Business Continuity Planning

A Primer for Management and IT Personnel

Prepared by
John Williamson
jw@anykeynow.com

The AnyKeyNow Group
www.anykeynow.com

Rev: 2.07a

Updated July 15, 2002

Contents

Introduction

The terrorist attacks upon the United States of September 11th, 2001 proved to be a wake-up call to many who had looked at business continuity and disaster recovery planning as a task that was going to be done "down the road." Besides the terrible toll that was taken on human life, many businesses, especially those in New York City, were effected severely. Some will never recover.

There were, however, many examples where good business continuity planning resulted in successful resumption of operations. These example came from businesses and organizations that had made the investment in frequent disaster plan tests and updates, regular real-time backup of their data, and establishment of hot site capabilities to name a few. In this respect, many of our large financial organizations were able to quickly resume business due to the fact that they could quickly use alternate sites to restore their information systems.

We have all had to take a new look at the meaning of the "worst-case scenario" and use it as a model for good planning. It is necessary to look how disaster recovery plans and business continuity plans can compliment each other. We need to add the potential for terrorism effecting our business structures to the equation of good, defensive planning, and use the example of the incidents of September 11th to our best advantage.

Business Continuity and Disaster Recovery

Being prepared is crucial to protecting your organization in case of a systems disaster.

Disasters can take many forms. While natural catastrophes like flooding, hurricanes or earthquakes may be infrequent events, more common causes of systems disasters can strike at any time, from system outages to computer viruses to disruption by discontented employees. Resuming normal operations as quickly as possible minimizes business disruption, and good preparation will ensure that.

Many organizations and companies aren't adequately prepared for systems disasters. Recent research shows that major barriers to preparation include lack of executive support and funding. Adequate funding for disaster recovery efforts requires a shift in priorities of an organization's IT initiatives. In the past, organizations implemented technology as a cost savings measure. Now, IT initiatives that support business continuity and revenue generation are getting top priority.

Terminology

In the early days of data processing, the mainframe computer was usually housed in a large room with very large windows so everyone could see the computer. This led to the term "glass house." The term "Disaster Recovery" is usually related to only the restoration of the

"glass house." In the same vein, the term "Disaster Recovery Plan" related more to a plan on how to restore the "glass house" and its contents in the event of a crisis.

In today's complex work environment, we not only have to take the concept of the "glass house" into consideration, but also the client/server computer networks and the work-areas where essential business functions occur. The work-area includes all the needed facilities, such as desks, chairs, telephones, office supplies, and so on. Another often-overlooked aspect is the human factor. Any recovery efforts would surely fail without having an adequate number of trained personnel on hand to actually perform the critical business functions. Today's more encompassing recovery environment is usually referred to as "Business Continuity."

According to the Business Continuity Institute (http://www.thebci.org), a Business Continuity Plan (BCP) is:

> *A document containing the recovery timeline methodology, test-validated documentation, procedures, and action instructions developed specifically for use in restoring organization operations in the event of a declared disaster. To be effective, most Business Continuity Plans also require testing, skilled personnel, access to vital records, and alternate recovery resources including facilities.*

Properly written, a BCP is a collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of an emergency or disaster. This would include the elements of a disaster recovery plan (DRP).

Putting it simply, business continuity is the process of planning to ensure that an organization can survive an event that causes interruption to normal business processes. Disaster recovery is the process that takes place during and after an organizational crisis to minimize business interruption and return the establishment as quickly as possible to a pre-crisis state.

> *The process of creating, testing, and maintaining an organization-wide plan to recover from any form of disaster is called Business Continuity Planning (BCP). Every BCP strategy includes three fundamental components: risk assessment, contingency planning, and the actual disaster recovery process. BCP should encompass every type of business interruption -- from the slightest two-second power outage or spike up to the worst possible natural disaster or terrorist attack. (http://www.sun.com/datacenter/continuity/recovery)*

The objective of disaster recovery planning is to enable an organization to recommence normal IT functions as quickly and as effectively as possible following a disaster or disruption to computing services.

An impartial, bottom line assessment of the true impact of a systems disaster on an organization can quickly point out the need to be prepared. Up-front integration of BCP budgeting into all of an organizations' strategic IT initiatives will help spread the financial overhead fairly among all users of IT systems. It will get people thinking about the importance of BCP as an essential ingredient of any computing initiative.

Creating a Business Continuity Plan

The KISS Principle: Keep It Simple, Stupid!

Creating and maintaining a workable business continuity plan (BCP) is an essential factor in ensuring your organization's continued survival and prosperity. Although planning methodologies may vary among organizations, there are standards common to all.

There are five main steps in the business continuity planning process. The process is sequential by nature, so for the best understanding, the material should be approached in the order presented.

A Business Continuity Coordinator should be appointed. This can be a temporary role, but a better approach would be for this to be a permanent role even if it is considered a part-time responsibility once the actual BCP has been put in place.

Look into purchasing BCP software. There are a number of good packages on the market, and they would make the Business Continuity Coordinator's job go that much smoother. Most packages offer a facility for producing reports.

An approach is suggested to organize, promote, and manage the project to construct one or more business continuity plans for your organization. It focuses on the development process steps and the interactions among project participants to achieve project objectives.

This material is especially useful for the first time developer, project manager, or newly appointed Business Continuity Coordinator.

It is assumed that senior management has decided to support the development of business continuity plans for your organization. Their support is vital to the project's success by generating enthusiasm, credibility, and visibility.

Essential Steps

The steps indicated here are intended as proven standard guidelines. They can be modified as needed to suit your organization.

