Business Continuity Management
The Basics
September 24, 2003
Background
What is Business Continuity Management?

- A Program that manages risks
- Planning for recovery and continued availability of operations in face of foreseeable events
- Designing and implementing secure, fail-proof (fault-tolerant) systems for continuous availability
- Designing and implementing threat prevention and detection systems
- Encompasses development of procedures, acquisition of resources, testing and maintenance
Risk Management

- Identify exposures to loss
- Examining the feasibility of alternative risk management techniques
- Selecting what appears to be the best risk management techniques
- Implementing the chosen risk management techniques
- Monitoring, testing, and improving the risk management program
# Business Continuity Objectives

- Provide for safety and well-being of people on premises
- Continue critical business operations
- Minimize immediate damage and losses
- Establish management succession and emergency powers
- Limit financial losses and hardships
- Restore workforce, facilities, and equipment in a timely manner
Business Continuity Priorities

Define priorities in terms of relevance and criticality:

1. Human safety issues
2. Collection of essential data and records, media protection and recovery
3. Protection and restoration of physical equipment
4. Preservation and restoration of the working environment
Terminology and Concepts
Disaster Phases …

First 72 Hours

Emergency Response

Life-Safety

Damage Assessment

1 Day – 3 Weeks

Short-Term Recovery

Business Recovery

Months – Years

Long-Term Recovery
<table>
<thead>
<tr>
<th>Acronyms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCP:</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>BCM:</td>
<td>Business Continuity Management</td>
</tr>
<tr>
<td>DRP:</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>BRP:</td>
<td>Business Resumption Plan</td>
</tr>
<tr>
<td>BIA:</td>
<td>Business Impact Analysis</td>
</tr>
<tr>
<td>MAO:</td>
<td>Maximum Allowable Outage</td>
</tr>
<tr>
<td>RTO:</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>RPO:</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>SPOF:</td>
<td>Single Point of Failure</td>
</tr>
</tbody>
</table>
Components

- Comprehensive coverage includes the following documented procedures:
  - Emergency response and evacuation procedures;
  - Declaration procedures;
  - Executive and employee notification procedures;
  - External communication procedures;
  - Recovery resources and procedures for the mobilization of employees and resources; and
  - Employee responsibilities and action steps for emergency, backup operations, recovery and restoration of operations.
Approach
Business Continuity Planning Methodology

- Current State Assessment
- Risk Assessment
- Business Impact Analysis

- Availability Strategies
- Recovery Strategies
- Plan Documentation

- Resource Acquisition/Implementation
- Plan Training and Exercising
- Plan Maintenance & Change Control

Process Improvement
• **As-Is State** – What capabilities currently exist to mitigate risks?

• **Risk Assessment** – What are the key threats to your business?

• **Business Impact Analysis** – What are your business’s major business processes, the impact of disruptions, and your availability and recovery objectives?
What Is An Initial Assessment?

• Enterprise-Wide Operational Impact Assessment That Analyzes:
  – Business Risk
  – Operational Impact
  – Financial Implications
  – External Factors

• Strategically Identifies Business Risks, Vulnerabilities, and “Gaps”
Project Scope

• Entire Enterprise?
• Emergency Response, Business Recovery, IT Recovery?
• Project Leader?
• Activities Timeline?
• Responsibilities?
Initial Assessment

• Hazards
  – Internal vs. External
  – Natural vs. Man-made

• Operational Vulnerabilities
  – Critical Functions
  – Vital Records
  – Key Systems

• Business Risks
  – Competitive Strategies
RISK ASSESSMENT

• Natural – floods, earthquakes, tornadoes, etc.
• Human:
  – Man Made – fires, explosions, accidents, bombings, cyber crime, etc.
  – Political – riots, civil disturbances, terrorist attacks, etc.
• Technological – telecommunications, equipment failure, etc.
BUSINESS IMPACT ANALYSIS

- **Business Process Analysis**
  - High-level understanding of process flow through interviews with appropriate functional management and documentation review

- **Operational Impact Analysis**
  - Define Maximum Allowable Outage (MAO) or Recovery Time Objective (RTO), and Recovery Point Objective (RPO) for each business process

- **Financial Impact Analysis**
  - Difficult to quantify and fairly personnel-intrusive
  - Only provides “order of magnitude” accuracy over a period of time
  - Used for cost-justification of strategy implementation
Objectives of BIA

• Identify Critical Functions
• Understand Flow of Information, Materials, & Services
• Determine Organizational Dependencies & Resource Needs
• Describe Operational & Financial Impacts
• Define Timeline For Restoring Critical Functions & Critical Data
**Who Will You Interview?**

- Steering Committee
- Project Sponsor
- Business Unit Managers
- Key IT Representatives
- External ISP/ASP Provider
- Other Key Vendors/Suppliers
- Building Owner/Management
Operational Impact Analysis

