   b. Establish a good business continuity and disaster recovery plan
   c. Set procedures in place to prevent incidents from happening
   d. Determine BCP/DRP approach
2. **Identification**
   a. Once there is an indication of an incident, someone needs to be assigned
   b. Need to determine if it is really a disaster
   c. Coordinate with rest of BCP/DRP people
   d. Notify proper authorities
3. **Containment**
   a. If there has been a disaster, secure the area
   b. Determine if you should continue operations
4. **Eradication**
   a. Determine the cause of the disaster
   b. Could the disaster be avoided in the future?
   c. If you need to re-build the system, make sure not to reintroduce the same problem
5. **Recovery**
   a. Restore the original system
   b. After the disaster, is it safe to return?
   c. Monitor the recovered system closely
6. **Lessons Learned**
   a. Write the follow-up report for your team and for management
   b. Review findings with team
   c. Determine the lessons learned and areas of improvement
   d. Use this information to revise/update the documents

THE STEP-BY-STEP PROCESS FOR BCP/DRP

The consensus among experienced business continuity planners divides the process into seven phases: project initiation, risk assessment, business impact analysis, building the plan, testing the plan, plan modification, and plan acceptance and implementation.



PHASE 1 PROJECT INITIATION

The first step in developing a business continuity/disaster recovery plan is obtaining management approval.

Action 1.1 Obtain commitment from management

Obtaining management approval affirms the value of the plan and ensures cooperation between the business units, documents management's responsibilities, allocates the budget, sets goals and expectations, demonstrates importance of plan, and sets a precedent for employee support throughout the organization.

Action 1.2 Collect materials in support of your plan

It is a good idea to collect historical documentation in order to help convince management to support the BCP/DRP development effort. Collect news articles or publications that discuss the need for BCP/DRP plans, and how companies are affected if they do not have such plans in place. Illustrate the problem. If you can graphically show them the effects of the disaster, it might help management understand the problem and support the BCP/DRP development effort. Refer to Appendix A for a list of BCP/DRP related links that can be used to provide data to support the BCP/DRP development effort.

Action 1.3 Identify objectives and goals

Before tackling the task of writing the BCP/DRP plan, it is recommended that the business requirements be identified.

The business requirements might include the following:

- Minimize interruptions to business
- Resume critical operations within a specified time
- Minimize financial loss
- Maintain positive image during and after the crisis

Depending on the business environment, there might also be a need to identify external requirements for government, industry, and legal needs.

Action 1.4 Identify the person in charge of the BCP

While there might be many people and/or groups involved in the BCP/DRP process, only one person should have overall responsibility for its timely development. This person is typically called the Business Continuity Plan Leader. The BCP Leader's responsibilities include the following:

- Lead in the definition of objectives, policies, and critical success factors
- Coordinate, organize, and manage the BCP project
- Provide a point of contact and coherent message throughout organization
- Oversee the BCP project through effective control methods and change management
- Present the project to management and staff
- Develop project plan and task level budget allocations
- Define and recommend project structure and management
- Manage the process
- Monitor plan implementation
- Plan and lead training on the plan
- Periodically review the plan

Action 1.5 Establish a Business Continuity Plan task force

Throughout the development of the plan, it is beneficial to create a task force, or business continuity working group, to coordinate the activities involved in the development of the plan. All pertinent areas of the organization should be represented by an individual that is knowledgeable with their element of the business process. For example, a typical organization might have representation from departments including accounting, payroll, legal, customer service, production, distribution, information technology, shipping and receiving, facilities, security and human resources. Representation will vary depending on the composition of the organization and critical business functions represented in the BCP/DRP.

As the plan evolves, the task force and Business Continuity Plan Leader will usually be responsible for identifying and assigning personnel to various teams for response and recovery tasks. Some of the typical teams and their duties include the following:

- **Continuity Plan Coordinator** - Manages the process and coordinates the various teams.
- **Senior Management Team** - Approves the plan, allocates budget and sets expectations
- **Human Resources Team** - Handles hiring temporary personnel, if needed, to support the business operations
- **Media Relations Team** - Interfaces with the media regarding the effect of the disaster
- **Legal Team** - Handles any legal and/or insurance ramifications as a result of the disaster
- **IT Security Team** - Responsible for overall security before, during, and after the disaster. This team concentrates on making sure that data confidentiality, data integrity, and data availability are maintained throughout the process.
- **Physical Security Team** - Responsible for the security of physical assets such as facilities, equipment, and supplies. Coordinates with emergency personnel at the disaster and backup sites.
- **Facilities Management Team** - Responsible for facilities operation and maintenance during the crisis
- **Emergency Response Team** - Responds to the disaster by putting the business continuity and disaster recovery plan into action
- **Damage Assessment Team** - Responsible for determining the level of damage that was caused by the disaster
- **Off-site Storage Team** - Maintains corporate records and files (either in paper or electronic format)
- **Alternate Site Team** - Responsible for the configuration of the alternate site with the necessary hardware and software components for business resumption
- **Repair Team** - Responsible for repairing systems damaged as a result of the disaster (if applicable)

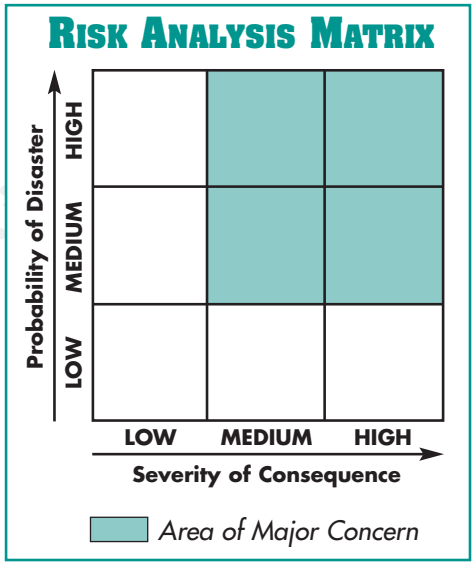
Action 1.6 Costing

BCP/DRP planning is like fire insurance, you need one but hope that you never have to claim it. With the current economic climate costing should be an integral part of the plan. BCP/DRP can, and in most cases is, very costly to initiate but also to maintain. You should therefore include both initial cost and on-going cost.

