Risk Control Insights

A Travelers Risk Control Publication
Guiding the way toward helping you reduce risk, prevent loss and save lives

Strategy Guide For Business Continuity Planning

This guide comprises the core component of Travelers' "Business Continuity Planning." It has been designed to help companies understand basic fundamentals of business continuity and disaster management – the need for a process and a plan for assessing and addressing potential business loss hazards and exposures posed by natural disasters or man-made events, such as fire, chemical spills, hurricanes, flooding/flash-flooding, tornadoes, earthquakes, and severe winter weather.

Whether you are a large or a small company and irrespective of your business or industry, the concepts in this guide are fundamental. These concepts are designed to serve as a foundation for helping your company assess its current potential vulnerabilities, its capabilities to withstand loss due to a natural disaster or a man-made event, and for building and implementing a written plan and key mitigation strategies to help you reduce your loss exposure potential. These concepts are also designed to provide guidance to help you in your recovery and restoration process and efforts.

Table of Contents

ABOUT THIS PLANNING GUIDE

Travelers' Strategy Guide for Business Continuity Planning reflects our commitment to help our customers survive the unavoidable and the unforeseen. The aim of this guide is to introduce executives and managers to the importance of planning for disasters and to discuss the factors that planners should consider.

Business continuity planning is the process of preparing for natural or man-made catastrophes that may result in business interruption, property loss, financial loss, and loss of life.

Business continuity planning aims to help:

- Ensure the survival of the organization.
- Protect corporate assets and control financial loss.
- Minimize the loss of customers.
- Facilitate the resumption of operations.
- Improve the ability to salvage damaged equipment and operations.
- Provide for the safety of personnel and the public before, during, and after a disaster.

Experience has shown that organizations that have contingency plans usually recover successfully. When plans exist and personnel are properly trained in them, hazards may be contained, reaction times reduced, and coordination improved. The purpose of this guide is to assist our customers in developing a plan that will minimize the financial, human and business operations impact if your company is faced with responding to a disaster.

Introduction

A 1993 survey of 200 senior executives at companies with average annual revenue of $2.5 billion found that 41percent of companies had NO DISASTER PLAN. By 1997 that figure had grown to 55 percent.

The number of U.S. companies that have developed formal business continuity management programs within the last six years has nearly tripled, according to a new 2005 survey by the Security Services and Privacy Practice of Deloitte & Touche, LLP.

Without a plan, many businesses experience severe losses due to man-made or natural disaster events such as fire, chemical spills, hurricanes, tornadoes, flood and flash-flooding, earthquakes and severe winter weather.

Over the past decade, the Federal Emergency Management Agency (FEMA) spent more than $25 billion to help people repair and rebuild their communities in the aftermath of a natural disaster. This was only in locations where the federal government declared the area an official "natural disaster emergency." Additional billions were paid out in personal and business claims, lost business revenues, and employee lost jobs.

Common Misconceptions

Misconception	Reality
Our people have been with us a long time and will know what to do in the event of a disaster.	When a disaster occurs, it is no longer business as usual. People have to think in terms of what is important to keeping the business running.
We have insurance to cover our losses.	Insurance is a part of your protection, but may not fully compensate you for things like loss of customers, loss of market share, set backs in development or release of a new product in the market.
We don't have time to develop a Business Continuity Plan.	Time spent developing and maintaining a Business Continuity Plan is an investment in the company.
Business continuity and disaster recovery planning are the same thing.	Business continuity deals with maintaining the financial viability of an organization when faced with a variety of emergency events no matter how big or small. Business continuity provides steps that can be taken before, during and after an event to accomplish its mission. Disaster recovery deals with restoring buildings, equipment and processes when damaged in a large scale disaster. It mainly covers actions to be taken after the event has occurred. Disaster recovery is a part of business continuity planning.

The Importance of Planning

We all are familiar with planning. Perhaps it's a savings plan – money we plan to save for a vacation, a new automobile, a house, etc. In the business arena, planning is a must. Owners engage in planning to ensure the financial stability and health of the overall organization. Businesses complete both short- and long-term strategic planning to ensure their products and services remain viable. We all engage in planning. But why is it so important to plan?

There are numerous examples of companies suffering due to poor business contingency planning. For instance, in the case of fires, 44% of businesses fail to reopen and 33% of these fail to survive beyond three years. 80% of all businesses that suffer a major data loss or failure lasting more than 24 hours close within a year.

The bottom line is that planning is a critical component in ensuring the success of most organization and business operations.

Planning for unexpected or unusual incidents is also a sound practice. Many organizations are unprepared to handle workplace crises, operating under the myth of "those things won't happen here." While most of us do not like to think about crises or traumatic incidents happening to us, planning to deal with them effectively is a key administrative responsibility. Experts agree organizations that are proactive in this area may be able to protect lives, prevent damage and destruction to organization property, and save hundreds of thousands of dollars by reducing the likelihood of lawsuits and diminished or lost performance and productivity.

