Business Continuity Plan

Recent research suggests that on average 20% of all organizations will experience some form of unplanned event once every 5 years. We who work in the United Way system think of ourselves as a resource in the daily lives of our communities – helping to build stronger communities, and among the “rescuers” in a crisis. However, if we personally, or collectively as an organization are impacted by a crisis, then our ability to respond to the needs of others is compromised.

In our first two crisis planning components, “Personal Preparedness Planning” and “Emergency Action Checklist,” the focus was on protecting the health and welfare of people. With those efforts completed, our attention turns to the organization and the plans and preparations we can take which will assist us in resuming operations and services as quickly as possible after a crisis.

Business Continuity Planning

The Business Continuity Plan is an interactive template. In a step-by-step process this component guides the user in building a simple, but effective, plan to minimize damage and speed the resumption of office operations after a crisis.

The template takes the user through four major planning steps:

- Identify and Assess Your Risks
- Understand Your Organization
- Creating the Business Continuity Plan
- Training, Testing and Plan Maintenance

Business Continuity Plan Template

Table of Contents

Introduction

United Way (UW) personnel are familiar with crises. Planning and preparing for various types of unfortunate events represents a fair portion of what you do. It is equally important that each United Way have its own viable plan for what to do if it is impacted in a crisis.

We cannot be rescuers while we ourselves are victims.

Every year crises take a toll on organizations – in both lives and dollars. But organizations are not helpless. Injuries and damage can be limited, and you can get back to normal operations more quickly by planning ahead. That is what this document is about: planning to limit damage and resume operations as quickly as possible when you are caught up in a crisis.

Emergency Plan vs. Business Continuity Plan
The primary goal of an emergency plan is the protection of life. We begin with the assumption that you have completed the personal preparedness planning process, and that your United Way has a workable emergency plan in place, which you have confidence in and have practiced. If not, complete those activities before going any further.

In contrast, this is a template designed to assist you in creating a basic Business Continuity Plan (BCP) for your UW. The distinction is important. While an emergency plan focuses on people and the prevention of injury and loss of life, a Business Continuity Plan focuses on the organization and those plans and actions that will limit damage and allow you to recover and resume operations more quickly after a crisis.

Why Plan?
There are lots of frightening statistics that can be quoted. But we prefer to approach this question in a positive manner.

- Because we are leaders in the community and should model effective behaviors in crises situations.
- Because loss can be minimized and recovery improved with planning.
- Because we cannot provide solutions for others if we ourselves are unprepared.

Most United Ways depend heavily on technology and automated systems, and the disruption of these systems for even a few days could cause severe problems.

Most offices have a collection of key skills, which reside in selected people, including the operation of certain equipment, inputting or retrieving important data, or managing key processes. If these people are lost for any reason, forward movement on important projects could be severely impacted.

You can be impacted by events occurring elsewhere, too. Because a hazardous chemical is spilled a few blocks away, you may be denied access to your building. Because lightening strikes a transformer on the other side of town, you may experience a power failure.

There must be an awareness of potential crises, and a plan to deal with them. In a clear methodical way, this template will take you through a step-by-step process to identify potential threats, prioritize them, and then assist you in finding ways to deal with each.

About This Template

This template is designed to be an interactive tool to assist and guide you through a simplified Business Continuity Planning process. Before you begin the project in earnest, assemble your planning team and read through the entire document to make sure you understand the process, its sequence and its logic.

In general you will find that the document asks one or more pertinent questions and takes you through a series of guided exercises. You will then take some time to assemble and enter the resulting information. At several points you will be asked to make a judgment and enter a numerical value related to that judgment. As you reach these points where judgment must be applied, make sure that you include other team members and key staff in the discussion. A process of inclusion, while somewhat slower, greatly increases the likelihood of well-thought-out responses. Enlisting others is also important from the standpoint of everyone having comfort and ownership in the final product.

Dispersed throughout the tool are a number of tables and charts with sample information. Treat them as references; documents can be found in the Appendix for you to complete your plan.

Definition of an Emergency

An emergency is any unplanned event that can cause death or significant injury; or can shut down your organization, disrupt operations, threaten your reputation, or cause physical or environmental damage.

Risks and Threats

For our purposes, the terms "risk" and "threat" have the same meaning and are interchangeable. We will use them to describe those elements lurking in our environment that are the precursors to emergencies.

Depending on where you look and who is speaking, risks are categorized in several different ways. For the purposes of our discussions, we will break risks into two categories:

- Environmental – Severe weather including high winds, tornados, lightening, ice storms, flooding, extreme heat and cold, and other events such as tsunamis, earthquakes, and forest fires.

- Manmade intentional acts – Theft, vandalism, cyber attack, workplace violence, bomb threat, terrorism.

Note: Generally speaking, the greatest single threat to businesses in North Carolina is related to severe weather.

Vocabulary

In this document, there are unique terms and phrases from the field of emergency/crisis planning with which you may not be familiar. Should you run across one of these terms, please refer to the ***Glossary*** in the appendix.

Creating a Business Continuity Plan

There are a variety of approaches to the process of business continuity planning. When completed, no two plans are alike, because no two organizations are alike. In its most advanced form, organizations will hire a consultant to come in and manage the process. This approach can be complex, expensive and lengthy.

Because United Ways are diverse organizations, each with their own assets and capacities, we have opted to create a do-it-yourself process. This is a simplified and basic form of business continuity planning. We believe it is possible to enjoy great benefit from even a simplified approach. Essentially we have created a template that includes guidance, asks pertinent questions and provides tables for you to insert the appropriate information. The end result will be a viable Business Continuity Plan (BCP).