PHASE 2 PERFORM A RISK ANALYSIS

There is a need to determine the potential losses due to a threat vs. the cost of the protective measure against the value of the asset (or business process). Risk assessment weighs the losses of information resources in the absence of security controls against implementing the control.

This diagram shows the relationship between the probabilities of an event happening versus the impact of the event.



Many times the CIO and IT organization believe that they know what information, systems, and personnel are critical to the overall business. The most accurate assessment of a critical asset is gained by asking users and the executive committee of a company. A critical asset is an asset that supports company security, company finances, and company continuity of operations.

The first step required is to determine what information systems, data, and associated assets — facilities, equipment, and personnel — are critical.

The purpose of this phase is to solicit identification of critical assets. Various groups within the organization, such as finance, legal, HR, and administration, as well as other relevant business partners should complete the questionnaire in Appendix C. The response from several organizational departments is required to provide a big picture of what is truly occurring inside of the network.

There are no hard and fast rules for determining what is or is not a critical asset. In general, the more goals an asset supports — and the more "significantly" answers to questions on the survey list for each goal — the more important it is. It may help to rank the critical assets you have tentatively identified in order of importance to assist you in allocating resources to their protection.

Action 2.1 Identify major areas of risk in the business operation

Ask all business process owners, users, and systems administrators to participate in a roundtable discussion to identify their areas of concern. Critical operations, processes, and associated assets must be identified and prioritized.

Action 2.2 Understand the function of probabilities and risk reduction/mitigation within the organization

The team must understand the functional and return on investment (ROI) limitations that are placed on risk mitigation efforts. Cost benefit must be understood. Follow the adage that risk mitigation should never cost more than the impact from the risk whereas impact is the probability of the risk multiplied by the cost consequence of the risk.

Action 2.3 Identify outside expertise required

Consider using subject matter experts (SMEs), such as information risk management consultants, to conduct an unbiased risk assessment, and to help you determine the value of your critical assets and/or business processes.

Action 2.4 Identify vulnerabilities/threats/exposures

Obtain information from insurance companies, the local weather service, law enforcement agencies, and newspapers. Collect risk/exposure information based on actuarial data. This should include any available statistical data (this can come from the government or impact studies) as well as weather and site studies, and man-made risks.

Subscribe to reliable newsletters that provide the latest information on vulnerabilities. Reliable sources of information include:

- SANS Institute (www.sans.org)
- SANS Incident Web Site (www.incidents.org)
- The CERT® Coordination Center (CERT/CC) (www.cert.org)

Action 2.5 Identify risk reduction/mitigation alternatives

For each threat, identify reduction and mitigation alternatives and then provide multiple solutions. When it comes to handling risk, there are usually several courses of action. First you can accept the risk — this means accepting that the risk could occur and that you can live with the consequences. You can mitigate or reduce the risk to an acceptable level. Or you can transfer the risk — for example, getting insurance to cover the potential loss.

Action 2.6 Determine Threat/Vulnerability/Exposure Thresholds

For each identified threat/vulnerability/exposure, determine the time the threat/vulnerability/exposure has to exist before the organization is severely impacted. These threats/vulnerabilities/exposures may have critical impact immediately, but many times may exist for several hours to weeks before they have critical impact.

Action 2.7 Identify credible information sources

Trust only information available from credible sources, and be sure to validate the information before using it. Sample agencies include the following (additional sources can be found in Appendix A):

- Systems Administration and Network Security Institute (SANS Institute)
- Federal Emergency Management Agency (FEMA)
- Local and State Offices of Emergency Services (OES)
- Occupational Safety and Health Administration (OSHA)

Action 2.8 Meet with management to determine acceptable risk levels

Once the critical assets have been identified, management should then determine the acceptable risk level. In essence, you need to determine the maximum tolerable downtime (MTD) and recovery time objective (RTO).

- Maximum tolerable downtime is defined as the longest period of time a business process can remain inoperable before it loses its ability to fully recover or severely impacts the overall business with things such as fines, negligence suits, breach of contract suits, or significant drop in stock price.
- Recovery time objective is defined as the time from when the disaster event occurs until the business process must become available again. It is worth considering that some business activities are date-critical; therefore, their importance will vary during the business year. An example of such a date-critical system would be financial systems at the close of the quarter.

Action 2.9 Establish priorities for processing and operations

Based on the identification of critical business functions and operations (provided by management), the priorities should focus on those systems. Much of this information will be obtained from the business risk analysis.

Action 2.10 Evaluate backup site facilities

Examine current backup sites to determine if they meet your needs – remember if you have hot-site agreements with a major provider, in a major disaster, you may be competing with other organizations for provider resources. When evaluating backup sites, determine exactly what services that may or may not be provided. Evaluate carefully. Be sure to ask for references from companies that have had to activate their plans.

Here are some evaluation questions:

- Are there multiple hot or cold site locations?
- Are there multiple locations networked together?
- What are the contract terms: length of contract time; minimum/maximum fee; test hours allowed under contract; cost of additional test time not included in contract; lead time for notification of scheduled tests; maximum number of subscribers per location?
- What is the policy regarding site availability for testing while in use for recovery of a declared disaster by another subscriber?
- What is the number of other clients; from what geographical area?
- Were there any former inabilities to accommodate a subscriber in a declared emergency; how were they resolved?
- What is the base list price for equipment size and different contract terms?
- What is the availability of mobile recovery services and normal set-up time?
- How isolated is the site from events that could affect your organization? Ensure the site is on a different electrical distribution circuit, that it has backup power supply, and that communications tie into a different central office.
- In the event of a biological weapon release at your primary site, you must be prepared for the entire area being quarantined. This will prevent access to the facility, including supplies, personnel and spare parts. Be sure to select a backup site that is sufficiently far away from the primary site so that a regional quarantine will not affect your backup site as well. Have a plan that evacuates key personnel and recovery team members before the quarantine is declared.

