



Business Continuity Planning Basics

Terri Sinski
Disaster Preparedness Coordinator
BELFOR Property Restoration

Catastrophe Readiness Fair
Sept 24th 2009



What is Business Continuity Planning?

- Process of developing advanced arrangements and procedures that enable an organization to *respond* to an event in such a manner that critical business functions continue with planned levels of interruption or essential changes.
- Goal: To preserve the assets of an organization in the event of a disaster: its operational capability; its reputation and image; its customer base and market; its profitability.

***It's not how you do business....
its how you STAY in business!***

Question: **What are we Planning for?**

Answer: To protect the Business Organization from Disaster.

What is a
Business Organization?

- Any organization that provides goods and services, either to an individual, to other business organizations or to the public.

What is a Disaster?

- Any event that creates an inability on an organizations part to provide critical business functions for some predetermined period of time.

Factors that Increase a Company's Vulnerabilities

- **Human:** People must have the knowledge, skill and ability (KSA's) to execute your business process.
- **Resources:** Materials or infrastructure required.
- **"Extended Enterprise":** When the activities executed to deliver a product or service extend beyond the boundaries of the company, (vendors, suppliers, sub-contractors)

Increased dependency on others increases vulnerability!

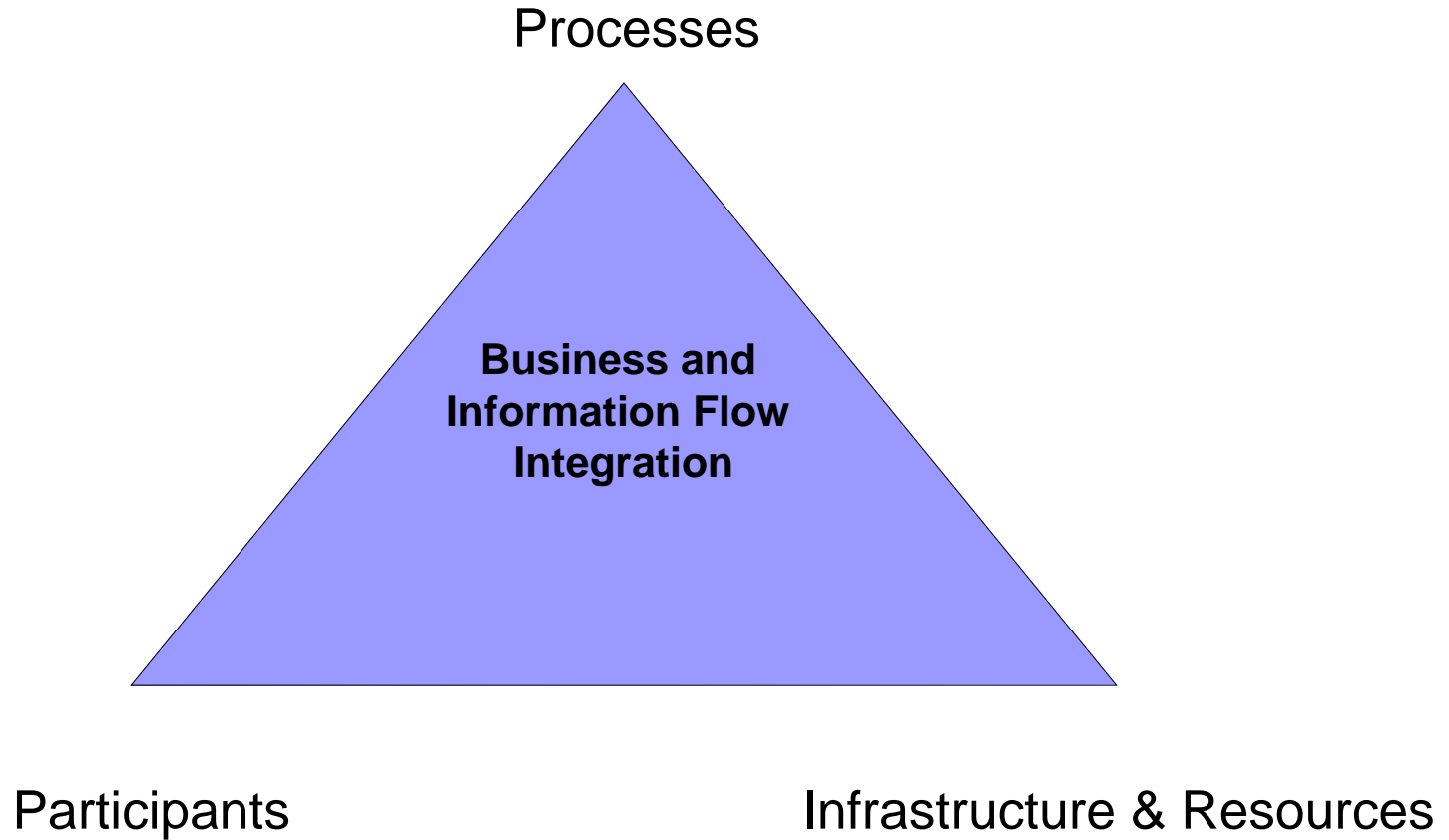


Factors that increase a Company's vulnerabilities

- Business process: The chain of activities required to deliver a product or service to a customer.
- Participants: The people who perform these activities.
- Infrastructure & Resources: Material and equipment used in the execution of the business process.

The same elements that make an Integrated Organization successful also make the organization vulnerable.

Integrated Organization



Types of Disaster

- Act of Nature: hurricane, flood, earthquake, pandemic, etc.
- External Man-Made: terrorism, security breach, cyber crime, fraud, economic recession.
