Agenda

• Welcome!
• Introduction
• Protecting Your Employees
• Emergency Response
• How to Build a Robust Business Continuity Program
• Execution
• Quick Start
INTRODUCTION

Welcome to Business Continuity Planning!!!

Feeling Overwhelmed?

Testing

AAA, AA, A, B, C, D??????

Business Impact

Emergency Response

Risks

Recovery Plans

Emergency Notification Lists

Alternate Sites

Business Functions

Testing

Feeling Overwhelmed?
It’s Not Magic!!
Qualities of a Business Continuity Planner

- Inquisitive
- Ability to think “outside the box”
- Relentless
- Doesn’t need to be “liked” by everyone
- Doesn’t get “rattled” easily
- Available 24x7
- Business knowledgeable
- Not afraid to open “Pandora’s Box”
- Enjoys challenges
- Insane!
Why is Business Continuity Management Important?

• Safeguard human life
• Minimize critical decisions in a time of crisis
• Reduce dependency on specific personnel
• Minimize loss of data
• Facilitate timely recovery of business functions
• Minimize loss of revenue/customers
• Maintain public image and reputation
• Other ideas?
• Setting the strategic direction and plans for all business units to ensure business continuity and effective emergency management.
• Integrating the contingency planning process across business units when the nature of the business requires it.
• Providing consulting services and direction to senior management.
• Coordinating and integrating the activation of emergency response organizations with the business units.
• Provide period management reporting and status.
• Ensure executive management compliance with the contingency planning program.
• Ensure the identification and maintenance of all critical business functions and requirements.
• Develop, implement, and maintain policy and guidelines for all business units to follow.
• Develop and maintain testing and maintenance programs for all contingency planning functions.

• Provide primary contact for your company to handle a coordinated response during a business interruption.

• Act as a resource for contingency planning efforts with the company area of responsibility.

• Secure appointment, training, and back-up of all contingency planning and response teams.

• Assist in the design and maintenance of alternate sites.

• Maintain current contingency planning documentation.
Business Continuity Terminology

• **Critical Business Functions**
  - Those functions considered essential to the ongoing operation of the Company or Business Unit.
  - If these functions could not operate, there would be a significant adverse impact upon the products/services provided.
  - Includes anything that might significantly impair the financial integrity or reputation of the Company.
• **Command Center**
  
  - Location set up for Management and BCP to operate from during emergency situation.
  
  - Maintain Contingency Plan Document and other needed resources at Command Center.
• **Alternate Site**
  - A location where critical business functions can resume processing in the event of a business interruption.
Business Continuity Terminology (cont’d)

• Vital Records
  - All data and information required to support a business function (i.e., historical, regulatory requirements)
  - Includes:
    • Policy and Procedures Manuals
    • Input documents or data
    • Manuals for software and other applications
    • Vendor/Customer List
    • Telephone/Rolodex
    • Backup tape files
  - Should be maintained off site at third-party vendor or Command Center
PROTECTING YOUR EMPLOYEES
Life/Safety is #1

- Access control
- Alarm monitoring
- Floor Warden program
- Evacuation drills conducted annually
- Shelter-in-Place drills conducted annually
- Background checks
- Procedures for emergency response in place
- Workplace Violence Programs
What to do if there is a FIRE…

What to do if...

there is a FIRE

and you find it:
1) Call Corporate Security.
2) Activate the nearest building fire alarm.
3) Follow the evacuation instructions given by the Floor Wardens, who will be wearing orange arm bands and carrying flags.

and you hear the public address system or fire alarm:
1) Follow the instructions given over the public address system.
2) Follow the evacuation instructions given by the Floor Wardens, (wearing orange arm bands and carrying flags).

EMERGENCY Numbers:
What to do if there is a BOMB THREAT...

What to do if...

you receive a BOMB THREAT

1) **TAKE NOTES** -- location and type of device, time of detonation, sex and age of caller, quality of voice, accent, background noise(s), etc. -- this is VERY IMPORTANT!
2) Immediately call Corporate Security.
3) Notify your supervisor/manager.
4) Wait for instructions from your manager or the Floor Warden, or to be broadcast over the public address system.

EMERGENCY Numbers:
What to do if there is an EVACUATION...

1) Prepare to evacuate, but wait for specific instructions via the public address system, telephone, a Floor Warden or a Security Officer. Some routes may not be safe.
2) Follow the Floor Warden out of the building.
3) DO NOT use elevators for emergency evacuation.
4) Walk quickly when directed to do so, but do not run.
5) DO NOT go back for any reason.
6) Proceed to the Evacuation Site for your building.
7) Wait for further instructions from Corporate Security or your company's Contingency Planner.
What to do if there is SEVERE WEATHER...

while you are at home:
1) Call the Contingency Information Line, 1-xxx-xxx-xxxx, for up-to-date information.
2) Check your local radio and TV stations for announcements.

NOTE: Remember, property damage may require that you report to work at a different location. Contact your manager or call the Contingency Information Line.

while you are at work:
1) Follow the instructions given over the public address system, SYMON*, by your manager or the Contingency Information Line.

*SYMON is a customized electronic message board displaying system status and market and critical business information. SYMON boards are located in key business areas throughout Fidelity.
What if someone needs MEDICAL ASSISTANCE…

What to do if someone needs MEDICAL ASSISTANCE:

1) DO NOT PANIC -- REMAIN CALM.
2) IMMEDIATELY call Corporate Security.
3) Provide your name, location, mail zone, call-back number and any information about the illness or injury. Don’t hang up until the dispatcher confirms the information.
4) Keep someone with the injured person at all times.
5) If possible:
   • have someone stay at the call-back number.
   • have someone meet the emergency team at the entrance.

Don’t try to apply first aid if you are not qualified. It could cause further injury.

If you need medical assistance, call Corporate Security and stay at your original location until help arrives.