Action 2.11 Evaluate hardware and software at the alternate facility

Make sure that you update and patch operating systems, have backup hardware for critical systems, and that the backups have kept pace and are capable of handling ongoing operations (at least at a level dictated by management). Depending on the criticality of the data, data mirroring or remote transaction journaling may be an option to consider.

Action 2.12 Evaluate communications systems

In most cases, communications capabilities will be less than the current, normal operating environment. Planning must include the degraded capability to ensure that minimum operational requirements can be met. An alternate communication method should be available in case normal channels are not available, such as cell phones, pagers, short-wave radio, etc.

Action 2.13 Evaluate the backup and restore process

Data must be transferred to the backup systems. If information was lost as a result of a disaster, the information must be recovered (or re-created). It is also possible that personnel performing backups may not be available to do the job as a result of the disaster, or that the offsite backups may not be available if recovery staff is not listed as authorized users.

Action 2.14 Evaluate customer services

If your company provides end-user services (such as phone customer support) and these services cannot be provided because of a disaster, these services might have to be suspended or transferred to another location. Determine if these services should be provided by a third party or at an alternate company location.

Action 2.15 Evaluate Facility Emergency Capability

Verify that backup power supply generators are periodically maintained and periodically tested. Ensure sufficient fuel is available. Verify battery backups are periodically maintained and tested. Verify any supplies needed for disaster recovery are present.

Action 2.16 Document and present findings to management

A formal presentation that outlines all applicable major identifiable risk scenarios and the potential impact that may result to ongoing operations of the business (quantify in business terms) should be presented to management to solicit their approval for ongoing BRP/DRP efforts.

PHASE 3 PERFORM A BUSINESS IMPACT ASSESSMENT (BIA)

An important and critical component of developing a business continuity plan is to determine the critical business processes, and to determine the impact of various disaster scenarios on your organization if these critical business functions are not recovered in a timely fashion. The Business Impact Assessment or Business Impact Analysis will fulfill this requirement. IT systems can be complex, with various components, interfaces, and processes. The person performing the BIA should identify and interview the various point of contacts responsible for the various IT operations. This process increases the awareness, interest, participation, and support of middle- and upper-level management.

Action 3.1 Project Planning

Obtain executive level sponsorship, assemble a project team, set goals and objectives with senior management, set a completion schedule, and announce the project to participants. The organization may elect to outsource this effort, or use automated tools to help conduct the BCP/DRP effort.

Action 3.2 Data Gathering

Choose data collection methods (questionnaire, interviews, group meeting, etc.); create collection criteria; collect the information, and validate it with BIA participants for accuracy and relevance. Use the following sample form as a guide:

SYSTEM	DESCRIPTION	PERSON RESPONSIBLE	CLASSIFICATION LEVEL	IMPACTING LEVEL

Legend:

Criticality Level 1 = restore immediately. This is highly critical to the survival of the business. Immediate recovery is required to prevent substantial loss to or degradation of business operations.

Criticality Level 2 = restore within 12 hours. This is relatively critical to the survival of the business. Further delay could raise this to Criticality Level 1.

Criticality Level 3 = restore within 24 hours. This is important to the survival of the organization. To delay further could raise the Criticality Level due to increase in volume or passage of time.

Impacting Level 1 = restore within 7 days. This is important to the effectiveness or efficiency of the management of the organization.

Impacting Level 2 = restore within 14 days. This is important to the effectiveness or efficiency of the management of the organization but is not important to the survival of the organization.

Action 3.3 Data analysis

Once the information is collected, the data needs to be reviewed and analyzed. The main purpose of this action is to assess the cost impacts and other implications of not performing certain business functions over time; identify critical functions and which data and applications they depend on; determine interdependencies between the various systems, and establish a recovery time objective for each critical function.

Action 3.4 Document Your Findings

Include an executive summary, recovery priority recommendations, graphs, charts, and other visual aids.

Action 3.5 Present Your Findings

Present written and oral reports to Senior Management. Be prepared to defend the BIA process and recommendations you've chosen, addressing the next steps in the planning process. Management will then use this information to prioritize the assets to be protected and direct scarce resources in the most effective manner, given budgetary and human resource constraints.

PHASE 4 BUILD THE PLAN

Once the critical business processes and assets are identified and requirements' time objectives established, the plan needs to be developed to implement and manage mitigating controls, and incorporate the procedures required to recover from the disaster. It is beneficial to segment the plans into manageable areas of responsibility, including creating sub-plans where necessary.

Action 4.1 Determine Recovery Strategies

Several options for recovery of the IT systems are available. Typical recovery strategies include the following:

- **Hot sites** — A hot site is a fully configured site that consists of your existing hardware and software, ready to fully take over operations when the main system fails. If you have a hot site, you can usually restore a system in a few hours.
- **Warm sites** — A warm site is similar to a hot site, but without all of the necessary hardware. You can add hardware when needed, but this delays getting the system up and running again. If you have a warm site, restoring a system can take longer than restoring from a hot site.
- **Cold sites** — A cold site is usually an air-conditioned room with electrical outlets but no equipment or software. The company plans to bring their equipment to the cold site and then rebuild the system. Restoration can take many hours, even days. A disadvantage of a cold site is that it very expensive to test, because testing requires the procurement of the second system to be installed.
- **Internal distributed systems and networks** — Refers to other internal IT systems, not normally used for disaster recovery, to be used as an alternate system for disaster recovery.
- **Reciprocal agreements** — In a reciprocal agreement, two or more companies agree to use each other's facilities in the event of a disaster. This requires that the sites have similar hardware and software environments. The advantages are that this type of arrangement is usually free or has a low cost. This solution does have many drawbacks. One is that it is hard to maintain the same hardware and software configurations at the locations. Any configuration changes must be documented and coordinated. Informal agreements are often not legally binding. More importantly, the reciprocating company probably cannot respond quickly to the event. There is also the issue of information protection.
- **Two data centers** — Some organizations have multiple data centers that can be configured to take over the processing of another center in the case of a disaster. This is similar to having a reciprocal agreement but with the same company.
- **Vendor-supplied equipment** — Some vendors can provide emergency equipment when needed. The problem with this approach is that if it is a major disaster event, the vendor might not be able to accommodate the request for equipment.
- **Combinations of the above**

