A Professional's Guide to the Contents of a Business Continuity Plan

by William M. Adney
InfoSolutions, Inc.
3642 Racquet Club Drive
Grand Prairie, TX 75052-6107
Phone: 972-642-4549
Email: billadney@compuserve.com

Reviewed by:
Kelley Goggins, MBCP

TABLE OF CONTENTS

List of Tables

List of Figures

EXECUTIVE SUMMARY

Objectives

If you have never created a Business Continuity Plan (BCP), it seems to be one of the most difficult tasks based on my observations and experience, and there always seems to be a lot of questions about what should and should not be included in the BCP.

This document will help you determine and structure the basic information that should be in an effective and viable BCP. Information in this document is based on DRI International's **Professional Practices for Business Continuity Planners** (see www.drii.org for the latest version) and other references as documented in the footnotes.

The objectives of ***A Professional's Guide to the Contents of a Business Continuity Plan*** are to:

- Document a structure for your Business Continuity Plan.
- Describe the general contents of each section and subsection.
- Provide guidelines, recommendations, and some examples of items that you may need in your Business Continuity Plan.
- Suggest a structure to integrate a Crisis Management Plan (CMP) with your Business Continuity Plan.

Business Continuity Plan (BCP) Overview

The Business Continuity Plan (BCP) is generally organized so that information required during a recovery operation is closer to the beginning of the document, except for detailed recovery procedures (e.g., Recovery Procedures for the Windows 2000 Server). The Table of Contents contains five chapters as shown in the following sections.

One other important point: this document is intended as a guide, not an absolute requirement, to help you determine the contents of a BCP that is most appropriate for your organization. For example, I have shown five (5) chapters because it is easy to obtain 5-tab indexes, but I have written BCPs that contain twenty (20) or more chapters. In general, how you organize your BCP is not as important as being certain that you have all of the information required to effectively implement your plan.

Chapter 1 – Overview and General Information

Chapter 1 contains an overview of the BCP including the purpose, scope, objectives, and assumptions made for the plan. Additional sections and subsections include, but are not limited to, a company's BCP Policy, BIA[1] Summary, recovery strategy, EOC location(s), damage assessment, escalation plans/procedures, and general information about the Crisis Management Team in this chapter. The BCP team organization chart are also included in this chapter.

Chapter 2 – Critical Business Continuity Plan Information

Chapter 2 contains the call lists, task lists, and various resource inventories by team to make it easier to execute the BCP, as well as improving the ease of distribution and updating. Inventories include lists of Customers, Equipment, Software, Supplies, Telecommunications, Vendors, and Vital Records that are required to support the BCP.

Chapter 3 – Plan Administration and Maintenance

Chapter 3 contains a variety of information related to administering and maintaining the BCP. It includes sections and subsections on administration, training, maintenance, awareness programs, education, and auditing the BCP. While most of this information is the responsibility of the Business Continuity Coordinator, it also documents important procedures such as the Board of Directors' annual approval of the BCP for bank and other financial institution operations as required by the Federal Financial Institutions Examination Council (FFIEC).[2] This policy applies to all FFIEC agencies including the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).

Chapter 4 – Plan Testing and Test Reports

Chapter 4 contains information on the various types and frequency of plan testing. New terms will be added to the Glossary as required, such as tactical exercise ("war game"), etc. This chapter also provides a repository for test reports, although some Business Continuity Coordinators prefer to place test reports in an appendix.

[1] DRII Professional Practices – Subject Area 3: Business Impact Analysis
[2] FFIEC Corporate Business Resumption and Contingency Planning Policy Revised March 1997

Chapter 5 – Appendices

Chapter 5 contains various appendixes, including detailed procedures, that support the BCP. For example:

A Glossary
B Recovery Site Information (e.g., directions, maps, contract copies, etc.)
Other appendixes (for detailed procedures, etc.) as required.

Appendix A includes a glossary which is a substantial revision of the current DRII terminology plus some new terminology, such as Business Continuity Coordinator, Business Continuity Plan, and Business Continuity Planner. Some of the current terms are not consistent with DRII Professional Practices and will be replaced in the glossary.

The Crisis Management Plan (CMP) and the BCP

Every organization has a variety of crises which may range from a simple building evacuation for some reason (e.g., a bomb threat) to full-scale, easily recognized disaster. The objective of the Crisis Management Plan (CMP) is to manage these crises, and provide a framework and structure for activating the Business Continuity Plan (BCP).

For example, I normally include three essential teams in the CMP:

- Damage Assessment/Salvage Team
- Logistics/Transportation Team
- Public Relations/Communications Team

Also, I include an Escalation Plan in the CMP to provide the Crisis Management Team (CMT) with a guideline on when a disaster declaration may be appropriate. A guideline is just that – a guideline, and it is up to an organization's most senior management (i.e., the CMT) to determine what is appropriate based on the circumstances at the time of the specific event.

For purposes of this paper, all teams shown above and the Escalation Plan will be shown as part of the BCP; however, you may need to adjust these teams and names for consistency in your own BCP and/or CMP.

About the Author

Bill Adney has over 35 years' experience in data processing and over 25 years' experience in

Business Continuity Planning.

Mr. Adney is currently president and owner of InfoSolutions, Inc. He has performed a wide variety of disaster recovery, information/physical security, and programming consulting assignments for major firms in the retail, insurance, financial, manufacturing, and aerospace industries, involving work with a wide variety of system configurations, including IBM mainframes, minicomputers, LAN/WAN networks, and personal computers. These assignments have included responsibility for large project management, business continuity/disaster recovery project planning and implementation/testing, and information security project planning and implementation, and have required knowledge of data center security and operations, applications development and implementation, and programming.

As Manager of Security and Contingency Programs for a large West Coast oil company, he was directly responsible for the planning and implementation of the corporate disaster recovery plan and user recovery procedures for the critical financial systems. His overall data processing dates experience dates back to 1967, and he has actively developed a wide variety of disaster recovery and business continuity plans since 1977. Mr. Adney has successfully developed DRPs and BCPs for companies such as Texas Instruments, McDonnell Douglas, Household International, E-Systems, Chief Auto Parts, FootActionUSA, Metropolitan Life, Texas Department of Criminal Justice, Sunbeam Corporation, The Associates, PEMCO Financial Services, The South Financial Group, Washington Mutual, and the Veterans Administration – Financial Services Center.

Contents of a Business Continuity Plan

Chapter 1 – Overview and General Information

Chapter 1 contains an overview of the BCP including the purpose, scope, objectives, and assumptions made for the plan. Additional sections and subsections include, but are not limited to, a company's BCP Policy, BIA Summary, recovery strategy, EOC location(s), damage assessment, escalation plans/procedures, and general information about the Crisis Management Team in this chapter. The team organization and an organization chart are also included in this chapter.

