Business Continuity and Disaster Recovery Planning

Jennifer Brandt, CISA
April 16, 2015
Stinnett & Associates (Stinnett) is a professional advisory firm offering services designed to help clients more effectively manage risk and improve performance by streamlining processes, reducing costs, and enhancing IT controls.

Stinnett provides a diverse range of services, including:

- Business Process Design and Re-engineering
- Co-source and Outsource Internal Audit
  - Operational, Compliance, and Information Technology
- Sarbanes-Oxley
  - Business Process and Information Technology
- IT Assessments
- IT Project Management
- Risk Management
- Fraud Investigation
- Enterprise Risk Management

**Doing the Right Thing**

We have the ability to identify and understand risks as well as leverage industry best practices to implement the right processes and controls to assist clients in managing and monitoring those risks. Working with clients toward solutions, we have established a reputation for “doing the right thing” and pride ourselves on being trusted business advisors.

Stinnett is a certified Women’s Business Enterprise through the Women’s Business Enterprise National Council. Stinnett provides services to a broad range of clients including several Fortune 1000 companies and many mid-size to large organizations with global operations.
Today’s Agenda

✓ The purpose of Business Continuity Plans and Disaster Recovery Plans
✓ Identify the components of a comprehensive Business Continuity Plan and Disaster Recovery Plan
✓ Understand the key phases of establishing a BC and DR program and the approach for each phase
✓ General Guidelines for Business Continuity / Disaster Recovery Audit
Disaster recovery and contingency planning have evolved throughout the years. “Disaster” has taken on a new meaning:

- 9/11 terrorist attacks.
- Computer attacks like the Stuxnet virus.
- Increasing severity of recent natural disasters.
- Increased threats against US infrastructure.

Continuity Planning has expanded from just IT Disaster Recovery to the continuation of mission-critical business processes enterprise-wide.

Disasters, both natural and intentional, are unpredictable and could include anything from fire, hurricanes, floods, virus/hacker attacks, and hardware failures to power failures.
Some realities in preparing a BCP:

✓ Basic Business Continuity Plans (BCP) can be established without costing the company a significant amount of money or resources!

✓ Once established, BCP plans are relatively easy to maintain.

✓ An effective BCP can make a tremendous difference in how an organization fares during and after that unlikely disaster.

✓ Crisis events are frequently NOT what you anticipated. So BE PREPARED!
The Growing Importance of a BCP

According to a recent survey by Forrester Research and the Disaster Recovery Journal, 61% of businesses with a Business Continuity Plan have invoked the Plan at least once in the past 5 years.

Base: 300 global business continuity decision-makers and influencers (2011)

The Growing Importance of a BCP (Continued)

“What was the cause(s) of your most significant disaster declaration(s) or major business disruption?”

- We have not declared a disaster: 36%
- Terrorism: 1%
- Earthquake: 1%
- Tornado: 2%
- Hurricane: 4%
- Other: 5%
- Fire: 6%
- IT software failure: 11%
- Flood: 13%
- Human error: 13%
- Winter storm: 14%
- Network failure: 15%
- IT hardware failure: 24%
- Power failure: 44%

Base: 200 disaster recovery decision makers and influencers at business globally (multiple responses accepted)
**Business Continuity vs. Disaster Recovery**

**Disaster Recovery vs. Business Continuity**
Typically, the term “Disaster Recovery” is used to describe procedures and processes meant to recover and restore key computer systems. However, since these systems are meaningless without the business processes and personnel that depend on them, companies now employ a more holistic view called “Business Continuity Planning” or BCP.

BCP considers all of the necessary elements to restore operations, not just the computer systems. Among other things, Business Continuity Planning addresses how the company will respond to:

- Alternative office space needs, including consideration of the complete destruction of company buildings.
- Communication strategies, including communications to employees and customers and properly handling PR and media issues.
- Employee responsibilities and instructions.
- Telephones, faxes, and other necessary equipment.
- Office supplies.
- Human Resources: Loss of key staff.
- How and in what priority vital records will be retrieved or reconstructed.
- Prolonged disruption of business processes and business survival.
Benefits to Planning

Besides the obvious benefits during an actual disaster event, BCPs provide additional value:

- Clear understanding of the most critical processes in the organization.
- Increased confidence in the company by:
  - Customers
  - Business Partners
  - Employees
  - Investors
  - The Board
- Compliance with Laws and Regulations (HIPAA, FERC, Finance, etc.)
- Positive impact on insurance and risk management
- Competitive advantage
  - Preparation for the inevitable before it occurs will allow businesses to handle it with the least impact when it occurs
  - Serve your customers when your competitors can’t
BUSINESS CONTINUITY PLANNING PROCESS
# Business Continuity Planning Process

## Business Continuity Plan

<table>
<thead>
<tr>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
<th>Phase 4</th>
<th>Phase 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform Business Impact Analysis, identifying key processes and determining maximum time each can be down before significant company impact occurs.</td>
<td>Determine what information, computer systems, personnel and materials are absolutely necessary to support each critical process. Perform an IT Gap Analysis.</td>
<td>Develop specific plans for each critical process and department to restore operations.</td>
<td>Document and distribute plans. Test recovery plans to verify objectives are achieved. Train management, key crisis response teams and employees.</td>
<td>Monitor business changes and update policies and procedures as needed (minimum annually). Conduct ongoing periodic testing as necessary.</td>
</tr>
</tbody>
</table>

