TASC Training & Advocacy Support Center

TASC is sponsored by the Administration on Developmental Disabilities (ADD), the Center for Mental Health Services (CMHS), the Rehabilitation Services Administration (RSA), the Social Security Administration (SSA), and the Health Resources Services Administration (HRSA). TASC is a division of the National Disability Rights Network (NDRN).

2006 Fiscal Managers Meeting

Disaster Planning, Emergency Preparedness
And
Business Continuity Checklists

Special Thanks

NDRN gives “special thanks” to the Nonprofit Coordinating Committee of New York for giving us permission to provide you with this document. This document was drawn from a series of disaster planning and recovery seminars given for NPCC by the following individuals and/or reviewed by: American Red Cross of Greater New York; William Krouslis; Allen Breslow, Esq.; Joshua Peskay and Kim Snyder Fund for the City of New York; Ken Liebman and Jack Stravidis, Frank Crystal & Company; John Burke, AIG; Bob Bender; and Marcia Brown.

About This Document

This document explains the points an organization needs to think about in order to prepare its own disaster recovery plan so that, should an interruption occur, it is able to resume operations.

To complete its plan, staff members will have to search for answers and fill in the blanks. It is important to recognize that there is no “magic” plan that an organization can purchase that will provide all the answers or that will create a plan for them.

In creating a disaster plan, don’t become overwhelmed by the tasks ahead. Work on it in sections, doing first the things that seems most important — e.g., personnel, computer/IT, etc. — and as time allows. The most important thing is to make some plans that can be implemented in the event of an interruption.

What a Disaster Recovery Plan Is — And Why You Should Do One

Whatever one chooses to call it — disaster planning, emergency preparedness, or business continuity (and experts note that there are differences) — the goals are ultimately the same: to get an organization back up and running in the event of an interruption. The problem causing the interruption could be one computer crashing or an entire network crashing. Or it could be an electrical outage or the result of a terrorist activity. The goal is to have some contingency plans in the event of a problem. A disaster recovery plan exists to preserve the organization so that it can continue to offer its services.

A disaster recovery plan is a users’ guide—the documentation—for how to preserve an organization. In order for a plan to be useful, it must be created before an interruption occurs. Business continuity is disaster recovery. Lost revenue is a driving force in business continuity. The reason to do a recovery plan is essentially to keep the funding coming in and the services going, and the clients being served.

Emergency planning are those procedures and steps done immediately after an interruption to business.

Disaster recovery are the steps taken to restore some functions so that some level of services can be offered.

Business continuity is restoration planning, completing the full circle to get your organization back to where it was before an interruption.

In order to write your plan, you have to do some planning. This planning is the process that will get you to the step where you then commit your plan to paper—you can't write a plan until you do the preparation. The most difficult thing is getting started; the second most difficult task is keeping the plan current.

Unfortunately, there are no cookie-cutter templates, and one size doesn't fit all. There are some common elements among plans, but every plan will be different because every organization's structure and circumstances are unique.

How do you know when it's a disaster? When critical services aren't happening.

Can all employees recognize what a disaster is and what they should do? In the event of an emergency, all personnel should know what their roles are, and where they should go.

Train and Drill: Staff has to know what to do. A disaster preparedness and recovery plan should include employee training. It should address general training for all employees, including:

- individual roles and responsibilities
- information about threats, hazards, and protective actions
- notification, warning and communications procedures
- means for locating family members
- emergency response procedures
- evacuation, shelter, and accountability procedures
- location and use of common emergency equipment
- emergency shutdown procedures

Build emergency preparedness into the culture of the organization. Orientation sessions for new employees should include an overview of the contents and a copy of the preparedness manual.

<u>Possible Disasters</u>
Part of writing a disaster plan is to think ahead to the possibilities of what can go wrong and make contingency plans. However, you can't possibly plan for every scenario; it would take all of one's time and the plan would never get done. The goal is not to create a separate plan that addresses every risk, but to create one plan that address all risks. In other words, you don't create one plan for a tornado, one for a flood, and one for a blackout. You just need one plan that addresses all possibly known scenarios. Keep in mind that during a disaster or an interruption, you can't count on being able to dial in, log in, or walk in.

□ What are the potential identifiable disasters (internal and external)?

□ How would each affect the organization's systems and programs?

When analyzing risks, factors to consider include:

Historical: What types of emergencies have occurred in the community, at your facility, or nearby? (for example, fire, natural disasters, accidents, utility, etc.)