Step One: Initiation

Prepare for the Initial Meeting with Senior Management

Know as much as possible about the issues associated with the development of disaster planning. To secure the senior management support necessary for success, you must present a well thought out approach and demonstrate management control of the proposed project.

When preparing for your management meeting:

1. Review your organization to determine what resources are appropriate to be assigned to the project team. Review any existing enterprise-wide disaster planning policies, strategies and procedures relative to emergency response or continuity of operations.
2. Review any continuity plans that are in place within your organization. Are they effective models for your project?
3. Research any local events in the recent past (fires, severe weather, major equipment failures, etc.) that had or could have had a negative effect on your organization.
4. Review any pertinent laws and regulations.
5. Prepare a Project Introduction Memo for senior management's signature to communicate to the organization at large the need for BCP and the program's goals.
6. Prepare to discuss project funding. Ensure that management realizes that business continuity planning is an ongoing budget item, not a one-time project.
7. Research and recommend any necessary training for yourself or other members of the proposed project team.
8. Ensure access to personal computers for all team leaders. If you've purchased and are using a LAN version of your BCP software, make sure that a server has sufficient space and capacity to run the program. Budget for any required computers.
9. Draft the Project Schedule - Develop an initial project schedule that contains the important tasks, timing and resources required to accomplish your objectives. Start with the basics and add detail as necessary. A project management software package might be a worthwhile investment if your Coordinator is comfortable with its functions.
10. Invite a management representative to kickoff meeting from every department section who will be helpful in presenting a more thorough understanding of the project.

Conduct Kickoff Meeting with Senior Management

Suggested Agenda Overview:

- Begin the meeting with a background statement on the project and its goals and objectives.
- Present your proposed project schedule, including the project goals and objectives at a summary or highlight level.
- Review your proposed meeting agenda and schedule. Identify clearly the resources that are required.
- Respond to any questions.

Presentation Considerations:

- Make sure you understand senior management's business goals and objectives.
- Do not dive into details unless you're required to.
- Recommend the members of the project team to senior management for concurrence.
- Highlight the impact of management's decisions on any strategies that will be developed. Secure their time commitments for decision and directional reviews.
- Suggest that a security and emergency preparedness program be sponsored and closely coordinated with the BCP project.
- Commit to prepare the project introduction memos and present them to senior management for signature at the next scheduled management meeting.
- Develop a PowerPoint presentation, and use it to kick off the meeting.

Meeting Closure and Follow Up

- Close the meeting by securing management's concurrence and support. Identify your senior management project champion; schedule a meeting with him/her to review the drafts.
- Once senior management has issued the project introduction memos, forward memos to all managers notifying them of the project and of suggested times and places for scheduled meetings and requesting that they involve key members of their staff.
- Communicate frequently about the project's goals and objectives.

Form the Project Team

Conduct the initial meeting of the project team. Discuss the continuity planning project, senior management's commitment to the project, the continuity planning methodology, and the initial project plan that was developed. Clearly delineate the roles of the project team members.

Finalize the Detailed Project Schedule

- The project team should complete the following activities to finalize the project schedule for presentation to senior management:
- Obtain and review the detailed project schedules from all project team members.
- Finalize the project's scope statement and planning assumptions. Finalize the overall project schedule.

Prepare a Business Impact Analysis (BIA) Questionnaire

But what is *business impact analysis*? At a basic level it is a means of systematically assessing the potential impacts resulting from various (unavailability) events or incidents

Commonly, impacts resulting from other types of incident (such as breach of confidentiality or loss of data integrity) are simultaneously explored, but this need not be the case when only considering business continuity planning or disaster recovery. However, there are certainly advantages to undertaking a comprehensive and wider focused exercise.

The BIA is intended to help understand the degree of potential loss (and other undesirable effects) which could occur. This will cover not just direct financial loss, but many other

issues, such as loss of customer confidence, reputation damage, regulatory effects, and so on.

The project team should prepare a BIA questionnaire, introduction memo, and questionnaire instructions to gather the following information from the business operations to be surveyed:

- Financial impacts to the organization resulting from each business operation's inability to conduct operations for a prolonged period of time.
- Operational impacts relating to each business operation.
- Extraordinary expenses involved in continuing operations after a disruption.
- Current state of preparedness to resume business operations.
- Seasonal Impacts relating to each business operation.
- Technology requirements for resumption and recovery.
- Other special resumption and recovery resources.
- Information Systems support for resumption of time-sensitive operations.

Conduct Second Senior Management Meeting

Conduct a second senior management meeting to review the revised project schedule, the project scope statement, and the planning assumptions. Based on management feedback, revise the proposed schedule and overview documentation, as necessary, until approval is obtained.

Select BIA Questionnaire Recipients

Based on the scope of the planning project agreed to by senior management, the project team should identify the line managers who will be recipients of the BIA questionnaire.

Introduce the Project to Division, Branch, and/or Department Management

Conduct introduction meetings with the managers of all affected divisions, branches, or departments using a subset of the senior management presentation and subsequent memos as meeting material. Remember that you are asking for their support.

Suggested Meeting Agenda Overview

- Explain that the meeting attendees and their employees, will be asked from time-to-time to respond to questionnaires or give brief descriptions of their duties in time-sensitive areas.
- Explain the resource commitments and timing required.
- Request their input, comments and support throughout the planning process.
- Review the proposed project schedule and make any adjustments that appear necessary.

Distribute BIA Questionnaire to Recipients

The project team will distribute the BIA questionnaire either electronically (via LAN, E-mail, or diskette) or on paper. Automated processes are more easily maintained and are repeatable. Since a BIA is not a one-time exercise, an automated process is preferred. Some of the information collected for the BIA can be used as initial data for constructing plans. Recipients should be given approximately two weeks to complete their responses.