• Purpose:
  – Identifies Organizational Implications & Dependencies
  – Highlights Interrupted Functions & Outage Implications
  – Guides Recovery Alternatives Selection
Financial Impact Analysis

• Purpose:
  – Quantify Revenue Loss
  – Identify Potential Economic Implications
  – Include Additional Expenses or Losses
  – Evaluate Insurance Strategies
  – Help Provide Cost Justification for Recovery Alternatives
• **Availability Strategies** – Elimination of Single Points of Failure and other enabling strategies

• **Recovery Strategies** – Collaborative design of restoring time critical processes over various periods of time

• **Plan Documentation** – BCP policies and standards, recovery organization and functional recovery plans
Getting Your Hands Around “The Project”

- Incident Command System
- Emergency Roles & Responsibilities
- Emergency Response Plans
- Emergency Policies
- Business Unit Recovery Plans
- Facilities Recovery Strategy
- System/Telecom Recovery Strategy
**Emergency Operations Center**

Definition:

“A place where uncomfortable officials meet in unaccustomed surroundings to play unfamiliar roles...Making unpopular decisions based on inadequate information in much too little time.”
Command Center Roles

- Make Strategic & Policy Decisions
- Referred to as “Crisis Management Team”
- Composed of Executive Officers, PR, Legal & Support personnel
- Communicate With External Stakeholders
- Establish Priorities
- Provide Direction for Media Releases
- Initiate Long-Term Recovery Requirements
- Provide Legal Advice
Life Safety Program

• Evacuation & Accounting For People
• Emergency Response Team Training
• Tracking Injured
• Notify Families Of Injured
• Reunite Employees & Families
• Food & Shelter
• Child & Elder Care
• Emergency Loans
• Temporary Housing
• Informing Employees
**Alternate Work Locations**…

- Who Coordinates?
- How Much Space Do You Need?
- Where Will You Find It?
- What Equipment, Systems, Phones are Needed?
- Is the Alternate Location Already Part of Your Network?
- How Long Will It Take?
Creating Department Plans...

- Initial Actions
- Contact Information
- Critical Functions
- Vital Records & Assets
- Plan Maintenance & Audits
Systems Recovery

• Determine Strategy
  – Immediate – Mirroring
  – Next Day – Replication
  – Three Days – Hot Site Contract, etc.

• Network Requirements

• Funding & Testing
Telecom Recovery

- Voice
  - Call Forwarding
  - Notification:
    - Employees & Families
    - Customers
    - Other Key Stakeholders
  - Voicemail

- Data
  - Redundancy
  - Multiple Carriers

- Main Cause – “Single Points of Failure”
- **Resource Acquisition/Implementation** – Obtaining and implementing the resource requirements to meet strategies and assessment needs
- **Testing/Exercising** – Validate the strategies, usability and readiness of the plans
- **Maintenance/Change Control** – Ensure the strategy, requirements, and plan contents change as organizational and technology changes occur
Why Exercise?

- Increase General Awareness
- Reveal Resource Gaps
- Improve Coordination
- Clarify Roles & Responsibilities
- Improve Individual Performance
- Motivate Corporate Managers To Support Program
- Build Confidence in Participants
- Foster Cooperation – Public vs. Private Sectors
Five Types Of Exercises

- Orientations
- Drills
- Table Tops
- Functional
- Full Scale
Creating An Exercise

• Define The Scope
• Develop Purpose & Objectives
• Determine Resource Needs
• Obtain Commitments for Critical Dates
• Develop Scenario, Major Events, Messages
• Brief Players, Simulators, Observers
• Conduct Exercise
Evaluating The Exercise

- Needed Improvements in Plans
- Training or Staffing Deficiencies
- Exercise Objectives
- Equipment Operation
PROCESS IMPROVEMENT

- Assist in developing standards and methodologies for ensuring lessons learned are captured
- Plan testing and exercising feedback identify opportunities for plan improvement
Challenges
Challenges

The biggest issues companies face with BCM:

• Not given sufficient budget for adequate program development and implementation
• Finding resources with the knowledge to manage the program
• Finding internal resources with the bandwidth to focus on BCM
• Achieving the required cross functional communication and coordination
• Perceived as an expensive insurance policy
Changing Trends in BCM

Availability
Recovery Time
Dependencies
Expectations
Threats
Risk Profile
Cost of Interruptions
Regulations
Putting It All Together
Putting It All Together...

• Comprehensive plans should combine emergency response and business recovery!
• It is easy to get started if you focus on the right priorities.
• There are reliable techniques for getting executive buy-in.
• Include both a business impact analysis and a risk assessment in the Initial Assessment.
Putting It All Together...

- Before beginning the project, anticipate other costs.
- Using the Incident Command System is critical to “getting back in business” quickly.
- Businesses – Integrate plans with local authorities.
- Public Agencies – Integrate plans with businesses.
- Create the right exercises to test your plans, then follow through with the changes. Then test, test, test, test again!