

**Business
Continuity
Planning
Made Simple
- *almost***

JOHN GLENN, CRP

Certified Business Continuity & Disaster Recovery Planner

This effort is dedicated to the people who have worked with me on various projects to help organizations survive disaster conditions.

Business Continuity, as with most other professions, is one of never-ending education. Planners as a group are willing to share their experiences so we can gain from others' knowledge rather than learn at our Clients' and Employers' expense.

Knowing that no plan is perfect and that we can never plan for every contingency, we still go forth making a best effort.

As you read through this book, keep in mind two visual aids that should be before all Business Continuity planners:

1. Rodan's *Thinker* being taken out of a shipping crate
2. A household vacuum cleaner

Why these visuals?

Because, as you will learn in the following pages, a successful Business Continuity planner must

1. think outside the box
2. can't work in a vacuum

It may be corny, but it is true.

A handwritten signature in black ink that reads "John Glenn". The signature is fluid and cursive, with the first name "John" being more legible than the last name "Glenn".

JOHN GLENN, CRP
JGlennCRP@yahoo.com

Table of Contents

1 Introduction

- 1.1 Who needs a plan?*
- 1.2 About regulated industries*

2 Business Continuity vs. other things

- 2.1 Business continuity*
- 2.2 Disaster recovery*
- 2.3 Continuing operations*
- 2.4 Emergency management*

3 Author's philosophy

- 3.1 Disaster vs. disaster condition (or event)*
- 3.2 Subject Matter Experts (SMEs)*
- 3.3 Enterprise plan is the only plan*
- 3.4 Total disaster scenario is the only scenario*
- 3.5 Disaster Recovery and Continuation teams*

4 In the beginning: the SOW

5 Understanding the business: the BIA

6 Identifying risks

- 6.1 Think outside the box*
- 6.2 Risks to input*
- 6.3 Risks from business tools*
- 6.4 Risks to output*
- 6.5 When does it stop?*

- 6.6 The ubiquitous "other" risk*

7 Risk assessment - rating the risks

- 7.1 Probability*
- 7.2 Impact*
- 7.3 Tic-Tac-Toe*

8 Dealing with risks

- 8.1 Avoiding*
- 8.2 Mitigating*
- 8.3 Absorbing*
- 8.4 Insurance*
- 8.5 Bringing in the experts*
- 8.6 Additional things to consider*

9 The first deliverable

10 Specifically IS/IT/MIS

- 10.1 OS is not critical*
- 10.2 Know what's on the box*
- 10.3 Mirror the box*
- 10.4 RAID is nice, but not perfect*
- 10.5 The environment*
- 10.6 Remote site considerations*
- 10.7 Diagrams and documentation*
- 10.8 Licenses and other documentation*
- 10.9 Back-up hardware*
- 10.10 Got'chas*

11 Focusing on facilities

12 Management decisions

13 Declaring a disaster condition (& standing down)

13.1 Who may declare a disaster condition

13.2 Who can order a stand-down (business restored)

14 Continuation and Recovery plans

14.1 Who to include

14.2 Primaries and alternates

14.3 Teams defined

14.4 Team leaders

14.5 The CEO's role

14.6 Team member selection

14.7 A "kiss" for documentation

14.8 Defining Continuation Team tasks

14.9 Defining Disaster Recovery Team tasks

14.10 Corporate Team tasks

14.11 Contact information

15 Exercising the plan

15.1 Why

15.2 Exercise options

15.3 Critiquing the exercise

15.4 Including "the world"

16 Maintaining the plan

16.1 Calendar triggers

16.2 Event triggers

17 Random thoughts

17.1 Disaster Recovery vendors

Appendix 1: Risk list

Appendix 2: Forms

Appendix 3: Consultant's Generic Project Plan

About the author

1 Introduction

This booklet is written to introduce the concept of Business Continuity planning and to provide a working idea of what is required to create a Business Continuity plan. This book is *not* a plan.

This is not a tutorial on “How to become a Business Continuity planner.”

It does provide the basic framework for a Business Continuity plan and it may be used to create a “basic” plan. Such “basic” plans should, at a minimum, be reviewed by an experienced planner to assure there are no “gaps” in the plan (hence the term “gap analysis” for the review).

If the contents are followed fairly closely, it is possible to do a lot of “up front” work before a professional Business Continuity planner is brought in.

There are a number of benefits to the “up front” exercise, including:

- discovering risks that need to be avoided or mitigated “yesterday”
- reducing the time (and cost) a professional spends creating a plan
- closely examining processes, policies, procedures, and equipment to assure they meet current and anticipated requirements
- developing an awareness of regulations that directly or indirectly impact the business
- developing an awareness of the roles played by external organizations
- understanding the value of a Business Continuity plan as an integral part of the organization’s business plan.

1.1 *Who needs a plan?*

Every organization needs a Business Continuity plan. Period.

Regulated industries need a Business Continuity plan because regulations require it.

Public companies, companies that have stockholders, need a Business Continuity plan because management (and the board) has a fiduciary responsibility to the stockholders.

Private companies, family owned or otherwise closely held, need a Business Continuity plan to keep peace in the family and to pay the mortgages.

Non-profits need a Business Continuity plan to assure both their clients and the people and organizations supporting them that they will be able to meet their mandates.

Government agencies need a Business Continuity plan to assure they will be able to meet their mandates and, in turn, continue to receive funding.

Even families can benefit from a Business Continuity plan's risk assessment and disaster recovery portions.

1.2 ***About regulated industries***

Regulated industries, such as the financial, food, and pharmaceutical industries, have rules – and people to enforce the rules – that require Business Continuity plans. Fortunately or unfortunately, the regulations generally are fairly broad and require only that the Business Continuity plan be “feasible.”

“*Feasible*” is not an acceptable level for the professional planner or plan.

CAVEAT

This book is not, and shall not be considered, a complete Business Continuity or Disaster Recovery plan. The information contained in this book may be used as the BASIS of a plan, but it is not to be construed as a complete plan.

All plans are unique; a book, no matter how “all inclusive” cannot provide all the answers for every organization.

An experienced professional planner is your best defense against a disaster.

2 Business Continuity vs. other things

2.1 Business continuity

Business Continuity is a **proactive** approach to protecting an organization. A complete Business Continuity plan includes Disaster Recovery and Continuing Operations; it also includes interaction with Emergency Management teams.

2.2 Disaster recovery

Disaster Recovery is the **reactive** portion of a Business Continuity plan. Disaster recovery is the effort to restore, as quickly as possible, the operation to “**Business As Usual**,” known in the alphabet-soup world as “**BAU**.”

Disaster recovery can mean anything from mopping up after a broken pipe to finding a new building to replace one destroyed by a tornado.

2.3 Continuing operations

Continuing Operations runs simultaneously with Disaster Recovery. Continuing operations is at least a **minimum Level Of Service (LOS)** to meet customer or mandated commitments. For example, an insurance company considers cutting checks for its insured to be its minimum level of service; it will worry about getting the paperwork transferred to data later. Continuing operations typically utilizes work-arounds and alternate sites to maintain the minimum LOS.

2.4 Emergency management

Emergency Management (EM) is the realm of government – the umbrella coordinating organization for police, fire, highway/road department, ambulance services, hospitals, etc.

Before September 11, 2001, Emergency Management and Business Continuity often went their separate ways. This was wrong then and it would be wrong now; EM resources need to be included in every Business Continuity plan, particularly where hazardous materials (**HAZMAT**) are present.

(Before you think there are no hazardous materials where you work, check the custodian's closet. These materials must be noted and the appropriate OSHA documentation must be on-site.)

3 Author's philosophy

3.1 *Disaster vs. disaster condition (or event)*

While others may disagree, this scrivener defines a “**disaster**” as an event that results in death or serious injury to personnel or one that results in the organization going out of business. A “**disaster condition**” or “disaster event” is a condition that seriously interrupts *business as usual*. If no one is injured or killed and the organization continues in business, the organization has been inconvenienced, but a disaster has been avoided.

3.2 *Subject Matter Experts (SMEs)*

The Business Continuity planner needs to be a **Subject Matter Expert (SME)** for Business Continuity planning. He or she need **not** be an SME for anything else, even when creating a plan to cover some esoteric business function. The SMEs for the business functions (including the support functions) are the managers and line personnel who daily work with the procedures, equipment, etc.