Recovery methods could include establishing a line of succession in management, identifying a temporary agency from which you can draw secretarial and other employees, and establishing a "resumption" relationship with an IT consulting services group.

Action 4.2 Develop and maintain a list of emergency contacts

During an emergency situation, there is no time to figure out who are the right people to call. A list of emergency contacts should be maintained and kept someplace easily accessible offsite. Personnel on the list might include the following:

- Appropriate management personnel
- Critical IT personnel
- Medical and mental health service providers
- Vendor list
- Federal and/or state agencies
- TV and Radio contacts for public relations and communications

Note: Contracting with grief counseling services ahead of time may be helpful in obtaining these services in a timely manner, as they are often very busy in times of crisis.

Action 4.3 Develop and maintain a list of inventory items

A list of inventory items should be kept in a safe location and available to the Business Continuity Plan Leader. The inventory list might include the following:

- Communication equipment inventory
- Documentation inventory
- Computer hardware and software inventory
- Equipment (other than IT) inventory
- Off-site storage location inventory
- Software and data files backup/retention schedules
- Temporary location specifications (address, phone numbers)

Action 4.4 Talk, meet, and agree to plans with your suppliers

An agreement with vendors may need to be established in advance (depending on the recovery time objectives) so that the business could still receive supplies and/or services in the event of a disaster.

Action 4.5 Investigate alternate supply sources

In some cases, it is advisable to have additional supply sources in the event that normal suppliers are unable or unwilling to provide the products and services needed.

PHASE 5 TEST AND VALIDATE THE PLAN

To this point, the development of the BCP-DRP document has been arduous, and the coordinator might like to think the job is finished. However, the plan is of limited use until it is tested to expose areas that require updating to correct deficiencies and/or omissions.

Action 5.1 Define the objectives of the test

The first step in the testing of the plan is to define the objectives of the test. The purpose of testing the plan should include the following:

- Prove the plan really works
- Verify alternate facility meets the needs of the BCP/DRP plan
- Verify the adequacy of the team procedures
- Identify deficiencies and omissions in the plan
- Provide training for everyone
- Provide input for updating the plan

Action 5.2 Identify the required equipment and resources

Depending on the testing methodology, certain equipment and resources might be required. Make sure management has authorized the purchase of the equipment. Make sure to address these issues:

- Storage location of equipment when not in use — can the equipment be accessed at a moment's notice?
- Determine who will have access to equipment and whether can it be used for other purposes — typically this equipment is reserved for DR use only.
- Transportation of equipment to DR site — how soon can the equipment be transported to the DR site and by whom?
- Determine how personnel resources will get to the DR site

Action 5.3 Identify the necessary personnel

Not all of the personnel will necessarily be needed during all of the test scenarios, as defined in Action 5.5. Determine what teams will be involved and their responsibilities. See Appendix E for examples of the different BCP teams. For example, the legal team is usually not involved during the "checklist" test.

Action 5.4 Document testing schedules and locations

Depending on the testing methodology (see Action 5.5), it is advisable to create a schedule that will not interrupt normal business operations. Testing could occur on weekends or holidays. Depending on the complexity of the test, make sure that all external support personnel are available. If the organizations have multiple testing locations, determine which locations will be tested first.

NOTE: Because there is nothing else going on during off hour testing, this might give you a false sense on how long it takes to accomplish these tasks. During a real disaster there is an increased sense of urgency and there will be many activities going on at the same time.

Action 5.5 Determine the test methodology

Structural walk-through — This test involves getting the various testing teams together to review the plan in detail. This involves a thorough look at each of the plan steps, and the procedures that are invoked at each step. This ensures that the actual planned activities are accurately described in the plan. This minimal testing scenario will at least familiarize the teams with one another and establish cross-team communication.

Checklist tests — This method is implemented by distributing copies of the plan to each of the team groups. Each group reviews the plan and checks off the points that are listed to ensure that the plan addresses all concerns and activities.

Simulation tests — The operational and support functions meet to practice execution of the plan. Because it is a simulation, the test is run only to the point of the actual relocation to the alternate site and installation of the replacement equipment.

Parallel tests — This test verifies the operational readiness of the plan. During this test, the critical systems are placed into operation at the alternate site, and a check is performed to see if everything operates as planned. Any discrepancies or differences between the real operational systems and the alternate site are noted and resolved.

Full interruption tests — In this test, normal operations are completely shut down, and the processing is conducted at the alternate site using the materials that are available in the offsite storage location and with personnel that are assigned to the recovery teams. Use this test with caution, because if the contingency and disaster recovery plans do not adequately restore the system, normal business operations are at risk.

Action 5.6 Define the expected test results

In order to determine the effectiveness of the BCP/DRP, the test results should be measured against pre-defined expected results. Using this method, you can then determine if the test actually measured up to the desired results. If the test did not, you can either lower the expected test results or increase the effectiveness of the test procedures.

Action 5.7 Pre-plan the exercises

Write a BCP test plan. The plan should detail the exact steps to be taken during the test, the personnel or departments involved, and the expected results.

Action 5.8 Coordinate and exercise the test plan

The test administrator is responsible for the coordination of the testing procedures, as well as recording the results of the test.