- Internal Unintentional: accidents, computer failure; fire, loss of key personnel, human error.
- Internal Intentional: strike, sabotage, disgruntled employee



Impacts of Disaster:

- ❑ Failure of an individual infrastructure element.
- ❑ Long term interruption of a critical information flow.
- ❑ Long term interruption of a critical business process.
- ❑ Long term business interruption.
- ❑ Complete business interruption.

Consequences of a Disaster

- Immediate
 - -Damage from the event
- Long Term
 - -Unavailability of infrastructure or resources
 - -Loss of information
 - -Loss of key personnel

There is an important distinction between damage caused by the event and the impact on the business process.

Disasters do happen

- Comdisco survey: 19% of companies experience an IT failure lasting more than 24 hours.
- Hiles: 60% to 90% of companies are out of business within 24 months following a disaster
- Fulmer: 93% of companies without plans fail within 5 years after the disaster
- Fortune 500 companies- downtime costs \$96,000 per minute

Types of Plans

- **Business Continuity Plan (BCP)**
 - Sustains business functions during and after a disruption.
- **Business Recovery Plan (BRP)**
 - Restoration of business process after a disruption but doesn't ensure continuity through out the emergency.
- **Continuity of Operations (COOP)**
 - Restoring essential functions at an alternative site for up to 30 days. Typically refers to government organizations.
- **Disaster Recovery Plan (DRP)**
 - Typically refers to IT focused plan designed to restore operations of a disrupted system, application or computer facility.
- **Incident Response Plan**
 - Detailed procedures to address a specific type of disruption or event.
- **Occupant Emergency Plan (OEP)**
 - Plans for evacuation or shelter in place. Provides for coordinated procedures for minimizing loss of life or injury for facility occupants.



Business Continuity Strategy

What is Business Continuity Strategy?

- Contingency Planning is based on:
 - Understanding the organization.
 - Understanding the tools that support the operations.
 - Evaluating the loss of such tools.
 - Determining WHO will handle a crisis situation and.....
 - HOW they will handle it.