1.0 Before You Begin

In accordance with the DRII Professional Practices, there are several steps you should have completed before you begin the preparation of your Business Continuity Plan:

1. Project Initiation and Control
2. Risk Evaluation and Control
3. Business Impact Analysis
4. Developing Recovery Strategies
5. Emergency Response and Operations
10. Coordination with Public Authorities

I have found that item 5. Emergency Response and Operations and item 10. Coordination with Public Authorities seem to be most appropriate in the Crisis Management Plan.

The following DRII Professional Practices areas will be specifically addressed in this Business Continuity Plan:

6. Developing and Implementing Business Continuity Plans
7. Awareness and Training Programs
8. Maintaining and Exercising Business Continuity Plans
9. Public Relations and Crisis Coordination

There are at least two documents you should prepare before you get too far along in your BCP: a cover page and a table of contents. Other documents you should also have are described in the following sections.

1.0.1 Cover page

The cover page may be the most important part of your BCP, at least in the beginning. When someone asks to see your plan, even if you don't have a professional binding, a nice cover page will make a good impression. Your company logo on the cover page helps convey a professional image. Keep the cover page simple and professional.

1.0.2 Confidentiality Statement

The information in your BCP is quite sensitive and usually confidential within your organization or company, so you should at least have a Confidentiality Statement immediately after the cover page. Some organizations have security requirements that dictate a statement of confidentiality appear on every page, usually in a footer. Be sure to find out any special requirements for your organization or company.

1.0.3 Distribution/Update List

Your BCP will need updating, especially the call lists when people change positions or leave the organization, and you will need some way of tracking who has the BCP and when the last update was made to that particular copy. A distribution/update list helps with this task, especially if you are the Business Continuity Coordinator and need to be able to look at a particular BCP to determine its latest update.

The distribution/update list only needs to have the following information:

Name	Phone	Mail Location	Date Issued	BCP Updated on	BCP Updated by

Table 1 – BCP Distribution/Update List

If you have the mail location on your list as shown above, you can simply attach the page to the updates you send out and highlight the name and mail location.

1.0.4 Table of Contents

I have found it's always helpful to prepare a draft table of contents, or at least an outline, of what I expect to have in a BCP before I actually begin writing. A few minutes' thought and planning can save you a lot of time later on. Of course, you will want to use the automated feature of most word processors to generate your table of contents as a final document.

1.1 Business Continuity Plan Overview

An overview and description of the organization of the Business Continuity Plan.

For example…

Chapter 1 contains an overview of the BCP including the purpose, scope, objectives, and assumptions made for the plan. Additional sections and subsections include, but are not limited to, ABC company's BCP Policy, BIA Summary, recovery strategy, EOC location(s), damage assessment, escalation plans/procedures, and general information about the Crisis Management Team in this chapter. The team organization and an organization chart are also included in this chapter.

Chapter 2…etc.

1.1.1 Objectives

A list of objectives for the Business Continuity Plan, such as:

- Develop a Business Continuity Plan structure for managing a disaster that affects the ABC Company.
- Document critical information as required for the implementation of the Business Continuity Plan.
- Provide guidelines with an escalation plan for the ABC Company for a disaster declaration that will result in the execution of this Business Continuity Plan.

1.1.2 Scope

A definition of the scope of this Business Continuity Plan, such as:

The scope of this Business Continuity Plan is limited to the business offices of ABC Company, 123 Main Street, Anytown, XX 99999.

In general, it is best to limit the scope to a specific location because a disaster is generally location-specific. Don't try to write a BCP that covers all of your company locations or you will not be able to manage the project, let alone write the plans. Remember that you will probably have to provide status reports on your progress, and it's easier to see progress on location-specific plans.

1.2 Business Continuity Plan Policy

For documentation purposes, I recommend that you include your Business Continuity Plan Policy as part of your BCP. If your organization does not have an officially approved policy, I recommend that you create one before you begin the BCP; otherwise, you will almost certainly have major issues attempting to get information and cooperation in the development of your BCP.

If your organization is subject to any regulatory agency, you may find there is a requirement for you to have a BCP policy. And even if you do not have any regulatory concerns, it is still a best practice to include a copy in your plan.

1.3 Business Continuity Plan Assumptions

All BCPs should contain a list of assumptions upon which the plan has been developed.

For example…

The Business Continuity Plan has been developed and maintained based on the following assumptions:

- That the Plan is designed to address a worst-case scenario – the ABC Company's business offices are unavailable for an extended time on the order of four to six weeks.
- That a backup of critical computer systems occurs daily (usually around midnight) and these backups (usually tape) are sent to offsite storage early the next morning.
- That, if the interruption occurs during the end of a normal business day, ALL transactions generated during that day will be lost (daily backup tapes have not been created and sent to offsite storage).
- That the level of Plan detail is based on the premise that sufficient and knowledgeable ABC Company personnel will not be incapacitated by the interrupting event, and can execute the Business Continuity Plan. This may not be a valid assumption if your plan must include the capability to handle a 9/11 scenario; be sure to check with your senior management on this.
- That items in offsite storage are in a secure, environmentally protected facility sufficiently remote from the ABC Company to not be affected by the same interrupting event.

Keep in mind that the above are samples only, and you will have to develop your own assumptions based on the planning directives of your senior management. Also, I recommend that you get senior management approval on your BCP assumptions before you develop any additional BCP details.

1.4 Business Impact Analysis (BIA) Summary

It is a best practice to conduct a Business Impact Analysis before you begin your Business Continuity Plan. This section includes a short summary of the most important data obtained from the BIA such as the business unit, responsible manager, process/business function, recovery time objective (RTO), estimated daily financial losses.

For example…

Business Unit	Manager	Process	RTO	Daily Loss	Comment
Accounting	J. Doe	A/P	2 days	$1,000	Loss of discount

Table 2 – BIA Summary Example

I suggest using a spreadsheet for this summary because it makes it much easier to sort information to answer questions such as: "What is the shortest (longest) RTO?" or "What is the maximum (minimum) daily loss". And of course you will want to know what the total estimated daily loss is for your organization to help justify the cost of the Business Continuity Strategy.

1.5 Business Continuity Strategy

After you have completed the BIA, it is a best practice to document a formal Business Continuity Strategy and have it approved by senior management. Why? Because it will almost certainly require funding, and your senior management needs to know at least the estimated cost before they can approve it.

For BCP documentation purposes, I suggest including two simple statements in your BCP that reflects your Business Continuity Strategy such as:

In the event of a declared disaster affecting the ABC Company's business offices, business operations will utilize the Wazoo Business Recovery Center located at 1234 Center Street, Yourtown, XX 99999.

Contact information for the Wazoo BRC is located in Section 1.5.2 of this Business Continuity Plan. Additional information, including the contract and a map, can be found in Appendix B.

1.5.1 Emergency Operations Center (EOC) Locations/Contacts

Many organizations have three designated EOC locations: (1) a large conference room in the business office facility, (2) a hotel that is relatively convenient for all team members, and (3) the Alternate Site facility.

You will need to make sure that you have an address and contact phone listed in this section if you designate a hotel or other similar meeting place.