Step Two: Business Impact Analysis

The BIA is one of the most important steps in the overall BCP process. The data gatherer is pivotal to identifying key business issues and justifying to executives the resources needed.

The BIA determines the financial exposures and operational impacts resulting from a major disruption of services. It will provide your organization with:

- The identity of its time-sensitive business operations and services
- An analysis of the organization's financial exposures and operational impacts
- The time-frames in which time-sensitive operations, processes and functions must resume
- An estimate of the resources necessary for successful resumption, recovery and restoration.

In addition to a BIA, it is important to conduct a facility/structural vulnerability analysis. The BIA will provide the rationale and cost justification for risk mitigation and response, resumption, recovery and restoration-related decisions.

Gather Business Impact Analysis Data

BIA questionnaires should be tracked against the recipient list. Follow up with any individuals who are overdue in returning their responses. If the organization is large or complex, evaluate automating this process as much as possible. Some BIA software automatically tracks questionnaires sent out and received.

Review Initial Business Impact Analysis Results

Review initial BIA questionnaire data for completeness and consistency; request additional information as necessary. The initial review of returned survey data would allow the project manager to uncover any area of ambiguity in questions asked or answers given.

Conduct BIA Interviews

- Every major business operation should be evaluated using the BIA approach. Each line manager must be aware of the length of time that a particular service, business operation or application system may not be available, and devise interim procedures to ensure the continuity of the most time-sensitive activities.
- The resumption sequences, potential time delays, or service postponements for each business operation must be documented and endorsed by senior management. Senior management may be called upon to refine business time-sensitivity definitions, adjust resumption priority sequences or allocate additional resources and funding where resumption capacity becomes an issue.
- The project team should use this information to support the organization's strategies and any necessary investments in backup alternatives.

Identify Time-Sensitive Business Operation Processes and Application Systems

- Establish a method of grouping business operations, processes and application systems in line with their importance to the overall function of the organization like

business time-sensitivity ratings. Time-sensitivity ratings are usually expressed in terms of the minimum and maximum time that the organization can withstand an interruption of a particular business operation or application system.

- Record each business operation, process, function or application system along with its time-sensitivity rating. A comprehensive business continuity plan will document a single or multiple strategy and tasks for every level of business time-sensitivity.

Step Three: Disaster Readiness Strategies

Define and Cost Business Continuity Alternatives

Using the information from the BIA, the project team should evaluate the alternative strategies that are available to the organization, narrow the list of alternatives to the two or three most plausible, and develop budgetary costs for each strategy. The resumption timeframes will play a significant role in determining which components may require pre-positioning.

Recommend Disaster Readiness Strategy

Based on the needs of the business and your evaluation of alternatives, the project team should develop recommendations on which strategies to fund for implementation.

Prepare Senior Management Report and Presentation

Prepare a formal report and presentation on the findings of the BIA, the strategy alternatives that were developed and investigated, and the project team's recommendation.

Obtain Disaster Readiness Strategy Approval

Obtain approval from senior management to proceed with the project. Ensure that they understand and approve the funding required to continue the project and to implement the selected strategies. Some of the funding components for the project are:

- One-time cost of plan development (external consultants, internal resources, BIA and BCP software acquisition, initial training, etc.).
- Ongoing cost of plan maintenance (personnel training, plan exercises, software maintenance, etc.).
- One-time and annual costs for alternate sites (computer and business operation).
- One-time and annual costs for pre-positioned alternate communications (voice/data).

Step Four: Develop and Implement the Plan

Define the Scope and Number of Business Continuity Plans

Define the scope of the planning effort. The scope will directly affect the size of the continuity organization, the number of teams involved, and the number of plans you will need to develop. For example, the largest plan development scope, enterprise-wide disaster readiness planning, may require plans for:

- Multiple physical locations over broad geographic areas
- Various operations or departments at each location
- Business operations, processes or functions that require multiple agency cooperation to succeed
- Information technology ranging from desktop personal computers to inter-connected LANs to secure work resources to multi-server data centers, etc.
- Telecommunications (data, voice, video, multimedia, etc.) serving all internal locations and key client locations

Consider the size, complexity and scope your project. Clear definitions of scope and how plans relate to each other are essential to a well-managed plan development project.

Develop Alternate Site Request for Proposal

- Develop an alternate site Request For Proposal (RFP), if required by the approved strategies. This RFP should contain sufficient criteria and specifications to elicit accurate, detailed responses. Develop an evaluation matrix to review the RFP responses and evaluation criteria weighting, modified as necessary.
- The evaluation of responses should be agreed upon and placed in the evaluation matrix. The project team should document any points that they would like to negotiate with the vendors. The project team should make a recommendation for selection of the vendor to senior management.

Define the BCP Team Organization

Many teams have responsibilities that span multiple levels of continuity activities. Any teams that would be activated for response, resumption, recovery or restoration of operations should be represented on the BCP team.

- Each team should have an appointed team leader with all the management authority necessary to make and approve any reasonable team decisions (personnel scheduling, assignment scheduling, expenditures, etc.) for resumption, recovery and restoration. Document decision-making limitations and any assumptions that were made during the planning process. Clearly state all reporting relationships of team members.
- Create positions for every major operational area that will be addressed by the team. Team positions with tasks that require unique skills must be identified and specific personnel should be assigned to those positions. Designate alternates as back up and train them.
- In some cases it may be necessary to use specific contract or vendor personnel as team members. When personnel outside the organization are used in team(s), the

planners should develop support agreements/contracts that define the response time and support level(s) that will be required for training, exercise, response, resumption, recovery, and restoration operations.

