A *business continuity plan* (BCP) is a plan to help ensure that business processes can continue during a time of emergency or disaster. Such emergencies or disasters might include a fire or any other case where business is not able to occur under normal conditions. Businesses need to look at all such potential threats and devise BCPs to ensure continued operations should the threat become a reality.
Objectives

- Understand why you need to plan
- Understand the components of planning
- Understand the process involved
- Provide resources to help in the planning
Agenda

- Definition
- Why Have One?
- Planning Components
- Continuity Planning Domains
- Continuity Development Process
- Continuity of Government Checklist
- Tests & Exercises
- Resources
Why Have One?

- Federal Mandates
- Threats
- Risk
Federal Mandates

  - National Continuity Policy
- Executive Order 12656 - 11/18/1988
  - Assignment of Emergency Preparedness Responsibilities
- Federal Continuity Directives (FCD) 1 and 2 – Feb. 2008
Federal Continuity Directive 1 (FCD 1) – Continuity Evaluation Tool (CET)

Federal Executive Branch National Continuity Program and Requirements

◦ Program Plans and Procedures (21 questions)
◦ Budgeting and Acquisition of Resources (8)
◦ Essential Functions (13)
◦ Orders of Succession (10)
◦ Delegations of Authority (9)
◦ Continuity Facilities (22)
◦ Continuity Communications (10)
◦ Vital Records Management (20)
◦ Human Capital (15)
◦ Test, Training, and Exercise Program (34)
◦ Devolution of Control and Direction (10)
◦ Reconstitution Operations (16)
◦ Operational Phases and Implementation (47)
Federal Continuity Directive 2 (FCD 2) – Business Process Analysis (BPA)

- Implements the requirements of FCD 1, ANNEX C.

- It provides guidance and direction to Federal executive branch departments and agencies for identification of their Mission Essential Functions (MEFs) and potential Primary Mission Essential Functions (PMEFs).

- It includes guidance and checklists (7 worksheets) to assist departments and agencies in assessing their essential functions through a risk management process and in identifying potential PMEFs that support the National Essential Functions (NEFs) – the most critical functions necessary to lead and sustain the nation during a catastrophic emergency.

- The FCD provides direction on the formalized process for submission of a department’s or agency’s potential PMEFs that are supportive of the NEFs.

- Includes guidance on the processes for conducting a Business Process Analysis (BPA) and Business Impact Analysis (BIA) for each of the potential PMEFs that assist in identifying essential function relationships and interdependencies, time sensitivities, threat and vulnerability analyses, and mitigation strategies that impact and support the PMEFs.
Types of Threats

Government

- **Natural** – Tornado, Fire, Ice, Wind, Lightning, Extreme Heat, Flood
- **Environmental** – HVAC, Power, Hardware & Software Failure
- **Intentional Internal** – Disgruntled Employee, contractor, Dishonest Employee, Political Activist
- **Unintentional Internal** – Under Trained Employee, Irresponsible Employee, Apathetic Employee, Lack of Separation of Duty
- **External** – Hacker/ Cracker/ Criminal, Terrorist, Espionage, Former Employee

Business

- Corruption
- Extortion
- Floods
- Global hotspots
- Hurricanes
- Kidnapping
- Pandemic
- Tornados
Sample Threats

- Terrorist Attack
- Biological
- Bomb/Explosion
- Chemical
- Civil Disturbance
- Fire (direct or nearby)
- Water Damage or Stoppage
- High Winds (Hurricane/Tornado)
- Power Loss/Utility Failure
- Hostage Situation
- Radiological
- Structure Damage
- Building Deterioration (electrical, pipes, roof)
- Telecommunications Loss
- Community Disaster
- Metropolitan Commuting Failure
- Requests for Shelter
- Airborne Crash
- Health/Pandemic
- Work Stopage
What’s at Risk?

- Revenue Loss
- Data Loss
- Business Reputation Loss
- Quality of life or life itself
Types of Risk

- Risks under control
  - Employees, software and hardware systems, network
- Risk beyond control
  - Hacker, terrorist
- Risks with prior warning
  - Tornados, hurricanes, snow, flooding
- Risks with no prior warning
  - Earthquakes
Risk Management

- Security
- Insurance
- Vital Records
- Business Impact Analysis
Planning Components

- Challenges
- Types of Plans
- Types of Sites
- BCP Components
- Elements of a Continuity Plan
- Sample BCP Table of Contents
Challenges

- Time
- Expense
- Defining the scope
- Maintenance
Types of Plans

- Strategic (including succession planning)
- Tactical
- Operational
- Emergency Response
- Incident control and damage assessment
- Continuity and recovery
- Return to normal operations