Businesses and organizations are not immune to crises. When a crisis occurs in your organization, you need to act immediately and appropriately. You need to know what to do and when to do it. You need to know who to notify and who to involve in the response. These additional people also need to understand their roles and what they are expected to do. Everyone needs to work together as a team.

The time to plan for crisis management and response is not when a serious incident occurs, but long before, when conditions are normal. Many organizations have learned this lesson the hard way – they did not have a plan in place and muddled their way through when the crisis occurred, often making mistakes. Unfortunately, those mistakes were not only costly, but in some cases, fatal.

Although traumatic events cannot be completely prevented, the impact on the organization and its staff can be minimized. Implementing a Business Continuity Plan in your organization should prepare you to handle a crisis when one occurs. If you already have a Business Continuity Plan in effect, this guide can serve as a thorough review of your existing plan.

Before outlining the steps involved in Business Continuity Planning, it is important to review the types of traumatic events for which to plan.

Unexpected Events

It is important to understand the types of incidents for which you need to plan. The items below address some of these unexpected events that you may want to include in your plan:

Natural Disasters
- Tornadoes
- Hurricanes
- Floods
- Earthquakes
- Severe Storms
- Lightning Strikes
- Wildfire

Man-Made / Organization Traumas
- Fire and Explosions
- Terrorism / Bomb Threats
- Illnesses and Fatalities
- Industrial Accidents
- Acts of Vandalism
- Chemical Spills
- Transportation Accidents

Form A Team

Establishing the Planning Team

The most effective way to write a plan is to form a planning team. The size of the planning team will depend on the facility's operations, requirements and resources. Involving a group of diverse people is best because a team approach:

- Encourages participation and gets more people invested in the process.
- Increases the amount of time and energy participants are able to give.
- Enhances the visibility and stature of the planning process.
- Provides for a broad perspective on the issues.

Team Selection

First begin by determining who can be an active member and who can serve in an advisory capacity. In most cases, one or two people will be doing the bulk of the work. At the very least, you should obtain input from functional areas that include:

- Upper management
- Line management
- Labor
- Operations (including procurement, warehousing, shipping)
- Information Technology
- Human Resources
- Engineering and maintenance
- Safety, health & environmental affairs
- Public information officer
- Security
- Community relations
- Sales and marketing
- Legal
- Finance and purchasing

Team members should be appointed in writing by upper management. Their job descriptions could also reflect this assignment.

Complete your list of team members on page 4 of the Business Continuity Sample Plan.

Establish Authority

Establishing authority for the team is a way to demonstrate management's commitment and promote an atmosphere of cooperation by "authorizing" the planning group to take the steps necessary to develop a plan. The group should be led by the chief executive or the plant manager. Establish a clear line of authority between group members and the group leader, though not so rigid as to prevent the free flow of ideas.

Review the sample authority statement on page 4 in the Business Continuity Sample Plan. Modify the authority statement to meet your organization's needs.

Issue a Mission Statement

Have the chief executive or plant manager issue a mission statement to demonstrate the company's commitment to emergency management. Consider including the team in developing the statement. The statement should:

- Define the purpose of the plan and indicate that it will involve the entire organization.
- Define the authority and structure of the planning group.

Complete and modify the sample mission statement on page 5 in the Business Continuity Sample Plan.

Establish a Schedule and Budget

Establish a work schedule and planning deadlines. Timelines can be modified as priorities become more clearly defined.

Develop an initial plan development budget for such things as research, printing, seminars, consulting services and other expenses that may be necessary during the plan development process.

Review and complete the template on page 6 in the Business Continuity Sample Plan.

The Major Steps in Business Continuity Planning

Effective business continuity planning is a process that moves through five major steps. These steps have key planning activities associated with them and are best described as:

1. **Threat Assessment –** The Threat Assessment allows you to understand which man-made or natural disasters could have the most significant impact on your company.

2. **Identify Critical Functions –** The second step involves identifying the critical functions. A Critical Function can be defined as a part of your operation which, if interrupted, would disrupt your company's ability to deliver its goods and services to your customers. This step will help you identify those functions that are most important and when a specific function needs to be restored before it has an impact on your company and its customers.

3. **Business Impact Analysis –** The Business Impact Analysis combines the Threat Assessment and Critical Functions steps to help you best prioritize your resources and efforts.

4. **Prevention and Mitigation Planning –** This step will help you identify the sequence of steps that need to be taken to help prevent damage and restore business operations.

5. **Implement and Maintain the Plan –** Your plan should be updated no less than annually (and more frequently if facilities or operations change) and drills should be conducted to be sure the plan is working as designed.

Step 1 – THREAT ASSESSMENT

Conduct a Threat Assessment

The first step is to assess the vulnerability of your facility – the probability and potential impact of each event.

Use the Threat Assessment form on page 7 in the Business Continuity Sample Plan to guide the process.

This entails assigning probabilities, estimating impact and assessing resources, and using a numerical system. The lower the score, the better.