The Business Continuity planner must be a good interviewer and a good listener. If the planner has a natural curiosity about the business function, he or she will be able to ask questions whose answers will lead to additional questions. Journalists frequently make good Business Continuity planners.

**Business Continuity planning cannot be performed in a vacuum;
a planner cannot work alone.**

3.2.1 Business function

A **business function** is a group level activity. Example of business functions include call centers, accounts receivable, IT, HR.

3.2.2 Business process

A **business process** is a process performed by a business function. In the case of a call center, handling an incoming call for an account is a business process.

3.3 **Enterprise plan is the only plan**

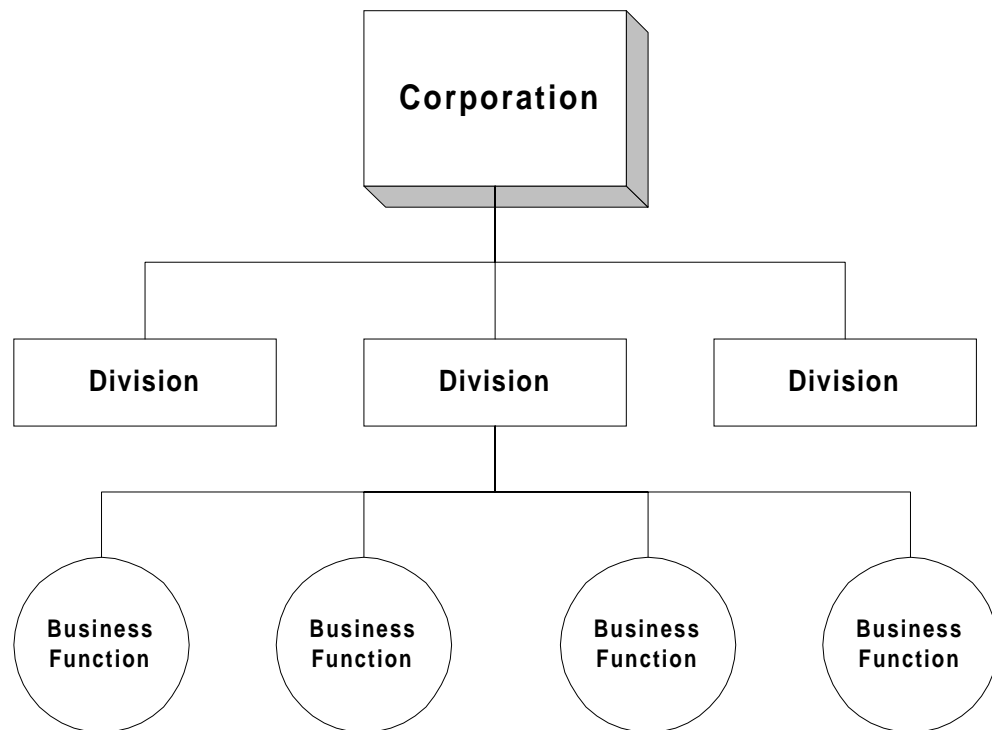
There are planners who believe a successful plan can be created for a single business function. Typically this is the IT/IS/MIS operation.

At a very low level this may be possible. By “low level” I refer to replacing a printed circuit board or network component with a “known good” equivalent.

In the event of a true disaster event (see Paragraph 3.1 Disaster vs. disaster condition (or event)), the computer people will need help from many other departments – accounting, purchasing, shipping/receiving, maintenance, facilities, and perhaps others. Planners can’t work in a vacuum and business functions don’t operate in a vacuum.

**Departments have dependencies on other departments; the only reasonable Business Continuity planning approach is the enterprise-wide effort.
Not just business functions, not just support functions,
but the complete enterprise.**

This does **not** mean that Business Continuity plans should not be created for each business function; it means that each individual Business Continuity



plan should be “rolled up” into the next higher group.

3.4 Total disaster scenario is the only scenario

“The only scenario,” the very senior planner said, “is that you go to work and there is nothing there.”

I was about to debate the point when I realized he was right – if you plan for the “worst case” event, all lesser events are covered.

3.5 Disaster Recovery and Continuation teams

Disaster recovery teams have one task – restore the operation as quickly as possible to Business As Usual (see Paragraph 2.2 Disaster recovery). The people who make up the disaster recovery team are the people who have an in-depth knowledge of the process or resource. These people need to have initiative, responsibility, and authority.

Continuation teams are charged with maintaining at least a minimal Level Of Service (LOS). In the example given in Paragraph 2.3 Continuing operations, the insurance company’s minimum LOS was cutting checks for its insured.

Both teams need personnel from support organizations. A roster should include personnel to:

- document all expenditures
- document all equipment scrapped, sent for repair/replacement, received
- assure adequate housing, on-site food and amenities
- assure that workers’ families are taken care of (insurance forms processed, payroll checks delivered, etc.), particularly when the employee is working away from his or her home
- communicate with the other teams and management

Depending upon the organization and given some time to thoroughly consider the requirements, many other functions can be identified.

The bottom line is that no one can successfully accomplish his or her tasks while trying to work in a vacuum.

4 In the beginning: the SOW

This is a short chapter.

Before starting the plan, create a **Statement of Work**, a **SOW**. Define what the plan is to cover. This may sound like a waste of time, but very often a business manager will try to use the plan (or the planner) to achieve goals outside the scope of a plan ... maybe get the programmers to “just tweak” an application to add a feature or function the manager was unable to get through normal channels.

Even an “in-house” planner needs to work from a SOW; external planners should wait until they have a signed off SOW before the first interview.

Get top – and I mean **stratospheric** – management buy-in and its enthusiastic support; anything less means failure. As we learned September 11, no business is immune, whether Wall Street brokerage, or falafel push cart, *everyone* needs a plan.

Identify the participants. The planner needs to start off with the managers, but expect to get most of the necessary information from the troops. Some managers can manage without getting “down and dirty.” The planner needs to talk with everyone.

The SOW should be a prose form of the project plan; it should identify the tasks to accomplish, who is responsible for each task (in the end its is the planner and the sponsoring Chief * Officer), how long the task is estimated to require to complete, and when the sponsors can expect the deliverables.

A consultant’s generic project plan is provided as Appendix 3.

5 Understanding the business: the BIA

The Business Continuity planner is **not** a business function SME.

Yet.

The first task after getting sign-off on the SOW is to meet with all business and support organization managers and explain the purpose of a Business Continuity plan, how it will help them and their troops (keep them employed, get them some new “toys” perhaps, help stay ahead of the competition).

The “introduction to Business Continuity” ideally will be presented by one or more of the sponsors, the folks from the stratosphere (see Paragraph 4 In the beginning: the SOW).

The Business Continuity planner needs to meet with each manager to define what *really* is done by the manager’s organization and what is the impact on the business if the work is not done. In the Business Continuity world, this is known as a **Business Impact Analysis**, or “*BIA*.” The meetings can be “one-on-one” or with a group of managers.

The benefit of the group meeting is that one manager’s comments may trigger another’s memory so a fuller picture of all functions is presented at the end of the meeting(s). The planner can then go to individual managers to fill in the inevitable blanks.

A good tool for these meetings, if it is available, is a “white board” that can photocopy the contents; an expensive tool, but very valuable.

**Whether dealing with managers in a group or one-on-one,
the planner should be accompanied by a “scribe,”
a person who can capture the main points while the planner guides the session.
A good scribe can be the planner’s most valuable resource.
As an alternative to a permanent scribe, consider asking the manager(s) to
second a technically-aware person to take notes.**

6 Identifying risks

6.1 *Think outside the box*

After identifying the critical business functions (see Paragraph 5 Understanding the business: the BIA) the Business Continuity planner meets with the business managers, to uncover as many risks to those functions that the managers and their troops can identify.

According to Ace Jackson, a fellow planner and IT guru, “The thing that helps me in this role is to put myself in the situation as a “victim” If the company is hit by a disaster, what would I, as a client, need/want from that company at the lowest level of service. Identifying risks is a little easier if you have something personal at stake; we’re all a little selfish (self-aware of our needs) that way and that’s how we survive!”

The risks will be the primary concerns and should be given suitable weight when examining the business function’s processes. (Paragraph 3.2 defines business functions and business processes.)

As the Business Continuity planner, you need to “think outside the box.” (To help you remember this, think of Rodan’s *Thinker* being removed from a box. It works for me!)

6.2 *Risks to input*

Input risks are risks that would prevent the business process from being completed. For example, if a process depends upon input via

- email
- faxes
- snail mail
- telephone calls

the planner needs to look at risks to each.