Geographic: What can happen as a result of your location? (e.g., proximity to: flood-prone areas; hazardous material production, storage or use; major transportation routes; power plants, etc.)

Human Error: What emergencies might be caused by employees? Are employees trained to work safely? Do they know what to do in an emergency? Human errors can result from poor training and supervision, carelessness, misconduct, substance abuse, fatigue, etc.

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 office; the facilities for storing combustibles or toxins; hazardous processes or byproducts; lighting; evacuation routes and exits; shelter areas, etc.

Consider what could happen as a result of: a computer crash; prohibited access to your office; loss of electricity; ruptured gas mains; water damage; smoke damage; structural damage; air or water contamination; building collapse; trapped persons; chemical release.

In spite of everything said above, there are, ultimately, only four

different scenarios that you need to plan for, regardless of the catastrophe or interruption:

1. Only your local office in the building is unusable. For example, one or more offices in your space become temporarily unusable because of a flood. Some contents and material may be recoverable, some may not be.

2. The entire building is gone. For example, a fire destroys the structure and its contents.

3. A temporary disruption of services, such as an electricity outage.

4. An impact in the large geographic area, rendering the area uninhabitable for an unknown amount of time.

<u>Assign a Team—You Can't Create a Plan Alone</u>

□ Who in the organization should be responsible for creating the plan?

Assign a team to help create the plan. While small organizations may be able to get by with one person doing the work, larger organizations will have to enlist the assistance of others, particularly in coordinating various departments to provide needed portions. For example, assign one team/person to complete the computer/technical portion, and another team to complete the personnel portion. If appropriate, entitle this group the Emergency Management Team to help provide some positive reinforcement and instill a sense of credibility for their efforts, particularly when this task is in addition to their usual responsibilities.

□ Who is in charge of making decisions?

Appoint a person or a team that has the authority to make short-term emergency decisions, for example whether to evacuate the building, etc. What is the chain of command? There has to be a chain, and broad knowledge of who is in charge. In other words, who is #2 if the first person isn't present or can't be reached, and so on. These people should include those in leadership, but they shouldn't be only senior managers. However, if they're not senior management, they must have management's approval. These people should be long-term employees or those who are familiar with the disaster recovery plan. Those people should regularly be in the building so that they are more likely to be present in the event of an emergency.

Often, an issue for the people trying to create a plan is dealing with people’s complacency. Management may not want to spend money on tech-related systems that may never get used. One solution to this dilemma may be to outline the possible scenarios, what would happen if you don’t have resources allocated and plans in place, and demonstrate the effects on the organization’s operations.

The plan needs to be specific as to what recovery steps need to get done first, as well as detailing who has access to that information. The logic and order of steps depends on the nature of the organization and its services as well as the type of disaster or interruption. The members of the Emergency Management Team will address this during the planning stages, particularly when analyzing the organization’s services and programs.

Don’t make the plan so dogmatic that there isn’t any flexibility and doesn’t allow a manager to utilize it. The plan has to be able to be implemented without the person or the team that created it. It has to be legible, understandable, and able to be interpreted by a lay person. If only a techie can implement your plan, it will most likely not be successful. Also, common sense must rule.

As things change in the organization—people come, people go, programs fold, programs start—the plan has to be updated to reflect these changes. The ideal candidate for maintaining and updating the plan may be the person who oversaw the Emergency Management Team, or someone who was involved with the process.

II. Analyze and Know Your Organization

Determine Your Critical Services & Functions: Answer the following questions to help craft your recovery plan.

What are your organization’s functions and services? (what you do—in detail)

What staff is responsible for what functions?

Which functions and services are critical, and which are less so?

Do a client impact analysis: in the event of an interruption, what would be the impact on your services to your clients? For example, if your organization delivers meals to clients at home, how would you get those meals to them should your facilities be inaccessible?

Whom do you serve? (who are your clients, what are their ages, etc.)

Where do you serve them? (on-site, at their home, at another organization’s facilities, etc.)

How do you serve them? (What do you provide to your clients: information, food, medical care, transportation, etc. How are these services provided: via phone, fax, or internet, in person, etc.)

What are your personnel requirements? (are services provided by staff, volunteers, etc.)

What are your equipment requirements? (cars, computers, etc.)

How do your services impact the organization’s functioning? (For example, if fee-for-service is crucial to your operations, what will happen if you cannot perform those services?)

In order to make contingency plans, differentiate your organization’s services. If, for example, a phone system is needed to provide services to your clients, this may be the area that you should invest in by having phone service with multiple providers. If it’s your computer system or your web site, this may be where you want to focus your resources.