- Positions that do not require specialty skills do not need to have specific personnel assigned. However, employee, vendor or customer data must be maintained so the assignments can be made at execution time. Controlling less time-sensitive team assignments in this way will reduce the ongoing plan maintenance activities.

Conduct Initial Meetings with the BCP Teams

Setting the right tone with the BCP team is extremely important. Detailed planning is a time-consuming task and team members will have other duties to perform. It is imperative that all members know the priority and goals that senior management has placed on this important undertaking.

Try to schedule this meeting outside the normal work environment and attempt to have a different executive open each meeting with a few words of encouragement. Use the introductory materials that were presented to senior and line management.

Meeting Agenda Overview

- Provide an overview of the BIA findings, approved business continuity strategies, plan development project and the response, resumption, recovery and restoration processes.
- Recap the meetings with senior and line management.
- Review and distribute the project support memos from senior management.
- Provide each team member with an overall team description, a detailed list of their anticipated duties, and any examples of tasks, if available.
- Answer any questions relative to duty assignments. Consider any suggested team definition, membership or operational changes.
- Modify team operational descriptions and responsibilities as appropriate.

Meeting Conclusion and Follow Up

- Schedule one-on-one meetings with all Team Leaders to review their specific assignments.
- Allow time for all team members to review, in detail, the materials that will be used.
- If you have selected a data gathering method for the project, familiarize each team with the approach during individual sessions.

Organize Plan Data

Using your time-sensitive business operations or processes and your data collection methodology, work with each team to define the resources required to restore its business operation following an interruption. Response, Resumption, Recovery and Restoration resources include:

People - team members, vendors, customers/clients, other employees, services, contacts and representatives, etc.

Places - alternate offices, processing locations, manufacturing facilities, off-site storage locations, control centers, vaults, etc.

Things - supplies, equipment (office, computing, voice & data communications, manufacturing), vital records (business data, software, documentation, forms, references, contracts), etc.

The business continuity plans should be prepared in such a way as to:

- Define the detailed action steps that must be taken in response to a declared disaster
- Notify appropriate personnel, activate the plan
- Effect a timely resumption or recovery at the identified alternate facility, and restoration at a permanent facility.

Part of this task is to collect and prepare the specific documentation necessary to execute the plan's action steps. Also integrate or reference existing documentation for business operations and processes into the overall plan.

The BCP may include the physical loss or inaccessibility of the facility. You should also develop any training materials that will be used during the meetings to instruct the team members on plan development. This should include the data gathering method(s) to be used during the project:

- Familiarize team members with Business Continuity Planning information like that available on this site.
- Each team leader should review team positions. (Team leaders provide recommendations on the personnel assigned to these positions and additional positions they feel are necessary.)
- Review any previously developed plans that may be used as a model.
- Review project status reporting/problem management procedures.

Conduct Periodic Meetings with Teams

Conduct periodic project review meetings to discuss any problems or new issues uncovered since the previous meeting(s). Provide the data requested during the initial meetings (team positions, recommended personnel assignments, etc.) and report progress concerning data gathering efforts and resulting plan updates.

Each meeting agenda should be designed to raise and resolve issues and make whatever decisions are required.

Identify Team Tasks and Procedures

Assign team leaders the responsibility of organizing and drafting the sequence of tasks their teams will perform during response, resumption, recovery and restoration processes:

- Emergency response
- Problem escalation
- Activation and mobilization
- Resumption operations
- Recovery operations
- Restoration of facilities and contents

Develop a method for coding tasks for easy reference and maintenance. Each team should identify and document the procedures they will use to accomplish each task or group of tasks (normal business procedures or specialized alternates for resumption). Recommend that each team include references to these procedures in the appropriate task descriptions and store backup copies off-site as vital records.

Conduct Plan Document Reviews

Have project team members review selected reports of plan data and adjust the contents as necessary. Develop a sample plan execution script as a model for plan documentation, and meet with the project team to review and adjust the model. Review the contents of the text portion of each plan.

Present the agreed-upon plan documentation format with a completed plan to senior management for their review and approval.

Step Five: Maintenance and Testing

Establish a Plan Exercise Program

Develop and conduct plan exercises. Exercises will grow in complexity over time. Include announced and unannounced events.

Document your objectives for each exercise. Individual objectives should include responsibility assignments and measurement criteria. Evaluate the results of each exercise against pre-stated measurement criteria and document results along with proposed plan enhancements.

Establish Training Requirements

The requirements for team training will vary from plan to plan and by the category of team (e.g., operations, support and technology).

The complexity of the environment and the time-sensitivity of the functions will guide the project team in the development of training. Training materials should cover all Steps of disaster readiness planning.

Sample Emergency Response Exercises

Emergency response exercises should be ongoing, quarterly events using alternate scenarios and should involve every organization within a particular facility that may be affected by a system disaster.

Sample BCP Exercise - Phase 1

First-level activation of the continuity plan:

- Simulate outage to an Information Systems (IS) facility.
- Conduct initial damage assessments and report findings to the Team for use in decision making
- Activate the plan and resume a single business operation, process or application system.
- The Coordinator schedules a follow up meeting with all team leaders to modify the plan where necessary.

Sample BCP Exercise - Phase 2

Restore data from archive to resume business:

- The application system, business operation, process, or function is restored to a normal production status using data and records retrieved from off-site archive storage.
- This level of exercise verifies any and all changes made in Phase 1; it also verifies vaulting and logistics procedures.