NOTE:
(The injured employee or his or her manager must complete an occupational injury/illness report form within 24 hours of the incident and submit it to HR.)
EMERGENCY RESPONSE
What Should I Do in an Emergency?

**What do I tell my customers?**

How do I contact my employees and tell them where to report?

My house is destroyed; I can’t go to work!

**Where do I go?**

I need supplies and a PC to start working again.

The Press keeps asking me all of these questions. What do I tell them?

All my files were destroyed, What do I do now?

**How do I contact my customers?**
Take a Deep Breath..
All You Need is a Business Continuity Plan!

• What is a Business Continuity Plan?
  - The plan describes the pre-planned sequence of events that allows for the continuation/recovery of business functions, computer resources, networks, and facilities.
  - The documented process for continuation/recovery of business functions in the event of an unexpected disruption of service.
Don’t end up like this Guy!

“You have reached the Fire Department. If you’re reporting a smoke condition, press one. If you’re reporting an electrical fire, press two. If you’re...”
How Ready is Your Business?

• If you were evacuated from your building and you were standing in the evacuation area and they announced that you could not work at that site for at least the next 2 weeks,

Do you know what to do next?

Does your staff?
Emergency Response Checklist

- Write Down Information
  - Who Called
  - Building Location
  - Area of Impact
  - Expected Duration
- Relay Facts to Others
  - Escalate to Senior Management As Appropriate
  - Contact Teams As Needed
- Communicate
  - Inform Management
  - Inform Emergency Response Teams
  - Inform Corporate Contingency
- Respond and Recover
WHAT NEXT?

When disaster strikes, the most important thing --- after assuring the safety and welfare of employees--- is to get vital support services functioning to the best of our ability.
How to Build a Robust Business Continuity Program

1. Project Initiation & Management
2. Risk Analysis/Mitigation
3. Business Impact Analysis
4. Recovery Strategies
5. Develop The Plan
6. Exercise The Plan
7. Maintain The Plan
8. Training & Awareness
Don’t get caught without a Plan!

If you are reading your plan for the first time and you are in the middle of a disaster.....

........you are in trouble.....

“Well, thank God we all made it out in time. ...’Course, now we’re equally screwed.”
Example of Business Continuity Support Organization

Corporate Emergency Management Organization

- Real Estate
- Security
- Enterprise BCM
- Risk Management
- Corporate Affairs

Dedicated/Certified Business Continuity Program Manager

- Business Unit
  - Human Resources
- Business Unit
  - Systems
- Business Unit
  - Marketing
- Business Unit
  - Finance

Business Unit
#1: Project Initiation & Management

- **Define Project**
  - Scope - document what the Plan will cover
  - Objectives - Document what is to be achieved with this project
  - Assumptions - Document the assumptions you are making regarding the project, i.e. Commitment from management, phone lines operational, no regional outage

- **Estimate Project Resources**
  - Document the resources you will need to complete the project including human resources as well as physical & financial resources

- **Obtain Management Commitment**
  - Management should have a documented responsibility to the company in the development & testing of a viable business recovery plan - without it, the project will fail
  - Require management sign-off and approvals at each major milestone of the project
Project Initiation & Management (cont’d)

- Define Project Timeline, Major Milestones, and Deliverables
  - Define major steps toward plan development
  - Estimate how long each step will take
  - Identify the critical path
  - Document what will be produced from each step
  - Estimate when the project will be completed
  - Example of Phased Approach:
    - Emergency Notification Lists: Immediately
    - Vital Records Program in Place: Immediately
    - Risk Analysis/Business Impact Analysis: 1st 3 months
    - Define Recovery Strategies: 1-6 months
    - Select and Develop Alternate Sites: 1-12 months
    - Develop and Document Contingency Plan: 1-12 months
    - Testing, Maintenance, Periodic Audit: Annual or when significant changes occur
Emergency Notification...

- Identify the different types of recovery you will plan for
- Identify who would have the authority to declare a disaster depending upon the scenario
- Identify who would be part of the recovery effort
- Build your notification lists based on this information
Sample ERT...
Potential Scenarios

- Identify potential scenarios
  - Geo-Centric Scenarios
    - An event impacting both buildings and people in one location, i.e. WTC
    - Events impacting building and people in multiple locations, i.e. WTC & Pentagon
  - People Scenarios
    - Inability for employees to access facilities
    - Associates unable to work due to emotional trauma
    - Loss of workforce
    - Loss of key members of management team
Potential Scenarios (cont’d)...

- Identify potential scenarios (cont’d)
  - Infrastructure Scenarios
    - Telecommunications outage
    - Internet outage, i.e. Cyber attack
    - Loss of transportation service or access, i.e. airport closures
  - Market Scenarios
    - Failure of a market utility or exchange
    - Business interruption to a critical vendor
    - Counter-party failure
#2: Risk Mitigation Strategy Overview

- Protecting People and Workspaces
- Protecting Information
- Protecting Reputation
Protecting People and Workspaces

- Access Control
- Alarm Monitoring
- Floor Warden
- Evacuation Drills
- Background Investigations
- Landscape Design
- Lighting
- Cameras
- Visitor Procedures
- Backup Power systems
- Facility Design
- Facility Location
Protecting Information

- Information Security policy and procedures
- Privacy Policy
- Firewalls
- Intrusion Detection
- Strong Passwords
- Controlling access to information
- Vendor Management
- Secure offsite storage
- Proprietary Waste Disposal
- Virus Protection and Response
Protecting Reputation

- Strong Governance
- Media trained
- Communication Plans
- Internal and external audits
- Operational Management
- Recoverability
- Code of Ethics
Three Elements of Risk

• Threats
  - Events or situations which would cause financial or operational impact to the organization.
  - Threats are measured in probabilities, such as “may occur 1 time in 10 years”.
  - Each threat has a duration of time that the business or operation would not be able to function in its normal manner, if at all

• Assets
  - Assets are composed of many elements
  - Physical assets that are owned by the organization
  - Information assets
  - Financial assets
    • Revenues lost for the duration of the incident
    • Additional costs to recover
    • Fines and penalties incurred
    • Lost good will or competitive advantages
Elements of Risk (cont’d)

• **Mitigating Factors** -
  - Mitigating factors are the protection devices, safeguards, and procedures which are in place that reduce the effects of the threats.
  - They do not reduce the threat; they only reduce the impact of the threat.