List Potential Emergencies
In the first column of the chart, list the types of events that could affect your facility, including those identified by your local emergency management office. Consider both:

- Events that could occur within your facility
- Events that could occur in your community

Below are some other factors to consider, which may be broken down into two categories; **natural** and **man-made** events.

- **Historical** – What types of emergencies have occurred in the community, at this facility and at other facilities in the area?
  - Fires
  - Hazardous material spills
  - Transportation accidents
  - Terrorism
  - Utility outages
  - Severe weather
  - Earthquakes
  - Hurricanes
  - Tornadoes

- **Geographic** – What can happen as a result of the facility's location? Keep in mind:
  - Proximity to flood plains, seismic faults and dams
  - Proximity to companies that produce, store, use or transport hazardous materials
  - Proximity to major transportation routes and airports
  - Proximity to nuclear power plants

- **Technological –** What could result from a process or system failure? Possibilities include:
  - Fire, explosion, hazardous materials incident
  - Safety system failure
  - Telecommunications failure
  - Computer system failure
  - Power failure
  - Heating/cooling system failure
  - Emergency notification system failure

- **Human Error –** What emergencies can be caused by employee error? Are employees trained to work safely? Do they know what to do in an emergency?

  Human error is the single largest cause of workplace emergencies and can result from:
  - Poor training
  - Poor maintenance
  - Carelessness
  - Misconduct
  - Substance abuse
  - Fatigue

- **Physical** – What types of emergencies could result from the design or construction of the facility? Does the physical facility enhance safety? Consider:
  - The physical construction of the facility
  - Hazardous processes or byproducts
  - Facilities for storing combustibles
  - Layout of equipment
  - Lighting
  - Evacuation routes and exits
  - Proximity of shelter areas

- **Regulatory –** What emergencies or hazards are you regulated to deal with?
  Analyze each potential emergency from beginning to end. Consider what could happen as a result of:

  - Prohibited access to the facility
  - Loss of electrical power
  - Communication lines down
  - Ruptured gas mains
  - Water damage
  - Smoke damage
  - Structural damage
  - Air or water contamination
  - Explosion
  - Building collapse
  - Trapped persons
  - Chemical release

Estimate Probability
In the probability column, rate the likelihood of each event's occurrence. This is a subjective consideration, but useful nonetheless. Use a simple scale of 1 to 5, where 1 is the lowest probability and 5 is the highest.

Assess the Potential of Human Impact
Analyze the potential human impact of each event – the possibility of death or injury. Assign a rating in the Human Impact column of the Threat Assessment worksheet. Use a 1 to 5 scale where 1 is the lowest impact and 5 is the highest.

Assess the Potential Property Impact
Consider the potential for loss or damage to property. Property includes the buildings, machinery, equipment, computer equipment, raw and finished goods. Assign a rating in the Property Impact column, 1 being the lowest impact and 5 being the highest. Consider:
- Cost to replace
- Cost to set up temporary replacement
- Cost to clean or repair

Assess the Potential Business Impact
Consider the potential loss of market share. Assign a rating in the Business Impact column. Again, 1 is the lowest impact and 5 the highest. Assess the impact of:

- Business interruption
- Employees unable to report to work
- Customers unable to reach facility
- Interruption of critical supplies
- Interruption of product distribution
- Company's potential breach or violation of contractual agreements
- Imposition of fines, penalties or legal costs

Assess the infrastructure impact
Analyze the potential business impact due to loss of infrastructure that supports a facility:

- Loss of roads for shipping and receiving
- Restricted customer access
- Loss of communications lines
- Interruption of electrical power and/or natural gas
- Loss of water supply
- Scale of 1-5 where 1 is lowest probability

Assess Readiness Based on Internal and External Resources
Next, assess your resources and ability to respond to the event. Assign a score to your Internal Resources and External Resources, where 5 indicates weak resources and 1 indicates strong resources. The lower the score, the better.

To help you do this, consider each potential event from beginning to end and each resource that would be needed to respond. For each event, ask these questions:

- Do we have the needed resources and capabilities to respond?
- Will external resources be able to respond to this event as quickly as you may need them, or will they have other response priorities?

If the answers are "yes," move on to the next assessment. If the answers are "no," identify what can be done to correct the problem. For example, you may need to:

- Develop additional emergency procedures
- Conduct additional training
- Acquire additional equipment
- Establish mutual aid agreements
- Establish agreements with specialized contractors

Add the Columns

Total the scores for each event. The lower the score, the better. While this is a subjective rating, the comparisons will help determine planning and resource priorities – the subject of the pages to follow.

Step 2 – IDENTIFYING CRITICAL FUNCTIONS

Step two involves developing a list of the functions or processes that are critical to the survival of your firm. Critical functions are those functions necessary for you to conduct business, which, if interrupted, would disrupt your company's ability to provide its goods and services to its customers. Functions may also be identified as critical on the basis of cash flow or by externally imposed deadlines.

Purpose

The key to business continuity is to know what is absolutely critical to the survival of the organization following a disaster. Understanding how an outage or disruption could affect your business is vital to making the right decisions to protect your company's assets. The critical function analysis helps you identify the effect of disruptions in individual business operations and analyze the effect of such disruptions over time.