Using email as an example, the planner must consider:

- desktop equipment,

- electricity (or the business function that manages power for the organization)
- facility
- Internet
- intranet (LAN)
- IT (as an organization),
- telephone lines (or the business function that manages the telephone lines)

Try communicating via email sometime without a working mouse/pointer or with keyboard that is sending the wrong characters.

In other words, consider anything and everything that could interrupt email communication.

6.3 *Risks from business tools*

Play the “what happens if...” game. (This is Business Continuity 101.)

If the [name the equipment] fails, how can the business process be completed?

If [name a person or position] is unable to do his/her job, what is the impact on process completion? (This might be a good time to think about “succession planning,” determining who will assume the leadership in the event a the top managers are unable to fulfill their organizational responsibilities.)

The best way to find out what tools are critical is to tour the work area. What is used? On the desktop, in the file cabinet, the copy room.

While you are at it, find out what the manager and the troops think would help them complete the process more efficiently and economically.

A Client manager once told me that Business Continuity really is “PROCESS RE-ENGINEERING.” He was right.

We look at processes to protect them, but at the same time we should be looking for ways to improve the process.

**The exercise is good for us, good for the folks working the process,
and good for our Clients or Employers.**

6.4 *Risks to output*

Risks to output is simply the reverse of Risks to input (Paragraph 6.2 Risks to input). What happens to the process when this business function is through with it? How is it handed off? To whom or what?

6.5 *When does it stop?*

How far does the Business Continuity planner have to go to consider the process “protected?”

As a general rule, the planner must go to at least the neighboring business functions or the vendors to assure that the function or vendor has a Business Continuity plan to continue service for the process.

If you are an in-house planner creating an enterprise plan, you will know (sooner or later) what the neighbor business functions are doing to protect their processes (which in turn protect the current function’s processes).

If you are creating a plan only for one business function, you will need to diplomatically find out how the neighbor functions protect their processes.

When it comes to vendors, you may need support from the Contract’s people, but you, as the Business Continuity planner, have a valid reason to see each vendor’s Business Continuity plan.

When looking at vendor plans, make certain the plan is

(a) up-to-date,

(b) tested, and

(c) that there is a maintenance procedure in place.

THE Rule: No test = No plan; No maintenance = No plan

6.6 *The ubiquitous “other” risk*

Risks generally fall into three major categories:

1. human
2. natural events

3. technology

6.6.1 Human risks

Human risks range from “human error” to someone “going postal.” These are the hardest to avoid and sometimes the most expensive to mitigate. Consider the anti-terrorist activity at airports around the U.S. after the September 11, 2001 attack on New York’s World Trade Center and Virginia’s Pentagon. (Yes, the Pentagon is in Virginia, not Washington DC.)

6.6.2 Natural events

Natural events include flooding, the most common risk, and other weather and geological events. Many of these events can be predicted with fairly good accuracy; even tornados can be anticipated based on specific weather predictions, and mitigation measures are well known.

6.6.3 Technology risks

Technology risks run the gamut from a loose connection to a failed system. Technology risks usually can be avoided by redundancy, but that is an expensive option. It is far less expensive to perform preventive maintenance based on manufacturer’s Mean Time Before (Between) Failure (MTBF) and Mean Time To Repair (MTTR).

That still doesn’t prevent someone from tripping over a cable ... but is that a technology risk or a human risk?

6.6.4 Risk list

A list of risks is given in Appendix 1: Risk list. The list is **not** all-inclusive.

6.6.5 What about terrorism?

For the most part, terrorist activities parallel accidents.

For the Business Continuity planner, it makes no difference if a plane *crashes* into a building or is *flown* into a building. The result is the same. If the building in which the process you need to protect is in a take off or landing pattern, aircraft accidents must be a very real concern.

During World War II a B-25 bomber flying in a heavy fog crashed into the Empire State building. That was an accident

**caused by weather, a very tall building, and probably
an inexperienced flight crew or instrument failure.**

If the building is near a railroad track, barge canal, or major truck route, you must consider a HAZMAT event. It could be a terrorist action, but more likely it would simply be an accident.

With the exception of terrorism-by-mail, *most* terrorist actions mimic accidents or human risk; plan for accidents and human risk and you are planning against terrorists.

Final thought: You cannot **absolutely** defend against terrorists.

Philosophy: Plan for the worst; hope for the best.

7 Risk assessment - rating the risks

Risks are rated by “probability” and by “impact to the business.”

7.1 *Probability*

How likely is a risk to occur for a **business process**?

Some risks we can anticipate based upon history. We know, for example, that certain areas are prone to flooding. We know when flooding typically occurs. If our Client/Employer was foolish enough to build on the flood plain – and some are, I know – we know to load sandbags in the flood season.

We know that mechanical and electrical parts give out. Most “long-life” components have MTFB/MTTR ratings; when the equipment nears the end of the shortest MTBF-component, we know it is time for preventive maintenance of the equipment.

Some risks have a “high” probability in some locations or seasons, and “low” probabilities in other locations or seasons.

Probability is rated on a scale of 1 to 3 (or 1, 2, 3), equating to low (1), medium (2), and high (3).

7.2 *Impact*

What is the impact **on the business** if the risk occurs?

In order to measure the impact, the Business Continuity planner needs to know

- how much income is lost for, typically, 1 hour, 1 day, 1 week, and 1 month
- how much it will cost (overtime, supplemental staffing, additional equipment) to “catch up” after an outage of 1 hour, day, week, and month
- what damage can be expected to be done to the organization’s image
- what damage can be expected to be done to the organization’s financial status (stocks, bond rating)

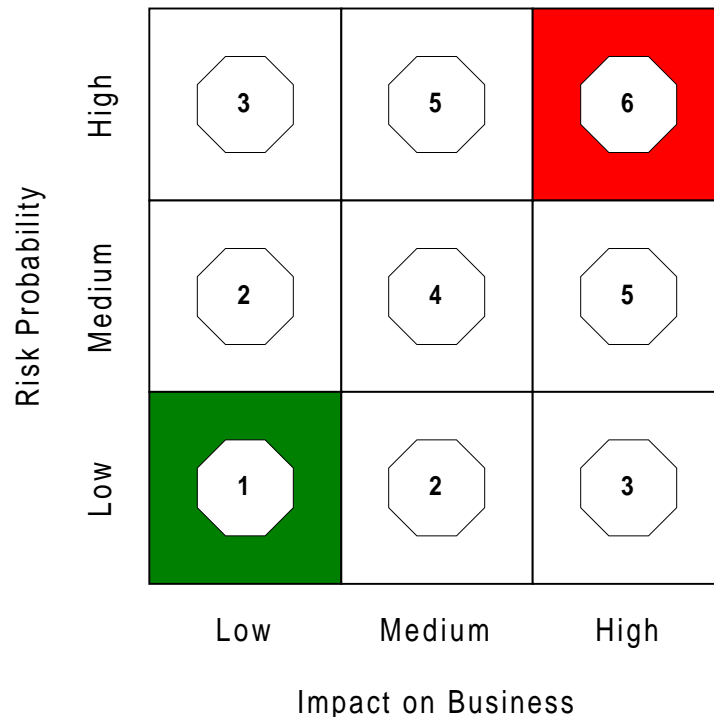
- what penalties will be applied by regulating agencies if the organization is unable to complete a critical process for 1 hour, day, week, month

The assumption is that full or nearly full operation will be restored within 30 days. The 30-day period may not see the entire operation functioning as it did before the disaster event – people may be working from temporary facilities – but the Level of Service will be (almost) Business As Usual.

Impact is rated on a scale of 1 to 3; low = 1, medium = 2, and high =3.

7.3 ***Tic-Tac-Toe***

In order to prioritize the identified risks, a 9-square “tic-tac-toe” matrix is used.



The planner marks the Probability and Impact rating on the matrix. Assume a Risk Probability of 2 and an Impact of 5. Add the numbers for a score of 7

($2+5=7$). Another risk may have a Risk Probability of 3 and an Impact rating of 1 for a total of 4 ($3+1=4$). Avoidance or mitigation measures would be applied to the “7” risk before the “4” risk.

Smart planners keep a coin handy to resolve equal-number risks.

8 Dealing with risks

Business Continuity planners may recommend, and management may accept or reject, one of three first-level means of dealing with an identified risk.