Examples of mitigating factors in use: UPS (Uninterruptable Power Supply) and Generator backups for replacement power, sprinkler systems to control the spread of fire, Assess Card Readers to control physical access to Fidelity space, etc....
## Threat/Effect Matrix

<table>
<thead>
<tr>
<th>Threat</th>
<th>Region (Y,N)</th>
<th>Site (Y,N)</th>
<th>Probability/Effect (H,M,L)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Earthquake</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hurricane</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tornado</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Volcanic Eruption</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Flood</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Power Outage</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Falling Aircraft</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Transportation Mishaps</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Rail</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Road</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Boat</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Fire</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Smoke</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Denial Of access from Contamination</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Civil Disorder</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Water Damage</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Bomb Threats</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sabotage/Vandalism</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mechanical Breakdown</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Other (specify)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Protecting Information

- Information Security policy and procedures
- Privacy Policy
- Firewalls
- Intrusion Detection
- Strong Passwords
- Controlling access to information
- Vendor Management
- Secure offsite storage
- Proprietary Waste Disposal
- Virus Protection and Response
Protecting Reputation

- Strong Governance
- Media trained
- Communication Plans
- Internal and external audits
- Operational Management
- Recoverability
- Code of Ethics
Three Elements of Risk

• Threats
  - Events or situations which would cause financial or operational impact to the organization.
  - Threats are measured in probabilities, such as “may occur 1 time in 10 years”.
  - Each threat has a duration of time that the business or operation would not be able to function in its normal manner, if at all

• Assets
  - Assets are composed of many elements
  - Physical assets that are owned by the organization
  - Information assets
  - Financial assets
    - Revenues lost for the duration of the incident
    - Additional costs to recover
    - Fines and penalties incurred
    - Lost good will or competitive advantages
Elements of Risk (cont’d)

• **Mitigating Factors** -
  - Mitigating factors are the protection devices, safeguards, and procedures which are in place that reduce the effects of the threats.
  
  - **They do not reduce the threat; they only reduce the impact of the threat.**

Examples of mitigating factors in use: UPS (Uninterruptable Power Supply) and Generator backups for replacement power, sprinkler systems to control the spread of fire, Assess Card Readers to control physical access to Fidelity space, etc....
## Threat/Effect Matrix

<table>
<thead>
<tr>
<th>Threat</th>
<th>Region (Y,N)</th>
<th>Site (Y,N)</th>
<th>Probability/Effect (H,M,L)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earthquake</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hurricane</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tornado</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volcanic Eruption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flood</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Outage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Falling Aircraft</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transportation Mishaps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rail</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Road</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fire</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smoke</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial Of access from Contamination</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Civil Disorder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Water Damage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bomb Threats</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sabotage/Vandalism</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mechanical Breakdown</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other (specify)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
#3: Business Impact Analysis

- May be unable to service customers
- Possible regulatory sanctions if your company could not recover quickly enough
- May cause damage to company reputation
- Customers could leave and never return
Components - BIA

• Business Impact Analysis
  - Resource requirements
  - Technology review
  - Interdependencies defined
  - By business function
    • Business function description
    • Primary Location
    • Business function criticality
    • Primary alternate site
    • Cost center
    • Function level BIA
BIA: Impact of a Disaster

A disaster may impact............

Your Paycheck

Company Reputation

Customers

Ability to meet regulatory requirements
BIA: Resource Requirements

Establish the resources that are required to continue to perform those functions

Two Phases should be defined:

- **Survival** - In the period immediately following the disaster, the emphasis will be to keep the business running at the minimum acceptable level.

- **Recovery** - In the longer term, the business will need to be restored to its original performance. Identification of all resources required to support the function is required to facilitate the longer term recovery.
BIA: Technology Review

• Must document all technology used to support the business functions
  - Hardware platform
  - Application owner
  - Location of hardware/application/data
  - Recovery strategy
  - Does the systems owner of the application, databases, hosting servers, etc. support the system at the same level as the business TSR?
BIA: Interdependencies

- It is critical that the internal and external dependencies for the business function be understood and documented
  - Inputs to the function and where they come from
  - Outputs of the function and where they go to
  - System Application dependencies
BIA: Business Functions

• Make a list of all Business Functions
• Conduct interviews with all business function managers
• Work with managers to identify loss potential of not performing the function
• Determine recovery timeframe to meet the business or regulatory requirements governing that function
BIA: Factors for Classifying Business Functions

• **Mission-Critical:**
  - Defined by the business units as those functions that are required to complete processes
  - Critical to the *continuity* of the business

• **Customer-Critical:**
  - Defined by the business units as those functions that are required to complete processes
  - That are critical to the *customer’s perception* of the business
## BIA: Sample Form

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>F = Financial</td>
<td>0 = &gt; 3 days</td>
<td>0 = none</td>
<td>0 = none</td>
<td>0 = none</td>
<td>Sum of 1 thru 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C = Customer</td>
<td>1 = 3 days</td>
<td>1 = Low</td>
<td>1 = Low</td>
<td>1 = 0 to 10K</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R = Regulatory</td>
<td>5 = 2 days</td>
<td>3 = Med</td>
<td>3 = Med</td>
<td>2 = &gt;10K but &lt; 100K</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10 = day 1</td>
<td>5 = High</td>
<td>5 = High</td>
<td>3 = &gt;100K but &lt; 500K</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20 = 4hours</td>
<td></td>
<td></td>
<td>4 = &gt; 500K but &lt; 1 Mil</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>40 = immediate</td>
<td></td>
<td></td>
<td>5 = &gt; 1 Mil</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NEDRIX Conference June 2004
### BIA: Business Function Recovery Time Sensitivity Rating (TSR)