Getting Started

Before we can begin the actual "process" of BCP, we must identify the individual or team who will manage the project. Business continuity planning must be a top-down effort. To be effective it must have the support and willing participation of the director and senior staff in each United Way. The director or a senior manager should take overall responsibility for the effort and be appointed as the sponsor or champion. Next, we recommend that a single person be appointed as the BCP coordinator for the UW and be appropriately announced and empowered. In larger settings it is wise to appoint a planning team representing all major areas of operations to assist the coordinator.

Budget

Some strategies can be implemented for little or no cost. Most will have either a direct or indirect cost associated with their implementation. Again, the importance of senior staff buy-in is essential. Experience has shown that for those organizations that ultimately face a crisis, the cost of doing nothing is almost always greater than the expense of BCP.

We suggest you include BCP in your short- and long-range strategic planning. Treat the BCP project like any other; have an annual BCP budget, track time and expenses, strive to complete the project on time and within budget. Since it is a prioritized process, you will deal with the most threatening items first, and those you don't get to or can't afford this year will still be there next year.

A Caveat

Don't attempt to complete this process in one, or even a few meetings. You will find that some parts of the BCP template are best done by discussion in a meeting format. Other tasks are most effectively accomplished alone by a key individual that reports back to the coordinator. Don't impose arbitrary time pressures on the project. Let it proceed at a natural pace, as the information is assembled and steps are completed. Of course, we are not suggesting that you go slower than necessary; loss of momentum on projects can mean loss of commitment and, ultimately, their abandonment. BCP is too important to allow that to happen.

BCP – In Four Easy Steps

Step 1. Identify and assess your risks.

In the Introduction we referred to undertaking a *simplified* BCP process. In the fully developed process you begin a detailed analysis of your business and the risks in its environment. This analysis is called Risk-Vulnerability Assessment (RVA). Since there are more similarities than differences in the United Ways, we have used historical data and information from other RVA's done in Michigan to complete this section for you.

Your first major task is to identify the risks/threats in your environment and determine how they might impact your operations. Review the list of risks/threats we've provided in Column 1, Table 1. After careful consideration, eliminate any that are not present in your environment, and add any that were missed. You may also want to consult with your local emergency management office for county-specific risk assessments.

Next, identify the actual impact each threat may have on your organization. Is it likely to cause physical damage to the building? Is it likely to result in the loss of one or more of your utilities? Might it have an impact on your staff or their families? There are no right or wrong answers, and you will find that as you progress through the threats there will be repetition of answers in the impact column. That's to be expected.

Finally, using common sense and available data, rate the likelihood of each risk for your particular area in Column 3.

We have assigned numerical values as examples. When you actually begin, use the blank ***Table 1*** provided in the Appendix and insert values appropriate for your setting and locality.

Table 1. Risk Assessment

Risk/Threat	Consequence	**Likelihood of Occurrence** High-5 Medium-3 Low-1 or None-0
NATURAL		
Tornado or high winds	Building damage Loss of electricity Loss of communications Trees down, roads blocked	2

	Mass transit down	
Lightening	Fire Loss of electricity Damage to computers and electrical equipment	3
Flooding	Denial of access to building Building damage Equipment damage Loss of HVAC Roads blocked	1
Extreme heat or cold	Impact on personnel/families HVAC outage Loss of utilities	2
Snow/ice storm	Roadways impassable Building damage Wires down (phone, electric, broadband-internet) Supplies/vendors can't deliver	4
Forest fire	Denial of access to building Building damage Loss of electricity Loss of telephones	0
Illness: public health emergency	Impact on personnel/families	1
INTENTIONAL ACTS		
Theft	Missing tools, equipment	3
Vandalism	Damage to building Damage to tools, equipment	2
Cyber Attack	Damage/loss of data Virus, worm, etc. Computer/network damage	1
Workplace Violence	Injury/death Emotional impact on personnel/families Denial of Access	1
Suspicious Package	Evacuation: Denial of access	1
Bomb Threat	Evacuation: Denial of access	1
Terrorism	Injury/Death Emotional impact on Personnel/Families Denial of access	1

- ✓ When you have completed this step, revise the table so that the risk/threats with the highest likelihood are at the top, and those with a lower likelihood are at the bottom. Now you've uncovered your first important information: **The Risks/Threats at the top of this list are the most threatening to your organization and operation.**

Step 2. Understand Your Organization

This step analyzes your organization and it provides information that is critical to later activities. *The central task in Step 2 is to identify critical elements that are vital to your organization and its activities.* Begin with three questions:

- **What are we about?** If you have a mission statement, begin there. Then list the overarching goals that drive your organization and your daily efforts.

- **How do we achieve our goals?** Identify the tools and systems that are critical to your mission. At their core, most United Ways are based on communications and data. Therefore you can identify telephones, cell phones, internet/email systems, and computers/data management systems as "mission critical." Continue from there. What other tools or systems allow you to maintain your relationships in the community, conduct your campaign and coordinate your people and activities? In a nutshell, what tools and systems are essential to your operations?

- **Who is involved, both internally and externally?** Identify the people and critical skills that are key to forward progress on each goal. Similarly, identify external services, suppliers, partners, and others who provide a service or product that is key to accomplishing your goals.