How quickly does each of your services have to get back up and running? In other words, what is the acceptable level of downtime? (This is also addressed in more detail in the Recovery Time Objective section.)

Alternative Work Sites: Do you have a place for your staff to go should your offices become unusable?

Make arrangements with another organization to set up an office, kitchen, classrooms or whatever is needed in order to provide your services.
Or alternatively, can you make arrangements for another organization to take over your services?

For organizations with multiple sites, make a plan, so that should something should happen, you can move programs or offices from site A to site B.

<u>Where is Your Organization’s Information Stored</u>?

□ Purchase a fireproof, crush-proof safe box to store crucial documents.

□ Scan critical documents and store on a CD, on the intranet, or in password-protected section of your website.

Aside from data, equipment and paper concerns, there is the issue of intellectual capital which an organization has to look at by answering the following questions:

□ What is your organization's intellectual capital? In other words, who knows what about your services? And, who knows what about your administrative infrastructure? For example, the staff social worker knows what to do for a particular client, and the CEO knows about your cash flow. The apex of intellectual capital lies in succession planning.

□ Who would provide this information if those with the answers were gone? Does anyone else know these answers/information? Is it written down anywhere?

Document Retention Program

A document retention program is the policy of what to keep, and what to store offsite. With other staff, brainstorm this list. Much of what to keep will also depend on legal requirements. The National Council of Nonprofit Associations has an outline of a records retention policy at www.ncna.org/index.cfm?fuseaction=document.showDocumentByID&DocumentID=2182.

Know where your organization's information is so that if you are displaced from your office, you could at least partially resume business or take the steps to do so.

	Onsite & Where	**Offsite & Where**	**Online & URL**
IRS Determination Letter	□ ________	□ ________	□ ________
IRS Form 1023	□ ________	□ ________	□ ________
Current and previous Form 990s	□________	□________	□ ________
Current and previous audited financial statements	□ ________	□ ________	□ ________
Financial Statements (if not part of the computer system and regularly backed-up)	□ ________	□ ________	
NYS Sales-Tax Exemption Certificate	□ ________	□ ________	

EIN #: ______________________
ER #: ______________________

Bylaws	□ ________	□ ________	□ ________
Mission Statement	□ ________	□ ________	□ ________
Board Minutes	□ ________	□ ________	□ ________
Corporate Seal	□ ________		
Blank Checks	□ ________		
Computer passwords	□ ________	□ ________	□ ________
Donor Records	□ ________	□ ________	□ ________
Client Records	□ ________	□ ________	□ ________
Vendor Records	□ ________	□ ________	□ ________
Volunteer Records	□ ________	□ ________	□ ________

Volunteers: Agencies that are heavily volunteer-based may need to know the following information about their volunteers: who they are, how to contact them (home and work phone, email, cell, etc.), where they live, where they work, expertise, special skills, or any information related to their usefulness or willingness to help the agency (for example, volunteer Jane Doe can walk to our satellite office, lift heavy boxes and knows CPR).

Employee Records/Personnel Info

Names, home addresses, phone numbers, email, emergency contacts, etc.

	Onsite & where	offsite & where
I-9s	□ ________	□ ________
Payroll		
Company Name		
Account Number		
Payroll Rep		
phone & email		
Office Lease (for renters)	□ ________	□ ________
Building Deed (for owners)	□ ________	□ ________

Insurance

General Liability / Commercial Umbrella

Company / Underwriter:

Policy Number:

Representative, phone & email:

Broker, phone & email:

Other Insurances (auto, professional liability, etc.)

Directors & Officers Liability

Company / Underwriter:
Policy Number:
Representative, phone & email:
Broker, phone & email:

Health Insurance Company
Company / Underwriter:
Policy Number:
Representative, phone & email:
Broker, phone & email:

Unemployment Insurance
Company / Underwriter:
Policy Number:
Representative, phone & email:
Broker, phone & email:

Workers’ Compensation
Company / Underwriter:
Policy Number:
Representative, phone & email:
Broker, phone & email:

Disability Insurance (short-term)
Company / Underwriter:
Policy Number:
Representative, phone & email:
Broker, phone & email:

Disability Insurance (long-term)
Company / Underwriter:
Policy Number:
Representative, phone & email:
Broker, phone & email:

Life Insurance
Company / Underwriter:
Policy Number:
Representative, phone & email:
Broker, phone & email:

Dental
Company / Underwriter:
Policy Number:

Representative, phone & email:
Broker, phone & email:

Long Term Care
Company / Underwriter:
Policy Number:
Representative, phone & email:
Broker, phone & email:

Retirement Plan
Company / Underwriter:
Policy Number:
Representative, phone & email:
Broker, phone & email:

Financial Information

Bank Name(s):
Account Numbers:
Branch Representative:
Phone, fax, email:

Investment

Financial Planner / Broker Company:
Rep name:
Phone, email:

Who is authorized to make transfers? Are there alternatives?