<table>
<thead>
<tr>
<th>Rating</th>
<th>Time Sensitivity</th>
<th>Recovery</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Immediate</td>
<td>Up to 4 Hours</td>
<td>Must be performed in at least two geographically dispersed locations that are fully equipped and staffed.</td>
</tr>
<tr>
<td>AA</td>
<td>Up to 24 hrs</td>
<td>Same Day</td>
<td>Must have a viable alternate site that can be staffed &amp; functioning within 4-hrs</td>
</tr>
<tr>
<td>A</td>
<td>Same Day</td>
<td>Up to 24 hrs</td>
<td>Must be operational same business day &amp; have viable alternate site staffed &amp; functioning same day</td>
</tr>
<tr>
<td>B</td>
<td>48-72 Hours</td>
<td>Up to 24 hrs</td>
<td>Can be suspended for 1 business day; must have alternate site staffed &amp; functioning next day</td>
</tr>
<tr>
<td>C</td>
<td>72 hrs or greater</td>
<td>48-72 Hours</td>
<td>Can be suspended for up to 2 business days, must have alternate site staffed &amp; functioning on 3rd day</td>
</tr>
<tr>
<td>D</td>
<td>72 hrs or greater</td>
<td>72 hrs or greater</td>
<td>Can be suspended for greater than 3 business days</td>
</tr>
</tbody>
</table>
Vital Records

- Do You Know:
  - Where they are?
  - What is included in them?
  - How to get them?
  - Who is authorized to retrieve them?
  - How long it will take to retrieve them?
  - Where to have them delivered?
  - How long it will take to restore them?
  - Who will restore them?
Common Vital Records

• Commonly a Legal Requirement:
  - Anything with a signature
  - Customer correspondence (statements, letters back and forth, requests, etc.
  - Customer conversations (recorded interactions with customer service reps)
  - Accounting records
  - Justification proposals/documents
  - Transcripts/minutes of meetings with legal significance
  - Paper with value - stock certificates, bonds, commercial paper, etc.
  - Legal documents - letters of incorporation, deeds, etc.
Common Vital Records (cont’d)

• Commonly a Business Requirement
  - Databases and contact lists for employees, customers, vendors, partners or others that your business unit deals with regularly or at time of emergency (includes ENLs)
  - Your business unit’s business continuity plans
  - Procedure/application manuals that your employees normally use and procedure manuals for operation in your alternate site if different from above
  - Back-up files from print/file (LAN) servers
  - Back-up files from production servers/applications owned by your business unit that support your critical functions
  - Reference documents used by your employees on a regular basis
  - Calendar files or printouts – particularly if your business unit schedules appointments with customers
  - Source code
#4: Recovery Strategies

- Define Recovery Strategies
  - General Recovery Strategies used to recover critical functions
  - Recovery Strategy for loss of the primary site
  - Recovery Strategy for Loss of dependent systems
- Estimate Cost
- Make Recommendation
- Gain Management approval
Selecting a Recovery Strategy

- Recovery strategies will be driven by the recovery timeframe of the function.
- Recovery options might include the following:
  - **Self-service** - A business unit can transfer work to another of its own locations which have available facilities
  - **Internal Arrangement** - Training rooms, cafeterias, conference rooms, etc.... may be equipped to support business functions.
  - **Reciprocal Agreements** - Other business units may be able to accommodate those affected. This could involved the temporary suspension of non-critical functions at the business units not affected by the outage.
  - **Dedicated alternate sites** - Built by your company to accommodate critical function recovery.
  - **External Suppliers** - A number of external companies offer facilities covering a wide range of business recovery needs.
  - **No arrangement** - for low priority business functions it may not be cost justified to plan to a detailed level. The minimum requirement would be to record a description of the functions, the maximum allowable lapse time for recover, and a list of the resources required.
Alternate Sites

**Mission/ Scope:**
- Provide viable alternate site for critical business functions

**Assumptions:**
- Must provide for on-going testing and maintenance
- Assume a single building and campus outage

**Requirements:**
- Functional at impact
- Flexible for any business
- Expandable per situation
- Recovery of business technology
- Ability to test

**Capabilities:**
- Internal owned alternate sites
- External Vendor-contracted alternate sites
### Example of Alternate Site Strategy

<table>
<thead>
<tr>
<th>PRODUCTION SITES</th>
<th>ALTERNATE SITES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MRO</strong></td>
<td><strong>Intra-Day</strong>&lt;br&gt;Up to 24 Hours</td>
</tr>
<tr>
<td></td>
<td>Fidelity Building&lt;br&gt;Marlborough, MA</td>
</tr>
<tr>
<td></td>
<td>Fidelity-Owned Alternate Site in Smithfield, RI</td>
</tr>
<tr>
<td></td>
<td>Redundant FITSCo Site&lt;br&gt;Salt Lake City, UT</td>
</tr>
<tr>
<td><strong>SLC</strong></td>
<td><strong>Intra-Day</strong>&lt;br&gt;Up to 24 Hours</td>
</tr>
<tr>
<td></td>
<td>Fidelity Building&lt;br&gt;Salt Lake City, UT</td>
</tr>
<tr>
<td></td>
<td>Fidelity-Owned Alternate Site in Salt Lake City</td>
</tr>
<tr>
<td></td>
<td>Redundant FITSCo Site&lt;br&gt;Marlborough, MA</td>
</tr>
</tbody>
</table>
Alternate Site, New Jersey
Developing the Plan

Master Recovery Plan: Sample Table of Contents...