1.5.2 Alternate Site Locations and Contacts

There are at least two locations with contact information you should have in this section:

Alternate Site: Wazoo Business Recovery Center

Offsite Storage: Wazoo Offsite Storage

If you have a declared disaster, you will need to notify your Alternate Site and Offsite Storage locations. Remember that some commercial vendors charge a declaration fee upon notification, even if you do not completely implement your Business Continuity Plan.

1.6 BCP Team Description and Organization Chart

Before you get into the details of your plan, you need to generally know how your teams will be organized. Each team should have a Team Leader and an Alternate Team Leader. This section provides a brief summary of each team's responsibilities and an organization chart showing their relationship.

1.6.1 BCP Team Responsibilities

Executive Management Team

Consists of the most senior manager (at that location) and an alternate. Responsible for the overall direction, decision-making, and approvals required to implement the Business Continuity Plan. The BCP can generally be activated only by the Executive Management Team, especially if a commercial vendor charges a declaration fee upon disaster notification.

Business Continuity Coordinator

Responsible for assisting in the activation of the Business Continuity Plan. The BCC should be the most knowledgeable person on the details of the BCP. The BCC is frequently designated to provide emergency notification to the Alternate Site and Offsite Storage facility.

Logistics/Transportation Team

Responsible for making emergency arrangements for personnel transportation, lodging, and dining at the Alternate Site. Also is responsible for ordering and ensuring the delivery of offsite

storage items and Supplies (from the Supplies List).

Damage Assessment/Salvage Team

Responsible for the damage assessment of the company's location and advising the Executive Management Team of the results. Works with the Facilities/Security Team to verify the building can be occupied after a disaster. After damage assessment is completed, this team will also be responsible for coordinating salvage operations as required.

PR/Communications Team

Responsible for all Public Relations (Public Relations and Crisis Communications[3]) and other communications (e.g., Coordination with Public Authorities[4])

Facilities/Security Team

Responsible for the facility and its security. In a disaster, this team is also responsible for providing security to the Alternate Site if required.

Accounting Team

A Sample Team – Responsible for ensuring that critical accounting business functions are operational and accurate.

Telecommunications Team

Responsible for the restoration and maintenance of all Voice Communications and Data Communications. Also responsible for ensuring telephones are operational at the Alternate Site.

IT Team

Responsible for restoring all critical computer systems and workstations (except telephones).

Marketing Team

A Sample Team – Responsible for ensuring that critical marketing business functions are operational and providing customer support.

[3] DRII Professional Practices – Subject Area 9: Public Relations and Crisis Communication
[4] DRII Professional Practices – Subject Area 10: Coordination with Public Authorities

1.6.2 BCP Team Organization Chart

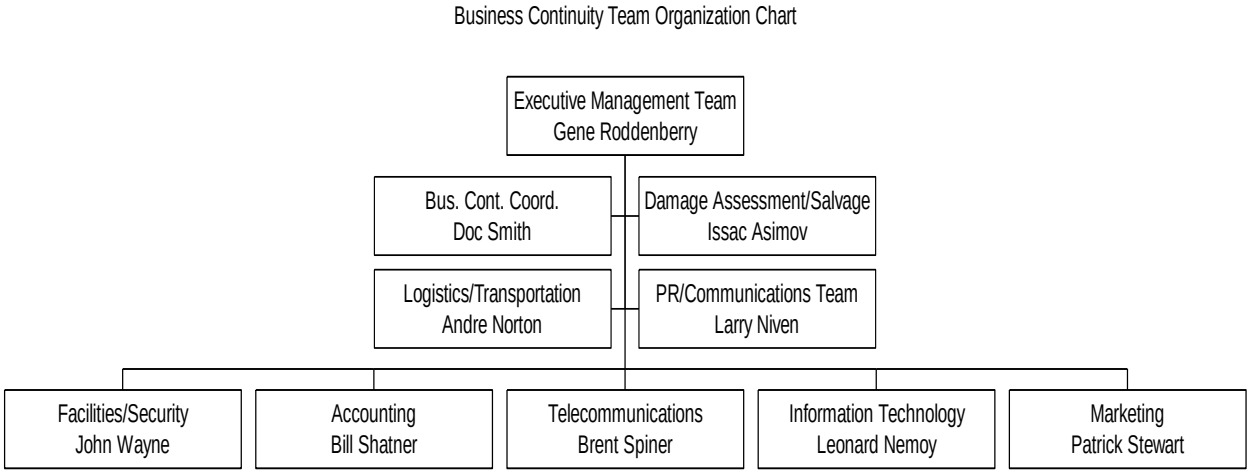

Figure 1 – BCP Team Organization Chart

Chapter 2 – Critical Business Continuity Plan Information

Chapter 2 contains the call lists, task lists, and various inventories by team to make it easier to execute the BCP, as well as improving the ease of distribution and updating. Inventories, shown in alphabetical order, include lists of Customers, Equipment, Software, Supplies, Telecommunications (voice and data), Vendors, and Vital Records that are required to support the BCP. The Glossary contains a definition of each of the following lists.

The Call List for each team is shown first because that makes it easy to find for emergency notifications. The Task List is shown next so that it is easy for the Team Leader to find it after the emergency notification.

Not all teams will have all inventory lists. For example, the Executive Management Team may not have any customers (Customer List) or vendors (Vendor List) because customers and vendors will usually be notified by other teams. If a team does not have one or more inventory lists, I recommend that a statement be placed in that section as a "place holder" such as: The Executive Management Team does not have a Customer List". This will remind each team leader that a Customer List does exist and should be updated if there has been a new inventory item which is a result of changing business operations.

As a final note, I have not shown the Call List, Task List, and all inventory lists for each team because they will be identical to the example shown for the Executive Management Team. Each team name is listed as shown in Section 1.6.2, Figure 1 – BCP Team Organization Chart.

2.1 Executive Management Team

2.1.1 Executive Management Team Call List

2.1.2 Executive Management Team Task List

2.1.3 Executive Management Team Customer List

2.1.4 Executive Management Team Equipment List

2.1.5 Executive Management Team Software List

2.1.6 Executive Management Team Supplies List

2.1.7 Executive Management Team Telecommunications List

2.1.8 Executive Management Team Vendor List

2.1.9 Executive Management Team Vital Records List

2.2 Business Continuity Coordinator (BCC)

2.3 Damage Assessment/Salvage Team

2.4 Logistics/Transportation Team

2.5 PR/Communications Team

2.6 Facilities/Security Team

2.7 Accounting Team

2.8 Telecommunications Team

2.9 Information Technology Team

2.10 Marketing Team

Chapter 3 – Plan Administration and Maintenance

Chapter 3 contains a variety of information related to the administration and maintenance of the BCP. It includes sections and subsections on administration, training, maintenance, awareness programs, education, and auditing the BCP. While most of this information is the responsibility of the Business Continuity Coordinator, it also documents important procedures such as the Board of Directors' annual approval of the BCP for bank operations (required by the FDIC).