Sample BCP Exercise - Phase 3

All functions of facility exercised:

- Exercise all functions for the facility or organization, instead of limiting the exercise to one business operation or application system

Sample BCP Exercise - Phase 4

Unannounced exercise:

- After the corrections from Phase 3 have been reviewed and the Plan has been modified, simulate a disaster in the facility or organization.
- There should be no notification outside of senior management and team members should not be allowed to enter their normal work areas.

Update and Refine the Plan Regularly

Develop Plan Maintenance Procedures

Maintenance procedures consist of two general categories: scheduled and unscheduled. Scheduled maintenance is time-driven. Unscheduled maintenance is event-driven.

In most organizations, changes in personnel, responsibilities, processing and communications equipment and the like are common. In a dynamic organization, changes in business processes, facilities and the like might be common.

Scheduled Maintenance

Scheduled maintenance occurs as the result of a scheduled review of the business continuity plan. Reviews are predictable (based upon established requirements) and are scheduled at decided time intervals (weekly, monthly, quarterly, etc.).

The purpose of the review is to determine what changes are required. Initiate scheduled plan reviews. Ensure that the necessary updates are made to the plan. Team leaders are responsible for reviewing their assigned portions of the plan.

The review will address any events that have occurred within each team's area of responsibility that may affect the organization's response, resumption, recovery or restoration capability. The review will expose any updates or changes that may be required.

Unscheduled Maintenance

Certain maintenance requirements are unpredictable and cannot be scheduled. The majority of these unscheduled plan changes occur as the result of major changes to the organization, business operations, processes, functions, hardware configurations, (voice/data) networks, etc.

Stay on top of all changes to the plan resulting from unscheduled maintenance. The team leader whose area of responsibility is affected may submit changes.

Prepare Yourself to Declare a Disaster

Selected members of senior management declare a disaster as it involves the expenditure of money, manpower, and corporate resources. A small problem such as a power outage or leaking pipe could escalate into a full-blown disaster with time.

You must establish procedures for escalating to a disaster declaration, including notification of appropriate recovery team members, senior management, outside vendors, and others involved in disaster readiness planning.

Steps towards Creating a Business Continuity Plan

Preliminary Phase

1. Use the BCP Scorecards as an introductory step to measure of your organization's readiness.
2. Appoint a Business Continuity Coordinator.
3. Look into purchasing and implementing BCP software.
4. Confirm that senior management is open to discussing support of business continuity plans for your organization.
5. Develop a Business Continuity Plan Checklist that fits the needs of your organization. An example of such a checklist is provided.

Additional BCP Items - Scorecards

Would your organization be able to recover from a computer systems failure? Could this be substantiated? The *Executive BCP Scorecard* shown on the next page offers a quick measure of your organization's readiness.

On the following page is an *IT Management BCP Scorecard* which is designed to have both your IT management and staff measure readiness to handle a serious business interruption.

Both of these would be useful in a preliminary analysis of your organization's readiness. Also remember that some of the questions may not apply to your organization. Additionally, since every organization is unique, add items as necessary to create your own BCP scorecard.

Further, explore the *Business Continuity Plan Checklist,* which outlines the ideas and concepts presented in this document in a checklist format.

Executive BCP Scorecard

#	Executive BCP Scorecard	Yes	No	?
1.	Do you have a written business continuity plan?			
2.	If so, have you fully tested it?			
3.	If tested, did you pass your test?			
4.	Have you quantified and ranked the business and financial risk of outages to all vital functions?			
5.	Are you prepared to address liabilities and fiduciary responsibilities in case of disaster?			
5.	Are business continuity plans kept current and updated for business changes?			
7.	Do you perform back-ups faithfully and include every server and hard disk?			
8.	Do you regularly send you back-ups to a safe, off-site archive?			
9.	Have you standardized on a proven media, drive, software, and automation back-up solution?			
10.	Does business continuity and disaster recovery readiness have support of top management in your organization?			

IT Management BCP Scorecard

#	IT Management BCP Scorecard	Yes	No	?
	Back-up and Recovery Best Practices			
1.	Do you backup your data regularly and include every server and hard disk?			
2.	Does your current backup and recovery methodology meet management's business uptime needs?			
3.	Do you always use the "verify" option to ensure your backups are working?			
4.	Do you use backup rotations to provide a good depth of file versions?			
5.	Do you know how fast your data is growing?			
6.	Have you selected a scalable backward- and forward-compatible solution (hardware and software) that supports data growth?			
7.	Are backups fully automated for unattended operation (autoloaders, etc.)? If manual, do you have a bulletproof process and follow written procedures?			
	Archive Best Practices			
1.	Do you regularly send your backup copy to a safe, off-site archive?			
2.	Do you retain archive data for legally required duration?			
3.	Is media properly cared for when shipped, handled, stored, and used?			
4.	Is your archive system designed to facilitate data format standards and an archive tape tracking method?			
5.	Do you have a migration policy to "refresh" tape technology and data formats every three to five years to ensure truly permanent access?			
	Business Continuity for Disaster Recovery Best Practices			
1.	Is senior management fully committed to disaster recovery?			
2.	Have you conducted a business impact analysis (BIA) to quantify and rank the financial risk of outages to all vital functions?			
3.	Have you taken action to mitigate known risks and single points of failure (e.g. power loss, physical access, etc.)?			
4.	Do you have a written BCP that includes backup and archive procedures?			
5.	Have you tested your plan using a worst-case scenario (loss of a facility)?			
6.	Did testing prove that you can meet all recovery time requirements?			
7.	Is your business continuity plan updated regularly to keep it current with business and staffing changes?			
8.	Do you have an adequate budget to support your disaster recovery program?			
9.	Have you standardized on industry-standard media, tape drives, software, and automated back-up solutions?			
10.	For 7x24 applications, do you remotely journal, log, mirror, or electronically vault data to your hot site?			
11.	Do you understand your disaster recovery costs, options, and disaster declaration procedures?			
12.	Do you bring multiple tape sets to a test or recovery with current, self-reliant documentation?			