8.1 **Avoiding**

The best option, albeit usually the most expensive and resource-intensive is to avoid the risk. Eliminate the risk.

There are two ways to eliminate a risk:

1. eliminate the process to which the risk is attached
2. duplicate or triplicate the process at a distant and unrelated location

The first option usually is not an option. It could be if the organization finds the risk is too great to bear, if the organization is about to change directions, or if the process is about to be replaced.

The second option is the more common.

How much replication is enough replication?

The author's personal preference is to have primary and secondary "back-up" facilities.

If external back-up is the choice, make certain the vendor's Business Continuity plan includes redundancy for its services.

Because of its cost, duplicating or "triplicating" a process must be carefully considered against available mitigation (work-around) options; if the process really so critical that it must be replicated

8.1.1 Hot, warm, and cold sites

Hot, warm, and cold sites typically are considered only for IS/IT/MIS operations. Humans, unlike computers, can take their lunch and go elsewhere if something happens to their mechanical or electrical resources. They need a place to go, but in many cases their time to resume a minimal Level of Service is greater than a data center's requirements (e.g. a day for humans, 5 minutes for the data center).

If an operation must be fully replicated – out-of-service time is measured in minutes and human safety is an issue – the only option is a “hot site.”

A hot site is a fully resourced (personnel and equipment) facility that can assume the functions of the failed site within the permitted time frame. A true “hot” site runs in parallel with the primary system, with systems automatically switching back and forth to confirm each system’s “health.”

In addition to the cost of additional personnel and hardware resources, hot sites demand replicated communications facilities.

One replicated site looked great on paper. Everything was in place and working smoothly. Then a Business Continuity planner discovered that the phone lines connecting the two facilities shared the same conduit at one of the sites. One misdirected cut by a back-hoe and good-bye primary and secondary communications lines; good-bye hot site.

Any time you are dealing with hot sites, very carefully look for “single points of failure” such as power from a single source and adjacent replicated phone and electrical connections.

Warm sites are similar to hot sites in that the equipment is in place, and similar to cold sites in that they must be staffed and data loaded before they come on line. If the allowable out-of-service time permits use of a warm site, the organization can realize substantial savings over a hot site.

Cold sites are bare rooms. They must be equipped, utilities must be turned on, and staffed.

A former client has an agreement with a major retail chain to use excess space in the chain's stores in the event a disaster condition knocked out one of the client's regional data centers. Equipment for the cold sites was palletized (strapped to pallets) and ready to be shipped to the cold site. Given the client's minimum time-to-restore basic operations, the cold site was the preferred option. (Although the client had internal resources, management decided the cold site option was better.)

Cold sites are perfect for processes which can be delayed several hours. Non-emergency call centers, support services (HR, Finance, etc.) are good examples of this type process.

The reason to have a “cold site contract” in place is to guarantee work space in the event the facility is damaged. The risk to the cold site contract is that the cold site may also be damaged. Hotels and motels, particularly those with meeting rooms, are prime candidates as personnel cold sites. Contacting with a hotel or motel chain may make finding an undamaged facility that can accommodate your people a little easier.

**Check with HR before inking a contract.
Some companies restrict personnel relocations to
a specific distance from the normal work facility.**

There are no restrictions to use of multiple backup options.

In a business environment, there are functions which must be restored immediately, as within a minute. A hot site that mirrors the primary site is required to provide this level of service; nothing less will suffice.

Hot sites, however, are expensive and the ideal situation is to move the function to a non-hot site environment as quickly as possible.

If business as usual is quickly restored at the primary site, the function is restored at the primary site. If restoration at the primary site is not possible, the function can be restored at any site able to accept the function.

Before restoring the function at any location, make certain that the restoration site has been tested to assure it can handle the function. Replicate the function at the restoration site and mirror the hot site until the restoration site has been proven.

Finally, if contracting for a commercial backup facility, make certain the vendor has a tested and maintained Business Continuity plan and plan to budget for at least one annual test that exercises the vendor’s capabilities.

8.1.2 Site considerations

When selecting any site, including a vendor-provided hot site, bear in mind requirements for:

- personnel space
- equipment (printers, scanners, copiers, telecommunications, etc.)
- amenities (break areas, toilet facilities, etc.)
- private space for secure information and personnel matters

Other things to consider are listed in Paragraphs 10.5. The environment and 10.6. Remote site considerations.

8.1.3 Internal redundancy

Organizations with dispersed facilities with similar operations are prime candidates for internal (in-house) redundancy.

The primary benefits of internal redundancy are two:

1. cost – the organization already has resources available
2. control and security – internal personnel are working with sensitive information

While internal redundancy usually is to be preferred, management may be aware of situations which make external redundancy the better option.

8.1.4 External redundancy

External redundancy is the only option for single-site organizations.

The most common option is to contract with an organization that specializes in Business Continuity and Disaster Recovery services.

Cost depends upon a number of factors, including the equipment use (hot, stand-by), personnel (yours, the vendors), and testing (frequency, duration).

8.2 **Mitigating**

Mitigating risks – reducing both the probability and the impact of a risk – typically is less expensive than avoiding the risk.

Mitigation can mean many things and can be applied to almost every process.

For example, paper forms might be used to mitigate a data entry process that depends upon computers; WATS lines and faxes can be used in lieu of Internet and intranet communications (email, forms).

**The risk was *loss of microwave towers to hurricane-force winds.*
The mitigation option: *contract with builders to use their cranes.*
The truck-mounted cranes are mobile and designed for off-road use;
they can be driven to, or close to, the site of the disabled tower.
Attach an antenna to the crane's rigging, raise and aim the antenna
and instant tower.**

**(The guy that came up with the idea got a cash award from
his government employer!)**

Just as group participation was suggested for risk identification, group dynamics can help identify means to mitigate risks. Nothing is too “strange” to be considered – picture the box and Rodan’s *Thinker*.

8.3 *Absorbing*

Absorbing a risk may at first seem counter to the aims of the Business Continuity plan.

But there are instances when it simply is not worth the money to protect a resource.

Put in terms most planners can understand: you have a car worth \$2,000. You can put comprehensive insurance on it for \$100-a-year with a \$500 deductible. Is it worth it, or could the money be better set aside for a newer car? Management decision.

8.4 *Insurance*

Insurance is a major ingredient in a Business Continuity plan.

The insurance *agent* can be an important resource for the planner, especially if the insurance company is aware of Business Continuity and Disaster Recovery planning.

Some insurance companies have built a reputation for workplace risk identification; the focus usually is on protecting personnel (read “avoiding workman’s compensation claims”), but the expertise is there and should be utilized.

8.5 *Bringing in the experts*

It was written before and probably will be written again, but Business Continuity planners cannot be (expected to be) experts in everything.

We are Business Continuity Subject Matter Experts (SMEs) who know enough to go to the professionals.

Many of the professional expertise is available to us at no cost.

- Personnel and facility security? Police department.
- Fire safety? Fire department.
- First aid training? Fire department or local health organizations.
- HAZMAT? Fire department, OSHA.
- Flood probability? Municipal planner’s office.

Resources abound. Use them.

As someone told the Ace¹ planner: “you know all the answers”. Ace replied that he didn’t really know all the answers; he just knew where to look for them.

Get to know the Emergency Management personnel for your county. The manager coordinates all activities in the event of a “global” disaster condition. In this case, “global” is anything greater than a single business or residence.

The Emergency Management folks *may* even be able to help your organization finance some mitigation activities.

8.6 *Additional things to consider*

Policies and procedures governing, alphabetically,

¹ Martin Ace Jackson

- business expenses
- communications options
- internal communications
- overtime
- personnel expenses
- support for families of employees working at a remote (back-up) facility
- travel

9 The first deliverable

The first deliverable – the documentation you deliver to your sponsor(s) – needs to include

- a recap of the SOW
- a list of business functions and business processes covered by the document
- the people who provided information
- a list of the identified risks
- the risks prioritized, with comments to support the assigned priority level
- avoidance and mitigation options for each risk
- your recommendations for implementing an avoidance or mitigation option

Keep the document simple; your sponsors probably want “just the facts.”

Give all the contributors a chance to review the draft document and be prepared to make some – but not all – changes. If there are concerns about the priority of a risk for one business function compared to another business function, hold a conciliation session and invite the respective managers to resolve the issue.

Remember, risk priority is based upon
(a) the probability it will occur to a process and
(b) the impact it has on the business (not only the process).