Action 5.9 Document the results

The test administrator should collect all of the test results for each step of the test and prepare a final report document. These findings will be used to either validate that the test works or, if not, the findings will be used to update the plan accordingly.

Action 5.10 Evaluate the results

Are the test results as expected? If not, what can be done to fix the problem? Is the problem related to the way the testing is performed?

Action 5.11 Report results to management

Document the test results in a manner that can be easily understood by management. When possible, use charts and graphs to better represent the results.

Action 5.12 Update the plan based on the results and management's recommendations

Since the plan is a living document, it should be updated and revised based on the test results and management's recommendations. The BCP/DRP test results should be used to improve the plan by determining the parts of the plan that require improvement and by making the changes.

Action 5.13 Coordinate plan maintenance

Determine how often the plan should be reviewed, tested, and updated. It is a best practice to review/update the plan every year, unless there are significant changes to the business operations and/or IT systems.

Action 5.14 Develop a Business Continuity Plan training program

Having a business continuity plan is great, but if personnel are not trained on the plan and how to respond in the event of a disaster, they will not know the steps to take if a disaster occurs. Training should take place periodically and especially when there have been significant changes to the plan.

PHASE 6 MODIFY/UPDATE THE PLAN

The business continuity and disaster recovery plan is a living document, and should be updated to reflect changes in business operations, changes in personnel, and to incorporate deficiencies found during the testing phase.

Best practices dictate that the plan should be updated yearly. However, conditions in your organization may prompt for more frequent updates. This list will help you determine when your plan should be updated:

1. Changes to core system(s) or technology or business process(es)
2. Increased dependence on existing technology or dependence on new technology
3. Organizational restructuring — acquisition, outsourcing, key personnel turnover, realignment, or layoffs
4. Clients, regulators, investors, insurers, or creditors are showing interest in your continuity planning efforts
5. Financial loss — previous disasters have resulted in financial losses
6. Downtime – previous disasters have resulted in system downtime
7. Increased threat factors (higher probability or higher impact)
8. Plan hasn't been updated or tested within the last year

Action 6.1 Use results of testing to see what improvements/changes are needed

The testing phase will probably uncover deficiencies and/or omissions in the plan. This information should be used to revise the plan.

Action 6.2 Update the plan if hardware/software components have changed

The plan should be updated to include new hardware and/or software components that are added to the organization. For instance, if the company adds a new wireless network as part of the mission-critical infrastructure, then this should be addressed accordingly in the testing procedures.

Action 6.3 Update the plan if new business systems are added or changed

When a new critical business process is changed, removed, or added to the organization, the plans should be changed accordingly. For example, if a new payroll system is being installed to replace an older version, the plans should be updated (and tested) to reflect this change.

PHASE 7 APPROVE AND IMPLEMENT THE PLAN

Once the plan is developed and tested, the plan must be reviewed and approved by management. This assures that the plan meets the business goals set by management. Once the plan is approved, the plan needs to be implemented within the organization.

Action 7.1 Evaluate adequacy of plan

Management should make sure that the plan meets the business needs of the organization. Management should then establish policies, procedures, and responsibilities for continuity planning. If your organization relies on outside service bureaus for its business operations, management must also evaluate the adequacy of their continuity plans, and make sure that their plans are compatible with your organization's plans.

Action 7.2 Get management approval and plan signoff

Make sure management approves and signs the BCP/DRP plan. Management should review the plan, and compare the observed test results to the expected results to ensure they reflect organizational goals and expectations.

Action 7.3 Train employees in the contents and purpose of the plan

Set up real life scenarios to test the elements of the plan. This would include department-isolated incidents such as the loss of financial database access, etc. Also, the training should include an area-wide disaster such as an earthquake, hurricane, etc.

Action 7.4 Critique the Training

Have a meeting with all participants to discuss what worked and what did not. Record the meeting minutes and establish a work plan with timeline to fix any outstanding issues.

Action 7.5 Audit the Plan

Periodically review the plan (suggested annual periodicity) and audit the organization to ensure the plan is still properly implemented:

- Employee training is current, new employees have been trained, and replacements for departed critical employees are trained
- Plan assumptions and initiating events are still valid
- Plan threats/vulnerabilities/exposures are reviewed and updated
- Plan implementation actions such as drills, backups, supply procurement, equipment maintenance, etc. are being performed
- Recall and subject matter expert lists are updated
- Management has received refresher briefings.

LESSONS LEARNED/PERSONAL OBSERVATIONS

Many contributors to this guide wished to express their personal recommendations on how they implement their business continuity/disaster recovery plans. This section contains simple ideas and observations that might be applicable to your environment.

Observation #1:

It is important to segregate the type of disaster and types of resources needed.

Different disasters require different crew and resources and should be completely different plans. Two things to keep in mind during the design of your plans are

1. Simplicity

2. Testing has to be thorough.

Data backup schemes should not be complicated. Use simple rotations, simple schemes, simple tape naming conventions, and if something goes wrong, try to have a minimum number of tapes to restore from (and perhaps have a hot machine waiting). If possible, don't use incremental or differential backups — even if it means buying more and bigger tape libraries.

When something happens, your mind is not going to be able to concentrate on complicated procedures and you may have to walk someone through over the phone.

To test, it might be beneficial to make a duplicate lab of your equipment/system; kill it and bring it back to life. Most managers are resistant to spending money for this. You have to be vigilant about upgrading your backup hardware and software. You should not completely rely on vendors to come and hot-swap products. Keep at least one of everything onsite.

Observation #2

One practice that I recommend for some clients is that backups should be taken from the real site to the offsite (hot or warm), and immediately restored onto the offsite system. This proves the usability of the backup, keeps the offsite synced as a matter of course, and keeps the operators practiced on the restoration process.

Once backups are verified through successful restoration onto the offsite system, they can be shipped to permanent storage. Bad backups (and they happen) can be immediately returned and the problem corrected. Some big problems have been prevented through this step.