Identify Your Critical Functions

If you were asked to prepare for an emergency that was going to force your family to be homeless for three months, what would you take? What would you do first, second and third to recover from the disaster?

Below is a table that would list the typical items in order of priority that you would consider:

Time	Items you would need	Importance
First 72 hours after the disaster	Food Shelter Water	Critical – without these items your health and well-being would be threatened immediately.
Three days to one month after the event	Cash money Clean clothes Personal hygiene, bathing, brushing teeth, etc. Clean shelter Clean running water Bedding Sanitation	Essential – these are items that you need to begin to live comfortably and to maintain long-term health.
One month to three months after the event	Television Communications Furniture Private shelter Personal computer	Secondary – these are items that would begin to restore your life back to a point you were at prior to the disaster.

As you can see, we have to think about our basic survival needs first. We call these the Critical Functions, because these items are needed immediately to sustain our health and well-being.

After the critical functions have been addressed, we can focus on the essential functions. These are functions that will have to be replaced soon after the event and, if ignored, could threaten our health and well-being over the longer term. Essential functions typically have a little more flexibility in what order they are restored and the amount of time we can take to restore the

function.

The secondary functions are the items that start to return us to the level of comfort and convenience we had prior to the disaster.

Your business has similar needs. For your business to remain viable and provide its products and services after a disaster, you need to restore the critical functions first, then the essential functions and finally, the secondary functions of your business.

Start the critical functions analysis by looking at where the revenue comes from in the company. This is your product or service, what your customer ultimately pays you to do for them.

Once you identify your product or service, you can then understand the critical functions. The critical functions of the business are similar to the critical functions of sustaining your life in an emergency: shelter, water and food for your body. For the business, the critical functions are what is vital to keeping your customer's needs met and the revenue flowing. These are the functions that must be restored quickly to avoid financial harm to the business.

Example: ABC Grocery Store. ABC sells groceries to a local area from its single location. The 100,000-sq. ft. building is brand new. It includes a state-of-the-art climate control system, sprinkler system and alarm systems. All of the inventory control and office equipment is new, including a new mainframe computer.

60 percent of ABC's revenue is generated from dry goods sales, 15 percent is from meat sales, 15 percent from produce and 10 percent from frozen food products. The following is an example of how the critical, essential and secondary functions for ABC Grocery Store might be broken out if the company were to experience a large fire or some other disaster.

Time	Items ABC needs	Importance
First 72 hours after the disaster	Need access to their building or a nearby substitute. Electricity and facilities to keep meat, produce and frozen goods from spoiling. Staff for customer transactions. System to accept and track payment for goods.	Critical – In order to maintain the revenue stream, the company has to have access to emergency power, continue to have clean, dry floor space and have staff to run the operation with a method to receive payment.
3 days to 1 month after the event	Roads and trucks to move product to the building to replenish stock. Sanitation to remove waste. Electronic connections for credit card payments. Payroll to keep employees.	Essential – these are functions that that need to be restored so the company can produce revenue and maintain customer service.
1 month to 3 months after the event	Mainframe computer to maintain product inventories. Advertising. Climate control. New office equipment.	Secondary – these are functions that begin to restore the company back to the pre-disaster status.

Turn to page 8 in the Business Continuity Sample Plan. Follow these instructions as you complete the Critical Function worksheet.

1. The first step is to develop a list of the critical functions carried out by your business.
2. Decide how quickly the functions must be resumed before damage is critical; within 72 hours, three days to one month or over a month.
3. What would the effects of the loss of the function be on revenue?
4. In the last column, identify how the length of the disruption would affect that function.

Using the time element, the functions can be ranked in order of importance. The greater the time period that can be tolerated, the lower ranked the function becomes.

Step 3 – BUSINESS IMPACT ANALYSIS

Step three combines the process of the threat assessment and defining critical functions and then asks you to assess:

- If you have a current plan in place to address the loss of the function.
- Additional actions that may need to be taken.
- Ideas on what can be done to mitigate damages long before a disaster occurs.
- The sequence and priority of steps to include in the final business continuity plan.

Take your greatest threat identified in Step 1 and the information from your Critical Functions worksheet from Step 2. Use this information to complete the Business Impact Analysis on pages 9-11 of your sample plan.

Business Impact Analysis Form Instructions

On top of the form, indicate which event was the greatest threat to your business. Using the information from your Critical Functions worksheet from Step 2, list critical functions according to similar time priorities and rank them by their effect on revenue with greatest effect at the top.

In column three, list any alternative means to accomplish the critical function evaluated.

For example:

- Emergency generator to replace public utility.
- Secondary warehouse to store additional stock.
- Remote server in place that mirrors data.

In column four, list any actions being considered to protect this critical function.
Such as:

- Provide sprinklers to protect the building in the event of fire.
- Upgrade roof to higher wind-resistance rating.
- Purchase hurricane shutters for windows.