Who are the authorized check signers?

Computers & Technology

A computer crash can be just as devastating as the results of a disaster or terrorist activity. If computers are integral to your organization's mission or operations, take the following steps to prepare for resuming the computer/IT functions.

□ Inventory: Hardware

Create a document that lists every piece of hardware your organization owns and would need to replace if damaged or destroyed. Include the make, and model as well as the serial number. Also document all printers and other peripherals (scanner, zip drives, etc.). Another form of documentation would be to keep a book containing all the purchase receipts with details of the hardware. Also document all other technology equipment, i.e., phones, faxes, pagers, beepers, cell phones, etc.

□ Inventory: Software

Document the software being used. One way to create this documentation, computer by computer, is to go online to www.belarc.com and run the Belarc Advisor that builds a detailed profile of the installed software and hardware and displays the results in your web browser (for Windows computers only). Macintosh computer users can use the System Profiler which is part of every Mac. Print these pages out and store them offsite. This, however, has to be done to each individual computer.

□ Create a diagram of your network structure. Document your current computer configuration so that your backup tapes can be restored and function in a new installation.

□ Maintain a list of vendors and contact information.

□ What company provides website hosting:

□ What company provides email service:

□ Document all passwords needed to access files and data and store offsite.

□ Phones: know how to program phones to forward to another number, change voice mail messages, retrieve voice mail, and any other necessary features.

□ Be able to update your website from outside your office.

□ All employees should know how to access their email from alternative sites.

Computer Data

Whether your office has one computer or hundreds, once data is lost, it’s almost always lost forever. There will never be a full recovery without data.

□ Analyze your data backup routine.
Create backups, verify the data, and take it off-site. This can be as simple as having someone regularly taking the backup home or it could be high-level, clustering or mirroring the server. The latter, however, is an expensive way to ensure data security.

□ Do a backup, test for validity, and restore. If you're going to bother doing backups, you need to test to ensure that you can actually restore the data. Decide how frequently you will test the backup-up system. Some recommend testing restoration every six months, by bringing the entire system down and then restoring it to see that everything is working properly.

Be sure that your backups include all important and pertinent files. For example, are all staff email address books being backed up? Another option may be to synchronize address books with PDAs. Or, encourage employees to make a hard copy of their contacts. Those who use a Rolodex should make a copy and take offsite.

□ Determine what kind of archival system of the backup media you will maintain. For example, one tape used repeatedly will not provide an archive. You may need to establish a rotation system to get to, at a minimum, one-month old data. Always keep a copy off-site as a theft of the only existing backup tape won't help with data restoration. If an organization needs to maintain a history of data, you have to deal with constantly changing media. So, if you're storing data on a yearly basis, you'll need to move it to new media. To read an article about backups, go to www.npccny.org/members_only/goi16.htm.

Other Data Options

Make your databases web-based. For example, use an ASP (application service provider) or house your database online, so that nothing is stored in-house.

What are the security requirements versus availability requirements? Security concerns and availability considerations are inherently at odds, and they cannot be reconciled. For example, an organization that has data on clients' health records needs a high level of security to ensure that this data cannot be accessed by those not authorized. This issue needs to be addressed when arranging for alternatives to on-site computer access.
Store essential data on portable computers. However, this raises other security concerns such as theft, damage, or lost computers. It also raises

issues of security of documents and data that you don't want others to access. And, if documents and data stored on the laptops are accessed and altered regularly they will still require some form of backup.

Purchase an external, easily portable way to backup data and take offsite, for example an iPod.

Investigate a co-location server. A co-location server is where an organization purchases and installs a server in another location. The data from the main office is then mirrored to the co-location site. There are numerous companies providing this service. Conceivably, nonprofit organizations could set this up between themselves, ideally not down the block from each other. For example, an organization in the Bronx could arrange for colocation server to be housed in its sister-organization in Manhattan, and vice versa.