Business Continuity Plan Checklist

☑	*STEPS & ITEMS* (*MODIFY, DELETE OR ADD AS NEEDED*)	**Duration** (days or hrs)	*START* (*DATE*)	**Finish** (date)
	Step One: *Initiation*			
	Prepare for meeting with Senior Management			
	Review any existing policies & procedures.			
	Research local events with negative effect.			
	Prepare to discuss project funding.			
	Research necessary training.			
	Access to PCs for team leaders. BCP software?			
	Draft the Project Schedule.			
	Conduct Kickoff Meeting with Management			
	Form the Project Team – delineate roles.			
	Finalize the Detailed Project Schedule			
	Prepare BIA questionnaire			
	IS support for resumption of operations.			
	Select BIA questionnaire recipients			
	Distribute BIA Questionnaire to Recipients			
	Step Two: *Business Impact Analysis*			
	Gather & review BIA analysis data			
	Conduct BIA interviews			
	Identify time-sensitive processes.			
	Step Three: *Disaster Readiness Strategies*			
	Define & cost Business Continuity Alternatives			
	Recommend DR Strategy - business needs.			
	Prepare Management Report and Presentation			
	Obtain Disaster Readiness Strategy Approval			
	Obtain approval for funding components.			
	Step Four: *Develop and Implement the Plan*			
	Define the scope and number of BCPs			
	Develop alternate site RFP			
	Define the BCP teams, conduct meetings			
	Organize plan data			
	Resources lists: people, places & things.			
	Schedule BCP team meetings.			
	Identify team tasks and procedures			
	Emergency response			
	Identify problem escalation			
	Identify resumption & recovery operations			
	Identify restoration of facilities and contents			
	Conduct plan document reviews			
	Step Five: *Maintenance and Testing*			
	Establish a Plan Exercise Program			
	Establish training requirements			
	Prepare and run sample exercises			
	Update and refine the plan regularly			
	Develop plan maintenance procedures			

BCP Resources

There is a variety of helpful resources listed here, running from software to online resources to books. One of the most valuable resources, however, is the Internet and the wealth of information available there. The best thing that we can offer to you is advice to use search engines, such as *Google* (www.google.com) or *Yahoo!* (www.yahoo.com) to locate new information. We will continue to update our own online resources at AnyKeyNow.com, much as this version of our Business Continuity Planning document has been updated.

Business Continuity Planning Companies & BIA Software

A number BCP companies and software tools are available to help develop a BIA, some of which come as part of a larger business recovery software package. A few are listed here. BIA software should only be used as an aid. It is no substitute for thought and analysis.

All Hands Consulting
Simpsonville, MD (410) 730-5677
http://www.allhandsconsulting.com

BRProactive, Inc.
Diamond Bar, CA, (909) 861-8805
http://www.brproactive.com

Comdisco Inc.
Rosemont, IL, (800) 321-1111
http://www.comdisco.com
(*SunGard acquires Comdisco Business Continuity Assets 11/15/2001*)

DavisLogic, Inc.
Columbia, MD (410) 730-5677
http://www.davislogic.com

Computer Security Consultants Inc.
Ridgefield, CT, (800) 925-CSCI
http://www.csciweb.com

McGladrey and Pullen
Bloomington, MN, (800) 648-4030
http://www.disaster.mcgladrey.com

Risk Associates
Altrincham, Cheshire, UK +44 1625 869 326 (International)
http://www.securityauditor.net/bcp-generatoor/

Strohl Systems
King of Prussia, PA, (800) 634-2016
http://www.strohlsystems.com

SunGard Planning Solutions
Wayne, PA, (800) 434-0002
http://www.sungard.drexperts.com/software

Disaster Recovery Articles

The Twenty Most Critical Internet Security Vulnerabilities (Updated): The Experts' Consensus
Copyright 2001-2002, The SANS Institute, Version 2.504 May 2nd, 2002
The SANS/FBI Top Twenty List is valuable because the majority of successful attacks on computer systems via the Internet can be traced to exploitation of security flaws on this list.
http://www.sans.org/top20.htm

Business Continuity Lessons Learned from September 11th: A Summary
Global Continuity plc, December 12, 2001
The whole Western world was stunned by the events of September 11th, 2001. Three months after the attack on the World Trade Center, David Honour summarizes the business continuity lessons. *This is a must-read article.*
http://www.globalcontinuity.com/default.asp?Art=6219&Type=News

September 11, 2001, Terrorist Incidents Lessons Learned: New Approaches Needed for Disaster Recovery and Business Continuity Planning
National Infrastructure Protection Center, Highlights, Issue 11-01, December 7, 2001
http://www.nipc.gov/publications/highlights/2001/highlight-01-11.htm

Lessons Learned
EMC Corporation, December 28, 2001
Who could have guessed that bridges and tunnels could become single points of failure in the information technology infrastructure? September 11th demonstrated that the physical scope of a disaster can go far beyond the local facility, cutting off support people from the site and breaking communications between sites. (Note: you will need the Adobe Acrobat Reader to view this file.)
http://www.emc.com/continuity/lessons_learned.pdf