As you answer the questions, don't be concerned that some tools, systems and skills are listed several times (because they are important to more than one of your core goals). This is to be expected.

A sample response to these questions is provided below. As you work through each of these questions, capture your thoughts and place them into ***Table 2*** provided in the Appendix.

Table 2. Understanding the Organization

Mission and Goals	Critical Tool or System	Critical Skills (People)
General office operations	Building: for shelter, work areas and meeting space	
	HVAC (heating and cooling)	Building maint. staff

	Work space: desk, chair and lighting	
	Meeting space (seating for 10 minimum)	
	Computer/network	
	Internet connection: email and web access	
	Telephone	
	Copier	
	Fax machine	
	Misc. office supplies	
	Hard files stored on-site	
	Quick access to emergency funds	Pat (Director)
	Payroll	Sue
	Accounts payable	Sue
	Purchasing	Sue
Fundraising	Print pledge cards	Acme Printing Inc.
	Computer: access to data base	Bill
	Telephone and cell phone communications	
	Internet: email and web access	
	Computer: financial accounts	Sue
	Required reports to state and federal government	Bill
Distribute funds	List of accounts and account numbers	Skill: data entry/retrieval
	Checkbook	
	Computer: agency contact list	Bob
	Internet: email and web access	
	Telephone	

At this point you should have information in all three columns of Table 2. Before you go any further, make sure you've got a complete picture. Ask your planning committee if there are other events like Campaign, which occur only in certain seasons or times of the year. What about internal skills, which are important but not used every day? Are there other suppliers or vendors that you see only occasionally yet provide key products or services?

- ✓ With the completion of Table 2 you have identified the second important set of information necessary to the BCP: **The critical skills, tools and systems which are essential to achieving your organizational goals.**

Step 3. Creating the Business Continuity Plan (BCP)

Business Continuity Planning is about getting back to work as quickly as possible. Getting back to work is about restoring critical skills, tools and systems as quickly as possible.

With the completion of the previous two steps you have now assembled the information necessary to begin to actually formulate and write a continuity plan.

The plan will be organized around four steps that have become a mantra in the world of crisis planning:

Mitigation > Preparedness > Response > Recovery

BCP – Mitigation

From this point on we are building a plan of action, and we should be quite clear about what ACTIONS we are considering.

- **Mitigation** describes those efforts made proactively before an crisis to either eliminate or to lessen the impact of a threat.

Mitigation statements should begin with a verb; "remove," "install," "plan," "purchase," and so on.

Now go back to your revised Table 1, where you prioritized the threats in your environment. Begin with the threat with the highest likelihood of occurrence and enter it and its consequences into ***Table 3a***. In the third column "Mitigation Actions," identify a strategy that will eliminate the risk/threat entirely. Failing that, work on finding strategies to lessen its impact. Continuing the example of weather as our greatest threat, begin to assemble your thoughts on possible mitigative actions should an ice/snow storm occur.

Table 3a. Mitigation Actions

Threat	Consequences	Mitigation Action
Snow/ice storm	Roadways impassable Building damage Water leaks Wires down (phone and electric) Supplies/vendors delivery interrupted	Actions to eliminate: Can't eliminate bad weather Actions to lessen impact: Choose office location less vulnerable to snow/ice. Ensure building is structurally sound to take snow load. Ensure eaves will shed ice to avoid ice dams and leaks. Choose office site with underground services. Waterproof main computer and phone equipment areas.

Remember, mitigation is about eliminating some problems entirely, and reducing the impact of the rest. Begin to implement all viable mitigation strategies immediately

within the limits of your time and budget. What you have created is an outline for action. Begin now with the understanding that it may take months, even years, to complete all viable strategies. With the mitigation process completed, you'll now turn to a different strategy to deal with those threats that remain.

BCP – Preparedness

As much as you might wish to eliminate all threats from your environment, it is impossible to do so.

Essentially, a crisis for your UW, no matter what the cause, involves losing one or more of the skills, tools or systems you have identified as essential. So our approach to building a BCP will be to take each skill/tool/system individually, and identify actions that can be taken in the event of its loss.

To begin, combine and transfer all the critical skills, tools and systems identified in Step 2 into the first column of Table 3 below (eliminate any redundant entries). Next, work with your planning team to identify as many strategies as possible for dealing with the loss of each. When you enter a strategy, try to use a verb to emphasize that a particular action takes place; "*install* backup power supply" or "*create* a cache of office supplies."

You will find listed below several fairly standard categories of preparedness strategies. But don't limit your discussions to these alone. Encourage creativity – all ideas should be considered. If you come up with several seemingly viable strategies, so much the better. Record them all. As you get into implementation, you may well find that some are no longer attractive either because they are too expensive, too time-consuming, or for some other reason. It is better to have an excess of possible solutions than a shortage.

- **Backup** – The obvious and standard choice for all electronic data is backup and off-site storage. This strategy can be more widely applied; it is a form of backup when you train additional people in the critical skills you have identified. You can "back up" your essential office supplies with an off-site cache. A second checkbook, list of accounts, purchasing materials and phone list stored in a safe (off-site) location is a key backup strategy. Installing a secondary power supply to run your electronic equipment during a power outage can be a key backup strategy.

- **Protective systems.** A security or access control system helps guard against theft, vandalism and workplace violence. Fire alarm systems, smoke and heat sensors and sprinkler systems all assist in early detection and limitation of damage in the event of a fire. Virus protection and firewall software are protective systems that should be installed on a computer and updated regularly to lessen the likelihood of damage from a cyber attack.