□ Power and Servers

A UPS (uninterrupted power supply, also known as a battery backup system) will supply a limited amount of power in the event of an electrical outage. Ideally, servers power switches, and routers have power backups so that in the event of power loss, you are able to shut down your network without causing damage to the server and other equipment.

The website of American Power Conversion (www.apcc.com) has a resource to help determine what battery backup system is best suited to your equipment configurations and desires. It's not necessarily a good idea to have monitors plugged into UPS devices because they will drain the power quickly.

□ Firewall drives are imperative for network systems that are always on. Without a firewall, you are opening up your system to hackers and others who can hijack your site without permission.

If you have a T1 line, and all phones, internet, and email services go through this line, and it goes down, you'll be dark. If appropriate, make contingencies for this such as setting up back-up landlines for clients and/or staff use.

Set up a free email account (Hot Mail, Yahoo, etc.) for emergency use. Document this and share this email address with key personnel.

<u>Know Your Physical Plant</u>

□ Document the Building

An organization that owns its buildings should create a site map for each property that indicates: utility shutoffs, water hydrants, water main valves, water lines, gas main valves, gas lines, electrical cutoffs, electrical substations, storm drains, sewer lines, floor plans, alarm and sounders, fire extinguishers, fire suppression systems, exits, stairways, designated escape routes, restricted areas, hazardous materials (cleaning supplies and chemicals), and high-value items.

□ Emergency Contacts

Create a list of emergency contacts, including: local police precinct, fire department, gas, power and other utility companies, poison control, electrician, plumber, architect, building managers, etc.

These documents should be accessible to the appropriate personnel (office manager, building super, etc.) and available to them both on and off-site.

□ Examine your plant for security weaknesses. For example:

— are the batteries for emergency lighting checked regularly?
— do stair treads have reflective glow-in-the-dark strips to aid in dark exits?
— do electric door/key pad locks have a manual bypass cylinder lock?
— are fire extinguishers easily accessible? Are they checked regularly? Do people know how to use them?
— test your emergency exit routes; post emergency exit routes on the back of restroom doors.

Facilities Management: Plenty of information can be found online about facilities management. Go to Google.com and run a search for “facilities management.”

III. Risk Analysis

□ Conduct a Risk Analysis.

Risk analysis is the process of identifying credible threats that could cause an interruption in an organization’s business. It is important to recognize that some risks can come from within, for example, an organization that has a kitchen on its premises or one that stores hazardous cleaning chemicals onsite. Other risks come from external forces such as flood, fire, etc.

The potential may include fire, water damage, explosion, physical security, loss of power, and natural disaster. A thorough risk analysis should take into account an organization's physical surroundings, and includes such things as security, emergency lighting in halls and stairways, fire escape routes and exits, storing of toxic chemicals, etc.

An analysis of risk, done by a numerical rating system (which is somewhat subjective), quantifies (again subjectively) the possible threats and also looks at ways to reduce the threats. This is also known as disaster avoidance. Some threats you can mitigate or avoid. While you can't prevent a natural disaster, you can plan for what to do if such a catastrophe occurs.

Credible risks depend on your location. Create a list of possibilities. Use your common sense, but also use your imagination. Is it hurricane, fire, flood, or terrorism? Then evaluate these. There are organizations and professionals that have laid out all of these steps that one can hire to help with this process. Additionally, most insurance brokers have experts that they can recommend as well.

Resource: National Fire Protection Association publishes codes and standards intended to minimize the possibility and effects of fire and other risks. Go to www.nfpa.org

□ What evacuation procedures and life safety systems (lighted signs, smoke detectors, sprinklers) do you have in place?

How will you handle evacuating disabled people who cannot use the stairs from your offices during a fire or a blackout when the elevators cannot be used?

In analyzing risks, it may be appropriate for very large organizations to meet with government agencies, community organizations, and utilities to ask about potential emergencies, plans and available resources. These may include the fire and police departments, the Red Cross, telephone, gas and electric utilities, local planning commissions, the New York City Office of Emergency Management, etc. Also see Resources at Section X.

IV. <u>Business Impact Analysis</u>

In brief, a Business Impact Analysis determines in how many days or weeks without your regular stream of income you will go out of business. This may be easy to determine with regards to cash, but may be more difficult when it's more complicated funding equations.

□ How long will it take before the loss of income affects the delivery of your organization's services?

□ How many payroll periods can you meet with no income?

□ How many vendors will get paid? Which ones?

□ What is your cash reserve?

□ What is your RTO (Recovery Time Objective)? RTO is that point in time when a business expects to be back in operation. The RTO is at the discretion of the organization; it could be immediate or it could be protracted.