10 Specifically IS/IT/MIS

The computer world is a little different than the Business Function world.

The Business Continuity planner is charged with protecting platforms on which critical applications are running. The planner also is charged with protecting the networks – both internal and external - that carry information.

10.1 *OS is not critical*

The Operating System (OS) is not critical - all computer systems have the same basic requirements. The only time the OS should concern a Business Continuity planner is when he or she is looking for a back-up or replacement unit.

10.2 *Know what's on the box*

The Business Continuity planner needs a list of all applications and utilities on the computer. This means all patches and upgrades. It also means knowing which applications, scripts, and utilities go together. This can be a major task if homegrown software was created by contractors, vendors, or no-longer-present employees.

Most computers include a utility to “map” the hard drive(s); that is Step 1 toward identifying all the code for each application.

10.3 *Mirror the box*

Create a back-up of the entire computer, including the OS. The optimum way is either to write directly to a CD or to write to tape and then copy the tape to a CD (since most newer platforms default to read CDs for essential data). If you are fortunate enough to start with a clean machine, so much the better. Copy the OS (and patches) separately, then each application as it is “tweaked” for your particular organization. Finally, copy all data to separate media.

10.4 *RAID is nice, but not perfect*

RAID 5 set ups (with redundant hot drives) are great for those who can afford it, but they give a false sense of security.

We know hard drives **will** fail. The RAID set up covers that.

But RAID 5 will not protect against floods, tornados, fires, etc.

Copy everything and keep a copy at a remote site.

Never “assume” data can be restored from a back-up tape when it is needed. Tape degrades with time and use. Even data on new tapes should be checked to assure that it can be restored.

Don’t assume just one thing will go wrong at a time.

In fact, don’t assume – period.

10.5 The environment

Consider

- climate control – if the A/C fails, is there a back-up and is it sufficient?
- communications – are there alternate providers; are the wires close together as they exit the site (can a trencher or backhoe cut both at once);
- electricity – is it filtered, is there a generator if 24*7 service is required; is the UPS sufficient to allow a controlled shut-down; is AC provided from separate grids?
- facility security - are separate IDs required to access the area; is access restricted to those with special clearance?
- network security – are firewalls in place; are the firewalls tested; are all security patches installed (this often is a gapping security hole)?
- shut-down – does everyone know how to perform an emergency shutdown; the main switch is obvious and not hidden behind a box?

10.6 Remote site considerations

- 24*7 access.
- Hardened (tornado-proof, earthquake proof) building.
- Climate control with independent back-up unit.
- Multiple phone lines (if data are transferred electronically).
- Multiple power grid feeds (or a generator; a UPS is not sufficient).

10.7 *Diagrams and documentation*

Confirm that all network diagrams are up-to-date (including patch panels and punch-down boards) and that all documentation is up-to-date (hardware configurations, telecommunications [type lines, numbers, pilot numbers, etc.], and circuit diagrams).

Make certain all procedural documentation is accurate; this becomes part of the Continuation and Disaster Recovery plans.

In a true “worst case” situation, the folks who normally maintain the operation may be unavailable; other replacement personnel will be depending upon the available documentation to restore the function.

10.8 *Licenses and other documentation*

Store copies of software licenses, hardware ownership papers, backup copies of all programs and applications, network diagrams, policy and procedure manuals, and vendor agreements off-site. If there is any question about replacements or operations, the documentation will be available for reference.

10.9 *Back-up hardware*

It usually is **not** necessary to have matching hardware.

In the event of a failure, critical operations need to be restored within a minimum acceptable Level of Service. This can range from a few seconds to a few hours.

Non-essential functions may be restored later (but keep in mind that even the so-called “non-essential” functions have time constraints).

The Business Continuity planner must make certain capacity is available on compatible platforms for the critical functions. Capacity requirement is gained during the “Know what’s on the box” exercise (Paragraph 10.2 Know what’s on the box).

Depending upon the criticality of the functions/applications and the organization’s size and structure, the planner may be able to enjoy advantages of scale and keep the back-up operation in house. The alternative is to find a vendor to provide back-up for the operation. See Paragraph 8.1.1 (Hot, warm, and cold sites) for a brief presentation about hot sites and other options.

10.10 **Got'chas**

There are a number of “got'chas” waiting to foil the best plan. These include:

- Failing to confirm the backup media can restore the data; tape ages and its ability to record and to restore is reduced by time and use.
- Failing to make certain both the primary equipment and the backup equipment are *functionally* identical - has the backup media format changed (e.g. from one tape type to another)?
- Failing to update the backup system with the same level of software running on the primary equipment - Version 4B may not be backward compatible with Version 4 that is available on the backup system.

**Every time the primary system is updated,
even with a home-grown script, update backup system(s).**

11 Focusing on facilities

One aspect of Business Continuity plans frequently overlooked by junior, and sometimes not-so-junior, planners is the facility. Planners can't do much to avoid or mitigate risks to a building once the foundation is poured.

They can, however, do a lot to insure the safety of the people who work inside the building.

Count the number of fire extinguishers and carefully note how well the locations are marked. Can the locations be identified from afar? The same goes for fire call boxes; and are they at a height everyone can reach?

Is there an evacuation route map on the walls, with "You are here" and primary exits clearly marked?

If you have someone who has a mobility handicap, ask that person how easily it is to exit the building through an emergency exit; to exit the building and to get far enough away from the structure that flying debris will fall short. A wheelchair is hard to move in snow, sand, mud, and high grass, and barriers of all types - fences and culverts - are impossible to navigate. Ask a person who is sight impaired to tell you how easily the exits are to find.

Since we mentioned fire extinguishers, are people trained to use them **after the fire department has been called**?

Are there "hall monitors" to assure that everyone clears the building, and is there a "buddy system" in place to account for everyone?

Have primary and alternate site "safe areas" been identified, areas that are protected by distance and obstructions from flying debris?

If the building has multiple levels, can a mobility-handicapped person escape?

How long does it take - really - to evacuate the building? Not how long does someone **think** it will take, but how long did it take the last time there was a drill.

There **was** a drill, recently, wasn't there?

12 Management decisions

A very short chapter.

Management will make the decisions to implement or ignore your recommendations.

If some recommendations seemingly are ignored, don't be upset. There probably are organization plans to which you are not privy. If you feel a serious risk is not being addressed, go back to the people threatened by the risk and re-examine the process, the risk, and the impact on the organization.

If the risk still seems as dangerous, document it with the respective managers and present it again to the most understanding of your sponsors.

When management makes its decisions on what to implement – and when – you can begin creating the Continuation and Recovery team plans.

Caveat: If implementation is more than 6 months out, create your plans as if there was **no** implementation. Plans can be revised.

13 Declaring a disaster condition (& standing down)

13.1 *Who may declare a disaster condition*

Any manager may declare a disaster condition if specific criteria are met. While this will vary by organization, typically, the criteria include a condition that

- cannot be remedied before impacting the organization
- impacts two or more Business or Support Functions

As an example, if a computer fails and

- the MTTR is 30 minutes
- the maximum acceptable outage is 1 hour

no disaster condition is declared.

Another example: if a pipe breaks and water floods the area where a critical Business Function is performed and

- the time to recover from the flood is 48 hours
- the maximum acceptable out-of-service time is 2 hours or
- the outage will impact Business Functions providing input to, and accepting output from, the flooded Business Function

a disaster condition is declared.

If the flooded Business Function could relocate and continue business within an acceptable time frame (2 hours), there would be no disaster condition declaration.

A disaster condition may be declared before an event. This is typical when the event (hurricane, tornado, sink hole, etc.) is imminent.

13.2 *Who can order a stand-down (business restored)*

A stand-down can be declared only by the Continuation or Disaster Recovery team leader or, on recommendation of the Continuation or Disaster Recovery team leader, a member or senior management.

14 Continuation and Recovery plans

14.1 *Who to include*

Enterprise plan: at least two (2) people from each department. Also include Emergency Management and insurance personnel. (Vendors are included on the contact list unless vendor personnel have a permanent function on site.)

Business Function plan: at least two (2) people from each Business Function. (Attach the Business Continuity plans from the support organizations.)

Support Function plan: at least two (2) people from each Support Function for which the plan is created. Document how Support Function personnel reached the risk and recovery priorities.

14.2 *Primaries and alternates*

Continuation, Disaster Recovery, and Corporate teams must have primary and alternate personnel for **every** position.

People go on vacation, take time off, terminate.