3.1 Business Continuity Coordinator (BCC)

The Business Continuity Coordinator has overall responsibility for the design, development, coordination, implementation, administration, training, awareness programs, and maintenance of the Business Continuity Plan. Accordingly, the BCC should have experience and training in most, if not all, of the **DRI International Professional Practices for Business Continuity Planners** (see www.drii.org for the latest version).

I believe it is critical that the BCC be a senior, experienced, and dynamic individual who has worked in project management for medium-to-large projects to assure successful implementation of a business continuity program. And the BCC must have access to senior management for approval of various items within the business continuity program, such as the Business Continuity Strategy, Business Continuity Plan Assumptions, and the Business Continuity Plan itself.

3.1.1 Responsibilities

In accordance with the DRII Professional Practices, the Business Continuity Coordinator has the following responsibilities:

- Provide BCP project coordination and management[5].
- Perform risk evaluation and mitigation as required[6].
- Conduct a Business Impact Analysis[7].
- Develop and obtain approval for the Business Continuity Strategy (ies)[8].
- Develop, implement, and maintain procedures for emergency response[9]. You may find it more appropriate to document Emergency Response procedures in your Crisis

[5] DRII Professional Practices – Subject Area 1: Project Initiation and Management
[6] DRII Professional Practices – Subject Area 2: Risk Evaluation and Control
[7] DRII Professional Practices – Subject Area 3: Business Impact and Analysis
[8] DRII Professional Practices – Subject Area 4: Developing Business Continuity Strategies
[9] DRII Professional Practices – Subject Area 5: Emergency Response and Operations

Management Plan.

- Develop and implement the Business Continuity Plan[10].
- Create, implement, and maintain BCP Awareness and Training Programs[11].
- Develop, maintain, coordinate, exercise, and evaluate the BCP[12].
- Develop, maintain, coordinate, exercise, and evaluate plans for public relations and crisis coordination[13]. You may find it more appropriate to document public relations and crisis coordination procedures in your Crisis Management Plan.
- Develop, maintain, and coordinate policies and procedures with local authorities[14]. You may find it more appropriate to document these policies and procedures in your Crisis Management Plan.

And I suggest another responsibility for the BCC:

- Assist the Crisis Management Team (in the CMP) and/or the Executive Management Team (in the BCP) during a crisis/disaster as required.

3.2 Business Continuity Plan Administrators (BCA)

It is not practical for a large, geographically-separated organization to have one single individual who can effectively perform all of the responsibilities listed in the previous section. Moreover, it is sometimes difficult in a smaller, single-site organization or company, especially if the BCC has other responsibilities beyond the BCP. Therefore, I suggest an additional designated position which I call a Business Continuity Administrator (BCA).

In a smaller organization, the BCA is responsible for a discrete section of the BCP, such as a department or business unit for which a team has been defined. The BCA is a team (i.e., department or business unit) representative at all BCP meetings, and is at least a senior individual on that team, if not the team leader.

If you carefully construct your BCP Team and structure your plan as described in Sections 1 and 2, you can assign the responsibility for maintenance and update for a section to the BCA for that team.

As always, this is only one way to develop and maintain a BCP with some help from other people in your organization, and the most important point is that you should develop your own BCP Team to fit your organization's specific needs.

[10] DRII Professional Practices – Subject Area 6: Developing and Implementing Business Continuity Plans
[11] DRII Professional Practices – Subject Area 7: Awareness and Training Programs
[12] DRII Professional Practices – Subject Area 8: Maintaining and Exercising Business Continuity Plans
[13] DRII Professional Practices – Subject Area 9: Public Relations and Crisis Coordination
[14] DRII Professional Practices – Subject Area 10: Coordination with Public Authorities

3.2.1 Responsibilities

The responsibilities for the Business Continuity Administrator (BCA) are similar to those of the BCC, but more limited in scope to a specific department or business unit.

3.3 Business Continuity Plan Administration

Administration of the BCP can be simple or complex, depending on the size of the organization, and this section contains two major areas that require your attention.

3.3.1 BCP Awareness and Training

This section contains basic information on how you administer the Awareness and Training Programs[15] for your Business Continuity Plan.

Virtually all organizations have a new employee orientation, and you can begin your training program by developing and presenting a brief introduction to the BCP policy and plan. Most organizations also have a requirement that new employees review the security policy and sign a statement they have read and understood the policy. You may be able add a statement about each employees responsibility for the BCP.

You can usually distribute a monthly BCP newsletter by hard copy or by email. In the beginning, you will probably use the newsletter as a status report, but you can also use it to document situations applicable to your Business Continuity Plan. What about bad weather? – snow, floods, tornadoes, etc. Emergency notification, regardless of the cause, should be part of your BCP. Do you ever have a power outage? – the BCP and Escalation Plan applies.

3.3.2 Exercising (Testing) the BCP

The Business Continuity Coordinator is responsible for conducting periodic exercises[16] of the Business Continuity Plan as documented in Chapter 4.

At least two separate exercises should be conducted every year:

- Structured Walk-through Exercise for training and updating the BCP
- Technical Exercise or Hot Site exercise for IT and users

[15] DRII Professional Practices – Subject Area 7: Awareness and Training Programs
[16] DRII Professional Practices – Subject Area 8: Maintaining and Exercising Business Continuity Plans

3.4 Business Continuity Plan Maintenance

Maintenance is perhaps the most difficult areas for most people to understand, primarily because of the view that, after the BCP has been written, exercised, and updated, it's just another project that has been completed. The fact is that a BCP is never completed because of change. People change, business needs grow and change, and business operations have to accommodate those changes. And so does your Business Continuity Plan. Therefore you need to have a provision to handle those changes as documented in the following sections.

3.4.1 When and How to Update the BCP

Ideally, the Business Continuity Plan should be updated every time there is a business or personnel change. A business change may also include a change in the IT hardware, such as a file server. But it is not very realistic to assume the BCP can be updated every time a change occurs.

To help keep track of changes, I recommend you have a monthly meeting with all team leaders and their alternates to review changes and impact on the BCP. Personnel changes occur most frequently, and you should be prepared to update your Call Lists monthly or quarterly for updated BCP distribution. Other changes, such as new applications and/or IT hardware occur less frequently, and many organizations have a formal change control process that can help you keep track of those changes.

As a minimum, I recommend that the Call Lists be updated and distributed monthly, if possible, or quarterly if not. This is one example of a scheduled change.

For other business changes, including any unscheduled changes, the BCP should be updated as soon as possible after the change occurs.

The Business Continuity Coordinator should ensure the required BCP updates have been completed and distribute them to the Distribution List described in Chapter 1.

3.4.2 Business Impact Analysis (BIA) Maintenance

The Business Impact Analysis (BIA) is not a one-time project because of business changes and growth as stated in the previous section. As a result, the BIA requires maintenance whenever a major business change occurs or at least once a year, whichever comes first.