To determine your RTO, you have to examine each discrete, definable component of an organization — each department and its critical services that you want to resuscitate.

□ What are your budget realities with regard to purchasing equipment that would be utilized in the event of an interruption?

This may be answered when you determine your RTO. If you require an immediate RTO, you will have to spend resources in order to achieve that. If your budget precludes spending resources, you have to adjust your RTO accordingly.

Your RTO will determine what resources you need to purchase or implement. It is important to recognize that if a quick recovery time objective is dictated, then resources will have to be spent in order to achieve that. For example, if it is imperative that your staff have electricity to power their computers and lights, then you will have to purchase a generator and you must allocate resources for this to be accomplished. A quick RTO will cost more than a slower RTO.

It is important to keep in mind that in an interruption there will always be a certain amount of downtime that you're going to have. In determining your RTO, another question to answer is what constitutes unacceptable downtime?

V. Implement the Resources

Once you've:

□ identified your critical services,
□ determined your RTO,
□ budgeted for the resources,

you can purchase those resources needed to implement your plan.

VI. Test the Plan

Test the plan to be sure that it works and that the resources you've indicated in your plan actually exist. For example, if your plan for evacuation of the building says that there are two fire exits on the 5th floor, you need to be sure that there are in fact two exits there and that they both work. Are the fire extinguishers actually where the plan says they are? Or backup tapes of computer data: you may be taking them offsite regularly, but have you ever tried to restore them to make certain that they would work correctly? Testing of a plan can be done on the desktop by looking at your plan as written and speculating as to its worthiness and as an actual parallel operation where you physically execute all the steps of the plan and set up operations elsewhere.

□ Determine what constitutes recovery.

Look at what happened, why it happened, and figure out how to ensure that it won't happen again. Could it have been prevented? What procedures worked well? What systems did not function well? Could these have been prevented?

□ What was your response to the August 2003 blackout? Did you have any systems in place? What worked, and what didn't? What procedures did you implement as a result of that interruption?

Maintain and Update the Plan

Keep the plan current. When you buy new equipment, document it. As staff come and go, change the plan to reflect who is doing what.

□ Who is assigned to keep the plan updated?

VII. Insurance

□ Review your current coverage to ascertain whether it is adequate in the event of either a catastrophe or an interruption in business activities;

□ Review your workers' compensation policy to ensure that all personnel, including volunteers, are covered;

□ Review all policies for exclusions. For example, what would happen if you were denied access to your premises by a civil authority? (Check your property coverage to see if this is included);

□ Are photographs and other records of facility assets up-to-date? Are they stored in a safe place?

Consider your property for possible losses and damage:

□ What is the cost to replace your equipment?

□ What would it cost to set up a temporary facility from which to operate?

□ What is the cost to repair the facility and the equipment?

Beyond property and liability insurance, and with regard to disaster planning, there are other types of insurance that an organization may want to investigate: Business Interruption, Extra Expense and Terrorism:

- BUSINESS INTERRUPTION pays for your loss of net profits plus expenses that continue for a period of time;

- EXTRA EXPENSE will pay expenses above your normal expenses so that you may continue to operate. For example, if you had to move and pay increased rent, extra expense insurance would pay the additional rent, assuming you purchased enough insurance to cover the additional rent.

- TERRORISM insurance used to be included in all forms of insurance. However, after 9/11 things changed; and this is no longer the case. Please consult your agent or broker.

□ Minimize Risks. One component in purchasing insurance coverage most cost-effectively involves analyzing and avoiding risk. For example, if you have plate glass windows, replace them with safety glass; if you have worn and torn carpeting, replace it; install self-locking safety exit doors, etc. Also see Section III – Risk Analysis.

When shopping for new coverage, ask your agent or broker for currently-valued loss experience from the insurance carriers for the past five years. You should actually check this every year, as you may find claims that are in excess of what you think they should have been and/or you may find claims that are charged to your policy that belong to another insured.

To determine how much insurance to purchase:

1. Determine the Replacement Value. Many insurance policies cover only the Actual Cash Value (depreciated value) of your property. On the other hand, if you are going to replace this property, you will probably want to insure it for what it will cost to replace it presently. Ask your agent or broker to tell you the difference in cost between Actual Cash Value and Replacement Value coverage. Then determine how you want to insure it

2. Look at your assets/cash reserve to see how much you are "willing" to spend on insurance, after you know what the premiums will be.