Know Your Enemy: The Tools and Methodologies of the Script Kiddie
The Honeynet Project, Last Modified: 21 July, 2000
The Know Your Enemy series is dedicated to teaching the tools, tactics, and motives of the blackhat (hacker) community. The script kiddie is someone looking for the easy kill. They do this by focusing on a small number of exploits, and then searching the entire Internet for that exploit. Sooner or later they find someone vulnerable - will it be your site? A "must-read" for those involved in computer security.
http://project.honeynet.org

A River Runs Through IT
CIO Magazine, April 1, 1998, COVER STORY: DISASTER RECOVERY
Your computer systems can be the lifeblood of your company. Here's how to make sure you'll be able to recoup your business if... A River Runs Through IT
http://www.cio.com/archive/040198_disaster.html

Daring To Look Down
CIO Magazine, June 1, 1995, COVER STORY: DOWNTIME Daring To Look Down
No one likes to think about computer downtime, but pretending that it can't happen is asking for even worse trouble.
http://www.cio.com/archive/060195_downtime.html

EmergencyNet News: Daily News Summary
This site offers 24-hour news, information, analysis & coverage of disasters and major emergency events.
http://www.emergency.com/ennday.htm

Online & Print BCP Resources

BCP & DR Forum
A service of globalcontinuity.com (below). This email bulletin board allows professionals involved in the business continuity and disaster recovery fields to discuss these subjects, share information and support each other. It will also provide a means of quickly sharing operational information in any future disaster scenario.
http://groups.yahoo.com/group/drmb

globalcontinuity.com
This information service is provided by Global Continuity plc (http://www.gcplc.com/). It is one of the largest and most organized BCP/DRP resources on the Internet, providing news, online education, an extensive knowlege database, links and more. Requires sign-in, and one may opt for an excellent newsletter subscription.
http://www.globalcontinuity.com/

Disaster Recovery Journal
Print subscriptions: free to qualified individuals
http://www.drj.com

Disaster Resource Guide
http://www.disaster-resource.com

SunGard Knowlege Net
White papers, briefs, and articles provided free of charge to improve the effectiveness of continuity planning. You must be registered with SunGard to access these materials.
http://www.sungard.drexperts.com/knowledgenet/

FEMA's Online Library
FEMA Information Technology Room. This excellent library is divided into four sections. Each section contains publications, reference materials, photographs, audio clips and video clips.
http://www.fema.gov/library/

National Infrastructure Protection Center (NIPC)
An entity of the Federal government offering national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation. Check their publications, especially their online *CyberNotes* section, published every two weeks.
http://www.nipc.gov/publications/publications.htm

SANS Institute
The SANS (System Administration, Networking, and Security) Institute 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. Certification programs, in-depth education and newsletters are just a few of the items they produce.
http://www.sans.org/

CERT Coordination Center
The CERT/CC is a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. They study Internet security vulnerabilities, handle computer security incidents, publish security alerts, research long-term changes in networked systems, and develop information and training to help improve site security. Advisories and summaries are available via free email subscription as well.
http://www.cert.org/

CIAC
The CIAC (Computer Incident Advisory Capability) Website is sponsored by the U.S. Department of Energy, and is an excellent source of technical bulletins regarding high-risk computer vulnerabilities. Numerous links to many other security-related bulletins and organizations. Has an excellent overview of security tools, including those in public domain or freely available on the Internet, some of which can be downloaded directly from their site.
http://www.ciac.org/ciac/

Hoaxbusters
Sponsored by CIAC (above), this frequently-updated site recognizes the fact that many Internet hoaxes, though seemingly humorous, can still be time consuming and costly to remove from all the systems where they exist. Their pages describe some of the warnings, offers, and pleas for help that are filling our mailboxes, clogging our email servers, and that generally do not have any basis in fact. They offer proactive suggestions on how to stem the flow of these hoaxes.
http://hoaxbusters.ciac.org/

The HoneyNet Project
This is a non-profit research group of thirty security professionals dedicated to information security research. Their goal to learn the tools, tactics, and motives of the blackhats (hacker, cracker, attacker, bad guy, etc.) and share these lessons learned, benefiting both its members and the security community. They volunteer their time and resources to conduct this research. All of their work is shared with the security community. If you're at all involved in computer security, this is well worth looking into.
http://project.honeynet.org/

Network Security Library
This resource is sponsored by GFI Software Ltd., a leading worldwide supplier of security tools for NT/2000 administrators. They also have excellent security articles covering UNIX, Windows, NetWare, the Internet, firewalls, intrusion detection, security policies and more. Also, don't miss their *Guides to (mostly) Harmless Hacking*, so that you'll understand where vulnerabilities in your own systems may lie.
http://secinf.net/

NIST Computer Security Division & CSRC Home
The National Institute of Standards and Technology (NIST) has a Computer Security Division (CDS) Website. This is also the home of the Computer Security Resource Center (CSRC). You can sign up for immediate email notification when new NIST computer security publications or news becomes available by subscribing to the NIST computer security publications email list.
http://csrc.nist.gov/index.html

Computer Security Resource Center (CSRC) Publications
Offers a wide variety of publications with focus areas including "*cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support*." An excellent resource.
http://csrc.nist.gov/publications/

Super DLTtape: Data Protection Best Practices
Formerly known as the *Prove It Initiative*, this Web site is a free, on-line resource that is sponsored and maintained by Quantum Corporation, developer of the core technology in the DLT tape system. Quantum and more than 20 leading technology companies, launched the Prove It campaign, a major educational initiative, to help mid-sized businesses better prepare for computer data related disasters.
http://www.dlttape.com/Practices/Default.htm

FAQS.org Computer Security Index
This is a regularly-updated list of numerous computer security FAQs available on the Internet.
http://www.faqs.org/faqs/computer-security/