Why does the BIA require maintenance? Well, it is the best way to verify that you have all of the required information. For example, there is a significant trend toward e-business, and many organizations are using the internet for that purpose, aside from an informational web site. At the beginning of a project, an *RTO* may be longer because the entire process is not usually fully integrated into business operations until that process has matured. That maturing process may take a year or longer, but that process or business function which was not critical during the original implementation (it may have been a pilot project) may become a very critical process over time.

Application implementations and enhancements are another frequently-encountered concern because a new application may essentially replace a manual process to improve productivity. Then, you will have a situation where, over time, people will forget (or leave the organization) how to do that original process; then, enhancements may be implemented that will make it virtually impossible to perform that process without that application. To make matters worse, that productivity improvement may have significantly decreased the Recovery Time Objective (RTO). So you must be prepared to revise your Business Continuity Strategy and Business Continuity Plan as a result.

Whether you conduct interviews or distribute questionnaires to update your BIA, I recommend you schedule it during a non-peak time of the year – Not at the beginning of the year which may conflict with year-end closing, not at month-end or quarter-end closing, and not during any holiday times when the responsible managers may not be available because of business requirements.

3.5 BCP Approvals

Regardless of how you develop your Business Continuity Plan, one of the last, but very important steps, is to make certain you have a formal sign-off by senior management on your initial Business Continuity Plan.

It is a best practice, and in some cases required, to obtain this approval every year. I recommend that you develop a procedure which "automatically" requests senior management approval after they have participated in a Structured Walk-through Exercise that should be conducted once a year for training and plan updates (see Chapter 4)

3.5.1 Senior Management Approval

This section is reserved for an "approval page" for your Business Continuity Plan. Some Business Continuity Coordinators prefer to have this page at the beginning of the plan. This is a best practice to ensure the BCP has been formally reviewed and approved. However, all federally regulated financial institutions have a special requirement as discussed in the following section.

3.5.2 Board of Directors Approval (if applicable)

For financial organizations that must comply with the Federal Financial Institutions Examination Council (FFIEC) regulations and policies (e.g., FDIC, OCC, NCUA, etc.), you **must** have a formal and documented approval from the Board of Directors every year in the board minutes[17]. For example, the National Credit Union Associate (NCUA) has also issued this identical policy for all credit unions.[18] This section is reserved for that approval.

I have found the easiest way to obtain this approval is to request an "extract" from the Board of Directors' meeting minutes which details the review and approval of the Business Continuity Plan, usually after a presentation on that plan. The extract is requested because the Board usually has company-confidential information in the minutes, and the Board Secretary will generally be able to help you with this. Required information includes the date and time of the Board Meeting, the participants, an exact extract of the minutes relating to the Business Continuity Plan, and a certification by the Board Secretary that the above is a true, accurate and complete copy of the board minutes related to the review and approval of the Business Continuity Plan.

[17] FFIEC Corporate Business Resumption and Contingency Planning Policy Revised March 1997
[18] NCUA Letter to Credit Unions Letter No. 97-CU-3 dated April 7, 1997

Chapter 4 – Plan Exercises and Exercise Reports

Chapter 4 contains information on the various types and frequency of plan exercises. This chapter also provides a repository for test reports, although some Business Continuity Coordinators prefer to place test reports in an appendix.

Many BCP specialists still refer to an exercise as a "test", but my experience is that it is preferable to use the word "exercise", primarily because a test implies a pass/fail kind of environment.

From a professional perspective, I believe the real objectives of a BCP exercise are to:

- Create a learning environment so that all participants can learn about the BCP
- Document changes and updates (including omissions) to the BCP

And regardless of how your plan is constructed, I always recommend a Structured Walk-through Exercise as the **first** exercise, regardless of whether you need to evaluate an IT-based BCP or a business-based BCP.

4.1 BCP Exercise (Testing) Methodology

The Business Continuity Plan can be verified and validated using any one of the following methodologies:

- Structured Walk-through Exercise
- Tactical Exercise
- Technical Exercise for the IT staff, usually at a commercial Hot Site
- Hot Site Exercise (both IT and business users)

You can also use any combination of these methodologies to develop an appropriate approach for exercising your Business Continuity Plan.

4.2 When to Exercise (Test) the BCP

It is a best practice to have a minimum of two BCP exercises every year: one Structured Walk-through Exercise and one Technical Exercise or Hot Site Exercise that includes the Technical Exercise and business user participation.

The objectives of a Structured Walk-through Exercise are to:

- Determine the state of readiness of your BCP by creating a learning environment so that all participants can learn about the plan.
- Validate the BCP resource lists (people and inventories) are sufficient to effect recovery of business operations and/or IT services as appropriate. Document changes and updates (including omissions) to the BCP.
- Verify the BCP is current and accurately reflects the organization's requirements.

After the exercise, you should make certain that all changes and updates are completed, and distribute those updates to your Distribution List as described in Chapter 1.

If your organization has a separate data center (and a separate Business Continuity Plan because it is in a different location), you will want to have a separated Structured Walk-through Exercise to verify the technical aspects and resources for that BCP. In fact, you may find it helpful to have a separate exercise for your IT recovery because business users only care whether their computer systems are available, not the boring technical details of how IT actually does it. In any case, I recommend you conduct a Structured Walk-through Exercise for your IT staff at least once a year.

For the very first Technical Exercise, I recommend that it be strictly limited to IT staff only. It is not unusual for issues to be identified during a Technical Exercise that cause problems during the restoration of systems and backup data. Missing tapes or media (e.g., install CDs), corrupted/unreadable media, telecommunications failures of all kinds, incompatible hardware, and various other hardware failures can contribute to a "less successful" Technical Exercise. If this occurs during your first Technical Exercise, it is important to remember the objectives are identical to those stated above for the Structured Walk-though Exercise, especially that this exercise is to help identify problems (and their corrective actions) and provide training.

When your IT staff has completed a Technical Exercise that accomplished all objectives for your IT systems availability, then you need to have a Hot Site exercise that includes both IT recovery and user participation to validate that all restored systems and data are accurate, operational, and synchronized.

4.3 Developing the Exercise (Test) Scenario or Plan

Regardless of which methodology you choose to exercise your Business Continuity Plan, you need to develop a test plan or scenario for the exercise. Consider the following as you develop your Exercise Scenario and/or Plan:

- Focus on teams which have had deficiencies in the past. For example, verify that the BCP has been updated to reflect resource requirements and any technical issues.
- Ensure that the exercise involves only the use of offsite resources to verify the accuracy

and completeness of Offsite Storage, including Vital Records.
- Choose a realistic scenario as discussed in the following paragraphs.

For a Structured Walk-through Exercise, you should first describe the objectives of the exercise, such as the ones stated in Section 4.2. Then, create a short, one-paragraph scenario that describes a situation where your location has suffered an obvious disaster, such as a fire, flood or tornado.