Successful Approach to BCP

- Must involve the entire organization
- Include manual records and information, not just computers.
- Pay attention to detail.
- Address small sections at a time.
- Must include a Risk Assessment
- Must include a Business Impact Analyses

Objectives of a BCP Strategy

- Framework- Establish a framework for evaluating business process which allows for a focused approach
 - Methodology – A structured approach
- Pragmatic- Cost effective and operable recovery plan which enables the **entire organization** to complete the business process in the event of a major disruption

Must be user friendly. People must be able to follow the plan!
- Mitigation- Minimize the impact of the disaster on the organization
 - Stay as close to normal activities of your people as possible



Objectives of a BCP Strategy

Structured Approach

1. **Assessment Phase**
 - Risk Assessment , Impact Analysis, Choose Solutions
2. **Implementation Phases**
 - Write Plans, Documents Training
3. **Management Phase**
 - Test, Review, Update



Assessment Phase

Risk Assessment – Business Impact Analysis
Choose Solutions

Risk Assessment / Analysis

- Risk analysis is the process of:
 - Identifying the risks to an organization.
 - Assessing the *critical functions* necessary for the organization to continue business operations.
 - Risk analysis often involves an evaluation of the *probabilities* of a particular event.



5 Layers of Risk

1. External:

Natural disasters

Man-made disasters

(Affect everyone; employees, suppliers, customers.)

2. Facility Wide:

Affect only your organization at 1 or more sites.

3. Data Systems:

Viruses, hackers, accidental breakdowns.

4. Department Risks:

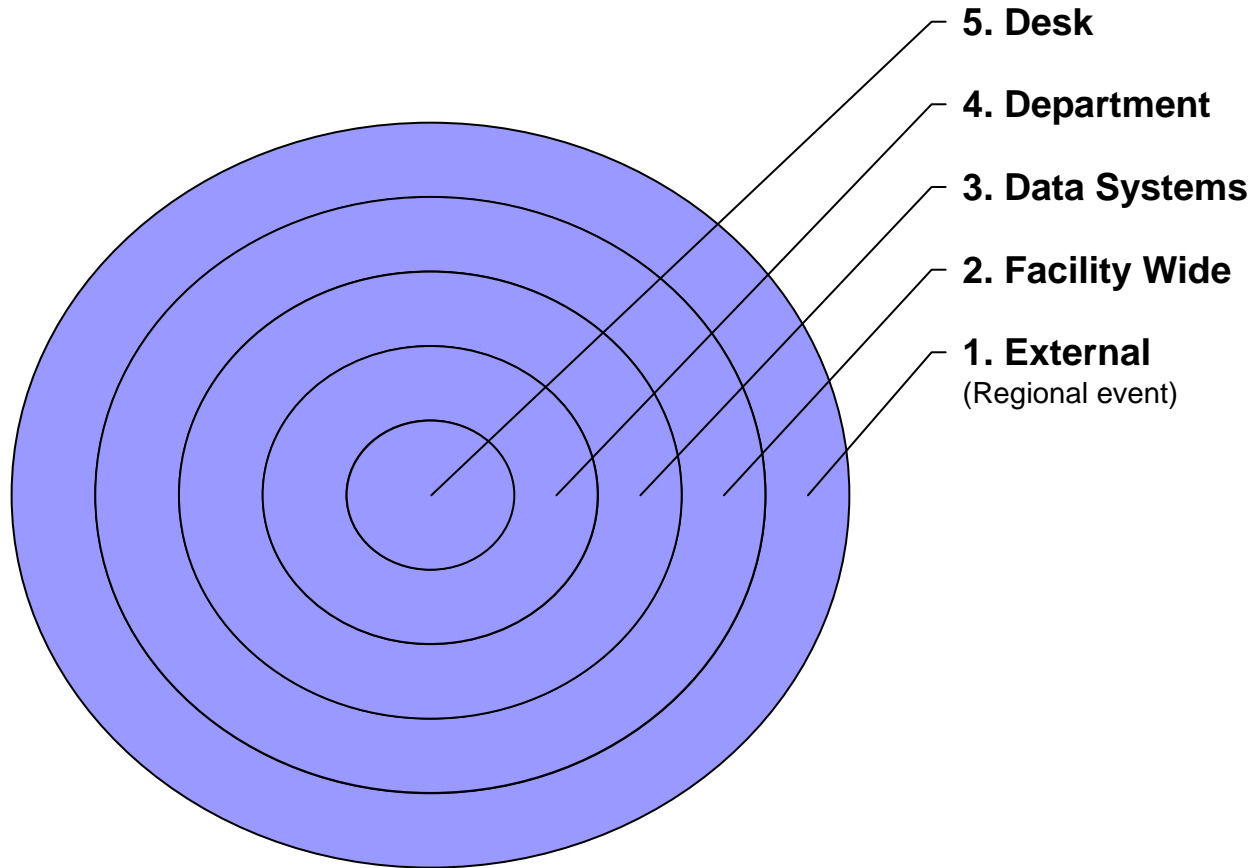
Key employees, specific files, key equipment, vital records.