“Different situations require different types of plans.”
Possible Plan Breakdowns

- Enterprise-wide
- By site
- By business line
- By product line
- By service provided
- By technology
Types of Sites

- **Hot** – Instantly operational
- **Warm** – A location with hot and cold devices
- **Cold** – Ready to move in
- **Mobile** – Brought to end users
BCP Components

A business continuity plan involves the following:

- Analysis of organizational threats
- A list of the primary tasks required to keep the organization operations flowing
- Easily located management contact information
- Explanation of where personnel should go if there is a disastrous event
- Information on data backups and organization site backup
- Collaboration among all facets of the organization
- Buy-in from everyone in the organization
Elements of a Continuity Plan

1. Determine Essential Functions
2. Develop Orders of Succession
3. Delegate Authority
4. Determine Continuity Facilities
5. Determine Continuity Communications
6. Manage Vital Records
7. Summarize Human Capital
8. Implement a “Test, Training, and Exercises” Program
9. Implement a Devolution Plan
10. Outline Reconstitution Procedures
# Sample BCP Table of Contents

1. Introduction
2. Policy statements
   1. Business continuity policies
   2. Confidentiality statement
3. Scope / Objectives
   1. Tied to organizational mission, goals and objectives and business continuity policies
   2. Identification of time sensitive operations and technology
4. Assumptions/exclusions
5. Recovery team description, organizational structure, and team responsibilities
6. Plan activation procedures
   1. Event notification
   2. Event assessment process
   3. Declaration procedures
   4. Escalation and mobilization procedures
7. Restoration and recovery procedures
Continuity Planning Domains

1. Program Initiation and Management
2. Risk Evaluation and Control
3. Business Impact Analysis
4. Business Continuity Strategies
5. Emergency Response and Operations
6. Plan Implementation and Documentation
7. Awareness and Training Program
8. Business Continuity Plan Exercise, Audit, and Maintenance
9. Crisis Communications
10. Coordination with External Agencies
1. Program Initiation and Management

- Establish the need for the business continuity program.
- Obtain leadership/management support for the BCM program.
- Coordinate and manage the implementation of the BCM program throughout the entity.
2. Risk Evaluation and Control

1. Work with management and any risk management/enterprise risk management groups within the entity to gain agreement on a clear and standardized risk assessment methodology and to gain understanding of the entity’s tolerance for risk.

2. Identify, develop and implement information gathering activities across the entity to identify threats/risks and the entity’s vulnerabilities.

3. Identify threats/risks and the entity’s vulnerabilities.

4. Identify probabilities and impact of the threats/risks identified.

5. Identify and evaluate the effectiveness of the current controls and safeguards in place.

6. Identify business resiliency strategies to control, mitigate, accept or take advantage of the potential impact of the risk/threat or reduce the entity’s vulnerabilities.

7. Document and present risk assessment to the entity’s leadership for approval.
3. Business Impact Analysis (BIA)

**Gartner:** A *business impact analysis (BIA)* is a process that identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputation and so forth) of natural and man-made events on business operations.

**Techopedia:** Business impact analysis (BIA) is a component of business continuity planning that helps to identify critical and non-critical systems. A business impact analysis also assigns consequences and usually a dollar figure to specific disaster scenarios. It will also include estimated recovery times and recovery requirements for such scenarios. The business impact analysis is often used to measure the risks of failure against the costs of upgrading a particular system.

**Wikipedia:** A BIA differentiates critical (urgent) and non-critical (non-urgent) organization functions/activities. Critical functions are those whose disruption is regarded as unacceptable. Perceptions of acceptability are affected by the cost of recovery solutions. A function may also be considered critical if dictated by law. For each critical (in scope) function, two values are then assigned:

- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
4. Business Continuity Strategies

1. Utilize the data collected during the BIA and Risk evaluation to identify the available continuity and recovery strategies for the entity’s operations that will meet the RTO and RPO identified during the BIA process.