□ Know the phone number of the people in your agent's or broker's claims department. In the event of an emergency, call them immediately.

Talk to your insurance broker/carrier to see if they can help with your planning. It's in their best interest to see that your organization is prepared (to help mitigate their losses) and many are willing to help. Similarly, many large carriers have documents posted online to help with this process.

VIII. Personnel Policies & Crisis Communications

□ Review your personnel files. What information do you not have that you should? For example, emergency contact information.

□ Update your personnel manual to reflect new realities such as emergency closing policies, workplace safety, telecommuting, etc. Issues that may arise during a catastrophe may include paying non-exempt employees. For example, in the event of a blackout, there is no state law requiring an employer to pay employees for the day they were unable to come to work. Similarly, your manual should address what to do if an employee comes to work and finds the office closed. For a primer on personnel manuals, go to www.npccny.org/members_only/pmei1.htm.

□ Preserve Agency Records

Investigate storing records offsite. What this entails depends on the organization. Another way to look at it is what things (documents, records, etc.) might you need in order to get back into business? This could be as simple as storing crucial documents at a board member's country house, or could entail scanning and storing documents on a CD.

Communications

Create a system to communicate with the staff. You need a system in place in order to get in touch with people, whether to let employees know the organization is closed or to contact certain personnel in the event of a catastrophe. This can be as low-tech as a phone card that people can carry in their wallets listing names and phone numbers. Or, it can be high-tech—an emergency communication system such as a push-to-talk system available on Nextel phones.

□ Create a phone chain (or phone tree) that defines who calls whom. You don't want the work of contacting every employee falling on one person. Contact information should include every known way of getting in touch with people, e.g., phones, BlackBerry, pager, cell, email, etc. Unannounced, test the phone tree on a Sunday evening to see if it is possible to get in touch with everyone.

Organizations with many staff members may want to make other contact arrangements for staff should the facility (and phone lines) be unavailable. Have (and disseminate to everyone) a specific phone number only for staff to call. Or, arrange for an answering service with either a message or a live person with info for staff on what to do and where to report; or make arrangements with another agency to provide this service, and vice versa.

□ Have a communication plan. Beyond being able to contact each of your employees, do you also need to get a message out to the media? For example, will your theatre need to let the media know that a production is going on as scheduled?

□ Have contact information for all personnel, clients, volunteers, and any other people that regularly visit your premises. This may include out-of-state contacts.

Other Personnel Concerns

Workers Compensation

Workers' compensation is a no-fault system for accidents that occur within the scope of the job. Disability coverage is for off-the-job accidents. Workers' comp would include injuries that arise during an emergency at work. An injury at home for a worker who is telecommuting should be covered by workers' compensation. Stress (a mental injury without physical injury) would also be covered by workers' compensation.

An organization’s employee handbook should include a statement requiring all employees to immediately report all and any injuries to management.

Telecommuting

Telecommuting has to be planned, it can’t be haphazardly implemented, and personnel policies must address the situation. It is easier for an executive or other exempt employees to telecommute. You must figure out how to track the time of an hourly, non-exempt employee should telecommuting be offered to these people. Also, there are also supervisory issues with telecommuting.

Notify your workers’ compensation carrier that there are employees who are working from home and the days they are doing so. There is no home inspection requirement, since OSHA has come out with a ruling saying so. A workers’ compensation claim for a telecommuter may come down to the word “regularly.” If they work on Fridays at home, workers’ compensation may not cover an injury that occurred on a Wednesday.

Accommodating Employees’ Distress

In the event of a catastrophe, you may need to address scheduling problems as well as employees who are afraid to come to work. Telecommuting and split schedules may be some of the ways to help alleviate these issues. Organizations that have EAP’s (employee assistance programs) can get a lot of mileage out of them. For example, counseling after a traumatic event.

Workplace Safety

Do what you have to in order to make employees safe. This may necessitate badges or some other form of identification to be worn at all times. Don’t allow visitors to wander around unescorted. Require visitors to sign in and out of the building.

□ Emergency Contact Sheet. While everyone should know to call 911 in an emergency, you should still have a list with phone numbers of other emergency numbers, including the local police precinct, fire department, gas company, utilities, local hospitals, etc.

□ Train all employees and others regularly in your building in what to do in the event of an emergency: evacuation routes, meeting places, fire escapes, location of fire alarm or emergency phone systems, etc. Post emergency exit routes on the back of restroom doors.