5. Your Desk:

What do you need at your desk to do your job?

What information needs to be protected? (Clean desk policy)

5 Layers of Risk



Risk Evaluation Considerations:

■ Identify Risks and Threats

- What would effect your particular organization?
- Start by creating a list of potential threats based on the 5 Layers of Risk.

■ Identify Assets - Internal Resources and Capabilities

- Personnel- Response Teams, security, specialists
- Equipment- Fire Protection, communications, emergency generators
- Facilities-EOC (Emergency Operations Center), shelters, media areas

■ Seek Outside Opinions - Community

- Research what local authorities and utilities plan to do in an emergency. Ie., County Executives Office, Local OEM, (Office of Emergency Management), National Grid, FEMA etc.
- Seek out trade organizations related to your industry/business.

Business Impact Analysis (BIA)

- BIA - The process of analyzing all business functions and the effect that a specific disaster may have upon them. Serves as a tool to measure the effect of resource loss and escalating losses over time.
- Objective- To quantify the loss impact from both a business interruption (number of days) and a financial standpoint. \$\$ (Data derived from Risk Assessment activities assists this process)

Developing a BIA

- The development of a BIA typically involves interviewing all department heads (members of planning team) to determine and identify *mission critical functions*.
- There are numerous business models, resources, tools/forms and software available to assist corporations with this interviewing and data collection process.
- Regardless of the method chosen the most important factor is that all members of the planning team are aware of the criticality of the interviews and the questions being asked of their departments.

Gain support from department heads by appealing to their area of expertise!

Choose Solutions

- The final step of the Assessment Phase after the BIA is completed is to choose solutions.
- Appropriate solutions are chosen based on data gathered from both the Risk Assessment and BIA.





Implementation Phase

Write Plans - Document -Train

Implementation Phase

➤ Gather data:

- Contact information (staff and vendors)
- Resource requirements
- Existing plans
- Emergency Operations Center
- Alternate site (Hot site)

Plan Format

- The Plan should address the impact not the cause of the disruption, including:
 - Loss of facilities
 - Loss of personnel
 - Loss of communications
 - Loss of suppliers/customers
- Developing the written plan
 - Create plan templates
 - Use examples provided by BCP software or tailor your own to meet your industry needs.



General Outline for BCP

1. Introduction

- Overview of plan's purpose
- a. Instructions
 - When and how to use the plan
- b. Mission Statement
- c. Objectives
 - What is the plan trying to accomplish?
- d. Scope
 - What are the limits of the plan?
- e. Assumptions
 - What facts are being assumed by the company or department? (e.g. minimal staffing will be present, the main facility will be unavailable)

General Outline for BCP

2. Alert/Notification Procedures

- Call trees, e-mail, etc.
- Notification Procedures

3. Declaration Sequence- **Response**

- Immediate steps taken after a disaster is declared.
Who declares it?
- Organization Charts/Flow Charts

4. Departmental Action Plans

- Alternate Site (Hot Site)
 - Where is it? How do you get there?
 - What is present at that location?

5. Recovery

- Getting Infrastructure back to normal
- Emergency Response Vendor Agreements
- Return to primary site, When? Procedures?