2. Consolidate strategies where appropriate to reduce costs and/or complexity.

3. Assess the cost of implementing identified strategies through a cost/benefit analysis.

4. Recommended strategies and obtain approval to implement.
5. Emergency Response and Operations

1. Identify applicable emergency preparedness and response regulations.
2. Identify potential types of emergencies, scenarios that may occur and impacts that may result.
3. Identify the response capabilities needed.
4. Review existing emergency response procedures and assess capabilities to protect life, property, and the environment.
5. Recommend the development/improvement of emergency procedures.
6. Recommend the development and implementation of an incident management system for command, control, and coordination of personnel and resources during emergencies.
7. Review and coordinate emergency preparedness and response plans and procedures with trained, professional first responders.
Emergency Operation Center (EOC) Considerations

- Physical or virtual operations center
- Communications capability
- Size of location
- EOC security
- Operating procedures
  - Identification, assignment, and scheduling of persons
  - Management and operations of the EOC
  - Communication protocols, procedures, and information flow
  - Closure of the EOC
6. Plan Implementation and Documentation

1. Design, develop and implement agreed upon recovery strategies.
2. Design framework and define document structure for the plan documentation.
3. Coordinate the effort to document recovery plans for the entity’s operations and the technology that supports them.
4. Publish the plan documents.
7. Awareness and Training Program

1. Establish objectives of BCM awareness and training program.
2. Identify functional awareness and training requirements.
3. Identify appropriate internal and external audiences.
4. Develop awareness and training methodology.
5. Identify, acquire or develop awareness and training tools.
6. Identify external awareness and training opportunities.
7. Oversee the delivery training and awareness activities.
8. Business Continuity Plan
Exercise, Audit, and Maintenance

1. Establish an exercise/testing program.
2. Establish a plan maintenance program.
3. Identify or establish appropriate industry and/or organizational standards.
4. Establish a business continuity program audit process.
5. Communicate exercise/test/audit results and recommendations.
9. Crisis Communications

1. Design, develop and implement a crisis communications plan.
2. Communicate and train stakeholders on roles and responsibilities for the crisis communications plan.
3. Exercise the crisis communications plan.
4. Maintain the crisis communications plan.
10. Coordination with External Agencies

1. Identify and establish emergency preparedness and response procedures.
2. Identify applicable emergency preparedness and response regulations and the agencies having jurisdiction over the organization’s facilities and operations.
3. Coordinate emergency preparedness and response procedures with external agencies.
# Coordination of Plans with Public Agencies

<table>
<thead>
<tr>
<th>Agency</th>
<th>Plan to be Reviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire Dept.</td>
<td>Evacuation, fire, hazmat, rescue, bomb threat, suspicious package, special events</td>
</tr>
<tr>
<td>Local Emergency Planning Committee</td>
<td>Hazard materials response plan</td>
</tr>
<tr>
<td>Law Enforcement</td>
<td>Bomb threat, suspicious package, labor strife, civil disturbance, special events</td>
</tr>
<tr>
<td>Emergency Medical Services</td>
<td>Medical emergencies, hazmat</td>
</tr>
<tr>
<td>Emergency Management</td>
<td>Hurricane, tornado, earthquake, flood, regional disasters</td>
</tr>
</tbody>
</table>
Continuity Development Process

1. Establish Business Case
2. Follow Planning Process
3. Build and Train the Team
4. Develop the BIA
5. Evaluate External Resources
6. Build a Crisis Communications Plan
Step 1:
Establish the Business Case

- Use regulatory compliance to your advantage
- Aim to create a business continuity plan that reflects your company’s culture
- Encourage grass-roots support by meeting individually with people in different business units
- Stay flexible
- Find ways that business continuity can add to the bottom line
Step 2: Follow a Planning Process

Goals:

- To minimize the business impact of each event
- To address human safety
- To mitigate corporate liability due to lack of due diligence
- To meet regulatory requirements
- To protect the organization’s public image by a fast, professional response
Step 3: Build and Train the Team(s)

- Team manager
- Technical lead
- Public relations
- Security
- IS support
- Facilities management
- Labor unions
- Representatives of critical business functions
Step 4: Develop the BIA

1. Identify the criteria to be used to quantify and qualify the entity’s impact from events.
2. Establish the Business Impact Analysis (BIA) process and methodology.
3. Plan and coordinate data gathering and analysis.
4. Gain leadership agreement on BIA methodology and the criteria to be used.
5. Analyze the data collected against the approved criteria to establish RTO and RPO for each operational area and the technology that supports them.
6. Document minimum resource requirements for resumption and recovery of core and support business functions and their escalation over time.
7. Prepare and present the BIA results to the entity’s leadership and gain acceptance of the RTO and RPO for each process.
Business Impact Analysis (BIA)

Table of Contents

- Introduction
  - BIA Purpose
  - References (Authorities)
- System Description/Environment
  - System and Environment Description
  - Points of Contact (System, External, Customers)
- Data Collection
  - Determine Mission/Business Process and Recovery Criticality
  - Identify Outage Impacts (Severe, Moderate, Minimal – Cost)
  - Identify Estimated Downtime (RTO, RPO, MTD*)
  - Identify Resource Requirements
  - Identify Recovery Priorities for System Resources