The last column on the business impact analysis worksheet will reference the “Prevention

Mitigation Form," which will be used later in step 4. In this last column, you should list the prevention or mitigation action step name or number that corresponds to the critical function item in this row. The prevention or mitigation form will be used to provide details on specific actions that need to be taken to protect critical functions.

Step 4 – PREVENTION AND MITIGATION PLANNING

Writing the Business Continuity Plan

At this point in the process, it's time to develop a full plan of action so that your organization will be prepared to cope with a full range of emergency events. This is your business continuity plan.

Use information gained in the previous steps. The strategy should provide detailed information that covers what should happen before, during and after an event.

- Before – Preplanning
- During – Emergency Operations
- After – Disaster Recovery

The table below illustrates how prevention and mitigation strategies can be provided to cover actions that occur before, during and after an event. This sample shows how to cover the critical function of providing electrical power for a facility.

Before	During	After
Obtain an emergency diesel engine-driven generator.	Verify the generator is running.	Perform maintenance to repair any malfunctions that occurred during or as a result of continuous operation
Test the generator monthly.	Verify the fuel tank is full.	Refill fuel tank.

Pre-Planning
There are many things you can do long before an event to mitigate or prevent your damages. Prevention planning is taking steps that would prevent damage from occurring in a disaster. Mitigation actions typically involve actions that would reduce the impact of damage that occurs in a disaster.

It is important to use both prevention and mitigation techniques in tandem in your business continuity plan to complement each other and increase the overall benefit to the organization. The difference between prevention and mitigation is shown in the table below:

Prevention	Mitigation
Install high temperature cut offs to prevent overheating of oven.	Sprinkler system to control fire in an oven.
Design building with limited exterior windows to prevent potential wind damage.	Contract with a service to board up window openings in response to a hurricane warning.
Install emergency generators that would provide immediate power in event of a power loss.	Contract service to provide generators within 24 hours of a power loss.

Now you can take the information from your Business Impact Analysis and assign tasks for each critical function. Use the Prevention/Mitigation Tasks Worksheet on pages 12-14 in the Business Continuity Sample Plan.

The Prevention / Mitigation worksheets in the Sample Plan should be used to develop specific actions that can be completed as a result of the items identified in the Business Impact Analysis. Many of these are actions that can be taken prior to an event and some are steps that may need to be included in your Business Continuity Plan to occur during or after an emergency. Prevention or mitigation actions should be completed as soon as possible because if an emergency occurs, it will most likely be too late.

Your Pre-Planning should include:

Facility and Asset Protection Planning: Evaluate critical physical assets and potential business impact on the operations if these assets are damaged. These could include:

- Vehicles
- Stock
- Computers
- Records
- Facilities
- Office supplies
- Equipment

Process and Production Protection Planning: Evaluate critical processes and product flows for the operations, which can include:

- Incoming orders
- Accounts payable
- Accounts receivable
- Receiving of raw materials
- Shipping of products
- Credit card purchasing

Employee Planning:

- Contact numbers
- Evacuation plans
- Training
- Central call-in number for information

Examples of items that may need to be completed as part of the pre-planning phase are:

- Installing physical protection systems to mitigate loss, such as automatic sprinklers, hurricane shutters, flood control measures, emergency generators, etc.
- Reducing dependency on single source suppliers, local vendors and other bottlenecks in product flow
- Entering into reciprocal agreements with other locations or businesses
- Use of leased business centers or use of hot or cold sites
- Leasing of office equipment, temporary power generators, etc.
- Establishing alternate phone/communications centers (answering service)
- Establishing alternate or back-up facilities should be pre-arranged, (warehousing, cold storage, etc.)

Emergency Operations

Activities that should occur during a crisis event are called emergency operations. Since these activities must be structured so they can be completed quickly and efficiently, it is best to break them into groupings and assign them to teams. Consider the 10 functions listed below as you develop your team plans. You may adapt or combine them to meet your company's specific requirements. A checklist located in the Sample Plan (see pages 19-29) will help you to review and evaluate the current state of emergency operations planning in your company and to identify planning gaps and weaknesses.

Your emergency operations plan should include the following basic components:

1. Direction and Control

Your business continuity plan must provide for a Control Group that will exercise direction and control during an emergency. This group operates from an Emergency Operations Center (EOC) and is responsible for:

- Directing the operations of the emergency response teams.
- Coordinating all emergency activities.
- Gathering and analyzing information needed for further emergency decisions.

Your plans for central direction and control should also designate alternative locations for EOCs and/or subordinate command posts.

2. Communications

Communication between the Control Group and the emergency teams is essential. Your Emergency Operations Plan must, therefore, provide for establishing, maintaining, and securing a backup for all channels of communication.

Key personnel must understand all communications procedures. Communications procedures that are part of daily operating systems are likely to work best in an emergency: the equipment is regularly maintained, and the staff will know how to adapt these systems during the emergency period.

3. Alerting and Warning

During an emergency, the Control Group will need procedures to alert all response staff and other employees to anticipated hazards. Warning may arrive by:

- Switchboard operator or word-of-mouth reports.
- Devices such as smoke or heat detectors.
- Announcements from the Weather Service or local authorities.