- Planning Team Information
- Plan Maintenance History
- Executive Overview
- Executive Sign-Off
- Section 1: Emergency Response
- Section 2: Emergency Response Organization
- Section 3: Plan Overview
- Section 4: Recovery Strategies
- Section 5: Recovery Communications
- Section 6: Plan Activation
- Section 7: Alternate Sites
- Section 8: Business Unit Recovery Plans
- Appendices
- Business Partner Procedures
Event Management

**Built by Building/ Business**

- Teams
  - Assessment Team
  - Crisis Management Team
  - Emergency Response Teams
- Permanent standing conference bridge
- Event owners defined
- Escalation process defined
Event Management (cont’d)

• Contingency Plans are what we exercise when all other mitigating factors fail
• Contingencies start with Event Management
• If you do not properly manage Events, all the other Risks may occur
• Event Management is about Communication and Response
• Event Management needs to be practiced
• Requirements:
  - Strategy must be consistent regardless of event
  - Need to establish an assessment process
  - Event Ownership needs to be defined
  - Management teams identified
  - Response teams identified
  - Process for gathering of key decision-makers
  - Methods of communication to be defined
Event Management (cont’d)

- Assumptions:
  - Strategy will deal with non-data center events since those events should be handled by Systems
  - Communications on all events will begin with Corporate Security
  - Strategy will be used in every region
  - Strategy will be consistent regardless of event
  - Assessment group will always include Facilities, Security and Corporate
  - If the event causes any Life Safety issues for employees, Security owns the response to the event until all life safety issues have been resolved.
  - If the event has no life safety issues, or once the life safety issues have been addressed, Facilities owns the response to the event.
Event Management (cont’d)

• Procedures:
  - Security identifies or is notified of an event which requires a response escalation and notifies Assessment Team
  - Brief assessment is conducted and if event is deemed significant, first escalation process activated.
  - Individuals identified for that site for First Escalation are notified through an alpha-numeric page. Communications should be limited to “location of event, type, who generated the page, and conference bridge number.
  - Individuals identified for that site for First Escalation are notified through an alpha-numeric page. Communications should be limited to “location of event, type, who generated the page, and conference bridge number.
  - All First Escalation responders notified must attend the conference call, even if no impact.
  - If any group does not respond, back-ups will be contacted until response is received.
Event Management (cont’d)

• Procedures:
  - Assessment of impact provided to First Escalation group.
  - If event is resolved, page sent to all interested parties to notify of event, impact and resolution.
  - If event is not resolved, the following steps will be taken:
    • Conference bridge will remain open for technical response and recovery management.
    • A second conference bridge will be established if needed for management of event communications.
  - Response Team Leader will be identified.
  - Crisis Manager will be identified (Site GM will act as crisis manager for the site). For those sites which do not have a GM, and for escalations outside of the site, Corporate Contingency Planning will manage event.
  - Status meeting schedule will be established.
  - Escalations will be agreed upon (who else needs to know).
  - All communications regarding the event and its impact will be approved by the Crisis Manager.
  - Additional support requirements will be defined (who else needs help).
Command Center Locations

- **Command Center for Site Recovery**
  - Primary
  - Secondary
- **Command Center for Business Function Recovery**
  - Primary
  - Secondary
Human Resource Management

- Employee Injuries/Fatalities
- Reassigning of non-essential staff to support recovery
- Temporary Help/Contractors
- Family Issues
- Financial Assistance
Administrative Support

- Travel, Food and Accommodations
- Copying
- Answering Phones
- Arranging Courier Services
- Meeting Scheduling/Minutes
Finance Issues

- Provide Channel of Authorization for Expenditures
- Record Emergency Costs
- Provide Cash Advances
- Order Replacement Supplies and Equipment
- Provide Immediate Payment of Expenditures Required to Support Recovery Effort
- Expense Report Processing
Recovery Communications

- Recovery Status
- Updates to Contingency Information Line
- Communication to Employees
- External Communications
- Client Communications
- Problem Management
Site Recovery Plan

- Notification and Identification of Emergency Situation
- Initial Damage Assessment
- Business Risk Assessment
- Decision to Activate Plan
- Declaration Procedures
- Notification Procedures
- Command Center Activation
#6: Exercising the Plan

- **Recovery Plan Testing**
  - Table top exercises with recovery teams
  - Integrated test
  - Alternate site test objectives
  - Technical support resources are sufficient to meet RTO
  - Technical support resources are adequate to support end users
  - Employee awareness of issues – transportation, lodging, building access, recovery location
  - 30% of assigned seats tested

- **Event Management Test Objective**
  - Verify correct contact numbers for everyone on your ENL
  - Estimate how long it takes to contact everyone
  - Bring decision-makers/stakeholders and response team members together and walk through an event
Call Notification Exercise

• **What to Do:**
  - Call everyone on your Emergency Notification List and validate their phone numbers are accurate and that your team is prepared to respond.

• **How to Do It:**
  - Call them at work but require a response - no voice mails
  - Call them at home
  - Page them. If they do not respond within a certain timeframe, try again or try reaching the backup - require a response
  - Page them and have them call into a conference bridge

• **Why We Do It:**
  - Validate the phone numbers are accurate
  - Find out how long it takes to reach everyone
  - Determine what percentage of people are unavailable
  - Exercise Call Notification Procedures
Use the test to find out how prepared your teams are to respond…

“This has been a test. In the event of an actual emergency, I’m outta here!”
Walk-Through Exercise

- **What to Do:**
  - Walk through all or a portion of your recovery procedures with your teams

- **How to Do It:**
  - Set up meeting date and time
  - Contact Team Members and invite them
  - Walk through the plan with the team members
  - Take notes of comments, action items

- **Why We Do It:**
  - Use as Training and Awareness for Team Members
  - Identify plan weaknesses or deficiencies
  - Improve recovery capabilities
Simulated/Actual Exercise

• **What to Do:**
  - Simulate execution or actually execute recovery procedures

• **How to Do It:**
  - Create test scenario
  - Obtain Management approval
  - Team members respond to scenario by executing recovery procedures
  - Take notes of comments, action items

• **Why We Do It:**
  - Use as Training and Awareness for Team Members
  - Identify plan weaknesses or deficiencies
  - Improve recovery capabilities
  - Validate alternate site readiness
Recommended Alternate Site Test Requirements

• Were transportation issues addressed as part of the test? Was the alternate site environment established independent of the primary location?