It's somewhat vulnerable in the case where only incremental backups are being done. Incremental backups tend to fail less often than full backups, and can lead to errors and complacency. So you need policy that forces full backups on a prudent periodic basis.

LESSONS LEARNED/PERSONAL OBSERVATIONS

Observation #3

I have clients who don't understand what they need to restore a system or what kinds of backups need to be done.

On the telecom side, vendors either never, almost never, or hardly ever, provide information about backing up this system to clients. The customer gets told that a system does an automatic backup (at least in part) on a nightly basis, but clients don't understand

1. What gets backed up
2. That they need to change those tapes and not keep reusing the only tape that came with the system
3. They need to remove their backup tape from the switch room
4. What backups and what skill set is needed to restore that system.

One system I work with requires two different backups to restore. (The previous version only required one backup...so much for progress.)

Observation #4

We must make sure we don't obsess over the most rare occurrences and when we do, we must use proper context within the typical DR plan. With that, I ask, do we want to include proactive employee awareness training in order to mitigate the biggest hazard in weapons of mass destruction attacks?

In the event of a dirty bomb, the initial reports will be "bomb" and then the various detectors on the hazmat teams will start to go off as they arrive to make sure if it is or isn't just another conventional explosives attack. So, do we want the enterprise to be mentally prepared for the notification of nuclear, biological, and chemical issues? Again, looking at scope of the document. Is it reasonable to not mention these things in a paragraph about weapons of mass destruction, terrorism and put it in proper context? I agree that a mundane thing such as a leaky pipe in the ceiling tiles is more likely to cause actual damage to most organizations' IT resources than a terrorist attack.

Appendix A USEFUL LINKS

The contents used in this draft are a compilation of Business Continuity Plan and Disaster Recovery Plans from various sources including:

NIST Contingency Planning Guide for Information Systems
http://csrc.nist.gov/publications/nistpubs/

The MIT Business Continuity Plan
http://web.mit.edu/security/www/pubplan.htm

University of California Campus Business Continuity Planning
http://www.ucop.edu/facil/eps/continuity.html

State of Massachusetts Y2K Sample Business Continuity Plan
http://www.state.ma.us/y2k/Archive/projplanning/businesscontinuityplan_template.htm

University of Massachusetts Business Continuity Planning Guidelines
http://www.umassp.edu/policy/data/business.html

Treasury Board of Canada BCP
http://www.cio-dpi.gc.ca/emf-cag/busconplan/bconplan_e.asp

University of Sydney Business Continuity Plan
http://www.personal.usyd.edu.au/~stephen/network/disaster3.shtml

University of Wales Swansea Y2K Business Continuity Plan
http://www.swan.ac.uk/uws/y2k/bcplan.htm

Compaq Business Continuity: Ensuring Survival
http://nonstop.compaq.com/view.asp?IOID=4492

The Computer Emergency Response Team - Carnegie Mellon University
http://www.cert.org

University of Delaware Disaster Research Center
http://www.udel.edu/DRC

University of Delaware Disaster Research Center
http://www.udel.edu/DRC

GE Capital Disaster Recovery Services
http://www.gedisasterrecovery.com/

FBI/Infragard
FBI field offices have Infragard chapters that focus on infrastructure protection and disaster recovery, and collaboration with the private and academic sectors. www.infragard.net

Disaster Recovery Institute International
Founded in 1988 to provide a base of common knowledge in contingency planning. DRII also administers a certification program for qualified business continuity/disaster recovery planners. http://drii.org

Contingency Planning & Management
Periodical and a central resource for technology, products, services, information, and management strategies that support business continuity to safeguard the physical, informational, and communication assets of a business; ensure the safety of employees and the public; and protect the financial well-being of the company. http://www.contingencyplanning.com/

Disaster Recovery Journal's Homepage
Dedicated to the field of disaster recovery and business continuity. Over 50,000 subscribers. The DRJ also sponsors two annual conferences that attract over 2500 disaster recovery professionals from all over the world, which makes their conferences the largest in the entire industry.
http://www.drj.com/

Federal Emergency Management Agency
An independent agency of the federal government, reporting to the President. Since its founding in 1979, FEMA's mission has been to reduce loss of life and property and protect our nation's critical infrastructure from all types of hazards through a comprehensive, risk-based, emergency management program of mitigation, preparedness, response and recovery.
http://www.fema.gov/

Canadian Centre for Emergency Preparedness
The Canadian Centre for Emergency Preparedness is a Canadian non-profit organization devoted to the promotion of disaster management to individuals, communities, and organizations. http://www.ccep.ca/

NFPA 1600
Standard on Disaster/Emergency Management and Business Continuity Programs. It is a description of the basic criteria for a comprehensive program that addresses disaster recovery, emergency management, and business continuity.
http://www.nfpa.org/Home/AboutNFPA/index.asp

Appendix B ACRONYMS AND GLOSSARY

A list of some terms commonly used in a business continuity or disaster recovery plan.

Alternate site — A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster

Business Continuity Planning (BCP) — An all-encompassing term covering both disaster recovery planning and business resumption planning. Facilitates the rapid recovery of business operations to reduce the overall impact of the disaster, while ensuring continuity of the critical business functions

Business Impact Analysis (BIA) — The process of analyzing the various business processes and the effects a disaster can have on them.

Business recovery team — A group of individuals responsible for maintaining and coordinating the recovery process.

Cold site — The name given to an alternate facility that does not contain any resources or equipment, except for air conditioning and raised flooring. In the event of a disaster, equipment and resources are installed in this facility to duplicate the critical business functions.

Contingency plan — A contingency plan is a collection of procedures and processes deigned to help a company respond to disruptions in services caused by disasters or other emergency situations.

Database shadowing — A data backup of database maintained at a remote data center that is maintained in real-time.

Disaster — Any event that creates an inability to continue providing business functions.