- **Substitution.** If a copier or other essential equipment malfunctions, having a pre-identified vendor and contract in place to quickly rent or purchase a substitute can keep your operation running. If the telephone network goes out, having a plan in place that allows you to automatically switch to cell phones or email can eliminate communication difficulties.

- **Alternate services/site.** Think small; if you lost water in your building, is there a neighbor that might provide rest rooms and water for hygiene? Think big: In certain events your building may be so damaged that it is unsafe to occupy, or for a variety of reasons you may be denied access for a period of time. In such cases, a viable option may be to move your entire operation to an alternative site. This strategy requires not only the duplication of the physical elements of your workspace (desk, chairs, computers, phones, tools and equipment), but also requires that strategies for accessing key files and data are in place as well.

- **Alternative suppliers and vendors.** Few organizations are totally self-sufficient; almost all rely to some degree on outside sources for key products or services. Establishing relationships with alternative vendors is an effective planning strategy. To lessen the likelihood that they too are impacted by the event, they should be located in a different geographic location than your primary provider.

- **Insure against the risk.** Insurance is an effective and recommended way to cover against physical loss. It is not, however, a preparedness strategy in the sense that it does nothing to assist in the short-term resumption of organizational activities.

- **Accept the risk.** Occasionally, because the probability of a particular event is so low, or the expense of dealing with it so high, an organization will make a conscious decision to simply accept the risk.

Record the strategies in the second column of ***Table 3b*** as we have in the example below.

Table 3b. Preparedness Strategies

Lost Skill, Tool or System	Preparedness Strategy	Done
Building and individual workspaces	Establish work-at-home systems. Arrange for alternate facility.	
Heat (winter); AC (summer)	Establish emergency repair contract. Identify source for portable substitute equipment. Arrange for alternate facility.	

Electricity	Install backup power supply. Arrange for alternate facility.	
Water and sewer (hygiene and sanitation)	Identify alternate sources in nearby offices or buildings. Use portable commode/waterless hand cleaners. Arrange for alternate facility.	
Computers, individual and network	Water and fireproof server room. Establish rental source. Use nearby UW equipment. Arrange for alternate facility.	
Telephone systems	Water and fireproof phone equipment cabinet. Use cell phones. Use nearby UW equipment. Arrange for alternate facility.	
Internet connection (Web and email)	Use nearby UW equipment. Use nearby wireless networks. Allow work from home. Arrange for alternate facility. Make UW email/web accessible	
List of accounts	Individual daily backup to portable flash drive Office-wide backup to network server Retrieve info from backup off-site storage location.	
Agency contacts database		
People contacts database		
Financial accounts		
State and federal reporting info		
Checkbook	Retrieve extra from off-site supply cache.	
Purchase orders		
Outside printing services	Establish relationship with alternative printer.	
Copier Fax machine	Identify rental source. Use nearby UW equipment. Arrange for alternate facility.	
Office supplies	Purchase needed supplies. Establish off-site supply cache.	
Stored paper files	Store in fire and waterproof containers. Store off-site. Create digital off-site backup.	
Skill: data input and retrieval	Train additional staff in essential skills.	
Skill: state and federal reporting		
Skill: bill payment, purchasing		

Taken as a whole, Table 3b is your agenda for change. It is a comprehensive list of the critical elements that keep your organization healthy, and the corresponding strategies to recover from their loss. The remainder of your time and efforts should be focused on implementing one or more strategies for each critical skill, tool or system. Indicate completion with a check mark in the third column.

Reality Check

As you get into the details of implementing each strategy, you will be confronted with certain challenges.

Explore with your planning team what alternative choices may be available. Ask other business partners and United Ways if they have faced the same challenge.

Roadblock	Solution
Expense – Some attractive strategies are simply too expensive.	- Seek funding partner. - Request budget adjustment. - Investigate alternative strategy.
Time consuming –the time required to install a strategy is simply not acceptable.	- Seek additional staff assistance. - Investigate alternative strategy.
Resource intensive – the internal resources necessary to install a strategy are tied up or unavailable.	- Partner with neighbor or other UW. - Investigate alternative strategy.
No obvious solution – Some critical elements seem to defy solution.	- Ask other community partners and UW's if they have faced the same challenge.

BCP – Response

OK, plans and strategies are in place. You're done, right? Sorry, not yet.
Now, while things are quiet, is the time to create your plan for how you will react immediately after an crisis event.

Of course, the first consideration is always life-saving actions. Take an inventory of what skills your co-workers are able to provide. It would not be surprising to find that some have first aid, CPR, even fire extinguisher training. Having a clear knowledge of the skills and training at your disposal will give you a better sense of proper timing, and what professional emergency response skills you may need quickly.

This is also the best time to become familiar with the emergency response agencies that serve you. Meet with representatives of your local fire department, emergency medical services, and law enforcement agencies. Ask about the level of service they provide and what a typical response time would be. Ask about specialized services such as hazardous materials response, technical rescue or SWAT teams.

These preliminary conversations can lead to deeper and more valuable relationships. The more the agencies understand about your UW, its activities and setting, the more effective their response will be. Equally important, however, they will gain a better understanding of how you might be able to assist the community in the event of a crisis.

Since you've already dealt with life safety issues in your Personal Preparedness Plan and Emergency Action Checklists, it's time to move into the business continuity issues of getting you back to work.