**Organizations having multiple shifts need
two people on EACH shift for EACH position.**

14.3 *Teams defined*

Continuation team: Responsible to rapidly restore operations to minimum Level of Service. See Paragraph 14.8 for a more detailed description.

Disaster Recovery team: Responsible for restoration of the operation to Business As Usual as efficiently as possible. See Paragraph 14.9 for a more detailed description.

Corporate team: Responsible for “corporate-level” functions such as finance, public relations, purchasing, travel, and similar activities that (a) support the Continuation and Disaster Recovery teams (e.g. finance, purchasing, travel) and (b) represent the organization to the world (e.g. public relations). See Paragraph 14.10 for a more detailed description.

Note: Most traditional Business Continuity plans recognize only a Disaster Recovery team and assign all functions to this team. I feel multiple teams with specific tasks better serve the organization.

14.4 Team leaders

The team leaders must – not “may, but “must” –

- have authority equal to the responsibility
- thoroughly understand the organization and its goals
- work well under pressure
- know how to delegate

The Business Continuity planner may **not** be the best candidate for a team leader position. Likewise, a senior manager may **not** be a good candidate for the leader position; but if a senior manager is included as a team member, that manager must agree to do what the plan requires and any other tasks the team leader assigns – regardless of the leader’s position within the organization during a “normal” times.

14.5 The CEO’s role

The CEO, and all other CxOs, may or may not be part of a team. The CEO is the “final authority” for the plan and each teams’ assignments, and often the CEO is the “official” media contact. (In some cases it is better to let the PR or Media Relations folks do all the talking for the company.)

If the CEO is not a “player” he or she should know to stay clear of the action; it tends to be hectic immediately following a disaster event.

14.6 Team member selection

Team leaders should be given discretion in selection of team members, but all must remember there is a finite number of resources and that each function may have to supply two people for both the continuation and the disaster recovery teams.

14.7 A “kiss” for documentation

Documentation is critical to *both* Continuation and Recovery teams.

All expenditures must be documented.

All progress must be documented.

All “got’cha’s” – the things that failed to work as planned – must be documented.

All documentation should follow the KIS principle – **Keep It Simple**.

Be thorough, but concise. (The tech writer probably is a better choice than the advertising writer for the documentation duties.)

14.8 Defining Continuation Team tasks

Continuation teams, often overlooked by Business Continuity planners, are responsible for immediately restoring a minimal Level of Service for the organization. “Immediately” is relative to the organization’s mandate, but typically within 24 hours.

The Continuation teams need to assure:

- adequate facilities are available
- utilities and communications are available
- tools needed to accomplish the processes are available; these may be “work-around” tools (e.g. paper and pencils in lieu of a computer terminal)
- that everyone knows where to go (or not to go, as the case may be)
- that the processes are being performed at the minimum Level of Service or better
- all team activities are documented (Paragraph 14.7)

14.9 Defining Disaster Recovery Team tasks

The Disaster Recovery team is responsible to restore the operation to “Business As Usual” as quickly as possible.

The team consists not only of technical personnel (from Support Functions) but also personnel from the Business Functions. The technical personnel are responsible to put things back together – get the computers working, the wires in place, etc. The Business Function people, in addition to supporting the

technical staff at their level of expertise, are present primarily to test the restored system to assure it is fully operational.

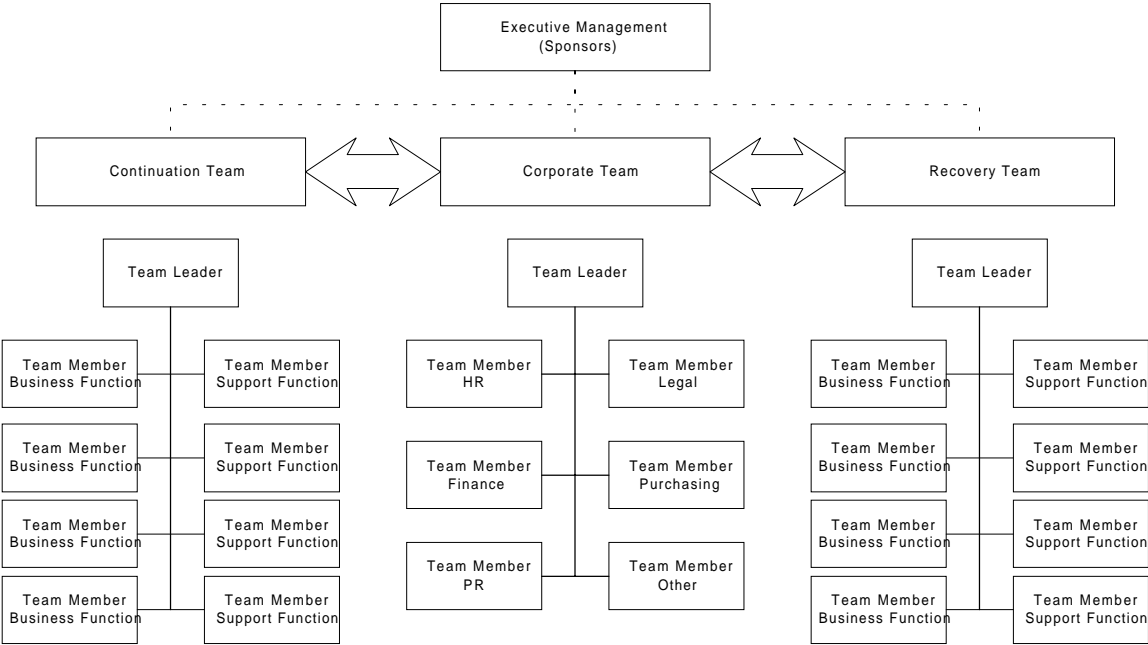
Business Function personnel may be required only later in the restoration process; when they are to be present is determined by the Disaster Recovery Team leader.

14.10 Corporate Team tasks

The “corporate” team – for want of a better title – provides services to both Continuation and Disaster Recovery teams.

Although the corporate team rarely is a separate entity in the Business Continuity plan, it makes sense to husband resources to derive the maximum benefit.

Corporate-level resources – Accounting, Finance, HR, PR, Shipping, Travel, and the like – should be available to both teams on an “as needed” basis. The functions performed by these people are critical to the success of both the Continuation and Disaster Recovery teams, but the presence of these people on each team is not necessary.



14.11 Contact information

Contact information for all personnel must be up-to-date.

Likewise, contact information for Emergency Management leaders and vendor representatives must be monitored to assure it is current.

Contact information should include, at a minimum (* = required)

- * Name
- * Phone numbers (office, home, cellular, pager)
- * Physical address (and mailing address, if different)
- * Job title/function – this person’s particular expertise may be needed
- * Team role (if on a Business Continuity plan team)

Supervisor

Direct reports (if supervisor)

External contacts must include two responsible people for each organization (e.g. vendors, Emergency Managers); the supervisor/direct reports information is not necessary.

Each Business Function and Support Function is to be considered an “internal vendor.” As such, each Function will have (at least) two contacts per shift listed in the contact information.

There should be two lists – an alphabetized name list and an alphabetized “vendor” list divided into “internal” and “external” vendors and Emergency Management contacts.

15 Exercising the plan

15.1 Why

No plan is perfect the first time out.

Period.

Only through exercising, or testing, the plan can it be improved.

In addition to finding the “got’chas” in a plan, exercising the plan helps team members develop confidence in their skills.

A disaster event is no time to find out someone really isn’t quite sure how to do a task or to learn that a team leader goes to pieces under pressure.

15.2 Exercise options

Most plans depend upon simulations to discover the “got’chas.” The simulations start with a simple “walk through” in which team members “talk through” the procedures. As team members’ confidence increases and as the “got’chas” are eliminated, the simulations become more realistic and pressure factures are integrated into the event.

Throw the switch exercises are both dangerous and expensive. If they must be done, make certain all the simulations have been completed and that there is a very high level of confidence that (a) the test will go well and (b) everything can be **quickly** restored in the event of a failure.

15.3 Critiquing the exercise

Each exercise must be critiqued.

The critique must look at “what can be done better” rather than “what went wrong.” Finger pointing is counter-productive, especially when everyone must work together for a plan to succeed.

15.3.1 Planner or team leader’s critique

The Business Continuity planner or the team leader(s) can critique the lower-level simulations and make recommendations for improvements. A wise planner or team leader makes certain to ask everyone involved how they think the plan can be improved, bearing in mind that the goal is plan improvement, not finger-pointing.