For any exercise involving a commercial Hot Site, be sure to make arrangements with the vendor first. You may find you will need to schedule exercises as much as a year in advance, depending on the vendor's schedule, so you will need to plan ahead with an Exercise Plan. Then you can create your exercise objectives and scenario as discussed above.

4.4 Exercise (Test) Evaluation

You should always document the evaluation of the exercise and include it as part of your BCP as discussed in the next section. If you have developed your exercise scenario and plan as discussed in the previous section, you already have completed part of the documentation. I usually create the Exercise Evaluation as a memo to senior management (i.e., the Executive Management Team) with a copy to all exercise participants. You should be able to use the Distribution List discussed in Chapter 1 for this purpose.

The memo documents the test objectives and the scenario. The remainder of the memo is organized by team, especially listing a due date and responsible person for corrective action on any plan update (Hint: provide an update form to each team leader so that any changes and/or additions can be recorded during the exercise. Collect all these forms at the end of the exercise.) You should also make notes of any comments at the conclusion of the exercise for inclusion in the Exercise Report as appropriate.

Finally, include your Exercise Report as part of the BCP as discussed in the following section.

4.5 Exercise (Test) Reports

This is a separate section reserved for documentation all of your BCP exercises. When your BCP is audited, you will almost certainly be asked: "When was the last time this plan was tested?" If you have all the test reports in your BCP, the auditor will always see them, and you will not have to keep a separate file.

Some people prefer to keep Exercise Reports in an appendix instead of the main part of the BCP, so the choice is up to you.

Chapter 5 – Appendixes

Chapter 5 contains various appendixes, including detailed procedures, that support the BCP. For example:

A Glossary
B Sample – Hot Site Information (e.g., directions, maps, contract copies, etc.)
C Sample – JCN Model 00 Server Recovery Procedure
Other appendixes (for detailed procedures, etc.) as required.

Appendix A is a glossary which is a substantial revision of the current DRII terminology with some new terminology that reflects current practices as of December 2002.

APPENDIX A – GLOSSARY

Special Note: Glossary definitions may include a reference to another definition which is shown in *italics.*

Alternate Site – An alternate location, other than the main facility, that is designated emergency use by an organization's *Emergency Operations Center (EOC)*, business units for business operations and/or data processing services (*IT*) when the primary location(s) are inaccessible.

Auditing – A thorough examination and evaluation of an organization's *Business Continuity Plan* and procedures to verify their correctness and viability.

Backlog – A measure of unfinished work in hours or days.

BIA – Acronym for *Business Impact Analysis*.

Business Continuity – Activities, plans, and programs designed to return an organization to an operational condition.

Business Continuity Coordinator (BCC) – A member of the Executive Management Team and/or the Crisis Management Team with the responsibility for the development, coordination, training, testing, training, and implementation of the *Business Continuity Plan.*

Business Continuity Plan – An approved set (usually by senior management and/or a Board of Directors) of arrangements, resources, and sufficient procedures that enable an organization to respond to a disaster and resume its *Critical Functions* within a pre-defined time frame without incurring unacceptable financial or operational impacts.

Business Continuity Planner – An individual responsible for the design and development of a *Business Continuity Plan*.

Business Continuity Planning – The process of developing advance plans and procedures that enable an organization to respond to an event so that *Critical Business Functions* can continue without significant or unacceptable *Financial Impacts* and/or *Operational Impacts*.

Business Continuity Strategy – A management-approved, documented, and funded course of action to be used in the development and implementation of an organization's *Business Continuity Plan*.

Business Function – A separate, discrete function or process performed by a Business Unit. For example, the Accounting *Business Unit* in a smaller organization may include accounts payable and accounts receivable as Business Functions while a larger organization may have separate business units that perform these Business Functions.

Business Impact Analysis (BIA) – The process of developing and distributing a questionnaire to determine the *Financial Impact* and *Operational Impact* on an organization if it's business offices and/or data center facilities are not available for an extended time (usually at least one month). The objective of the BIA is to provide a management-level analysis that specifically documents the daily financial impact and *Recovery Time Objective (RTO)* for each *Business Unit* and associated *Process*es.

Business Resumption Planning – See *Business Continuity Planning*.

Business Unit – A separate, discrete organizational entity that performs a specific business function or process. A Business Unit may be as small as two people or as entire company.

Call List – A list of all team members and their phone numbers (home, work, cell, pager, etc.) on a *Team* for the *Business Continuity Plan*.

CMP – Acronym for *Crisis Management Plan*.

CMT – Acronym for *Crisis Management Team*.

Cold Site – An *Alternate Site* consisting of space that can be configured to support business unit recovery and/or data center recovery operations. A Cold Site is basically "four walls" with access to *Voice Communications* and *Data Communications* circuits and sufficient available electrical power and HVAC to support the recovery operations. A Cold Site may or may not have raised floor, and ALL furniture and hardware must be delivered, installed, connected, and tested. May also be called a Shell Site. See also *Hot Site* and *Warm Site*.

Command Operations Center – See *Emergency Operations Center (EOC).*

Contingency Planning – Process of developing advance arrangements and procedures that enable an organization to respond to an event that could occur by chance or unforeseen circumstances.

Controls – A term usually associated with *Auditing* and defined as procedures or other measures designed to ensure that plans and systems function correctly.

Crisis – An event that threatens the security, integrity or facilities of an organization and/or the safety of its employees. A Crisis may range from a building evacuation due to a bomb threat to a full-scale, easily recognized disasters. For planning purposes, a Crisis includes, but is not limited to, severe weather threats or occurrences (snow, tornadoes, etc.), senior management succession planning, power and communications outages, medical emergencies, hostage situations, bomb threats, earthquakes, elevator entrapments, etc., in addition to an obvious, easily-recognized disaster.

Crisis Management Plan (CMP) – An approved set (usually by senior management and/or a Board of Directors) of arrangements, resources, and sufficient procedures that enable an organization to effectively respond to a *Crisis*.

Crisis Management Team (CMT) – The senior management team that activates the *Crisis Management Plan (CMP)* in response to a *Crisis*.

Critical Functions – Essential *Business Functions* that are time-sensitive and must be restored first in the event of a disaster or interruption to avoid unacceptable financial or operational impacts. ensure the ability to protect the organization's assets, meet organizational needs, and satisfy regulations.

Customer List – An inventory list of all primary customers –including name, address, telephone number, and contact (if required)– that must be notified during the recovery of a business unit or an entire company. The *Customer List* is an essential part of an organization's *Business Continuity Plan*. It is a best practice to have a complete inventory list of ALL existing customers compiled for an organization.

Data Communications – The transmission of data, usually in a digital form, between geographically separate locations via public and/or private electrical or optical transmission systems. Contrast with *Voice Communications*.

Declaration Fee – A one-time charge normally paid to a commercial vendor who provides an *Alternate Site* (usually a *Hot Site*) facility at the time a disaster is officially declared.

Department – A separate, discrete entity defined by each organization or company. A department usually performs a specific business function or process. See also Business Unit.