There are some steps you can take now to improve the efficiency and quality of your agency response to a crisis:

- ✓ Create a Recovery Team. If you've been forced to shut down operations, it makes little sense having everyone struggling to get in to the work site. Instead identify a recovery team that will measure your initial losses and begin a recovery plan.

- ✓ Decide who should be on your recovery team. It will probably look similar to your planning team in the sense that you will likely want someone who is familiar with each major area of your operation. Also, think now about identifying alternates for each team member in case some are not available.

- ✓ Have a communication plan in place now for how you will initially contact and mobilize your team. Factor in the possibility of lost communication systems in a larger event. Can you create some type of automatic response to get around such communication difficulties? Consider using a distant United Way as an out-of-area contact to collect then disburse information and instructions (similar to the concept used in the Personal Preparedness Plan).

BCP - Recovery

The final portion of your BCP has to do with organizing your recovery activities. You know what your critical skills (people), tools and systems are. You must now inventory them, determine which have been damaged or lost, and initiate the recovery actions (your BCP strategies) that you have in place.

Table 3b. Preparedness Strategies is ideal as a damage inventory form because it also reminds you of what you had in mind for recovery strategies. Build a simple kit to be used by the recovery team. Make sure the team leader and at least their alternate has one ready at all times. Items to include:

- ✓ Preparedness Strategies, Table 3b
- ✓ Emergency phone contact list
- ✓ Flashlights
- ✓ Work gloves
- ✓ Hard hats
- ✓ Protective eyewear
- ✓ Dust masks
- ✓ Clipboards and pens

Initiate your recovery actions as soon as possible. Since people and resources may be in short supply, make sure you are always applying them in a manner consistent with your priorities. Beyond the process of physical recovery, recall that there may be other, subtler human/emotional issues which must be dealt with as well.

One of the greatest challenges during and immediately after a crisis is thinking clearly. This is an ideal time for the use of a checklist. Think about the initial actions (after you've dealt with life safety issues) that your response team will need to be focused on.

Recovery Checklist

- ❑ **Call in recovery team members.**
- ❑ **Verify welfare of staff and families.**
- ❑ **Perform damage assessment.**
- ❑ **Identify lost critical skills-tools-systems.**
- ❑ **Report findings to MAUW.**
- ❑ **Implement recovery strategies.**
- ❑ **Keep staff and UWNC informed of progress.**
- ❑ **Notify community partners, suppliers and vendors and community of business resumption.**

After-Action Review

A recommended final step after every event, whether real or simulated, is to perform an "After-Action Review." This is a process where you ask two questions of everyone on your staff:

What went well in our plan and actions?
What would you do differently next time?

It is important to note that this is *not a faultfinding process*. It is critical to avoid criticism and blame. Holding this discussion simply recognizes that with all the effort and work that went into your BCP, it can always be improved upon. Do the after-action review as soon as possible after you've resumed operations so that details will still be fresh in everyone's minds. Take good notes and amend your BCP accordingly.

Step 4. Training, Testing and Plan Maintenance

No emergency plan is ever really finished. The environment outside your work place is constantly changing, and people, methods, tools and systems within your organization change. Therefore, there is no end point to the process of training, testing, and revising your plan.

Apply these concepts in the same priority order discussed in the introduction. Train, test and maintain: 1 – Your Personal Plan; 2 – The Emergency Action Checklist; and 3 – the Business Continuity Plan.

It is not enough to gather your resources and write the plan. If it is to remain functional, it must be continually tested and updated, and if that is to happen, it requires the ongoing support of senior management.

Training and Testing

Everyone in the workplace must be included in training, and at the appropriate times you may wish to include key partners and suppliers. Simply instructing staff to read the plan is not training, and doesn't provide the benefits of discussion and practice.

Training can be as simple as a friendly discussion over lunch, or as complex as a full-scale exercise. Training should be planned and scheduled so that you methodically move through each major area of the plan. We suggest you begin by appointing someone to develop a training plan for the year. For a 12-month period, determine:

- Who will be trained?
- Who will do the training?
- What training activities will be used?
- When and where sessions will take place.
- How the session will be evaluated and documented.

Use the sample ***Annual Training Schedule*** in the Appendix to plan and record training events.

Training Subjects

General training for all employees should address:

- Individual roles and responsibilities
- Information about threats, hazards and protective actions
- Means for locating family members in a crisis
- Office notification, warning and communication systems and procedures
- Proper crisis response procedures
- Location and use of common emergency equipment
- Testing of preparedness strategies and plans

Training Activities

Training can take many forms. There are several levels of training activities you should consider:

- **Orientation and Education Sessions.** These are discussion sessions to provide basic information, answer questions and identify needs and concerns.

- **Tabletop Exercise.** A session facilitated by one or more individuals. The staff meets in a conference room setting to discuss their responsibilities and how they would react to various crisis scenarios.

- **Walk-through Drill.** This is a facilitated exercise where all participants actually perform their functions for the given scenario. A walk-through requires more preparation, takes more time and in general is more labor intensive than the previous training methods. They often reveal problems not revealed in simpler forms of training.

- **Functional Drill.** These are targeted drills that are designed to test a specific area of response such as emergency medical response, warning and communications procedures or an evacuation or sheltering problem.

- **Full-scale Exercise.** A real-life emergency situation is simulated as closely as possible. This level of exercise would typically involve not only your staff, but community first-response agencies as well. These are complex drills that take a great deal of planning and coordination among all the internal and external actors. Never initiate a full-scale exercise without first notifying your 9-1-1 center and all first-response agencies in your community.