15.3.2 External (non-team member) audit

Once the team members are confident in their skills, invite outsiders to critique, or audit, an exercise.

The auditors should be given a pre-exercise presentation so they will understand the goals of the exercise; what is to be accomplished and what is “beyond the scope” of the effort.

15.4 Including “the world”

At least once a year, invite the Emergency Management people to participate. This is particularly critical when hazardous materials are involved. The exercise should be a full-scale alert and as realistic as possible.

Also “prove” both the internal and external (vendor) contact lists at the annual “super-simulation” exercise.

16 Maintaining the plan

A plan not maintained is not a plan.

16.1 *Calendar triggers*

Depending on an organization's dynamics, Business Continuity plans should be reviewed and updated at least once-a-year. If the organization's business plan is updated regularly, the Business Continuity plan should be updated at the same time (or shortly before so avoidance and mitigation options can be included in the business plan).

16.2 *Event triggers*

Plans require updating when certain events occur. These events include, but are not limited to,

- equipment and system changes
- key personnel changes
- location or facilities changes
- policy changes
- procedure changes
- product changes
- team personnel changes
- vendor changes

17 Random thoughts

As the book was reviewed additional thoughts crept into mind.

Such as:

17.1 *Disaster Recovery vendors*

Equipment and back-up site vendors were previously discussed.

In addition to these people, your plan should include the name and contact information for vendors who can, among other things,

- cater meals
- dry out the facility drenched by flood, storm, or sprinkler
- dry out critical papers and books
- dry out salvageable equipment
- clean up hazardous materials
- provide chemical toilets
- provide mobile offices (for personnel and for equipment)
- provide portable power
- recover data from damaged media
- remove debris (the biggest post-event cost)
- rent transportation (cars, vans, trucks)
- salvage damage equipment
- supply office and technical personnel
- supply site security (personnel, fencing,, lighting)

The list is only a sampling of the post-event vendors that may be needed in addition to the vendors identified previously.

Appendix 1: Risk list

The following is a *partial* list of potential risks.

aircraft accident	hazardous materials	security (networks)
car or truck accident	heat (extreme)	security (physical, facility)
cash flow interruption	human error	sink hole
cold (extreme)	hurricane	someone “going postal”
computer failure	ice	stock devaluation
concentration of personnel	insufficient cash flow	supplier failure
data loss	insufficient emergency exits	technology advances
distribution network failure	loss of key personnel	terrorism
drought	mechanical failure	tornado
earthquake	policy changes	transportation infrastructure failure
epidemic illness	procedure changes	utilities failure
fire	product changes	vendor failure
flood	railroad accident	work action

and the “ubiquitous other” that no one thinks about until after the fact.

Appendix 2: Forms

The following pages are a collection of forms that, with modifications, can be used for most Business Continuity plans.

Specific plans require unique forms; such forms are not included here.

Contact information for (business/support function name)

	Manager	Assistant Manager
Name		
Office phone		
Office location		
Home phone		
Cell phone		
Pager		
Supervisor		

Critical Business Processes for (business function name)

	Business Process
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

Rarely are there more than 10 “critical” business processes for any business function.

REMEMBER, a business function is a major task – e.g. “issue credit card”; a business process is a sub-task – e.g. receive application.

Value of Business Function

This is a critical transaction because of

Competition		Customer expectations		Lost revenue		Public image	
-------------	--	-----------------------	--	--------------	--	--------------	--

Multiple selection OK.

Number of transactions per	Complete for all durations	\$ Value of transactions per	Complete for all durations
Hour		Hour	
Shift (average)		Shift (average)	
Day		Day	
Week		Week	
Month (average)		Month (average)	

Support from Finance Department may be required for to complete this information.

Enter “N/A” if not applicable (e.g. for Shift if no shift work; for Month if a month-long outage is not acceptable).

When full capability is restored, how long and what resources are necessary to clear any backlog of work while maintaining the normal workload (that is normal workload + backlog)?

Each hour of outage requires {extra personnel} (hours of overtime with normal workforce): _____ [] people [] hours

Business Function Maximum Allowable Outage

This requires management input.

What is the maximum acceptable time the Business Function can be out-of-service (not performed)? _____

Business Function Documentation

Identify documents, including forms, regulations, policies and procedures, and training materials are required to accomplish this Business Function.

Document Name	Can be found at/in	Document Name	Can be found at/in

IT Specific

Applications and Utilities Supporting the Business Process

Business Process _____

Business Function _____

Business Function Manager _____

Application	Platform ID	App Size	Related apps, utilities

Contact Information – Page __ of __
Internal Vendors (Accounting, Finance, HR, IT, Mailroom, etc.)

Vendor function:			
Manager's Name		Deputy's Name	
Location		Location	
Internal phone		Internal phone	
Admin Assist phone		Admin Assist phone	
Mobile phone		Mobile phone	
Pager		Pager	
Home phone		Home phone	

Vendor function:			
Manager's Name		Deputy's Name	
Location		Location	
Internal phone		Internal phone	
Admin Assist phone		Admin Assist phone	
Mobile phone		Mobile phone	
Pager		Pager	
Home phone		Home phone	

Contact Information – Page __ of __
External Vendors (Equipment, Supplies, Utilities, Supplemental Staffing, etc.)

Vendor (corporate) name			
Vendor function			
Primary contact		Alternate contact	
Office phone		Office phone	
Admin Assist phone		Admin Assist phone	
Office fax		Office fax	
Mobile phone		Mobile phone	
Home phone		Home phone	
Email		Email	

Vendor (corporate) name			
Vendor function			
Primary contact		Alternate contact	
Office phone		Office phone	
Admin Assist phone		Admin Assist phone	
Office fax		Office fax	
Mobile phone		Mobile phone	
Home phone		Home phone	
Email		Email	

Contact Information – Page __ of __
Emergency Managers

EM Director		Deputy Director	
Office phone		Office phone	
Admin Assist phone		Admin Assist phone	
Mobile phone		Mobile phone	
Pager		Pager	
Home phone		Home phone	

		Deputy	
Office phone		Office phone	
Admin Assist phone		Admin Assist phone	
Mobile phone		Mobile phone	
Pager		Pager	
Home phone		Home phone	

		Deputy	
Office phone		Office phone	
Admin Assist phone		Admin Assist phone	
Mobile phone		Mobile phone	
Pager		Pager	
Home phone		Home phone	

Business Continuation Team Member List

Team title/function		
	Primary	Alternate
Name		
Department		
Office phone		
Admin. Assistant phone		
Mobile phone		
Pager		
Home phone		
Will contact		
Will contact		
Will contact		
Will contact		
Will contact		

Disaster Recovery Team Member List

Team title/function		
	Primary	Alternate
Name		
Department		
Office phone		
Admin. Assistant phone		
Mobile phone		
Pager		
Home phone		
Will contact		
Will contact		
Will contact		
Will contact		
Will contact		

Appendix 3: Consultant's Generic Project Plan

The following pages represent a consultant's basic project plan.

Durations are omitted since this is determined by the size and complexity of the project and the responsiveness of the plan reviewers.

ID	Task Name	Resource Names	'01	
			T	W
1	Business Continuity Plan			
2	Develop Statement of Work			
3	Client execs/Planner meeting	Client execs,Planner		
4	Draft SOW created	Planner		
5	Draft SOW reviewed	Client execs,Planner		
6	Changes to SOW	Planner		
7	Client exec, planner sign-off	Client execs,Planner		
8	SOW accepted	Client execs,Planner		
9	Develop Business Impact Analysis			
10	Create data collection form w/following fields	Planner		
11	Identify business unit			
12	Identify business unit functions			
13	Identify criticality of business unit functions			
14	Identify tools to perform business unit functions	Planner		
15	Office tools			
16	Production tools			
17	Workstations			
18	Networked computers			
19	Communications tools			
20	Vendors			
21	Identify input to business unit functions			
22	Identify output from business unit functions			
23	Identify risks to business unit functions	Planner		
24	Man-made risks			
25	Natural risks			
26	Technological risks			
27	Vendors (Collect, perform gap analysis on Vendor BCPs)			
28	Meet with Client SMEs	Client SMEs,Planner		
29	Explain BIA purpose	Planner		
30	Explain form's purpose	Planner		
31	Client SME's complete form	Client SMEs		
32	Hold facilitated session with Client SMEs	Client SMEs,Planner		
33	Perform gap analysis of form data			
34	Add/Change/Delete data in forms			
35	Prioritize risk reduction effort	Client SMEs,Planner		