## Results

- Clear, tested and reliable instructions and procedures for most significant disaster events.
- Improved assurance to customers, employees and the investment community.
- Greatly reduced exposure to significant and prolonged business outages.
- Greatly reduced cost and confusion during a disaster.
- Improved internal and external communication channels and processes.
Phase 1: Business Impact Analysis
The Business Impact Analysis (BIA) is used to determine the critical business processes and related resources within all business units of the organization. The BIA establishes a foundation for developing well-reasoned and prioritized responses to disaster and ensures Business Continuity Plans are focused on reestablishing the most critical business processes in the most cost-effective manner to minimize loss and disruption.

The goal of the BIA is to define objectives for the recovery of host computing systems that run the applications supporting the critical business processes; specifically, the number of hours or days in which business systems must be recovered after an outage.

The output of the BIA is a prioritized list of critical business processes that becomes the focus of subsequent business mitigation and recovery processes.
HOW TO PERFORM THE BIA

1. Identify key process or operational areas in the business
2. Identify the key process owners
3. Interview the key process owners per the BIA interview guide (example: Payroll)
   - Priority of processes
   - Process recovery time requirements
   - Critical systems the processes depend on
   - System recovery time requirements
   - Interdependencies
   - Acceptable data loss: drives backup strategies and determines the amount of lost data or work that may need to be re-created, re-entered, and/or re-performed after the systems have been recovered. *(also known as Recovery Point Objective)*
Phase 2: Information Technology Assessment / Gap Analysis
**THE IT GAP ANALYSIS**

- The **IT Gap Analysis** compares the organization’s current system recovery abilities and procedures to the system recovery needs of the business.

- The **goal** of the IT Gap Analysis is to determine whether IT’s current system recovery abilities meet the business’ needs.

- The **output of an IT Gap Analysis** is a list of the critical systems, the current system recovery time, and the desired system recovery time (according to the business).

- Where there is a gap, the company’s technical team should design and implement a resiliency strategy which effectively balances management’s needs with the potential impact cost. If such a solution is cost-prohibitive, management must formally accept the risks associated with the longer recovery times and ensure that the backup / restoration solution developed is maintained in an optimal state.
THE IT GAP ANALYSIS

• Interview key personnel in the IT Department
• Review current Disaster Recovery Plans and Procedures (if any)
• Estimate the recovery time for systems and applications that support the critical business processes under the current IT recovery plans and procedures
• Perform a comparison of the current technology recovery times to the Recovery Time Objectives (Maximum Allowable Downtime) of the critical business processes
• Determine any gaps between the business RTOs and IT’s current recovery capabilities
• Present gaps to management
THE DISASTER RECOVERY PLAN

• Elements of an effective DR plan:
  ▪ Regular backups of all critical systems and data.
  ▪ Clear, complete instructions on how to restore systems.
  ▪ Offsite storage of backups and restoration instructions.
  ▪ Arrangements for an alternative data center location.
  ▪ An effective testing plan.

• An effective DR plan will address these types of situations:
  ▪ Hardware failure such as loss of a disk drive (Not much of a problem anymore, RAID, etc.)
  ▪ Loss of servers or power for extended period of time.
  ▪ Loss of access or use of the data center for an extended period of time.

• But - just having an effective disaster recovery plan is not enough when you lose access to the entire building!
DISASTER RECOVERY PLANNING – WHAT’S LEFT?

- How do we access the systems once they are up and running at the recovery center?
- Who’s in charge of what?
- What are the most critical things we need to do to continue operations?
- Where are our critical files (such as original contracts)?
- How do we communicate with:
  - Customers
  - Employees
  - Press
  - Stockholders
  - Etc.
PHASE 3: BUSINESS PROCESS RECOVERY PLANS
**Considerations for a Successful Business Continuity Plan**

- **Assign ownership**: Who will maintain the plan and keep it updated?
- **Identify a champion**: Preferably the CEO or COO
- **Don’t bite off too much.** Most plan efforts fail because the scope is too massive and ambiguous.

  **Recommendation**: Initial plan should be limited to the first 30 days after a disaster event.

- **KEEP IT SIMPLE!** (or at least as simple as prudent)
- **Clearly identify the targets** and stay focused throughout the project.
- **Build off any existing plans** that may exist, such as an established IT disaster recovery plan.
- **Communicate! Communicate! Communicate!**
Define the Recovery Process

0
Assess the situation

1-2
Inform Executives and Declare

2-4
Activate Departmental Plans

4-8
Notify 3rd parties

Alternate Facilities, equipment providers, telecom, etc.

IT Recovery, Accounting, HR, etc.