*MTD - Maximum Tolerable Downtime*
Step 5:
Evaluating External Resources

- Do you know what you need?
- Will the firm present several options?
- Are the consultants certified in business continuity planning?
- Are they willing and able to prioritize?
- Do they offer BC/DR solutions to fit your budget?
- Evaluating Business Continuity Services and software
- Weigh the benefits of specialized business continuity planning software
- Consider the major business continuity/availability service providers and some niche players
- Let recovery requirements dictate the level of dedicated BC services
- Use caution when outsourcing business continuity functions overseas
Step 6: Build a Crisis Communication Plan

- Internal communication
- External communication

Tips for dealing with the public:

- Be truthful
- Provide useful information
- Train your spokespeople
- Establish an ingoing relationship
- Don’t let the media be the only source of news
Crisis Management and Communications Plan

- Identify crisis management team
- Procedures to transition from emergency response to crisis management and business continuity
- Documented procedures
  - Notification procedures
  - Status updates
  - Media releases
  - Targeted communications
    - Media
    - Employees and their families
    - Regulatory bodies, emergency first-responders, agencies, special hazmat services
    - Investor relations
    - Labor relations
    - Relations with other involved groups (e.g., customers, vendors, suppliers, etc.)
Continuity of Government (COG) Checklist*

*By NGA Center for Best Practices (Issue Brief)
Continuity of Government (COG) Checklist

1. Describe essential governmental functions and activities with a list of appropriate personnel
2. Determine who is responsible for direction and control at the executive level
3. Identify mission-critical data and systems that support essential functions
4. Describe the decision process for implementing COG plans and procedures, including reliable, effective, and timely notification
5. Identify the agencies and personnel (including lines of succession) responsible for providing water, electricity, natural gas, sewer, and sanitation services in affected areas
Continuity of Government (COG) Checklist

6. Refer to Standard Operating Procedures (SOPs) for each state agency that provide specific authorities of designated successors to direct their agencies

7. Establish the location of primary and alternate Emergency Operations Centers (EOCs), mobile EOCs, and command posts as well as the individuals responsible for ensuring communications capabilities

8. Determine the location of and individuals responsible for ensuring communications capabilities of the primary, alternate, and mobile command posts

9. Provide instructions for relocation to pre-designated facilities, with and without warning, during duty and non-duty hours

10. Ensure operational capability within a specified amount of time (e.g., 30 days)
Continuity of Government (COG) Checklist

11. Establish procedures for the acquisition of resources necessary to sustain operations over the predetermined period of time

12. Understand the potential role of the national guard in the event that military forces are required to provide services normally under the jurisdiction of civilian authorities

13. Provide a process for ensuring interoperable communications

14. Include measures for the protection of vital records

15. Describe the location of and contact points for Emergency Management Assistance Compacts (EMACs), Memorandum of Understanding (MOU), and other cooperative agreements; and

16. Provide procedures for ensuring security, including employee security clearances and facility and communications security
Tests and Exercises

- Tips for Effective Tabletop Exercise
- Planning Scenario Types
- Sample Scenarios
- DHS Top 16 Scenarios
Tips for an Effective Tabletop Exercise

- Decide how much gloom and doom you want
- Test how quickly you can pull together key players
- Involve everyone
- Acknowledge that first-timers may be nervous
- Encourage misinformation
- Take the lessons with you
Planning Scenario Types

- Short-term (less than 1 month outage)
- Long-term (more than 3 month outage)
- Local (Site or campus)
- Regional impact
- Enterprise-wide impact
- Cascading impact potential
Sample Scenarios

1. A disgruntled employee starts a Data Center fire
2. An explosion at a nearby chemical plant releases deadly toxins
3. A pandemic flu hits
4. Natural Disaster: Tornado, Hurricane
DHS Top 16 Catastrophic Scenarios

1. Improvised nuclear device
2. Aerosol anthrax
3. Pandemic Influenza
4. Plague
5. Blister agent
6. Toxic industrial chemicals
7. Nerve agent
8. Chlorine tank explosion

9. Major earthquake
10. Major hurricane
11. Radiological dispersal device
12. Improvised explosive device
13. Food contamination
14. Foreign contamination
15. Foreign animal disease
16. Cyber attack
Resources

- Local Emergency Web Sites
- Training Web Site
- Books & Web References
Local Emergency Web Sites


- **Howard County** - [http://www.co.ho.md.us/displayprimary.aspx?id=4294969657](http://www.co.ho.md.us/displayprimary.aspx?id=4294969657)

- **Prince George’s County** - [http://www.princegeorgescountymd.gov/sites/emergencymanagement/Pages/default.aspx](http://www.princegeorgescountymd.gov/sites/emergencymanagement/Pages/default.aspx)
Plan, Prepare & Mitigate

There are actions that should be taken before, during, and after an event that are unique to each hazard. Identify the hazards that have happened or could happen in your area and plan for the unique actions for each. Local emergency management offices can help identify the hazards in your area and outline the local plans and recommendations for each. Share the hazard-specific information with family members and include pertinent materials in your family disaster plan.