General Outline for BCP

6. Maintenance and Testing

- Coordinator-One person responsible for changes
- Schedules

7. Outside Support

- Vendor, Supplier contact list

8. Glossary

9. Forms

- Samples of forms to be used
- Sample press releases

10. Supplies

- List all supplies needed, at least for the first 48 hours
- What software is being used at alternate site?

11. Travel

- Will travel be required for team members?
- Lodging? Food?

Fundamental Questions

➤ WHO?

- Is responsible for maintaining the Plan?
- Is responsible for activating the Plan?
- Will execute the procedures?
- Must be notified?
- Will handle the media/press?
- Will decide to return to normal operations?

Fundamental Questions

➤ WHAT?

- Actions must be taken to execute the Plan?
- Are the contact numbers of key personnel?
- Resources are needed to execute the Plan?
- What resources are needed at the alternate site?

Fundamental Questions

➤ WHEN?

- Will the Plan be activated?
- Will personnel change shifts?
- Will the Plan be deactivated?

Fundamental Questions

➤ WHERE?

- Are resources located?
- Will operations be re-located?
- Are locations of special activities (Command Center)
- Can employees go to get information?



Fundamental Questions

➤ HOW?

- Will operations be shifted to alternate site?
- Will personnel get to alternate site?
- Will notifications be made?
- Will operations be returned to normal?

Plan Format

➤ Distribution

- Only those who need it should have access to the plan
- Some people may only have access to parts
- Must be easily accessible to those who need it
- Store copies at alternate site
- Access from home or away
- Each copy must be numbered and dated
- Destroy old versions, keep a record
- Have backup copies on disks



Management Phase

Test – Review - Update

Management Phase

- The BCP should be tested on a regular and routine basis.

Why Test?

- Testing and updating a BCP is essential as every business organization is continuously evolving and changing.
 - New Products are purchased
 - New policies and regulations are developed
 - Staff members need to review the plan to maintain an awareness of procedures.
 - Opportunity to identify organizational gaps and weaknesses.

The Plan is a living document, it will change and improve over time as the business organization grows.

Various Testing Methods:

Check List Testing

- Ensures that adequate supplies are stored at alternate locations.
- Contact info of vendors, suppliers, customers and staff are current.
- Essential forms and tools are available to perform critical tasks.

Emergency Drills

- Evaluate Employee readiness.
- Evaluate equipment readiness and use.

Table Top Exercises

- A scenario is presented to lead discussion.
- The group uses existing procedures to lead the discussion.
- Tests the plan's procedures but also the knowledge of the participants.
- Tests staffs reaction to stressful environment.
- **Creates an awareness of the BCP!**

Management Phase

(Testing Methods Continued)

On Site Application Testing

- Objective: To see if the application can run on a back-up system.
- Identify any procedural changes that may affect the plan.
- Typically conducted quarterly.

Off - Site Application Testing

- Test at the alternate location (Hot Site)
- Usually conducted semi-annually
- Tests communication links, time to get up and running and employee familiarity with the Hot site
- Provides information about the Plan's procedures, equipment and personnel
- Usually announced or pre-scheduled
- Indefinites possible problems to be corrected

Management Phase

Testing

- Testing should be conducted after employees are trained and aware of the Business Continuity Plan.
- Testing process increases employee confidence and performance.
- Testing creates opportunity to update organizational changes.
- Testing with out training can lead to disaster.

Too often a BCP is written and placed on a shelf.
This makes the Plan useless.

Testing creates organizational awareness and ensures that the plan will guide the organization and the participants through an actual disaster should one occur!

BCP Resources

- **Association for Contingency Planning**
www.acp-international.com
- **Catastrophe Readiness Clearing House**
www.catastrophereadinessclearinghouse.org
- **CPE Contingency Planning Exchange**
www.cpeworld.org
- **Continuity Insights**
www.continuityinsights.com
- **FEMA**
www.fema.gov
- **DRI International (Disaster Recovery Institute)**
www.drii.org
- **Suffolk County Dept of Fire & Rescue Services (OEM)**
www.co.suffolk.ny.us
- **Nassau County Office of Emergency Management**
www.nassaucountyny.gov