Activate Communications Plans
Define the Plan Structure

Business Continuity Plan

- Initial Assessment and Communications Plan
- Executive Team Plan
- Responsibilities, alternative meeting site, contact plan
- IT Disaster Recovery Plan
- Departmental Plans
- Communications Plans
- Facilities and Supplies Plan
BUSINESS CONTINUITY PLANNING
SUCCESS FACTORS

- Management buy-in and support
- Effective processes to evaluate and identify key business functions
- Dedication of resources:
  - Team members
  - Management stakeholders
  - Executive sponsor
- Clearly stated targets
- Properly trained BCP team members
- Clear and concise project plan
- Clearly stated responsibilities
- Clearly stated budget considerations
Top Three Challenges of Implementing and Managing Effective Business Continuity Planning

- Implementing BCM corporate wide: 45%
- Inadequate funding: 43%
- Our BCM managers do not have enough authority/executive support: 24%
- Our BCM program is too focused on IT disaster recovery: 21%
- The scope and responsibilities of our BCM program are ill-defined: 20%
- Lack of executive level support: 15%
- Executive management does not take business continuity preparedness seriously: 14%
- None of the above: 12%
- Other: 17%

Business Continuity Ongoing Maintenance

Business Continuity Plans are living documents and as such, should be maintained on a regular basis, at a minimum of annually. Maintenance activities should include:

- General content: update key personnel and contact information
- Validate key processes and systems are included (consider any business changes or new system implementations)
- Confirm the Disaster Recovery Gap Analysis is still accurate and still acceptable to management
- Execute a test of the BCP and DRP to ensure the approach works and employees are familiar with the process
- Communicate changes in the BCP to employees
**Plan Testing**

The purpose of Business Continuity Plan is to reveal weaknesses in the following:

- Completeness of work procedures for critical processes
- Management’s understanding of their assigned roles and responsibilities
- Feasibility of work process recovery within established Recovery Time Objectives
- Ability of the company to support the recovery plan (resources, timing, accessibility to facilities and resources)

Common testing methodologies include:

- **Table-top Exercise**
  
  A disaster scenario is developed for a specific time, date, and facility. The disaster scenario is presented on an impromptu basis to the members of the recovery teams. Then, the recovery team members assume their business continuity roles as described in the plan and simulate the recovery activities.

- **Structured Walkthrough**

  Business continuity team members meet to orally walk through the specific steps of each component of the business continuity process as documented in the business continuity plan. The purpose of the structured walk-through test is to confirm the effectiveness of the plan and to identify gaps, bottlenecks, or other plan weaknesses.

- **Simulation Testing**

  The organization simulates a disaster during non-business hours (partial recovery procedures or full) so normal operations will not be interrupted.
Phase 5: Continuous Monitoring
BUSINESS CONTINUITY PLAN CHANGE MANAGEMENT

- Monitor Business Needs and Technology Changes
- Reassess RTOs
- Test Plans
- Update Plans
- Redistribute Plans
- Retrain Employees
- Test Plans
- Update Plans
Auditing The Business Continuity Plan
AUDITING THE BUSINESS CONTINUITY PLAN

**Business Continuity Policy**
- Assess entity coverage
- Management acceptance and approval
- Periodic review and updates
- Monitoring controls
- Names BC Committee and states responsibility

**Business Continuity Plan**
- Assess incident assessment and disaster declaration procedures
- Confirm chain of command is documented
- Confirm disaster notification and communication procedures

**Business Impact Assessment/Risk Assessment**
- Existence of BIA
- Criticality of processes and systems determined
- Periodic updates of the BIA /RA
- Management approval

**Business Process / Business Unit Recovery Plan**
- Recovery Plans exist and are formatted to follow the BIA
- Recovery strategies document all required supports
- Employee / customer / vendor contact information is available and current
- High likelihood events are identified and guidance for these events exist
- Plans for salvage, cleanup and rebuilding are addressed
- Alternate operational arrangements are pre-arranged
AUDITING THE BUSINESS CONTINUITY PLAN

Disaster Recovery Plan
- DR Plan is aligned with the overall plan to support business operations
- Critical systems are identified and prioritized
- Offsite storage and recovery facilities are determined and are periodically assessed for viability
- Hardware/software inventories exist
- Standard and Emergency contracts exist for key vendors
- Alternate processing arrangements exist

Recovery Testing / Staff Training
- Procedures for testing and training exist
- Testing of all functional areas has been performed
- Backups are performed and are periodically tested
- Organization members are trained regarding incident response and disaster responsibilities
- Necessary resources are identified and procedures in place to ensure availability
Business Continuity Resources

- Disaster Recovery Institute International   www.drii.org
- Disaster Recovery Journal     www.drj.com
- CSO Online                           www.csoonline.com
- Business Continuity Institute        www.thebci.org

Industry Best Practices:
- ✔ BS 2599-1:2006 (UK)
- ✔ NPFA 1600
- ✔ HB 221:2004 Business Continuity Management (Australia)
- ✔ ASIS Int’l. /BSI BCM.1-2010 Business Continuity Management Systems
- ✔ ISO/IEC 27031:2011 Guidelines for Information and Communication Technology Readiness for Business Continuity
Questions?

Jennifer Brandt, CISA | Principal
M (918) 607-5879
O (918) 728–3300
jennifer.brandt@stinnett-associates.com

www.STINNETT-ASSOCIATES.com