• Did the business unit recall and implement a sampling of stored electronic and hardcopy vital records, procedures manuals, forms, etc.?

• Was the DR Server(s) restored with backup information from offsite storage?

• Was the business able to connect to all required servers and directories and applications?

• Did end users validate functionality?

• Did the business navigate all the way through each application or process?

• Were phone, modem, and fax numbers transferred and did they work as planned?

• Does this location meet your minimum recovery capacity requirements? (phones, desktops, etc.)
Highly Recommended Alternate Site Test Components

• Was your management team notified at time of test?
• Were critical vendors contacted at time of test?
• Were interdependencies contacted at time of test?
• Did you contact CDS for mail delivery at time of test?
• Was your problem management strategy tested during the test?
• Was the Fidelity Network available on time and with sufficient bandwidth (for external sites)
• Was network response time acceptable?
• Was all information required for recovery available and did backups have good data?
• Was the desktop image complete and current and restored in time required?
• Was the business able to print? (LAN, PEGA, WIRE, Mainframe etc)
• Were end-user directions provided?
• Were there sufficient number of phones, inbound and outbound trunks available and tested?
• Was voice recording tested? (if applicable).
• Were phone instructions provided to the business users?
• Was voice mail available at the alternate site?
• Were you able to send and receive info via modem?
• Were action items documented and submitted to business unit management?
Success Criteria

- An actual exercise should be considered successful if the required resources, equipment, and connectivity of voice and data are recovered to the satisfaction of the business unit at the designated alternate site within the timeframe required.

- An actual test should be considered successful if the above didn’t happen so you can fix it before a real incident.
Compact Exercise

• **What to Do:**
  - Execute call notification and actual/simulated recovery exercise during one event

• **How to Do It:**
  - Create test scenario/Obtain Management approval
  - Simulate disaster scenario and contact team members
  - Team members respond to scenario by executing recovery procedures
  - Take notes of comments, action items

• **Why We Do It:**
  - Use as Training and Awareness for Team Members
  - Identify plan weaknesses or deficiencies
  - Improve recovery capabilities
  - Validate Alternate site readiness
Exercise Planning

- Determine what part of the Plan you want to exercise
- Determine type of exercise to be conducted
- Identify exercise participants
- Agree upon scope of the exercise
- Agree upon objectives of the exercise
- Set exercise date
- Obtain management approval for exercise
- Build exercise plan
- Build exercise timeline
- Walkthrough exercise plan and timeline with team
- Finalize plan and timeline
Conducting the Exercise

- Have final meeting with team and make final “go/no-go” decision for exercise
- Conduct exercise
  - Update timeline as events occur
  - Conduct exercise status meetings if needed
  - Manage problems as they arise
  - Make list of action items to be addressed
  - At conclusion of test, conduct a short debriefing session with the team
Business Recovery Exercise
Exercise Date: ____________

In the event of an unexpected business disruption at the primary site, recovery procedures exist to recover the critical functions of this company at the alternate site.

Scope: The scope of this exercise is limited to a site outage at the primary site only and validating the recovery capabilities of the critical functions performed at that site by this company.
Objectives: The objectives of this effort are as follows:

- Validate that recovery procedures exists for all critical functions at this site
- Validate the current recovery procedures will be available at the alternate site at the time of need
- Validate that the facilities at the alternate site are sufficient and properly equipped to allow for recovery of the critical functions within the timeframe required
- Validate the desktop connectivity at the alternate site is complete to support the critical functions
- Validate the recovery procedures are complete and accurately reflect the steps required to execute recovery of the critical functions
Sample Exercise Plan (cont’d)

Assumptions: The assumptions of this effort are as follows:

- Recovery teams will actively participate in the validation of the test objectives at the alternate site and for all critical business functions performed on the primary site.

- Each group participating in the test will follow the recovery procedures as documented. Any deviation from the procedures will be noted and reviewed in the test follow-up meeting.

- Necessary Network connectivity exists or will be implemented as part of the recovery exercise at the alternate site.
**Business Requirements:**

To recover the critical functions from the primary site within a timeframe which will allow this company to meet the business requirements of Fidelity Investments with minimal disruption to Fidelity’s Customers and the business units which are dependent on these functions to execute their critical business functions.
Sample Exercise Plan (cont’d)

**Contingency Planning Objectives:**

1. Validate the recovery procedures for the business functions at this site can be successfully implemented in the event of emergency at the designated alternate site.
2. Verify that the business units have full functionality in the designated alternate site.
3. Verify that the business units have full connectivity in the designated alternate site.
4. Validate the ability to send and receive the identified critical inputs and outputs of these business functions.

**Business Function Objectives**

1. Validate that the recovery procedure for this critical function is complete.
2. Validate that all required data for recovery is stored offsite and can be retrieved at the time of need.