Plan Maintenance

Time is the enemy of all crisis plans. *It can be argued that an old plan based on outdated assumptions is more dangerous than no plan at all*. With no plan, individuals are free to apply common sense to the situation. With an outdated plan, they may place their trust in instructions that will cause them harm. All crisis plans must be regularly updated. This includes BCP's.

The most common method of plan maintenance takes place after scheduled training. After each training session, a discussion should be held to summarize any shortcomings found. Recommendations for revisions should be sent up to the planning committee for final consideration prior to officially amending the plan.

In addition, the BCP should be evaluated and modified at the following times:

- **After each crisis**
- **When personnel or responsibilities change**
- **When policies or procedures change**
- **When critical skills, tools or systems fundamentally change**
- **When the layout or physical design of your office or building changes**
- **When you move to a new location**

Other Considerations

If your organization is not the only occupant of a building, check to see if your neighbors have crisis plans in place. You may find that you can be of assistance to some who have less well-developed plans, and in turn, learn from others who may have quality plans. Finally, you may find that integrating your plans with the others creates greater safety and effectiveness for everyone. You won't know until you ask. It's a great way to meet and get to know the neighbors!

Summary

If you have worked through the entire template and reached this point, then congratulations! You now have a draft Business Continuity Plan. Odds are, though, your work is far from over.

You have created a number of mitigation and preparedness strategies. Unless you have unlimited time and resources (and we know you don't), you will spend the next few months, even years, transforming these strategies from concepts on paper to reality. Even then you won't be done, because your organization and your environment will have changed in the meantime.

What you now have that can never be lost is a heightened awareness of the concepts of crisis planning.   Take and apply these concepts in all of your personal and organizational activities. Crisis planning should not be an activity that is done annually according to a calendar entry. At its best, crisis planning is accomplished by its integration into the very culture of your family, and your organization.

Glossary

Alternate Worksite – A work location, other than the primary location, to be used when the primary location is not accessible.

Business Continuity – A comprehensive managed effort to prioritize key business processes, identify significant threats to normal operation, and plan mitigation strategies to ensure effective and efficient organizational response to the challenges that surface during and after a crisis.

Business Continuity Plan – An on going process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential loses, maintain viable recovery strategies and plans, and ensure the community of operations through personnel training, plan testing, and maintenance.

Contact List – A list of team members and key players in a crisis. The list should include home phone numbers, unlisted numbers, cell numbers, etc.

Crisis – Any global, regional, or local natural or human-caused event or business interruption that runs the risk of (1) escalating in intensity, (2) adversely impacting shareholder values or the organization’s financial position, (3) causing harm to people or damage to property or the environment, (4) falling under close media or government scrutiny, (5) interfering with normal operations and wasting significant management time and/or financial resources, (6) adversely affecting employee morale, or (7) jeopardizing the organization’s reputation, products, or officers, and therefore negatively impacting its future.

Crisis Management - Intervention and coordination by individuals or teams before, during, and after an event to resolve the crisis, minimize loss, and otherwise protect the organization.

Crisis Management Center – A specific room or facility staffed by personnel charged with commanding, controlling, and coordinating the use of resources and personnel in response to a crisis.

Crisis Management Team – A group directed by senior management or its representatives to lead incident/event response comprised of personnel from such functions as human resources, information technology facilities, security, legal, communications/media relations, manufacturing, warehousing, and other business critical support functions.

Critical Function – Business activity or process that cannot be interrupted or unavailable for several business days without having a significant negative impact on the organization.

Critical Records – Records or documents that, if damaged, destroyed, or lost, would cause considerable inconvenience to the organization and/or would require replacement or recreation at a considerable expense to the organization.

Damage Assessment – The process used to appraise or determine the number of injuries and human loss, damage to public and private property, and the status of key facilities and services resulting form a natural or human-caused disaster or crisis.

Disaster An unanticipated incident or event, including natural catastrophes, technological accidents, or human-caused events, causing widespread destruction, loss, or distress to an organization that may result in significant property damage, multiple injuries, or deaths.

Disaster Recovery – Immediate intervention taken by an organization to minimize further losses brought on by a disaster and to begin the process of recovery, including activities and programs designed to restore critical business functions and return the organization to an acceptable condition.

Emergency – An unforeseen incident or event that happens unexpectedly and demands immediate action and intervention to minimize potential losses to people, property, or profitability.

EOC – Emergency Operations Center. A location for key personnel to assemble during a crisis that is designed and equipped to facilitate a coordinated response to the event.

Evacuation – Organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas.

Go-Kit – Built to anticipate an evacuation, the Go-Kit is a pre-assembled package of essential supplies. For a household, the kit might include a radio, a flashlight, extra clothes, blankets, maps, emergency phone list, cell phone, cash, water, non-perishable foods and essential medications. In a business setting, a unique kit is built for each key staff position. Such a kit might include a list of all staff, emergency contact phone numbers, key information on business accounts, supplier/vendor information, company check book, radio communications tools (cell phone, radio, extra batteries), building plan, pens, paper, clipboard and a copy of the BCP.

Haz-Mat – Common abbreviation for Hazardous Materials. A hazardous material is any substance or mixture of substances having properties capable of producing adverse effects on life and or the environment.

Incident Command – The highest leadership position in the incident management system structure. Never referred to as an individual, since at long and complex incidents "Command" may move seamlessly and invisibly among several individuals over the passage of time.