□ Decide on a central meeting place for staff and clients to gather for a head count should the building need to be evacuated — to be sure that everyone is safe and out of the building. Be specific as to location, for example, the south-west corner of xyz park, or in the middle of the block on 8th Avenue, between 18th and 19th streets (Intersections will probably be really crowded during an emergency, so between streets or other unusual sites may be preferable).

□ Make contingencies should staff be required to stay inside (i.e., a dirty bomb or a hurricane). Have sufficient water, food, first aid supplies, flashlights, radios, batteries, Go Kits, various communication devices (cell, land line, BlackBerry, etc.). Have staff bring in a change of clothing to store.

Emergency Planning Checklist

PLANNING TEAM

YES NO

Planning Team established? □ □
Planning Team Schedule Established? □ □
Budget Developed? □ □

INTERNAL PLANS AND POLICIES REVIEW

Evacuation Plan? □ □
Fire Protection Plan? □ □
Safety And Health Program? □ □
Security Procedures? □ □
Insurance Programs? □ □
Employee Manual? □ □

CODES AND REGULATIONS REVIEW

Fire Codes? □ □
Electrical Codes? □ □
OSHA Regulations? □ □

CRITICAL SERVICES AND OPERATIONS REVIEW

Services provided by your company identified? □ □
Operations vital to the continued functioning of the facility? □ □
Equipment vital to the continued functioning of the facility? □ □
Personnel vital to the continued functioning of the facility? □ □
Services provided by vendors identified? □ □

INTERNAL RESOURCES AND CAPABILITIES REVIEW

Personnel
Fire Warden(s)? □ □
CPR Training? □ □
First Aid Training? □ □
Equipment
Fire Protection? □ □
Communications? □ □
First Aid Supplies? □ □
Emergency Power? □ □
Backup Systems (Arranged with other facilities)
Payroll? □ □
Communications? □ □
Customer Services? □ □
Computer Support? □ □

EXTERNAL RESOURCES REVIEW

Emergency Management Office? □ □
Fire Department? □ □
Police Department? □ □
Emergency Medical Services? □ □

Telephone Companies? □ □

Electrical Utility? □ □

Insurance Policy Review With Broker? □ □

PLAN DEVELOPMENT

Plan Purpose? □ □

Responsibilities of key personnel? □ □

The types of emergencies that could occur? □ □

Where response operations will be managed? □ □

EMERGENCY MANAGEMENT ELEMENTS IN PLACE

Direction and Control? □ □

Communications? □ □

Life Safety? □ □

Property Protection? □ □

Community Outreach? □ □

Recovery and Restoration? □ □

EMERGENCY RESPONSE PROCEDURES ADDRESSED

Assessing the situation? □ □

Protecting employees, customers, visitors, equipment, vital records, other assets?

□ □

Getting the business back up and running? □ □

PROCEDURES FOR BOMB THREATS ADDRESSED

Warning Employees and Customers? □ □

Communicating with personnel and community responders? □ □

Conducting an evacuation and account for all persons in the facility? □ □

Shutting down operations? □ □

Protecting vital records? □ □

Restoring operations? □ □

SUPPORT DOCUMENTS AVAILABLE

Emergency Call Lists –People responding, their responsibilities and phone numbers?

□ □

Employee Lists - Employees with their home phone numbers? □ □

Resource Lists – Equipment and supplies that could be needed in an emergency?

□ □

DEVELOPMENT PROCESS

Task list identifying persons, tasks and timetables? □ □

Needs of disabled persons and non-English speaking personnel? □ □

Training schedule for employees established? □ □

PLAN DISTRIBUTION

Copies distributed to employees? □ □

Current date and revision number on plan? □ □

PLAN IMPLEMENTATION

All personnel trained in procedures? □ □

Orientation and Education Sessions? □ □

Walk Through Drills?	□	□
Evacuation Drills?	□	□
Plan tested to assure that employees know what to do?	□	□

EMPLOYEE TRAINING ADDRESSES:

Individual roles and responsibilities?	□	□
Information about threats, hazards, and protective actions?	□	□
Notification, warning and communication procedures?	□	□
Means for locating family members in an emergency?	□	□
Emergency response procedures?	□	□
Evacuation, shelter and accountability procedures?	□	□
Location and use of common emergency equipment?	□	□

PLAN EVALUATION AND MODIFICATION

A formal audit of the plan conducted at least once a year?	□	□
Does the plan reflect lessons learned from drills and actual events?	□	□
Are photographs and other records of facility assets up to date?	□	□
Are the names, titles and phone numbers in the plan current?	□	□