Implementing and Auditing a Successful Business Continuity Plan
Agenda

• Introductions
• Training Overview and Objectives
• BCP Background and Importance
• BCP Lifecycle
  • Initiate
  • Risk Assessment
  • Business Impact Analysis
  • Recovery Organization Structure and Business Continuity Plan (BCP)
  • Testing and Maintenance
• Conclusions and Takeaways
Business Continuity Planning – Introductions

Dan Steiner, MBA, CPA, CFE, ARM
Consulting Manager at Baker Tilly Virchow Krause

Alicia Thornton, MBA, CPA, CIA
Audit Manager at Oshkosh Corporation

Eric Wunderlich
Consulting Manager at Baker Tilly Virchow Krause
Training Overview and Objectives

Overview
• We will cover the lifecycle of a BCP program, with specific emphasis on the following areas:
  • Business Impact Analysis
  • Designing a living BCP
  • Testing & Maintenance

Objectives
• Understand what’s involved in a full BCP Program (for those that are unfamiliar)
• Provide insights based upon field experience that can be applied to Internal Audit work and BCP program work
• Provide you with tools that you can bring back to your company to improve upon BCP programs
• Improve ability to audit BCP programs and provide targeted recommendations
Successful Business Continuity Planning

Successful business continuity planning....... 

• Involves the entire organization 
• Requires clear and consistent communication 
• Encompasses how employees will communicate, where they will go and how they will keep doing their jobs 
• Prepares the organization for disruptive events
The value of preparation

Cyril Richard “Rick” Rescorla  
Hayle 1939 - 2001 New York  
Rick Gave His Life In The Terrorist Attack  
On The World Trade Center, New York  
September 11th 2001,  
While Directing The Evacuation.  
His Actions On The Day Saved Over 2,700 Lives.  
“Greater Love Hath No Man”
Background and Importance

---

Risks to Business Continuity

TORONTO: Forest Defenders Strike!
Six-legged machines tear through more and more of the Ontario Boreal Forest on a daily basis. Already, half of the stretch of northern Ontario that comprises the Boreal has been lacated by logging companies such as Weyerhaeuser, Bowater and Abitibi-Consolidated using unsustainable overcutting with detrimental effects to the environment and their own future.

Chavez says could nationalize Colombian firms

AIG Facing Liquidity Crisis, Seeks $40 Billion Loan from Federal Reserve

Venezuela will seek goods from other countries to replace products it gets in its $6 billion annual commercial exchange with Colombia, Chavez said. “We’re going to make a map, mini-

Blaze Breaks Out at Paper Warehouse

May 4, 2007 (WPVI) — New Jersey firefighters battled an internal inferno at a paper products warehouse overnight. Before it was over the blaze reached 3 alarms, and one firefighter was injured in the fight.

Dior sacks John Galliano over anti-Semitic tirade

John Galliano was sacked as chief designer of Christian Dior last night after a series of claims that he had subjected women to tirades of anti-Semitic abuse.

Insurance American International Group Inc., working to stave off rating downgrades [See related article] and shore up the capital of its holding company, has made an unprecedented approach to the Federal Reserve seeking $40 billion in short-term financing, the New York Times said.

---
Why is a BCP Important?

- 61% of companies surveyed had to invoke their BCP
- 43% had to invoke it more than once
- Key Causes: Natural Disaster, Power Outage, IT Failure, Flood, Fire, Telecom Failure, Utility Outage, Pandemic

- What were the top 3 lessons learned from invocation?
  - There had not been enough training and awareness efforts across the company: 48%
  - Plans didn’t adequately address emergency communications: 37%
  - Key staff had not been included in testing; as a result they did not know their roles and responsibilities in the plans: 25%

- Cyber attacks

Source: Forrester – the State of Business Continuity Preparedness 2011 from the Disaster Recovery Journal
Business Continuity
The Good, the Bad and the Unprepared

Other alternative suppliers
Business Continuity
Planning – Overview

Business continuity management program

• Implementation of a business continuity management program should result in:
  • Critical business functions meeting client or customer needs when events occur
  • Clear communication and decision making during an event
  • High degree of confidence that the plan can be executed

• The program should include the following activities:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify program leader and gain commitment</td>
<td>Evaluate scenarios for likelihood and impact analysis</td>
<td>Understand impact of lost operations and establish recovery objectives</td>
<td>Develop a command and control structure and ensure a communication plan is established</td>
<td>Identify and document steps to meet recovery objectives</td>
<td>Validate feasibility, ensure employee awareness, and update plan to address gaps and assumptions</td>
</tr>
</tbody>
</table>
## Business Continuity Planning – Overview