ID	Task Name	Resource Names	'01	
			T	W
36	Rate risks (from forms) by probability		<input type="checkbox"/>	<input type="checkbox"/>
37	Rate risks (from forms) by impact		<input type="checkbox"/>	<input type="checkbox"/>
38	Rate risks (from Vendor BCP gap analysis)		<input type="checkbox"/>	<input type="checkbox"/>
39	Compile risk data	Planner	<input type="checkbox"/>	<input type="checkbox"/>
40	Distribute compiled data for SME review	Planner	<input type="checkbox"/>	<input type="checkbox"/>
41	SME review of compiled data	Client SMEs	<input type="checkbox"/>	<input type="checkbox"/>
42	Revise document as necessary	Planner	<input type="checkbox"/>	<input type="checkbox"/>
43	Develop risk avoidance/mitigation recommendations	Planner	<input type="checkbox"/>	<input type="checkbox"/>
44	Rate recommendations by effectiveness		<input type="checkbox"/>	<input type="checkbox"/>
45	Define reasoning behind recommendations		<input type="checkbox"/>	<input type="checkbox"/>
46	Deliver Business Impact Analysis	Planner	<input type="checkbox"/>	<input type="checkbox"/>
47	Client execs accept BIA	Client execs	<input type="checkbox"/>	<input type="checkbox"/>
48	BIA recommendation implementation	Client	<input type="checkbox"/>	<input type="checkbox"/>
49	Client execs, SMEs review BIA recommendations	Client SMEs,Planner	<input type="checkbox"/>	<input type="checkbox"/>
50	Client SMEs recommend implementation options	Client SMEs,Planner	<input type="checkbox"/>	<input type="checkbox"/>
51	Client execs sign-off on implementation options	Client SMEs,Planner	<input type="checkbox"/>	<input type="checkbox"/>
52	Client execs, SMEs schedule implementation	Client SMEs,Planner	<input type="checkbox"/>	<input type="checkbox"/>
53	Client execs transmit schedule to Planner	Client execs	<input type="checkbox"/>	<input type="checkbox"/>
54	Client execs authorize Business Continuity Plan	Client execs	<input type="checkbox"/>	<input type="checkbox"/>
55	Business Continuity Plan development		<input type="checkbox"/>	<input type="checkbox"/>
56	Statement of Work review		<input type="checkbox"/>	<input type="checkbox"/>
57	Review SOW for modifications	Client execs,Planner	<input type="checkbox"/>	<input type="checkbox"/>
58	Modify SOW if necessary	Client execs,Planner	<input type="checkbox"/>	<input type="checkbox"/>
59	Client exec, planner sign-off modified SOW	Client execs,Planner	<input type="checkbox"/>	<input type="checkbox"/>
60	Create BCP based on BIA, implementation plans	Planner	<input type="checkbox"/>	<input type="checkbox"/>
61	Create Disaster Recovery team	Planner	<input type="checkbox"/>	<input type="checkbox"/>
62	Identify team reporting structure (hierarchy)		<input type="checkbox"/>	<input type="checkbox"/>
63	Define team members by assignments		<input type="checkbox"/>	<input type="checkbox"/>
64	Specify Disaster Declaration and Stand-down conditions	Planner	<input type="checkbox"/>	<input type="checkbox"/>
65	Identify pre-disaster conditions (fore-warning)		<input type="checkbox"/>	<input type="checkbox"/>
66	Identify disaster conditions (no warning)		<input type="checkbox"/>	<input type="checkbox"/>
67	Create non-team notification list by title	Planner,SMEs	<input type="checkbox"/>	<input type="checkbox"/>
68	Identify all external vendors		<input type="checkbox"/>	<input type="checkbox"/>
69	Identify all internal vendors		<input type="checkbox"/>	<input type="checkbox"/>
70	Identify relevant government and regulatory agencies		<input type="checkbox"/>	<input type="checkbox"/>

ID	Task Name	Resource Names	'01	
			T	W
71	Create Disaster Recovery forms			
72	Damage assessment form for facilities			
73	Damage repair form for facilities			
74	Equipment damage report			
75	Equipment repair and replacement report			
76	Infrastructure damage report			
77	Infrastructure replacement report			
78	Expense reports (if Client forms cannot be used)			
79	Personnel time reports (if Client reports cannot be used)			
80	Other forms as necessary			
81	Deliver Disaster Recovery plan to Client SMEs for review	Planner		
82	Client SMEs review, comment on DR plan	Client SMEs		
83	Client SMEs, Planner hold reconciliation meeting	Client SMEs,Planner		
84	Disaster Recovery plan revised as necessary	Planner		
85	Deliver Disaster Recovery Plan to Client execs	Planner		
86	Client execs, SMEs assign personnel to DR team	Client execs,SMEs		
87	Disaster Recovery plan updated	Planner		
88	Deliver updated Disaster Recovery Plan	Planner		
89	Client execs accept Disaster Recovery Plan	Client execs		
90	Disaster Team Training			
91	Client execs and Planner define training requirements	Client execs,Planner		
92	Planner creates training methodology	Planner		
93	Client execs review, approve training methodology	Client execs		
94	Planner develops training program	Planner		
95	Planner presents training program to Client execs and DR team	Planner		
96	DR team and Planner schedule training exercise(s)	DR team,Planner		
97	Planner develops exercises based on identified risks	Planner		
98	Deliver Training Plan & Schedule	Planner		
99	Client execs accept Training Plan & Schedule	Client execs		
100	Training exercises held	DR team		
101	Training exercises critiqued	Planner		
102	Critique delivered to DR team and Client execs	Planner		
103	Training, training exercises continue as scheduled	DR team		
104	Maintenance Plan			
105	Client execs and Planner define maintenance philosophy	Client execs,Planner		

ID	Task Name	Resource Names	'01	
			T	W
106	Planner documents maintenance philosophy	Planner		
107	Planner identifies "triggers" to initiate plan review/update	Planner		
108	Planner defines "routine" plan review schedule	Planner		
109	Client SMEs review maintenance schedule			
110	Maintenance schedule revised as required	Planner		
111	Deliver Maintenance Plan	Planner		
112	Client execs accept Maintenance Plan	Client execs		

Glossary

Backup (back-up) site	a facility to which functions are transferred in the event a disaster condition prevents the function being accomplished at the regular site.
BIA	Business Impact Analysis; determining the impact on the business if a business function cannot be performed.
Gap analysis	review of plan to identify any areas needing attention and to recommend remedial steps.
OSHA	Occupational Safety & Health Administration or Act.
Primary site	This may be the site where business normally is performed or as “primary backup site,” the main backup facility; this assumes a secondary backup facility .

30-day restoration period, 15
assuming - don't, 26
BAU. See Business As Usual
buddy system, 29
 accounting scheme, 29
Business As Usual. See
business function, 4
business process, 4
cold site contract, 19
conciliation (reconciliation), 24
Continuation team
 function, 6
disaster
 definition, 4
disaster condition, 4
 definition, 4
Disaster recovery team
 function, 6
emergency exits
 locating by sight-impaired, 29
emergency exit, 29
 mobility-impaired egress, 29
enterprise planning

Business Continuity Planning Made Simple – *almost*

Index

 reasonable approach, 5
evacuation route map, 29
evacuation time
 actual vs. supposed, 29
families, 2
fire call boxes, 29
 location and marking, 29
fire extinguishers
 location and marking, 29
 use of, 29
gap analysis, 1
global disaster condition (or event), 22
Government agencies, 2
hall monitors, 29
 need for, 29
HAZMAT
 hazardous materials, 3
hot site
 defined, 18
journalist
 as planners, 4
Level Of Service, 3
LOS. See Level Of Service

management buy-in
 required for success, 7

multi-level buildings
 escape from, 29

multiple backup options, 19

Non-profits, 2

OSHA
 Occupational Safety & Health
 Administration (Act), 3

Private companies, 2

proactive, 3

process re-engineering, 10

project plan, 7

Public companies, 1

reactive, 3

Regulated industries, 1

risk matrix, 15

safe areas
 defining and locating, 29

single points of failure, 18

SME
 Subject Matter Expert, 4

SOW. See Statement of Work

Statement of Work, 7

Subject Matter Expert, 4

succession planning, 10

triplicating, 17