**Telecom Objectives**

1. Support the business unit in validating the site recovery.
2. Test the implementation procedures of the alternate site to support this site outage.
3. Validate the full functionality and connectivity exists at the alternate.
### Sample Exercise Timeline

<table>
<thead>
<tr>
<th>Task</th>
<th>Responsible</th>
<th>Estimated Start/Stop time</th>
<th>Issues or comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Simulate Disaster Declaration and notify Teams</td>
<td>BCP and Emergency Mgmt Team Leader</td>
<td>8AM - 8:10AM</td>
<td></td>
</tr>
<tr>
<td>2. Team Arrives at alternate site</td>
<td>Team members</td>
<td>8:15AM - 9:30AM</td>
<td></td>
</tr>
<tr>
<td>3. Retrieve offsite storage and unpack</td>
<td>Off site storage Team</td>
<td>8:10AM- 11AM</td>
<td></td>
</tr>
<tr>
<td>4. Build out alternate site to support site outage</td>
<td>FTC Team</td>
<td>8:15AM - 2PM</td>
<td></td>
</tr>
<tr>
<td>5. Assigned staff to workstations as they become available and validate desktop connectivity</td>
<td>Business Function Team Leaders</td>
<td>8:30AM 0 2PM</td>
<td></td>
</tr>
</tbody>
</table>
Conducting the Exercise

• Have final meeting with team and make final go/no-go decision for exercise
• Conduct exercise
  – Update timeline as events occur
  – Conduct exercise status meetings if needed
  – Manage problems as they arise
  – Make list of action items to be addressed
  – At conclusion of test, conduct a short debriefing session with the team
Post - Exercise Tasks (Post-Mortem)

• Conduct a formal post-mortem on the test with the team members
  - Compare test results with test objectives
  - Note discrepancies
  - Document action items and due dates
• Publish test results and action items to Senior Management and Corporate Contingency
• Follow-up on action items till complete
• Update Plan documentation as needed
Sample Exercise Results

Business Recovery Exercise Results

Exercise Date _____

On _______ a recovery exercise was executed by this company’s recovery teams with the support and cooperation of FTC. An outage was simulated at our primary site, a disaster was declared, teams were contacted and assembled at the alternate site and our recovery plans for the critical functions at the primary site were executed.
The primary objectives and results of this exercise were as follows:

- Validate that recovery procedures exists for all critical functions at this site  
  COMPLETE

- Validate the current recovery procedures will be available at the alternate site at the  
  time of need  
  COMPLETE

- Validate that the facilities at the alternate site are sufficient and properly equipped to  
  allow for recovery of the critical functions within the timeframe required  
  PARTIAL

- Validate the desktop connectivity at the alternate site is complete to support the  
  critical functions  
  PARTIAL

- Validate the recovery procedures are complete and accurately reflect the steps  
  required to execute recovery of the critical functions  
  COMPLETE

A complete list of actions items is included for your reference
## Sample Exercise Action Items

<table>
<thead>
<tr>
<th>Action Item</th>
<th>Responsible</th>
<th>Estimated Complete</th>
<th>Issues or comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Update ENL with corrected phone numbers</td>
<td>BCP</td>
<td>7/20/xx</td>
<td>4% of staff unreachable due to inaccurate phone numbers</td>
</tr>
<tr>
<td>2. Update recovery procedures to reflect changes identified</td>
<td>Business Function Team</td>
<td>8/15/xx</td>
<td></td>
</tr>
<tr>
<td>3. Include missing data in offsite storage</td>
<td>Off site storage Team</td>
<td>7/25/xx</td>
<td>Missing manual to be included</td>
</tr>
<tr>
<td>4. Provide connections to SASVTAM for 3 desktops identified</td>
<td>FTC Team</td>
<td>8/3/xx</td>
<td></td>
</tr>
<tr>
<td>5. Install 2 additional phone lines and larger white board in the Command Center</td>
<td>BCP</td>
<td>8/15/xx</td>
<td></td>
</tr>
</tbody>
</table>
#7: Maintain the Plan

• Plan reviews should be performed on a regularly scheduled basis and must occur at least annually.

• Reviews should be linked where possible to change management controls to ensure the details of significant business changes are correctly incorporated into the plan.

• Results of review should be formally reported and where appropriate, the plan should be updated.
#8: Training and Awareness

- Building evacuations
- Shelter-in-Place
- Severe weather protocol
- Short and long term building outages
- Employee notification procedures
- Employee contact/call in procedures
  - Employee contingency information line
  - Call trees
- Emergency Reference Guides
- Contingency Information Lines
Execution...

• Planned Events
  - XIX Salt Lake City Winter Olympics, February 2002
  - Democratic National Convention, July 2004 in Boston
  - Republican National Convention, August 2004 in NY

• Unplanned Events
  - World Trade Center Disaster, September 2001
Business Continuity Strategy at Fidelity

- Committed at the highest level of Fidelity
- Each business has a Business Continuity Planner (BCP)
- Business functions are classified based on time-sensitivity to recovery (AAA-D)
- Customer facing functions operate in at least two geographically dispersed locations
- Time-sensitive back-office operations operate in multiple locations and/or have 4-hour or less recovery timeframes
- Alternate site tests performed four times a year per production site
Planned Event - example...

- Winter Olympics 2002 in Salt Lake City, UT
  - Road closures
  - Limited emergency vehicles
  - Protestors
  - Public transportation impacts
  - Terrorism
"Many financial services firms found that they were unable to maintain operations on September 11th in the face of simultaneous disruptions to people, facilities, communication systems, and the transportation network. September 11th demonstrated that firms need to re-examine the business continuity strategy for every aspect of their operations."

Ted DeZabala, Partner, Deloitte & Touche, New York

The World is riskier, and it’s not just terrorism..
How Close Were We (Fidelity Investments)?
Arial View After the Attack
What We Learned from 9/11...

- Testing was the key to the success of the recovery
- Critical operations in a single site are bad business
- We don’t have problem by business, we have problems by building
- Transportation was a major issue in the first few days
- Incomplete/inaccurate inventories make the insurance claim difficult
- People do not want to travel away from their families
- Very few business operations stand alone
- Voice is harder than data to recover
- Some of our vendors were in trouble too
- The devil is in the details
Planning Considerations Expanded Post 9/11

- The events of September 11th and the resulting business disruptions have highlighted the need for companies to revisit the assumptions underlying their disaster recovery and business continuity plans. Such plans have primarily focused on the loss of systems and information or the inability to access a main processing facility. After September 11th, planning considerations have expanded to include:
  - loss of key employees or emotionally-impacted staff,
  - loss of access to major business districts,
  - long-term operation at back-up sites,
  - need for alternative back-up sites,
  - availability of contact information for key employees,
  - loss of paper documentation, and
  - loss of critical vendors/business partners.
The Good News for Fidelity…

• We experienced no loss of life in New York and injuries were not serious. All the required personnel were available.