Disaster Recovery Plan (DRP) — The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.

Electronic vaulting — Transfer of data to an offsite storage facility via an electronic link rather than via portable media.

Hot site — The name given to an alternate site that contains all of the equipment and resources to continue business operations when the main facility is not operational.

MTD – Maximum Tolerable Downtime —A calculation performed during the business impact analysis that determines the maximum amount of time a system (or business process) can be inoperable before it begins to adversely affect the core business operations.

Reciprocal agreement — A mutual agreement between two departments, divisions, or companies, to provide backup processing capabilities in the event of a disaster.

RTO – Recovery Time Objective — The time from when the event occurs until the business process must become active again.

Risk assessment — The process of identifying the vulnerabilities associated with a business process, and how to mitigate the damage these exploited vulnerabilities can cause.

Appendix C PRELIMINARY CHECKLIST

- ☐ Do you have an alternate person with full authority for disaster recovery, in the event that the usual person in charge is not available?
- ☐ Do the Fire and Police departments servicing each of your locations have the phone number of both your person in charge and your alternate?
- ☐ Do you keep your backups where you can always get to them (not in a timed vault, etc.)?
- ☐ Have you tested that you can actually read and restore your computer and PC backup files?
- ☐ Do your alarms work without power (do they have battery back-up)?
- ☐ Are your safes fireproof or only "tool-resistant?"
- ☐ Do you have a binder off-site with a copy of every form you use, and the phone number of where you get them?
- ☐ Do you have the after-hours contact numbers for your insurance agents?
- ☐ Do you have at least one telephone at each location, which works if telephone system loses power or breaks?
- ☐ Is your payroll function cross-trained?
- ☐ Are your personnel records safe from fire? What about floods?
- ☐ Do you know the street addresses of your local radio stations, in the event that telephones are not working and you must get there in person to submit announcements?
- ☐ Are your telephones and electrical service "rooms" protected from "falling" water?
- ☐ Does someone have administrative access to employees' voice-mail passwords in order to retrieve messages when an employee is suddenly ill or incapacitated?
- ☐ Do each of your locations have "emergency cabinets," containing at least the following: candles, matches, flashlights with extra batteries, a radio with extra batteries, coins for vending machines, and a first-aid kit?
- ☐ Do all your locations have at least one exit that can be used without a key?
- ☐ Do you have an arrangement with a Temporary Staffing Agency to obtain additional or replacement personnel? Are these individuals fully trained in your operating procedures and functions?
- ☐ Do you have an arrangement with mental health providers to provide post disaster support?

Note regarding fireproof safes: You may need to have tapes sealed in waterproof containers inside safe. Fireproof safes work because they leak moisture from the insulation material when heated. Consult your safe supplier.

Appendix D CRITICAL ASSET IDENTIFICATION CHECKLIST

1.	To what degree is the asset required to perform essential business functions?	☐ Significant	☐ Moderate	☐ Indirect	☐ Not at all	☐ Unknown
2.	What role does the asset play in supporting the business operation and capabilities as a whole?	☐ Lead role	☐ Support	☐ Indirect	☐ Not at all	☐ Unknown
3.	Is the asset directly associated with a function of the company specifically identified in the financial plan?	☐ Lead role	☐ Support	☐ Indirect	☐ Not at all	☐ Unknown
4.	To what level does the asset support the execution of continuity of business?	☐ Significant	☐ Moderate	☐ Indirect	☐ Not at all	☐ Unknown
5.	To what degree would the loss or degradation of this asset limit the ability of the company to function?	☐ Significant	☐ Moderate	☐ Indirect	☐ Not at all	☐ Unknown
6.	To what degree does the asset affect external clients and customers?	☐ Significant	☐ Moderate	☐ Indirect	☐ Not at all	☐ Unknown
7.	To what degree does the asset affect internal and intranet connectivity and continuity?	☐ Significant	☐ Moderate	☐ Indirect	☐ Not at all	☐ Unknown
8.	Do our business partnerships and alliances require the availability of this asset?	☐ Significant	☐ Moderate	☐ Indirect	☐ Not at all	☐ Unknown
9.	What role does the asset play in providing a means to maintain company business?	☐ Lead role	☐ Support	☐ Indirect	☐ Not at all	☐ Unknown
10.	On what scale does this asset affect the business?	☐ Significant	☐ Moderate	☐ Indirect	☐ Not at all	☐ Unknown
11.	How would the loss of this asset reduce the ability of the company to maintain business?	☐ Significant	☐ Moderate	☐ Indirect	☐ Not at all	☐ Unknown
12.	Are there any other equivalent assets that could be substituted for this particular asset in order to maintain business continuity?	☐ Yes	☐ No	☐ Unknown		
13.	What role does the asset play in ensuring orderly functions of the business financially?	☐ Lead role	☐ Support	☐ Indirect	☐ Not at all	☐ Unknown
14.	What kind of business economic disruption would the loss or degradation of the asset cause?	☐ Economic Collapse	☐ Significant Disruption	☐ Minimal	☐ None	☐ Unknown
15.	Does the asset protect sensitive financial data?	☐ Yes	☐ No	☐ Unknown		
16.	Does the asset support large segments of the company?	☐ Yes	☐ No	☐ Unknown		
17.	This asset is needed to support what sized portion of the company?	☐ Large	☐ Medium	☐ Small	☐ None	☐ Unknown
18.	Is the basic intent of this asset to provide for the minimum of essential business services?	☐ Yes	☐ No	☐ Unknown		
19.	To what degree does the asset support the mission of other business entities?	☐ Significant	☐ Moderate	☐ Indirect	☐ Not at all	☐ Unknown
20.	To what degree does the asset rely on other business entities to perform its function?	☐ Significant	☐ Moderate	☐ Indirect	☐ Not at all	☐ Unknown
21.	Would the degradation of this asset affect other business assets?	☐ Yes	☐ No	☐ Unknown		