These warning systems, in turn, depend on communication systems to alert all employees and to request assistance from police or fire departments.

4. Facility Shutdown
Your Emergency Operations Plan must offer guidelines on when and how to shutdown your facility. This involves developing criteria for making the decision to stop operations and elaborating on procedures for shutting down equipment, utilities, and the entire facility. This function also includes establishing emergency protection measures, and damage control.

5. Evacuation
The goal of evacuation is to move people and resources (equipment, supplies, and inventory) away from threatened areas. Successful evacuation depends on sufficient warning of an impending disaster.

In planning for an emergency, you must establish clear and detailed procedures for carrying out complete or partial evacuations from buildings or from an entire neighborhood. Neighborhood evacuations require coordination with all elements of your Emergency Plan, as well as with government authorities in the communities affected.

6. Shelter
In some situations, evacuation of the worksite may not be possible. Under these conditions, an Emergency Operations Plan considers how to provide shelter for employees and visitors.

Your Emergency Operations Plan should describe the conditions under which people would be placed in shelters and the criteria for making this decision. The plan should describe the capacity of on-site shelters and identify public shelter facilities that local emergency management officials have allocated for company employees.

7. Emergency Services
Implementation of an emergency response depends on the availability of trained personnel. Plan to provide the following emergency services:

- Security
  - control access
  - employee and visitor safety
  - safeguard assets from theft or looting
- Fire fighting
- Rescue
- Medical and health
- Engineering support

Many companies are large enough to create teams that can provide these services. Such internal emergency teams have a faster response time and a greater technical knowledge of the company's facilities, processes, and materials than public fire and medical services.

8. Emergency Information
In developing your plan, consider how to increase the employees' awareness of hazards, and how to advise employees about appropriate actions before, during, and after an emergency. Effective collection and dissemination of information will help to focus emergency action and minimize confusion.

Your Emergency Operations Plan should also establish procedures and responsibility for dealing with the media.

9. Supporting Materials

Your Emergency Operations Plan will be much more helpful if you supplement it with the following information:

- Floor plans and maps (site and street) that indicate the location of manpower and equipment.
- Assignment charts (simple organizational charts) that show the names, titles, addresses, and phone numbers of key emergency personnel. These charts should also indicate the responsibilities of each person during an emergency.
- Call-up lists that contain the names, addresses, and telephone numbers of the people responsible for emergency operations. Alternates should be named in case the primary personnel are not available.
- Employee phone numbers
- Customer and vendor lists
- Lists of local resources that provide additional labor, equipment, and supplies.
- Mutual aid agreements that indicate companies willing to assist during emergencies.
- A glossary that defines key terms. The plan should use words that mean the same thing to everyone.

10. Administration and Logistics

Emergency Operations Plans require approval from senior management and agreement from departments that will be providing services during an emergency.

Senior management should also direct that testing and updating of the plan be done on a regular basis.

After – Disaster Recovery

The disaster recovery strategy will involve the careful documentation of current procedures and the development of special procedures to be put into effect after a disaster. It will focus on the most critical functions, as identified in the previous steps. For example, you will need to consider how operations are being performed now (by hand, by machine, or by computer). For each method, you should consider alternative methods to be used during the recovery period. Manual operations will be the most easily restored, while mechanical operations may be complicated by the loss of power or damage to specially built equipment.

Recovery operations may, therefore, involve unorthodox solutions. For example, you may decide to contract certain functions to a competitor, or to process information at another company's facility outside of normal business hours. You may even decide not to resume a function for some time, if at all.

Disaster Recovery Team

One approach that can be used when developing a disaster recovery strategy is to divide the responsibilities into groupings and assign them to teams. This approach automatically provides back-up personnel to accomplish certain tasks since several individuals have been assigned and trained to complete them. One possible arrangement of teams would be in the four main groupings listed below:

Control Group

- Takes control of the situation and directs the remaining teams
- Responsible for the development and testing of the plan

Employee Relations

- Responsible for employee communication
- Responsible for communicating the situation to all involved
- Assist in evaluation of medical and emergency support needs
- Provide guidance of personnel to shelters
- Communicate any needed information to local authorities

Safety, Security and Salvage

- Responsible for security and medical support
- Responsible for evacuation of personnel and visitors
- Assist in evaluation of medical and emergency support needs
- Secure the property, valuables, and equipment
- Begin salvage operations as soon as it's safe to do so

Information Resources

- Responsible for archiving and retrieving vital information
- Identify time frame needed for recovery
- Secure equipment needed
- Begin salvage operations

Resources

Critical Personnel

After deciding what functions to restore, the next step is to identify your critical personnel. List each critical function, the job titles required to perform it, and the order in which the personnel will be needed. Arrange this list according to the time frame in which each position will be required as you move toward full recovery of operations.

Workspace

Document your workspace requirements in the disaster recovery plan and communicate them to the corporate planning group. To determine your workspace needs, consider the number of employees required, time of day, and the phase of recovery.