Incident Command System or Incident Management System – A standardized system of leadership for organizing and coordinating the personnel and physical resources at a critical incident. The national model used by most agencies is called the National Incident Management System (NIMS).

Mutual Aid Agreement – A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement.

Prevention – Plans and processes that will allow an organization to avoid, preclude, or limit the impact of a crisis occurring. The tasks included in prevention should include compliance with corporate policy, mitigation strategies, and behavior and programs to support avoidance and deterrence and detection.

Readiness – The first step of a business continuity plan that addresses assigning accountability for the plan, conduction a risk assessment and a business impact analysis, agreeing on strategies to meet the identified in the risk assessment and business impact analysis, and forming Crisis management and any other appropriate response teams.

Recovery – Plans and processes to bring an organization out of a crisis that resulted in an interruption. Recovery steps should include damage and impact assessments, prioritization of critical processes to be resumed, and the return to normal operations or to reconstitute operations to a new condition.

Response – Executing the plan and resources identified to perform those duties and services to preserve and protect life and property as well as provide services to the surviving population. Response steps should include potential crisis recognition, notification, situation assessment, and crisis declaration, plan execution, communications, and resource management.

Risk Assessment – Process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an organization's operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls.

Shelter-in-Place – The process of securing and protecting people and assets in the general area in which a crisis occurs.

Tabletop Exercise – A test method that presents a limited simulation of a crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation.

Testing – Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties and to reveal weaknesses in the Business Continuity Plan.

Training – An educational process by which teams and employees are made qualified and proficient about their roles and responsibilities in implementing a Business Continuity Plan.

Vital Records – Records or documents, for legal, regulatory, or operational purposes, that if irretrievably damaged, destroyed, or lost, would materially impair the organization’s ability to continue business operations.

Table 1. Risk Assessment

Risk/Threat	Consequence	**Likelihood of Occurrence** High-5 Medium-3 Low-1 or None-0
NATURAL		
Tornado or high winds	Building damage Loss of electricity Loss of communications Trees down, roads blocked Mass transit down	
Lightening	Fire Loss of electricity Damage to computers and electrical equipment	
Flooding	Denial of access to building Building damage Equipment damage Loss of HVAC Roads blocked	
Extreme heat or cold	Impact on personnel/families HVAC outage Loss of utilities	
Snow/ice storm	Roadways impassable Building damage Wires down (phone, electric, broadband-internet) Supplies/vendors can't deliver	
Forest fire	Denial of access to building Building damage Loss of electricity Loss of telephones	
Illness: public health emergency	Impact on personnel/families	
INTENTIONAL ACTS		
Theft	Missing tools, equipment	
Vandalism	Damage to building Damage to tools, equipment	
Cyber Attack	Damage/loss of data Virus, worm, etc. Computer/network damage	
Workplace Violence	Injury/death Emotional impact on personnel/families Denial of Access	
Suspicious Package	Evacuation: Denial of access	
Bomb Threat	Evacuation: Denial of access	
Terrorism	Injury/Death Emotional impact on Personnel/Families Denial of access	

Table 2. Understanding the Organization

Mission and Goals	Critical Tool or System	Critical Skills (People)
General office operations	Building: for shelter, work areas and meeting space	
	HVAC (heating and cooling)	
	Work space: desk, chair and lighting	
	Meeting space (seating for 10 minimum)	
	Computer/network	
	Internet connection: email and web access	
	Telephone	
	Copier	
	Fax machine	
	Misc. office supplies	
	Hard files stored on-site	
	Quick access to emergency funds	
	Payroll	
	Accounts payable	
	Purchasing	
Fundraising	Print pledge cards	
	Computer: access to data base	
	Telephone and cell phone communications	
	Internet: email and web access	
	Computer: financial accounts	
	Required reports to state and federal government	
Distribute funds	List of accounts and account numbers	
	Checkbook	
	Computer: agency contact list	
	Internet: email and web access	
	Telephone	

Table 3a. Mitigation Actions

Threat	Consequences	Mitigation Action
Snow/ice storm	Roadways impassable Building damage Water leaks Wires down (phone and electric) Supplies/vendors delivery interrupted	Actions to eliminate: Can't eliminate bad weather Actions to lessen impact: Choose office location less vulnerable to snow/ice. Ensure building is structurally sound to take snow load. Ensure eaves will shed ice to avoid ice dams and leaks. Choose office site with underground services. Waterproof main computer and phone equipment areas.

Table 3b. Preparedness Strategies

Lost Skill, Tool or System	Preparedness Strategy	Done
Building and individual workspaces	Establish work-at-home systems. Arrange for alternate facility.	
Heat (winter); AC (summer)	Establish emergency repair contract. Identify source for portable substitute equipment. Arrange for alternate facility.	
Electricity	Install backup power supply. Arrange for alternate facility.	
Water and sewer (hygiene and sanitation)	Identify alternate sources in nearby offices or buildings. Use portable commode/waterless hand cleaners. Arrange for alternate facility.	
Computers, individual and network	Water and fireproof server room. Establish rental source. Use nearby UW office equipment. Arrange for alternate facility.	
Telephone systems	Water and fireproof phone equipment cabinet. Use cell phones. Use nearby UW office equipment. Arrange for alternate facility.	
Internet connection (Web and email)	Use nearby UW office equipment. Use nearby wireless networks. Allow work from home. Arrange for alternate facility.	
List of accounts	Individual daily backup to portable flash drive Office-wide backup to network server Retrieve info from backup off-site storage location.	
Agency contacts database		
People contacts database		
Financial accounts		
State and federal reporting info		
Checkbook	Retrieve extra from off-site supply cache.	
Purchase orders		
Outside printing services	Establish relationship with alternative printer.	
Copier Fax machine	Identify rental source. Use nearby UW office equipment. Arrange for alternate facility.	
Office supplies	Purchase needed supplies. Establish off-site supply cache.	
Stored paper files	Store in fire and waterproof containers. Store off-site. Create digital off-site backup.	
Skill: data input and retrieval	Train additional staff in essential skills.	
Skill: state and federal reporting		
Skill: bill payment, purchasing		

