BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

Marci McCloskey, CISA, ABCP
Toan Nguyen, CIA, ABCP
SPEAKER INFORMATION

Marci McCloskey, CISA, ABCP

Oklahoma City, Oklahoma

University of Oklahoma

Stinnett: 2015, Sarbanes-Oxley, IT Internal Audit

Traveling, adoring my Pomeranians, CycleBar, ultimate foodie
Toan Nguyen, CIA, ABCP

Oklahoma City, Oklahoma

University of Texas at Dallas

Stinnett: 2015, Internal Audit, Higher Education/Non-Profits

Baking, running, and scholarship pageants
Stinnett & Associates, LLC (Stinnett) is a **professional advisory firm** which excels at maximizing value for both **public and private organizations**. Our services are designed to help clients more effectively manage risk and improve performance by streamlining processes, reducing costs and enhancing controls.

Stinnett offers **co-source and outsource solutions** within a diverse range of services, including:

- Internal Audit
- Vendor Audit
- Cybersecurity
- Business Process Improvement
- Fraud & Forensics
- Sarbanes-Oxley
- Business Continuity / Disaster Recovery
- Governance Risk & Compliance
- Foreign Corrupt Practices Act
- Cost Recovery
- Information Technology
- Banking / FDICIA
- Sales and Use Tax Recovery
- Joint Venture Audit

**Doing the Right Thing**

Founded in 2001, Stinnett has grown to have offices in **Dallas, Denver, Houston, Oklahoma City, San Antonio and Tulsa**. We provide services to several Fortune 1000 companies as well as many mid to large-size organizations with global operations.

We are primarily recognized for offering relevant advisory assistance and exemplary client service with the unique ability to deliver what our clients need. Working toward solutions, we have a reputation for “**doing the right thing**.”

Stinnett is a **certified Women’s Business Enterprise** through the Women’s Business Enterprise National Council. We pride ourselves on being trusted business advisors who focus on assisting clients to reach strategic milestones positioning them for future success.
AGENDA AND LEARNING OBJECTIVES

✓ Understand the purpose and benefit of Business Continuity Plans and IT Systems Disaster Recovery Plans

✓ Understand core components of a comprehensive business continuity plan and IT disaster recovery plan

✓ Understand the key phases of establishing a BC and DR program and the approach for each phase

✓ Describe how to approach business continuity planning to collect critical information from the organization and then validate/test the plan documentation later.
In honor of the IIA San Antonio’s I Heart Audit Conference:

- San Antonio is the most visited city in Texas.
- Oldest church in Texas – San Fernando Cathedral (est. 1738)
- Fiesta San Antonio is the city’s biggest and most attended festival.
- Largest Mexican market outside of Mexico – El Mercado Shopping District
- Church’s Chicken first opened in San Antonio – 1952
- San Antonio’s largest employers include: H-E-B (20,000); USAA (17,000); Cullen/Frost Bankers (3,982); Bill Miller BBQ (3,540)
Disaster recovery and contingency planning have evolved throughout the years. “Disaster” has taken on a new meaning:

- Cyber attacks
- Natural disasters
  - Flooding (Hurricane Harvey)
  - Wild fires (California)
- Power outages (heat wave in San Antonio)
- Human error
- Disgruntled employee sabotages systems
- What else?
Business Continuity vs. Disaster Recovery

Terminology

- Business Continuity: Continuation of or resumption of critical business processes.
- Disaster Recovery: Continuation of or resumption of technology services. DR is a subset of the overall BC program.

BCP considers all of the necessary elements to continue or restore operations, not just the computer systems:

- Alternative office space needs, including consideration of the complete destruction of company buildings
- Communication strategies (employees, customers, suppliers) and properly handling PR and media issues
- Employee responsibilities and instructions
- Computers, printers, 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
BCPs provide additional value and benefit:

- Clear understanding of the most critical processes
- Increased confidence in the company by Customers, Business Partners, Employees, Investors, Board
- Compliance with Laws and Regulations (HIPAA, etc.)
- Potential positive impact on insurance and risk management
- Competitive advantage
  - Preparation for the inevitable before it occurs
  - Serve your customers when your competitors cannot
BUSINESS CONTINUITY PLANNING PROCESS
## BUSINESS CONTINUITY PLANNING PROCESS

<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 <strong>Business Impact Assessment</strong>, 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 <strong>IT Gap Analysis</strong>.</td>
<td>Develop specific <strong>plans for each critical process and department</strong> to restore operations.</td>
<td>Document and <strong>communicate</strong> the plans. <strong>Test</strong> the recovery plans to verify objectives are achieved. <strong>Train</strong> management, key crisis response teams and employees.</td>
<td>Monitor business <strong>changes and update</strong> policies and procedures as needed (minimum annually). Conduct refresher <strong>training</strong> and periodic <strong>testing</strong> as necessary.</td>
</tr>
</tbody>
</table>
PHASE I: BUSINESS IMPACT ASSESSMENT
The Business Impact Assessment (BIA)

• Determines the critical business processes and related resources within the organization.
• Establishes a foundation for developing well-reasoned and prioritized responses to disaster.
• Focuses on reestablishing the most critical business processes to minimize loss and disruption.