Disaster – A sudden, unplanned calamitous event causing great damage or loss. In the business environment, any event that creates an inability on an organization's part to provide essential products and/or services for an indefinite period of time.

Disaster Mitigation – Actions, plans, and activities to reduce or eliminate the effects of a disaster on business and/or data center operations.

Disaster Preparedness – Activities, plans, programs, and systems developed prior to a disaster that are used to support and enhance mitigation, response, and recovery to disasters.

Disaster Recovery – Archaic term for *Business Continuity* but still occasionally used in reference to a data center's *Business Continuity Plan*. See *Business Continuity*.

Disaster Recovery Plan – Archaic term for *Business Continuity Plan* but still occasionally used in reference to a data center's *Business Continuity Plan*. See *Business Continuity Plan*.

Disaster Recovery Planning – Archaic term for *Business Continuity Planning* but still occasionally used in reference to a data center's *Business Continuity Planning*. See *Business Continuity Planning*.

Disaster Response – See *Emergency Response*.

Electronic Vaulting – The transmission of journal transactions or data records to an Alternate Site or Offsite Storage using telecommunications facilities.

Emergency Operations Center (EOC) – An *Alternate Site* with sufficient *Voice Communications* capabilities and work space used to manage the initial recovery efforts including emergency notifications using the *Call List* from the *Business Continuity Plan*. The EOC may initially be a temporary location (e.g., hotel, team member's home, etc.) used by the management team to begin coordinating the recovery operations or it may be the designated *Cold Site, Warm Site* or *Hot Site* designated for recovery operations.

Emergency Response – The initial activities and plans designed to address and mitigate a disaster's immediate and short-term effects.

EOC – Acronym for *Emergency Operations Center*.

Equipment List – An inventory list of all equipment and associated vendors which are required for the recovery of a business unit or an entire company. Equipment includes, but is not limited to, FAX machines, printers, computer systems, monitors, cables, scanners, mail processing hardware, etc. The Equipment List is an essential part of an organization's Business Continuity Plan. It is a best practice to have a complete inventory list of ALL existing equipment compiled and used by an organization.

Escalation Plan – A plan that documents decision-making criteria, usually based on the *Recovery Time Objective (RTO)*, to determine whether a *Disaster* declaration and implementation of the *Business Continuity Plan* is in the best interest of the organization or company.

Financial Impact – An tangible impact, measured in dollars and usually negative, resulting from the unavailability of an organization's business office and/or data center facilities. Financial impacts are usually reported during a *Business Impact Analysis (BIA)* and are typically estimated on a daily basis. See also *Operational Impact*.

Hot Site – An *Alternate Site* consisting of designated office space and/or a data center facility that is equipped with sufficient workstations (including desks, chairs, telephones, etc.), voice and data communications hardware and connectivity, power, raised floor, computer hardware (including workstations if required), and appropriate heating, ventilating, and air conditioning capacity. Commercial vendors typically provide separate space/facilities with monthly subscriptions for recovering business unit operations and computer operations. See also *Cold Site* and *Warm Site*.

Alternate facility with equipment and resources to recover the critical business functions affected by a disaster. Hot sites vary depending on the type of facilities offered (such as data processing equipment, communications equipment, electrical power, etc.).

HVAC – Acronym for heating, ventilation, and air conditioning.

Initial Assembly Point (IAP) – A pre-defined location, such as a parking lot, hotel or person's home, where all designated team leaders and members can meet if the organization's business offices and/or data center are not accessible for any reason. See also *Emergency Operations Center (EOC)*.

Inventories – Specific lists of items required for the Business Continuity Plan which includes the *Customer List* with contact information, *Equipment List* (with *Vendor List* and contact information), *Supplies List* (with *Vendor List* and contact information), *Software List* (with *Vendor List* and contact information), *Telecommunications List* (with *Vendor List* and contact information), *Vital Records List* (with location of vital records). See the specific inventory item (shown in *italics*) for additional information.

IT – Acronym for Information Technology. A *Department* or *Business Unit* that provides computing systems support to an organization or company.

Infrastructure – The basic supporting installations and facilities upon which the continuance and growth of a community depend, such as power plants, water supplies, transportation systems, and communications systems, etc.

LAN – Acronym for *Local Area Network*.

Local Area Network (LAN) – A short-distance network used to connect terminals, computers, and peripherals under a standard topology, usually within one building or a group of buildings. A LAN does not use public carriers to link its components, although it may have a "gateway" outside the LAN that uses a public carrier. See also *Wide Area Network*.

Loss – Unrecoverable business resources that are impacted or removed as a result of a disaster. Such losses may include loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability. See also *Financial Impact* and *Operational Impact*.

Mitigate – To make or become milder, less severe, or less painful.

Mobile Recovery Facility (MRF) – A mobile Warm Site, normally a large tractor-trailer available from a commercial vendor, that can be transported to a pre-determined location so that needed equipment can be obtained and installed near the original location. Depending on the vendor, an MRF may be available in a "business office" and a "data center" configuration.

Modem – An acronym for **mo**dulator/**dem**odulator, a device that converts analog signals to digital signals and back again, usually on *Voice Communications* circuits.

Operational Impact – An intangible impact resulting from the unavailability of an organization's business office and/or data center facilities. An Operational Impact cannot be quantified in dollars, but may be critical because of its effect on an organization. Examples of operational impacts include, but are not limited to customer service, stockholder confidence, industry image, regulatory, financial reporting, employee morale, vendor relations, cash flow (that cannot be quantified), and increases in liability. Operational impacts are usually reported during a *Business Impact Analysis (BIA)* and are typically estimated on an arbitrary scale, such as 1-5, with the highest number representing the most severe impact. See also *Financial Impact*.

Offsite Storage – A designated storage facility, other than the main facility, where duplicate *Vital Records* and critical documentation may be stored for emergency use during the execution of an organization's *Business Continuity Plan*.

Project Team – A group of people representing key organizational areas that work together and follow documented responsibilities for the design, development, and implementation of a *Business Continuity Plan*.

POTS – Acronym for Plain Old Telephone Service.

Project Management – The development, planning, organizing, and management of tasks and resources to accomplish a defined objective, such as a *Business Continuity Plan*, usually under time and cost constraints.

Reciprocal Agreement – An agreement between organizations with basically the same business processes and/or data processing hardware that allows one organization to continue business operations for the other in case of disaster.

Recovery Point Objective (RPO) – The measure how much data loss, in hours or days, is acceptable to an organization. The point in time at which backup data (e.g., backup tapes) must be restored and synchronized by *IT* to resume processing. Most *IT* organizations usually have an *RPO* of at least –1 day (–24 hours) because backups are usually performed daily (usually at night) and transported to *Offsite Storage* early the following day. The **best** *RPO* is zero (0) which basically means that all affected computer systems utilize "mirroring" (real-time data/transaction copying) technology to concurrently copy all incoming data/transactions to another identical system in a remote location that is sufficiently remote from the primary site.