Annual Training Plan

Describe Training Event	Jan	Feb	Mar	Apr	May	June
Describe Training Event	July	Aug	Sept	Oct	Nov	Dec

Office Equipment List

Recovery Area Needed	Item Needed	Number
Office Space	Offices – XXXX sq ft	
	Storage Area XXXX sq ft.	
	Conference/Meeting Space	
Phone System	Regular Phone Lines	
	Fax Lines	
Furniture	Desks & Chairs	
	Storage Containers	
	Conference Tables & Chairs	
Storage	File Cabinets	
	Book shelves	
Network Server	Kind of servers	
	Monitors	
Desktop Computer	Kind of computers	
	Monitors	
	Printers	
Office Equipment	Fax Machines	
	Typewriter	
	Copiers	
	Postage Meter	
	Shredders	
	Paper, Pens, Paper Clips etc.	
Data Bases	Kind	
Records	(hard copy)	
Communications Equip	Kind & modes of use	

Possible sources for acquisition:

- Rental Offices
- Other offices associated with the United Way
- Computer and Office Supply Stores
- Telephone companies, cell phone and other suppliers
- Board of Directors, volunteers, and other temporary labor suppliers

Power Protection Checklist

American Power Conversion provides ten power protection points to consider during business continuity plan development.

Start with AC line surge protection
At the very least, any critical electronics should be protected from harmful high voltage (surges or spikes). Regular outlet strips are not helpful unless they contain a surge suppression capability. Look for surge protectors with low let-through voltage ratings. How does this help during a blackout? When the utility restores power, it can sometimes fluctuate (causing surges, spikes, and sags) until it returns to normal.

Bulletproof
Surges can enter electronic equipment by any connection leading into the unit, by either electrical cord, telephone cord, data line, coaxial cable, etc. Be sure to close off any possible entrance to equipment by selecting surge protectors with telephone/data line/coax protection (whatever your particular application calls for).

Think "Runtime"
In addition to basic surge protection, electronics users should consider those devices they think would benefit from continued operation in case of an outage. An uninterruptible power supply (UPS, also known as battery backup) provides battery-supplied backup power during a blackout. These units can be sized to the anticipated application according to the amount of VA/watts consumed by the connected devices and the amount of runtime required.

Monitor and manage
Computer users can benefit from use of a power management software utility. In tandem with a serial/USB connection to a UPS, power management software can monitor the quality of power coming into the user's building, keep a log of any power events, and notify the user (via pager, e-mail, etc.) if any pre-set threshold has been reached. In addition, most power management software provides the ability to automatically and safely shut down operating systems and certain running applications, as well as save any data "in progress."

Mobility
In addition to any stationary computer or electronic devices, users should consider availability solutions for mobile equipment as well, including laptops, PDAs, cell phones, etc. Notebook computers alone require power accessories such as removable batteries, power adapters mobile surge protectors, etc. New solutions include cables to recharge PDAs and cell phones via a laptop's USB port.

Compatibility
Information technology continues to grow, as do the number of vendors bringing products to the marketplace. Compatibility is especially important when trying to keep

everything up and running. Your chosen availability solutions vendor should be able to integrate not only with a wide array of desktop operating systems, network management tools, and popular software applications, but also with the wide array of device plug types, data line connectors, and voltage requirements.

Shutdown not an option?
Should your particular application require constant runtime, safe system shutdown may not be the best option. In such instances, customers should size their UPS according to the required runtime should the power go out. Battery backup units range from a few hundred VA (appropriate for desktop electronics protection) to the millions (for entire facility protection). For such larger- sized applications, customers have options as to whether single-phase or three-phase UPSs are the best fit for their power needs.

Need an extension?
Many UPS models have the means to add extra batteries to increase power capacity. This option is available for battery backup units suitable for desktop, server, networking/telecom equipment, and environments where power is considered at the rack, row, or room level.

No obsolescence
Users should have multiple options (both in and out of warranty) for update or replacement of older power protection solutions. UPS batteries do eventually wear out, but this occurrence should not mean the end of the unit's usefulness. Choices vary from easy battery replacement (handled by the vendor, including return shipment of the used battery for proper, environmentally friendly disposal), battery replacement with warranty renewal, or trading an existing unit (even competitive brands) towards purchase of a new one.

General integrator
During the initial moments of a blackout, many business users anticipate the kick-in of an on-site generator and imagine this to be sufficient for the normal, continuous operation of their sensitive IT equipment. Battery backup is still considered a wise investment for several reasons. Most large on-site generators take time to start up, requiring a crossover solution until they reach the appropriate power level. A quality UPS can handle this transition. Also, the operation of motor-driven generators is typically accompanied by voltage transients. A quality UPS helps to filter the sags and surges that can harm sensitive electronic components. The same advice is applicable to smaller generators meant for home applications.

www.apc.com