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

1. Identify key process or operational areas in the business (e.g., AP, Payroll, Operations)

2. Identify the key process owners to interview

   - Priority of processes and process recovery time requirements
   - Critical systems the processes depend on and system recovery time requirements (also known as Recovery Time Objective)
   - Interdependencies: systems, departments, processes, people, third parties
   - 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)

   - Critical people, files, systems, abilities
EXAMPLE BIA QUESTIONS

1. For each department, identify the **critical processes** that must be resumed in the event of a disaster or outage.

2. For each critical process, identify the **Maximum Tolerable Downtime (MTD)**, which is the maximum acceptable time for a department's critical processes to be unavailable before *manual* processes need to begin.

3. Identify the IT systems and interfaces that support the critical processes.
   1. For each critical system, identify the **Recovery Time Objective (RTO)**, which is the maximum acceptable *time to recover* or restore IT systems in the event the IT systems are unavailable during a disaster.
   2. For each critical system, identify the **Recovery Point Objective (RPO)**, which is the maximum acceptable amount of *data entry loss* the department can sustain.

4. Identify **critical team members**. Identify any specialized skills or access those critical team members have. Identify whether the team members need to perform their work onsite or offsite.

5. Identify **personnel from other teams** that could perform the work if the original department team was unavailable. Are documented procedures available as reference documents for substitute staff?

6. Other
BIA DELIVERABLES

1. List of key process or operational areas in the business (*e.g.*, AP, Payroll, *Operations*) and the key process owners

2. Priority of processes and process recovery time requirements (manual)

3. Recovery Time Objective (RTO): Critical systems the processes depend on and system recovery time requirements

4. Recovery Point Objective (RPO): 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.

5. Other useful information and recommendations
# RECOVERY TIME OBJECTIVES

<table>
<thead>
<tr>
<th>Critical System/Application</th>
<th>APPLICATION RECOVERY TIER</th>
<th>Geology</th>
<th>Revenue</th>
<th>Accounts Payable</th>
<th>Drilling</th>
<th>Midstream</th>
<th>Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>StarSteer</td>
<td>Tier 1</td>
<td>1 day</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>SSI</td>
<td>Tier 1</td>
<td>N/A</td>
<td>2 days/ 2 weeks</td>
<td>3 days</td>
<td>4 days</td>
<td>N/A</td>
<td>2 weeks</td>
</tr>
<tr>
<td>Merrick ProCount</td>
<td>Tier 1</td>
<td>1 week</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>1 week</td>
<td>N/A</td>
</tr>
<tr>
<td>Petra</td>
<td>Tier 2</td>
<td>1 week</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Petrel</td>
<td>Tier 2</td>
<td>1 week</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ArcGIS</td>
<td>Tier 3</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>AFE Navigator</td>
<td>Tier 3</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>&lt;30 days</td>
<td>N/A</td>
</tr>
<tr>
<td>Techlog</td>
<td>Tier 3</td>
<td>&gt;30 days</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Infrastructure/Communications**

<table>
<thead>
<tr>
<th></th>
<th>APPLICATION RECOVERY TIER</th>
<th>Geology</th>
<th>Revenue</th>
<th>Accounts Payable</th>
<th>Drilling</th>
<th>Midstream</th>
<th>Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet connectivity</td>
<td>Tier 1</td>
<td>1 day</td>
<td>1 day/ 2 weeks</td>
<td>3 days</td>
<td>4 days</td>
<td>1 day</td>
<td>&lt;1 week</td>
</tr>
<tr>
<td>Email</td>
<td>Tier 1</td>
<td>1 day</td>
<td>N/A</td>
<td>3 days</td>
<td>N/A</td>
<td>1 day</td>
<td>&lt;1 week</td>
</tr>
<tr>
<td>VPN / Remote Access</td>
<td>Tier 1</td>
<td>1 day</td>
<td>1 day/ 2 weeks</td>
<td>3 days</td>
<td>4 days</td>
<td>1 day</td>
<td>1 day</td>
</tr>
<tr>
<td>Network (File Shares, K drive)</td>
<td>Tier 1</td>
<td>1 day</td>
<td>1 day/ 2 weeks</td>
<td>3 days</td>
<td>&lt;30 days</td>
<td>1 day/ 4 days</td>
<td>2 weeks</td>
</tr>
</tbody>
</table>