Find out whether your personnel have any special work station requirements that could not be filled by standard office furniture. Ask these questions:

- Will space be required for special equipment?
- Are there any special environmental requirements, such as air conditioning?
- Are there requirements for some personnel or divisions to be located adjacent to others?

Equipment

In your plan, specify the phases of recovery during which each piece of office or production equipment will be used. Commonly, included in the office equipment category are telephones, calculators, personal computers and printers. Do not forget to include software.

Forms and Documents

Your disaster recovery plan should list only those forms and documents that cannot be replaced by plain paper. For confidential or negotiable documents, consider not only how to obtain them, but also how to secure them at the recovery location.

Special Supplies

Compile a list of special supplies and indicate when they may be required during the recovery period. They may be non-standard office supplies, printed materials, or supplies for your production equipment.

Communications

After an event, normal communication channels may not exist. Some divisions may have to resume immediate contact with persons or organizations. List these contacts, along with the means of communications and the time period in which the communication must be re-established.

Vital Information

Vital information refers to information recorded on any media (paper, microfilm, magnetic tape, disk, etc.) that is absolutely critical for the continuance of business operations. This information must be routinely backed up at an off-site location.

Your recovery plan must include a list of vital information and the procedures necessary for retrieving it. This information must also be safeguarded at the recovery site so that it is not lost in a secondary disaster.

Employee Notification

In your plan, list the coordinators who will notify employees of disaster recovery plans and tell them when/where they are to report for work. Also provide a list of the employees who need to be contacted. It may also be a good idea to provide a phone number that employees can call to obtain important information.

Vendor Notification

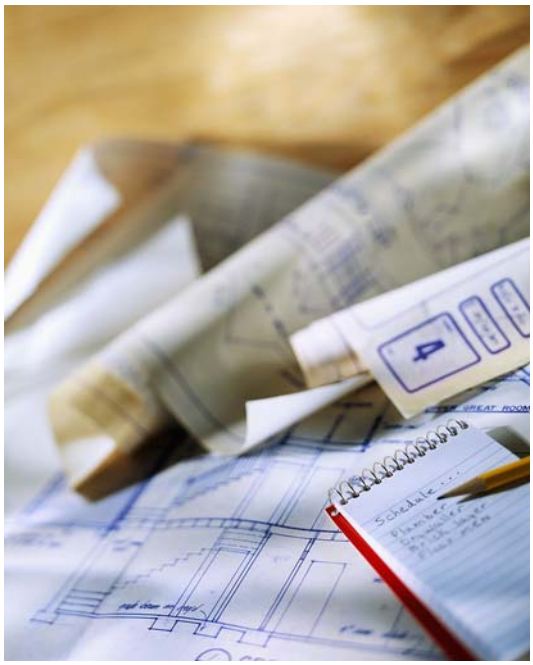
A list of vendors that should be notified following an emergency is important to include in your plan. In an emergency they should be contacted to advise them of the recovery locations and changes in scheduled deliveries, etc.

Customer Notification

It is important to have a list of key customers that should be notified of a disaster. They should be advised about various recovery efforts/locations and changes in scheduled deliveries, etc.

Go to pages 15-41 of Business Continuity Sample Plan to review an example of a business recovery team's responsibilities.

Step 5 – IMPLEMENT AND MAINTAIN THE PLAN



Implement your plan and your mitigation strategies.

This includes:

- Releasing a written mission statement
- Communicating your Plan to employees, visitors, contractors
- Training the team and your workforce on their roles and responsibilities in the event of a fire, natural peril or man-made event
- Making the Plan accessible to employees for their review
- Posting emergency contact numbers and your evacuation instructions
- Conducting drills
- Establishing a periodic plan reassessment and improvement process

The importance of a plan reassessment process and drills cannot be overstated. It is very rare that a business remains static. Something is always changing, whether it is adding new equipment, making renovations, hiring a person with special needs, even moving part of your business operations to another location. Your Plan needs to continually reflect the changes in your people, operations, facility, and location. For this reason, it is critical that you periodically reassess your vulnerabilities and capabilities and be prepared to make necessary changes and improvements to your Plan and mitigation strategies. By doing this, your Plan actually becomes a part of your business' process for improvement.

Training and drills are key to the success of your Plan's implementation and your "response mode." During an event, things may not always happen the way you expect them to happen. Because of this simple truth, it is important that everyone has the opportunity to participate in a drill to assess their understanding of their respective roles and actually have an opportunity to carry out their responsibilities, including sending out the "alert" and participating in a facility shutdown.

The drill can help you identify where you are strong… and where you are weak. What was forgotten? How well did your alert/communications system work? What activity did not take place? What action went wrong? What did not happen the way you had expected it to happen? If it doesn't work during a DRILL, it is more likely to fail in the event of a real disaster.

Your drill, then, is intended to give everyone the opportunity to prepare for "the real thing" – to participate in a practice "response" mode, and to make improvements and recommendations for improvement. It is key to the success of your "response mode."