Center for Internet Security
CIS is a not-for-profit cooperative enterprise helping users and operators, along with their insurers and auditors, to reduce the risk of significant disruptions to e-commerce and business operations due to technical failures or deliberate attacks. More than 170 companies, educational organizations, government and law enforcement agencies and individuals from around the world are members.
http://www.cisecurity.org/

ISO 17799
ISO 17799 is the most widely recognized security standard to date. Originally published in the mid-nineties and based upon BS7799 (May 1999), the first version of ISO 17799 was published in December 2000. This standard is comprehensive in its coverage of security issues, and contains a substantial number of complex control requirements. Compliance with this standard is far from being a simple task, even for the most security conscious of organizations. ISO 17799 should be approached step by step, beginning with an assessment of the current status and followed by identification of what changes are needed to meet ISO17799.
http://www.iso17799software.com/presentation/index.htm

Books

Sorted by author

Enterprise Operations Management Handbook, Second Edition
by Steven F. Blanding (Editor)
Hardcover - 672 pages 2nd edition (October 22, 1999)
CRC Press - Auerbach Publications; ISBN: 084939824X
Price: $66.50

Computer-Related Risks
by Peter G. Neumann
Paperback - 367 pages (10/1995)
Addison-Wesley Pub Co; ISBN: 020155805X
Price: $29.95

Information Warfare & Security
by Dorothy E. Denning
Paperback - 522 pages 1st edition (12/1998)
Addison-Wesley Pub Co; ISBN: 0201433036
Price: $39.99

Business Continuity Planning, 2000 Edition:
A Step-By-Step Guide With Planning Forms on CD-ROM
by Kenneth L. Fulmer
Paperback - 134 pages Book & CD edition (08/2000)
Rothstein Associates Inc; ISBN: 0964164817
Price: $99.00

Exercise Alternatives For Training Emergency Management Command Center Staffs
by Walter Guerry, III Green
Paperback - 200 pages 1 edition (6/2000)
Upublish.com; ISBN: 1581127480
Price: $19.95

Command and Control of Disaster Operations
by Walter Guerry, III Green
Paperback - 286 pages (10/2001)
Unknown; ISBN: 158112659X
Price: $25.95

A Primer for Disaster Recovery Planning in an IT Environment
by Charlotte J. Hiatt
Paperback - 276 pages (12/1999)
Idea Group Publishing; ISBN: 1878289810
Price: $64.95

Disaster Recovery Library : Data Recovery3
by IBM International Technical Support Organization (IBM Redbooks)
Softcover - 192 Pages (10/1999)
IBM Corporation; ISBN: 0738405396
Price: $25.00

Manager's Guide to Contingency Planning for Disasters:
Protecting Vital Facilities and Critical Operations
by Kenneth N. Myers
Hardcover 2nd edition (8/1999)
John Wiley & Sons; ISBN: 047135838X
Price: $55.00

Encyclopedia of Disaster Recovery, Security & Risk Management
by Tari Schreider
Spiral-bound - 300 pages (11/1998)
Crucible Publishing Works; ISBN: 0966272900
Price: $69.00

Emergency Planning on the Internet
by Rick Tobin, Ryan Tobin
Paperback (12/1997)
Abs Group Inc; ISBN: 0865876002
Price: $65.00

Disaster Recovery Planning: For Computers and Communication Resources
by Jon William Toigo
Paperback - 352 pages 1 edition (12/1995)
John Wiley & Sons; ISBN: 0471121754
Price: $70.00

Disaster Recovery Planning: Strategies for Protecting Critical Information Assets
by Jon William Toigo, Margaret Romano Toigo (Illustrator)
Textbook Binding - 325 pages 2nd edition (11/1999)
Prentice Hall; ISBN: 013084506X
Price: $51.00

The Definitive Guide to Business Resumption Planning
by Leo A. Wrobel
Hardcover - 290 pages (10/1997)
Artech House; ISBN: 0890069484
Price: $85.00

Note: these books can be ordered by their noted ISBN from Amazon.com or from your favorite bookseller. All of the ISBN numbers are correct and current as of this writing.

In Closing…

We face new challenges when we look at the BCP issues of today, especially since the events of September 11th in New York City, Washington DC and Western Pennsylvania. These are thoughts that few of us anticipated, and had someone suggested that an organization or commercial establishment in one of our cities prepare for *counter-terrorism* as a part of current BCP and DRP practices, it's likely that a few eyebrows would have been raised. Yet the warning signs have been there for years, as the earlier terrorist attack on the World Trade Center in 1993 and the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on an April morning in 1995 should have taught us.

But preparing for such events is only one small facet of the overall picture of good business continuity planning. A small business owner asked me last summer what he could do to start his own homegrown BCP effort. I asked him if he was backing up his data on a regular basis, and he laughed and replied that he did when he thought about it. He had a change of heart last fall, and by the beginning of October was not only backing up his data nightly and storing his tapes off premises, he had implemented his own new BCP using the scorecards, checklists and some of the resources found in this document. He also employed the *KISS Principle (Keep It Simple, Stupid!)*, enabling him to get his simple BCP and DRP enacted within weeks.

Whether you're the owner of a small business or someone employed by a large corporation, the same principles apply: *Being prepared is crucial to protecting your organization in case of a systems disaster.*

It's just good business practice.

--==*==--

It is hoped that you found this document to be beneficial in your own business continuity and disaster recovery planning. If you did, please drop us a note and let us know how it helped you. If you found it lacking in some way, or found any errors, please let us know that as well.

John Williamson
jw@anykeynow.com

The AnyKeyNow Group
http://www.anykeynow.com

July, 2002