• The Full Market remained closed, allowing initial recovery efforts to be augmented and the business to prepare to conduct business for a long period of time in the alternate sites.

• Two-way pagers. They worked consistently when other forms of communication were either busy or completely unavailable.

• Buildout of all of the alternate sites occurred very quickly to allow critical business functions to resume.

• Bench Strength - All of the people involved exhibited teamwork, flexibility, availability and an excellent attitude. Many volunteered to work longer hours and additional shifts to get the job done.

• The ability to use alternate network resources to get the New York Operations back online quickly and to provide redundancy for network lines running in backup mode.
Planning Assumption Cautions

• **Do not build your disaster recovery plan just for a short interruptions in business and only for the data center - plan for a long term outage**
  - This type of planning assumption led many business units to assume that plans only needed to be done for very small numbers of employees or only for their technology infrastructure. This led to scrambling during a disaster and not necessarily the best recovery plan for the employees involved. Recovery is for the whole business.

• **Do not assume only one disaster strikes at the same time**
  - We lost access to World Financial Center (WFC) and simultaneously lost access to key buildings in Boston that were evacuated as a precaution
  - This led to multiple disaster declarations in diverse locations that had to staffed at the same time by multiple support groups

• **Do not assume required infrastructure for recovery is in place**
  - Telecommunications, power and transportation were all impacted. No one had ever imagined a scenario where all the planes in the country would be unavailable.
Planning Assumption Cautions (cont’d)

• **Do not assume your disaster recovery team and the rest of the corporation survive the attack**
  - We were unaffected by this, but other New York based corporations lost entire recovery teams and the documentation required to recover
  - Other corporations were struggling to do required day-to-day business functions because those responsible died in the event and the training materials for the position were stored in the building

• **Do not assume you will be able to get the required equipment from your vendors very quickly**
  - This did not impact us, but the drop in the economy left many vendors with little or no inventory. The ability to obtain required equipment quickly was hampered.

• Do not assume you will be able to fly/transport your team members or associates anywhere
  - Airport closures, subways closures, road closures
  - Develop alternate transportation plans
Follow these 11 steps to develop a solid recovery program for your business
Step 1
Identify Business Recovery team

- Identify your team and make certain they know how to reach you in an emergency
Step 2
Identify Business Vital Records

• Identify vital records
  - procedural manuals
  - forms
  - vendor lists
  - contact lists
  - customer lists
  - contracts
  - source documents
Step 3
Identify Business Functions

- Identify the business functions for functional areas
- Perform risk and business impact analysis for each function
- Establish the recovery time for your business functions
- Identify minimum staff requirements
- Identify interdependencies (internal and external)
Step 4  
Identify Desktop Requirements

- Minimum desktop configuration
- Application connectivity
- Voice Requirements
  - Phones (desktop, Aspect, turret)
  - Fax (dedicated, networked)
  - Modems
- Print requirements (dedicated, networked)
- Proprietary software running on desktop
Step 5
Define Recovery Strategy

- Develop recovery strategy for business functions based on the recovery priority

<table>
<thead>
<tr>
<th>TSR</th>
<th>Downtime Allowable</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>None, immediate recovery</td>
</tr>
<tr>
<td>AA</td>
<td>4 hours</td>
</tr>
<tr>
<td>A</td>
<td>Same day</td>
</tr>
<tr>
<td>B</td>
<td>Within 24 hours</td>
</tr>
<tr>
<td>C</td>
<td>48-72 hours</td>
</tr>
<tr>
<td>D</td>
<td>72 hours or more</td>
</tr>
</tbody>
</table>
Step 6
Internal Site Survey

• Survey existing sites
• Identify equipment/phone services
• Identify desktops to be used for contingency
• Identify staff to be displaced or moved to off shift
Step 7
External Site Recovery

- Prepare Request for Proposal (RFP) which includes all requirements
- Identify essential vs. “nice to have”
- Receive proposals from vendors
- Compare requirements against costs - “apples to apples”
- Visit sites identified as potential vendors
- Select vendors
Step 8
Internal Systems

- Identify all platforms and applications supported by internal systems group
- Identify recovery priority for each application
- Identify recovery strategy which meets the business requirements
- Develop recovery procedures for critical applications
Step 9
Document Plan

- Pull the information together into a plan document and distribute
Step 10
Train Your Staff

Everyone should know the answer to the question:

If you couldn’t get back in your building today, what would you do next?
Step 11
TEST, TEST, TEST

- Event Management tests
- Alternate site tests
It could happen anywhere, anytime...

Don’t be the one taken by storm!!
Websites

- **Industry Group Websites**

  **DRI International**
  www.drii.org

  **Continuity Insights**
  www.continuityinsights.com/ conf.cfm

  **Contingency Planning and Management**
  www.contingencyplanning.com

  **Disaster Recovery Journal**
  www.drj.com/

  **Global Association of Risk Professionals (GARP)**
  www.garp.com

  **Professional Risk Managers International Association (PRMIA)**
  www.prmia.org

  **Institute of Internal Auditors**
  www.theiia.org
Other Factors to Consider in Your Planning...

- Weather
- Cyber Terrorism
- Mobile Workforce Cost of Down Time
- Enterprise Applications
- IT Infrastructure Regulations
- Economy

Source: A New Paradigm for Business Continuity Management by Deloitte-Touche Tohmatsu
Business Continuity Management - Questions?

- People
- Business Continuity Management
- Business Resumption
- Strategy
- Execution
- Disaster Recovery
- Emergency Response