Protecting Homes
- Flood Insurance
- Flood Hazard Mapping
- Living with the Levees

Protecting our Communities
- Mitigation Planning for Communities
- HAZUS

Protecting Your Business
- Protecting Your Business from Flood Loss
- Protecting Your Business

National Preparedness
- Whole Community
- National Preparedness Goal
Emergency Management News

Social Media - Stay Informed

The Fire Department, Police Department and the Office of Emergency Management provide current information, including updates on breaking news, on Twitter and Facebook.

Our Emergency Management Twitter account is [www.twitter.com/BACOemergency](http://www.twitter.com/BACOemergency). Followers receive updates during weather and other emergencies, emergency preparedness information and information about programs and events.

For Police and Fire news, follow [www.twitter.com/BACOPoliceFire](http://www.twitter.com/BACOPoliceFire). Followers receive updates during weather and other emergencies, emergency preparedness information and information about programs and events.

George Abdallah Darraj has been located in Dundalk and returned home safe. (Twitter Link)

Have you seen George Abdallah Darraj? #CriticalMissingPerson Please help us find him. (Twitter Link)
Office of Emergency Management

The City of ANNAPOlis
Maryland

Home Visitors Residents Business Government Online Services Contact Us

Upcoming Events Maps and GIS Elections 2013 Search...

Office of Emergency Management

Kevin J. Simmons, Director

Mission Statement:

The City of Annapolis Office of Emergency Preparedness & Risk Management provides vision, direction, and subject matter expertise in order to coordinate the City's all hazards emergency preparedness, response, recovery, and mitigation efforts and develop an overall culture of safety.
Emergency Preparedness

Hurricane and Storm Preparedness Resource Information

Knowing what to do before, during and after an emergency is a critical part of being prepared and may make all the difference when seconds count. Some of the basic protective actions are similar for multiple hazards. Developing a family communications plan or making an emergency supply kit are the same for most accidental emergencies and natural disasters. To start with the basics go to Ready.gov.

For hurricane information and resources click on the links below:

- Ready.gov - Hurricane Information
- Hurricane Season is Flood Season Information Sheet
- Generator Safety Tips
- Storm Safety and Preparedness
- In This Section:
  - Health:
    - About Us
    - Leadership
    - News & Alerts
    - Meetings & Events
    - Forms & Applications
    - Job Opportunities
    - Volunteering
    - Photo Gallery
    - Contact Us
    - Locations
    - Health RSS
Welcome to the Office of Emergency Management. Under the Office of Homeland Security, the mission for the Office of Emergency Management is to coordinate and sustain homeland security and emergency management operations that effectively support, mitigate, protect against, prepare for, respond to and recover from natural, technological or manmade emergencies or disasters, including acts of terrorism.
Training Sites

- Sentryx Business Continuity Training and Certification - [https://www.sentryx.com/?gclid=CLmM3q_bpL8CFSwS7AodlGsAhQ](https://www.sentryx.com/?gclid=CLmM3q_bpL8CFSwS7AodlGsAhQ)
- Disaster Recovery Institute International (DRII) - [https://www.drii.org/](https://www.drii.org/)
- BCS - [http://certifications.bcs.org/content/ConTab/7](http://certifications.bcs.org/content/ConTab/7)
- FEMA - [https://www.fema.gov/media-library/assets/videos/80219](https://www.fema.gov/media-library/assets/videos/80219)
- BCM Institute - [http://www bcm institute.org/bcmi10/](http://www bcm institute.org/bcmi10/)
- Sentryx - [http://www.sentryxshop.com/](http://www.sentryxshop.com/)
References

- CSO: The Ultimate Guide to Business Continuity (from CSO Magazine and CSOonline.com)
- DRI International: Professional Practices for Business Continuity Practitioners
- Continuity Central - http://www.continuitycentral.com/bcpd.htm
More References

- http://www.cio.com/article/742974/How_to_Create_an_Effective_Business_Continuity_Plan
Take Aways

- What needs to be understood to develop a Continuity Plan
- You now know the process in developing a continuity plan
- You have an understanding of what government authorities provide
- You now know where to get some training
Questions

L_Wlosinski@Hotmail.com