See page 42 of the Business Continuity Sample Plan for a summary of various test types and their recommended frequencies.

A Critical Consideration – Stress AND Your Employees

DO NOT OVERLOOK THE HUMAN SIDE OF A DISASTER

What are the effects of a disaster on employees?

Few people are prepared for the sudden and unexpected events that cause destruction of property or loss of life. After such events, people usually undergo a period of psychological readjustment as they resolve feelings of loss or powerlessness.

Psychological after-effects generally occur in three distinct stages:

- **The first 24 hours:** During this period, employees may display varying reactions. They may exhibit symptoms of numbness or denial, be physically sick or anxious, or may withdraw from contact with others. In a community-wide disaster, employees may have to deal with family responsibilities and cannot be expected to focus on work if their family is in danger. Alternatively, they may increase performance and suppress their anxiety in order to deal with the demands of the immediate crisis.
- **The first week:** After initial reactions wear off, employees may begin to feel isolated or alienated, anxious about the future, or angry at the situation. They may also withdraw from contact with each other or may exhibit demanding behavior.
- **Long-term effects:** These effects depend on how well employees have come to grips with the disaster. Employees who feel that the company has responded well to the disaster and to their individual needs will show more commitment to the organization and more perseverance handling future demands. Employees who have not come to grips with the disaster will be more prone to burn-out, to work with lower levels of commitment, or to leave the company.

All of these symptoms are common after any crisis – personal or professional. They have the potential to disrupt operations long after the apparent crisis has passed.

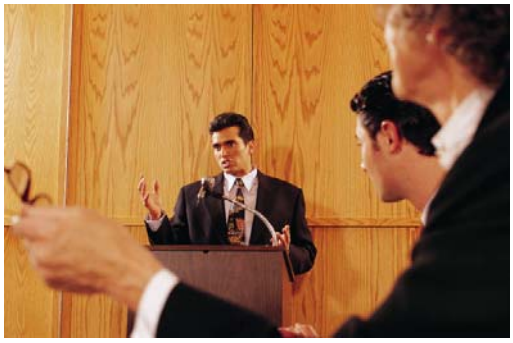
Why should a company plan for human reactions?

Employees are a company's most valuable asset. If an organization is to restore operations after a disaster, its employees will likely need support in dealing with shock and stress. It is wise, therefore, to plan for employee support before the disaster occurs.

Plans are also important because helping employees cope with stress requires technical expertise. There will be a need to arrange for outside support, to train supervisors to recognize and deal with the symptoms of stress, and to plan for communications from senior management. Assisting employees in overcoming a crisis will contribute greatly to employee commitment and to their confidence in meeting future challenges.

How should human reactions be handled?

A key to assisting employees is communication. While human reactions can be varied and unpredictable, most employees respond positively to increased communication. Therefore:



- Encourage senior management to share information about the disaster, the current status of the company, and future plans.
- Allow employees to express their feelings.
- Offer regular reinforcement and encouragement to employees.

When discussing future plans, remember to acknowledge the past. Since people do not instantly make transitions to a new situation, discuss with them the way things used to be. This will help employees bring closure to their experience of disaster.

In the days and months following a disaster, supervisors should be encouraged to identify signs of potential employee impairment:

- Changes in behavior
- Difficulty in concentrating or low energy level
- Illness or frequent pain
- Irrational behavior
- General withdrawal

To head-off these symptoms, the company can use a number of resources:

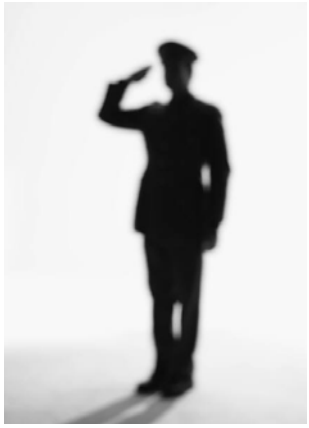
- A formal employee assistance program
- Community resources
- Lunch time speakers
- A wellness program

In addition, company policy should allow for:

- Flexibility in schedules
- Leaves of absence
- Re-assignment to new duties
- Supervisory discretion

The goal of all these actions is to minimize the effects of a disaster on the employees. No long term business resumption will be successful without positive morale. Paying attention to employees' needs will foster positive execution of any technical plans, and strengthen the employees' commitment to the future.

Final Thoughts



General Eisenhower, when reflecting on the preparations for the D-Day Invasion, remarked that "Plans are useless, but planning is everything." Like military plans, business continuity plans attempt to provide for and address the unpredictable. The actual scenario of a disaster as it unfolds may not be what the planners anticipated, but the business continuity planning process should provide the flexibility to respond to changing circumstances. No organization should be paralyzed when a disaster occurs. If it has used the planning process well, a company should have the tools and the resources to take charge of events as they unfold.

Please Contact Us

For more information, visit our Web site at stpaultravelers.com/riskcontrol, contact your Risk Control consultant, or e-mail Ask-STA-Risk-Control@stpaultravelers.com.

Disclaimer