Appendix E BUSINESS CONTINUITY TEAMS

TEAM NAME/ROLE	PURPOSE
Continuity Plan Coordinator	Manages the process and coordinates the various teams.
Senior Management Team	Approval of the plan, allocates budget and sets expectations
Human Resources Team	Handles hiring temporary personnel if needed to support the business operations
Media Relations Team	Interfaces with the media regarding the effect of the disaster
Legal Team	Handles any legal ramifications as a result of the disaster
IT Security Team	Responsible for overall security before, during, and after the disaster. This group ensures that data confidentiality, data integrity, and data availability are maintained
Physical Security Team	Responsible for the security of physical assets such as facilities, equipment, and supplies
Facilities Management Team	Responsible for facilities operation and maintenance during the crisis
Emergency Response Team	Responds to the disaster by putting the business continuity and disaster recovery plan into action
Damage Assessment Team	Responsible for determining the level of damage that was caused by the disaster
Off-site Storage Team	Maintains corporate records and files (either in paper or electronic format)
Alternate Site Team	Responsible for the configuration of the alternate site with the necessary hardware and software components for business resumption
Repair Team	Responsible for repairing systems damaged by the disaster (if applicable)

Additional Resources From The SANS Institute

The SANS (System Administration, Networking, and Security) Institute, founded in 1989, is a cooperative research and education organization through which more than 156,000 security professionals, auditors, system administrators, and network administrators share the lessons they are learning and find solutions to the challenges they face.

The core of the Institute is the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research, sharing knowledge, and teaching to help the entire sans community.

THE SANS COMMUNITY CREATES FOUR TYPES OF PRODUCTS:

In-Depth Education

During 2001, more than 12,500 security, networking, and system administration professionals attended multi-day, in-depth training by the nation's top security practitioners and teachers. For 2002, SANS programs will educate thousands more security professionals in the US and internationally.

Certification Programs

SANS' GIAC (Global Information Assurance Certification) is considered a blue chip of security education and certification programs. GIAC is classroom and online training that caters to the needs of security professionals, from those who are just getting started with the Security Essentials module, all the way through to the advanced GIAC Security Engineer "honors program." Over 2,700 students have achieved GIAC certification, and many more are currently in the process of doing so.
http://www.giac.org/

Breaking News

SANS Newsbites is a weekly summary of important published news stories concerning information security.
http://www.sans.org/newlook/digests/newsbites.htm

SANS Security Alert Consensus is a weekly summary of new security alerts and countermeasures. Produced in collaboration with Network Computing magazine.
http://server2.sans.org/sansnews

SANS Windows Security Digest is a monthly summary of new security alerts and new system administration guidance for people who manage and secure Windows NT and Windows 2000 systems.
http://server2.sans.org/sansnews

Monthly Web Broadcast: Internet Threat Updates is an exclusive service for SANS attendees and GIAC certified professionals that provides up-to-the-minute technical information about threats and how to block them.

incidents.org is a virtual organization of advanced intrusion detection analysts, forensics experts and incident handlers from across the globe, whose mission is to provide real time "threat-driven" security intelligence and support to organizations and individuals. Its most powerful tool for detecting rising threats is the internet storm center which analyzes data collected from more than 3,000 firewalls and intrusion detection systems in over sixty countries.

Special Research Projects

SANS helps the community keep up with the most current information security issues and helps them respond to those issues by addressing them with special up-to-date research projects and publications. Some of the noteworthy projects and publications are listed below.

S.C.O.R.E.
Developed by the SANS Institute/GIAC in cooperation with the CENTER FOR INTERNET SECURITY (CIS), SCORE is a community of security professionals working to develop consensus regarding minimum standards and best practice information.
http://www.sans.org/score/

Top Twenty Vulnerabilities
Developed by SANS and the FBI, the list is segmented into three categories covering General Vulnerabilities, Windows Vulnerabilities, and Unix Vulnerabilities.
http://www.sans.org/top20.htm

Center for Internet Security
A global, cooperative initiative through which industry, government, and research leaders are establishing basic operational security benchmarks and keeping them up-to-date. SANS is a founding member.
http://www.cisecurity.org

Information Security Reading Room An online library of the original research reports produced by successful candidates for GIAC certification.
http://rr.sans.org/index.php

Publications

Step-by-Step Guides

- *Step-by-Step Guides*
- *Windows 2000 Security: Step-by-Step*
- *Securing Linux: Step-by-Step*
- *Windows NT Security: Step-by-Step*
- *Solaris Security: Step-by-Step*
- *Computer Security Incident Handling: Step-by-Step*
- *14 Steps to Avoiding Disaster with Your Website*
- *Windows 2000 Vulnerabilities and Solutions*
- *Disaster Recovery: Step-by-Step Business Continuity Planning*
- *Securing Cisco Routers: Step-by-Step*
  Cisco routers are an increasingly common target for attackers. The number of exploit advisories for IOS has increased by over 300% in the past year. The complexity of attacks is also increasing to the point where an attacker can control all of the data entering or leaving the network. The SANS Cisco Consensus Guide clearly details the steps necessary to harden the configuration of your Cisco routers based on expert opinions from the leaders in Cisco Router security in the public, private, and government sectors.

To order these publications go to http://www.sansstore.org/

Posters

Roadmap to Network Security

MANY SANS RESOURCES, SUCH AS NEWS DIGESTS, RESEARCH SUMMARIES, SECURITY ALERTS AND AWARD-WINNING PAPERS ARE FREE TO ALL WHO ASK. INCOME FROM PRINTED PUBLICATIONS HELP FUND GRANTS AND UNIVERSITY-BASED RESEARCH PROGRAMS. THE GLOBAL INFORMATION ASSURANCE CERTIFICATION (GIAC) PROGRAM AND SPECIAL RESEARCH PROJECTS ARE FUNDED BY INCOME FROM SANS EDUCATIONAL PROGRAMS.