Recovery Time Objective (RTO) – The maximum length of time, in hours or days, that can elapse before the loss of a business function, a computer application, the business offices and/or a data center causes unacceptable *Financial Impacts* and/or *Operational Impacts* to an organization as documented in the *Business Impact Analysis (BIA)*.

The *RTO* has five (5) components:

(1) The time before a disaster is declared (see *Escalation Plan*);
(2) The time required to activate the *Business Continuity Plan*;
(3) The time required for the *IT* organization to restore computer systems;
(4) The time required by an affected business unit to perform assigned tasks to the point at which business operations can be resumed including the time to verify that restored computer systems data is accurate and synchronized to the last available backup; and
(5) The time for each business unit to re-enter/process all *Backlog* (including manually processed work, if applicable) to bring business operations into current status.

Recovery Timeframe – See *Recovery Time Objective (RTO)*.

Recovery Strategy – See *Business Continuity Strategy*.

Relocatable Shell – See *Mobile Recovery Facility*.

Resource Requirements – The resources (e.g., people, equipment, supplies, vendors, telecommunications, vital records, etc.) required for the recovery of a business unit or an entire company as documented in the *Business Continuity Plan*.

Risk – The potential for exposure to loss. Risks, either man-made or natural, are constant throughout our daily lives. The potential is usually measured by its probability in years.

Risk Analysis – The process of identifying the risks to an organization, assessing the *Critical Functions* necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure, and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

Software List – An inventory list of all software and associated vendors (see Vendor List) which is required for the recovery of a business unit or an entire company. The Software List is an essential part of an organization's Business Continuity Plan. It is a best practice to have a complete inventory list of ALL existing software compiled and used by an organization.

Supplies List – An inventory list of all supplies and associated vendors which are required for the recovery of a business unit or an entire company. Supplies includes, but is not limited to, forms (e.g., check stock), special rubber stamps, pens, pencils, paper, paper clips, staplers, etc. The Supplies List is an essential part of an organization's Business Continuity Plan. It is a best practice to have a complete inventory list of ALL existing supplies compiled and used by an organization.

Structured Walk-Through Exercise – A simulated method used to exercise or test a completed *Business Continuity Plan*. The exercise includes a disaster scenario and exercise moderator who observes one or more team leaders verbally walk through each step of their *BCP* to confirm its viability and identify omissions, gaps, bottlenecks, or other plan weaknesses.

Tactical Exercise ("War Game") – A simulated, scenario-based exercise of the *Business Continuity Plan* conducted in a "War Room" format in a large room. The exercise moderator conducts the exercise and reads a prepared scenario. All Team Leaders and Alternate Team Leaders are required to participate and "perform" their tasks under supervised conditions. Each team has a separate table or work area and can only communicate with another team using written notes that are given to "couriers" for delivery to simulate the communications problems (e.g., incomplete information) that occur during a disaster. The written communications are time-stamped so that an exercise report can be prepared. During the exercise, roving "referees" ensure there is no talking among the teams. This type of sophisticated exercise requires a considerable amount of planning and coordination, even though the actual event may take only a day or less.

Task List – A list of all tasks, usually in a checklist form, which must be performed by a *Team* to recover a specific portion of an organization, business function and/or business unit. The *Task List* is an essential part of an organization's Business Continuity Plan.

Team – A group of individuals assigned to work together to perform a specific function in the *Business Continuity Plan*. A *Team* consists of a Team Leader, Alternate Team Leader, and Team Members. The Team Leader is responsible for the successful completion of all tasks assigned (See Task List) to a team.

Technical Exercise – A *BCP* exercise, normally scheduled with a commercial Hot Site vendor, in which the *IT* and *Telecommunications* teams verify that computer systems and telecommunications can be successfully restored to operational status.

Telecommunications – A general term that applies to analog or digital data transmitted (See also *Data Communications* and *Voice Communications*) by electrical, optical, or acoustical means over public or private communications carriers.

Telecommunications List – An inventory list of all *Voice Communications* and *Data Communications* circuits which are required for the recovery of a business unit or an entire company. The Telecommunications List is an essential part of an organization's Business Continuity Plan. It is a best practice to have a complete inventory list of ALL existing telecommunications circuits compiled and used by an organization.

Threat – A potential event that may cause a risk to become a loss. Threats consist of natural phenomena such as tornadoes and earthquakes and man-made incidents such as terrorist attacks, bomb threats, disgruntled employees, and power failures.

Vendor List – An inventory list of all primary vendors (suppliers) –including name, address, telephone number, and vendor representative (if required)– that provide an essential service or product required for the recovery of a business unit or an entire company. The Vendor List is an essential part of an organization's Business Continuity Plan. It is a best practice to have a complete inventory list of ALL existing vendors compiled and used by an organization.

Vital Record – A critical business record required for recovering and continuing an organization's business operations. This may include employee information, financial and stockholder records, business plans and procedures, and the Business Continuity Plan. Vital records may be contained on a wide variety of media including, but not limited to, electronic (including tape, disk, and CD-ROM), hard copy (normally paper), microfilm, and microfiche.

Vital Records List – An inventory list that contains the name and offsite location of vital records (see *Vital Record*) required for the recovery of a business unit or an entire company. The Vital Records List is an essential part of an organization's Business Continuity Plan.

Voice Communications – The transmission of sound at frequencies within the human hearing range which may be in digital or analog form. Contrast with *Data Communications*.

WAN – Acronym for *Wide Area Network*.

Warm Site – An *Alternate Site* consisting of designated office space and/or data center space that has installed voice and data communications access and is partially equipped with telecommunications interfaces, such as a PBX and/or a router. A Warm Site is usually pre-wired for Voice and Data Communications so that telephones, PCs, and other computer hardware (e.g., servers) can literally be "plugged-in" as required. See also *Cold Site* and *Hot Site*.

Wide Area Network (WAN) – A network linking geographically separate metropolitan, campus, or local area networks across greater distances, usually accomplished using common carrier lines. See also *Local Area Network*.

Workstation – A single-person work area which usually includes office furniture (e.g., a desk), computer equipment (e.g., a PC), a telephone, and a wastebasket.

APPENDIX B – HOT SITE INFORMATION (Sample)

This is a sample cover page for an appendix.

This appendix contains the details of the Hot Site contract with the Wazoo Business Recovery Center.

Items included in this appendix are:

- Map to the Wazoo Business Recovery Center
- Emergency notification number for the Wazoo Business Recovery Center
- Contract between ABC Company and the Wazoo Business Recovery Center

If you have a hard copy document without a corresponding electronic copy, such as the contract mentioned above, I recommend that you scan the hard copy so that you will have a complete electronic copy of your Business Continuity Plan.

APPENDIX C – JCN Model 00 Server Recovery Procedure (Sample)

This is a sample cover page for an appendix containing a procedure. Each appendix should have a cover page that describes the contents of that appendix.