**Third Party Hosted (alphabetical order) - Internet Access is Only Requirement (NOT INCLUDED IN IT GAP ANALYSIS)**

<table>
<thead>
<tr>
<th></th>
<th>APPLICATION RECOVERY TIER</th>
<th>Geology</th>
<th>Revenue</th>
<th>Accounts Payable</th>
<th>Drilling</th>
<th>Midstream</th>
<th>Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Altus</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>2 weeks</td>
</tr>
<tr>
<td>Iberiabank (key fob needed)</td>
<td>N/A</td>
<td>N/A</td>
<td>3 days</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ScadaVisor (Fielding system)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>&lt;1 day</td>
</tr>
</tbody>
</table>
### RECOVERY POINT OBJECTIVES

<table>
<thead>
<tr>
<th></th>
<th>2 days</th>
<th>3 days</th>
<th>4 days</th>
<th>5 days</th>
<th>7 days</th>
<th>10 days</th>
<th>2 weeks</th>
<th>1 month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geology</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts Payable</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Production</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revenue</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reserves</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drilling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Purchasing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Regulatory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Land</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

- RPO should drive data backup strategy and timing (i.e., daily, hourly).
- RPO could drive process changes
PHASE 2: IT ASSESSMENT/GAP ANALYSIS AND DEVELOPMENT OF THE DR PLAN
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.
HOW TO PERFORM 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 and abilities to the Recovery Time Objectives and Recovery Point Objectives of the critical business processes
- Determine any gaps between the business RTOs and RPOs and IT’s current recovery capabilities
- Present gaps to management
THE DISASTER RECOVERY PLAN

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

- An effective DR plan will address these types of situations:
  - Loss of power, equipment, or connectivity for an extended period of time.
  - Loss of access or use of the data center for an extended period of time.
  - How users can continue working offsite.
PHASE 3: BUSINESS PROCESS RECOVERY PLANS
THE BUSINESS CONTINUITY PLAN

Elements of an effective BC plan:

- Identification of Emergency Response Team (ERT) members and their roles and responsibilities
- Emergency Response information
- Communication plan (employees, customers, vendors, other third-parties, media)
- Contact lists
- Alternate location plan, including necessary equipment
- Department-specific recovery / continuity plans, including procedures for how to perform key processes (system-supported and manually)
- IT Disaster Recovery plan
CONSIDERATIONS FOR A SUCCESSFUL BUSINESS CONTINUITY PLAN

- *Don’t bite off too much at once.* Many 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 and focus on core corporate operations. Then expand to other operations/locations.

- *Clearly identify the targets* and stay focused throughout the project.

- *Keep it simple* (or at least as simple as prudent)

- *Communicate! Communicate! Communicate!*

- *Keep an eye out for Lessons Learned*
PHASE 4: PLAN TESTING
The purpose of BCP Testing is to reveal weaknesses in the following:

- Completeness of information, including work procedures for critical processes
- Personnel’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 BCP testing methodologies include:

<table>
<thead>
<tr>
<th>Structured Walkthrough</th>
<th>Table-top Exercise</th>
<th>Simulation Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCP team members meet to verbally walk through the documented BCP to confirm the effectiveness of the plan and to identify gaps, bottlenecks, or other plan weaknesses.</td>
<td>Recovery teams are presented with a disaster scenario. Recovery team members assume their business continuity roles as described in the plan and simulate the recovery activities.</td>
<td>The organization simulates a disaster during non-business hours (partial recovery procedures or full) so normal operations will not be interrupted.</td>
</tr>
</tbody>
</table>
PHASE 5: PLAN MAINTENANCE
Business Continuity Plans are living documents and should be maintained, updated annually or when the business undergoes changes that would affect the existing Plan.

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 IT RTOs and RPOs are still accurate and still acceptable to management, including any known gaps
- 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
ONGOING MAINTENANCE CYCLE

Monitor Business Needs and Technology Changes

Redistribute Plans and Retrain Employees

Reassess Needs (BIA Refresh)

Test Plans

Update Plans
REMEMBER...

• Having the right people and the right resources available

• Having the right relationships in place BEFORE and during event

• Keeping people informed and up to date
Questions
CONTACT INFORMATION

Toan Nguyen | Senior Manager
Tel: (888) 808-1795
Email: toan.nguyen@stinnett-associates.com

Marci McCloskey | Manager
Tel: (888) 808-1795
Email: marci.mccloskey@stinnett-associates.com

www.stinnett-associates.com