Evaluating and Improving Your Business Continuity Plan

As presented to the Northeast Florida IIA Chapter

January 23, 2015
Contact Information

Karen Weir, MAC, CISA, CBCP
Manager
kweir@accretivesolutions.com

Jennifer Hensley
Client Development
jhensley@accretivesolutions.com
p 904-208-5607

Accretive Solutions
76 South Laura St., Suite 202
Jacksonville, FL 32202
www.accretivesolutions.com
Agenda

1. Business Continuity Overview
2. Industry Regulations
3. BCP Standards
4. Common Components
5. Determining Adequacy
Determine Adequacy

1. Determine your standard
2. Support your determination with facts, verify with management
3. Assess your organization’s current BCP policies, process, and procedures
4. Measure and document perceived gaps
5. Formulate and present recommendations
Business Continuity Overview
Business Continuity is…

- The method by which organizations can:
  - Identify the likelihood and potential impact of unplanned business interruptions,
  - Implement controls to prevent, alert, or mitigate effects of unplanned business interruptions,
  - Recover critical functionality within an acceptable timeframe, and
  - Restore full functionality to the organization, while suffering minimal downtime and revenue losses.
Business Interruption Examples

- **Natural Events**
  - Hurricane*
  - Tornado
  - Fire/Flood
  - Gas Leak/Explosion
  - Power Outage
  - H1N1

- **Corporate Image**
  - Scandal
  - Product Recall
  - Compliance Breach

- **Man-Made, Intentional**
  - Terrorism*
  - Sabotage
    - Hacker/Virus

- **Man-Made, Accidental**
  - Human Error
  - Hazardous Spill/Leak

*Indicates significant impact or rare occurrence.
Common Factors/Any Organization

- Business Continuity
- Internal Control Framework (Policy & Procedure)
- Trained & Experienced Workforce
- Facilities (Building, Office Space, Machinery)
- Technology and Infrastructure (Applications, Servers, Databases)
- Disaster Recovery
## Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM</td>
<td>Business Continuity Management</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity/Continuation Planning/Program</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
</tr>
<tr>
<td>BRP</td>
<td>Business Resumption Plan</td>
</tr>
<tr>
<td>CMP</td>
<td>Crisis Management Plan</td>
</tr>
<tr>
<td>CMT</td>
<td>Crisis Management Team</td>
</tr>
<tr>
<td>DAP</td>
<td>Damage Assessment Plan</td>
</tr>
<tr>
<td>DAT</td>
<td>Damage Assessment Team</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>EOC</td>
<td>Emergency Operations Center</td>
</tr>
<tr>
<td>ERP</td>
<td>Emergency Response Plan</td>
</tr>
<tr>
<td>ERT</td>
<td>Emergency Response Team</td>
</tr>
<tr>
<td>FEMA</td>
<td>Federal Emergency Management Agency</td>
</tr>
<tr>
<td>ICS</td>
<td>Incident Command System</td>
</tr>
<tr>
<td>MAD</td>
<td>Maximum Acceptable/Allowable Downtime</td>
</tr>
<tr>
<td>PRC</td>
<td>Property Risk Control</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>SCM</td>
<td>Supply Chain Management</td>
</tr>
</tbody>
</table>
Industry Regulations
Regulated Industries - Examples

- Financial Services
- Insurance
- Energy
- Telecommunications
- Political & Public Affairs
- HealthCare
- Automotive
- Catalog

- Retail
- Market Research/Surveys
- Banking
- Mortgage
- Life & Health
- Property & Casualty
- Credit Card
- Utilities
Regulatory Bodies - Examples

- PCI (Payment Card Industry)
- Consumer Product Safety Commission
- Federal Trade Commission (FTC)
- Food and Drug Administration (FDA)
- Communications Commission (FCC)
- Banking Fair Credit Reporting Act (FRCA)
- Fair Debt Collection Practices Act (FDCPA)
- Truth in Lending Act (TILA)
- Real Estate Settlement Procedures Act (RESPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Digital Millennium Copyright Act
- Federal Financial Institutions Examination Council (FFIEC)
Disaster Recovery Journal website provides a comprehensive document that pulls together the DR/BCP regulations by affected industries:

<table>
<thead>
<tr>
<th>For these Industries</th>
<th>Provides this Info on Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking &amp; Finance</td>
<td>Title</td>
</tr>
<tr>
<td>Public Health &amp; Healthcare</td>
<td>Regulation / Standard (Reg, Stf)</td>
</tr>
<tr>
<td>Transportation &amp; Shipping</td>
<td>Governing Body</td>
</tr>
<tr>
<td>Energy (including nuclear)</td>
<td>Country</td>
</tr>
<tr>
<td>Industry</td>
<td>Summary / Description</td>
</tr>
<tr>
<td>Agriculture, Food Supply &amp; Water</td>
<td>Significant Dates, Fines, Penalties</td>
</tr>
<tr>
<td>Information Distribution &amp; Communications</td>
<td>Category (Enf, Amb, Wat, IAI)</td>
</tr>
<tr>
<td>Government &amp; Public Agencies</td>
<td>Notes /Comments</td>
</tr>
</tbody>
</table>

www.drj.com
BCP Standards
BCP Standards

Three standards currently recognized by DHS as part of the voluntary certification program:

- BS 25999-2:2007-A Specification for BCM; and
- NFPA 1600:2010 Standard on Disaster/Emergency Management and Business Continuity Programs
Process approach

- Understanding an organization’s risk, security, preparedness, response, continuity, and recovery requirements;
- Establishing a policy and objectives to manage risks;
- Implementing and operating controls to manage an organization’s risks within the context of the organization’s mission;
- Monitoring and reviewing the performance and effectiveness of the organizational resilience management system; and
- Continual improvement based on objective measurement.
BS 25999-2:2007-A Specification for BCM

By the British Standards Institution (BSI)

- Part 1 provides concept introduction/ guidance
  - Ten (10) Sections, similar to DRJ/DRII Subject Areas
- Part 2 provides requirements for implementation, application, and continuous improvement of the BCM.
  - Six (6) Sections, uses PDCA model of continuous improvement.
  - Also in line with DRJ/DRII Subject Areas and GAP
NFPA 1600:2010 Standard on Disaster/Emergency Management and Business Continuity Programs

Process approach

- Understanding an organization’s risk, security, preparedness, response, continuity, and recovery requirements;
- Establishing a policy and objectives to manage risks;
- Implementing and operating controls to manage an organization’s risks within the context of the organization’s mission;
- Monitoring and reviewing the performance and effectiveness of the *organizational resilience management system*; and
- Continual improvement based on objective measurement.
Professional Practices for Business Continuity Practitioners:
- Joint effort of the Disaster Recovery Journal and the Business Continuity Institute based in the UK.

Generally Accepted Practices (GAP) includes input and cooperation from:
- Association of Records Management Administration (ARMA)
- DRI International (DRII)
- Financial Services Technology Consortium (FSTC)
- Standards Australia/Standards New Zealand
- National Fire Protection Association (NFPA)
BCP Components
Ten Subject Areas

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

- Establish the need for Business Continuity Management
- Obtain management support and project approval
Risk Evaluation and Control

- Identify Potential Exposures/Risks
- Qualify and Prioritize
- Identify Controls and Safeguards
- Evaluate Effectiveness
  - Prioritized
  - Approved by Management
  - Quantified, both in probabilities and potential impacts

Risk Assessment

- Corp. Scandal
- Flood
- Random Violence
Business Impact Analysis

- Identify the impacts of interruptions
- Identify time-critical functions
- Identify inter-dependencies
- Prioritize

**Time**
- RTO: Recovery Time Obj.
- RPO: Recovery Point Obj.

**Systems**
- Applications
- Alternative work-arounds

**Key People**
- Cross-training recommendations
- Back-ups

**Facility Needs**
- Alternate Office Space, Laptops
BIA Exercise
Business Continuity Strategies

- Determine organizational needs
- Determine functional/departmental needs
- Identify and Present Solutions to meet both

Guiding Decisions

- Go/No-go circumstances
- Facilities
  - Secondary/Tertiary
  - Office Space Relocation
Emergency Response and Operations

- Identify Potential Emergencies and Responses
- Review Evacuation Plans
- Command and Control Procedures (Alternate Hierarchy)
Emergency Response Exercise
Business Continuity Plans

- Identify Plan Requirements
  - Strategic
  - Tactical
  - Operational

- Assumptions & Scenarios

| BC Plan |
|-----------------------------|-----------------------------|
| Critical Functions | Recovery Procedures |

<table>
<thead>
<tr>
<th>Hurricane Prep, for example</th>
<th>Disaster Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning Signs</td>
<td>Alternate Facility</td>
</tr>
<tr>
<td>1-800 Employee Communication Line Info</td>
<td>Prioritized System Recovery</td>
</tr>
</tbody>
</table>
Awareness and Training Programs

- Corporate Awareness Programs
- Emergency Responder Training (CPR, Fire Extinguisher, etc.)
- Functional & Technical (Practice) Training
Business Continuity Plan Exercise, Audit and Maintenance

- Exercise/Testing Program
- Plan Maintenance Program
- Business Continuity Audit Process
- Communicate Exercise/Test Results

Diagram by Karn G. Bulsuk (http://www.bulsuk.com)
BCP Exercises
Crisis Communications

- Crisis Communications Program
  - Escalation procedures
  - Roles and Responsibilities
  - Audience groups and messages

- Crisis Communication Plan
  - ID Designated Speaker(s)
  - Scripts Development
    - By situation
    - Internal/External
  - Media Relationships
Coordination with External Agencies

- Coordinate Emergency Management with External Agencies
- Identify relevant external agencies (Police Department, Fire & Rescue)
- Identify statutory requirements
- Involve external agencies – as appropriate
  - Review plans & recommend improvements
  - Participate in exercises
  - Provide training
Determining Adequacy
Review and Evaluation

1. For each subject area, determine what is appropriate for your organization
2. Support your determination with facts, verify with management
3. Assess your organization’s current policies, process, and procedures
4. Document perceived gaps
5. Formulate recommendations
Questions?