<table>
<thead>
<tr>
<th>Plan</th>
<th>Responsibility</th>
<th>Focus of Plan</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency Response</td>
<td>Facility</td>
<td>Get the people out safely</td>
<td>Develop procedures and policies to ensure the safety of employees, visitors, and community immediately after the occurrence of an event.</td>
</tr>
<tr>
<td>Crisis Management</td>
<td>Crisis Management Team</td>
<td>Protect the company</td>
<td>Focus corporate efforts to respond to any incident that has a significant negative impact to the enterprise.</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>Facility or Major Function</td>
<td>Get the business up and running</td>
<td>Establish procedures that provide for the continuation of business operations in the event of a crisis on the corporate, divisional, or site level.</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>IT</td>
<td>Get the systems up</td>
<td>Establish system recovery plans to restore technology (access to data and systems) in the event of a disaster.</td>
</tr>
</tbody>
</table>
Business Continuity Plan

**Objective:** back-to-normal as quickly as possible

Timeline

- **Incident – Time Zero**
  - Starts within minutes after the onset of an event

- **Emergency Response**
  - Minutes to days

- **Crisis Management**
  - Minutes to days – depending on what’s needed to survive

- **Business Continuity**
  - Minutes to days

- **IT Disaster Recovery**
  - Minutes to days

- **Back to normal**
Business Continuity Planning – Overview

Business continuity management program - Involvement

• Who are you?
  • Risk Manager? Internal Auditor? Consultant?

• Who here has some responsibility related to their company’s Business Continuity Planning?

• Who has taken a class on Business Continuity Planning?

• Who has actually tested their plan?

• Who has audited a plan?
1. Program Initiation

• Establish senior leader commitment
• Name individuals to applicable roles
  • Team Leader
  • Team Coordinator
  • Deputies
  • Functional owners
• Communicate across organization
• Establish organizational network
Selling Points of a BCP

- BCP is about protecting your core assets
- View BCP as a long term competitive advantage
- Start by connecting BCP to the objectives of your organization
- What are the business plans for growth, restructuring, short/long term strategies?
- A BCP plan should have the fullest possible understanding of the important processes of the business and between you, your customers and suppliers.

“The time to repair the roof is when the sun is shining”

John F. Kennedy
Beginning a BCP Audit Program

- Is the program currently being audited?
- Who is responsible for auditing the BCP program?
- What level of sophistication is the audit program (i.e. basic checklist review or full blown mock crisis)?
Internal Audit Involvement

Role of Internal Audit in Program Initiation

• Become a knowledge leader and increase organizational awareness

• Help to identify appropriate parties and reporting channels

Areas of focus for Internal Auditors

• Have the right parties been engaged?

• What communication channels will be used?

• How will the program be governed?
2. Risk Assessment

Key Success Factors

- Identify and evaluate risks annually
- Evaluate current mitigation and recommend enhancements
- Develop contingency plans for those risks with the highest impact
- Ensure your BCP plan addresses the high impact, low probability risks (Black Swans)
2. Risk Assessment

- Inventory an organization’s universe of risk
- Determine the best method, or combination of methods, for effectively identifying risk
  - Facilitated workshops
  - Interviews or surveys
  - Department wide surveys
  - External review
- Schedule periodic sessions to reevaluate the risk universe and identify emerging exposures
- Leverage risk assessments performed previously
2. Risk Assessment

Develop tools to effectively assess risk
Internal Audit Involvement

Role of Internal Audit in the Risk Assessment

• Subject Matter Expert

• Facilitator and Collaborator

Areas of focus for Internal Auditors

• Have we accounted for all categories of risk and possible scenarios?

• Are sufficient mitigating controls in place?

• Black Swans vs. Leaky Faucets
3. Business impact analysis

- **A Business Impact Analysis (BIA)** is an information-gathering exercise designed to methodically identify:
  - The processes or functions performed by an organization
  - The resources required to support each process performed
  - Interdependencies between processes and departments
  - The impact of failing to perform a process
  - The criticality of each process
  - The Recovery Time Objective (RTO) for each process
  - The Recovery Point Objective (RPO) for each process

- The BIA, along with the Risk Assessment, provides the foundation for developing and selecting a business continuation strategy that will allow the organization to continue to perform critical processes in the event of a disruption.
3. Business impact analysis

- How long can your business last without the following processes in place:
  - Operations (Production / Engineering / Processing)
  - Customer Service
  - Financial (A/R, A/P, Reporting)
  - Procurement
  - Logistics
  - Communications

- How much could you afford to lose if an incident prevented you from doing business for days, weeks or months?

- How would employees, business partners, suppliers, customers and potential customers react if your business received adverse publicity because you were unprepared for an incident?
# 3. Business impact analysis

![Flowchart showing the process of business impact analysis]

<table>
<thead>
<tr>
<th>Process</th>
<th>Impact Description (Minor, Moderate, Significant)</th>
<th>Example of Impact to Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>First 24 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td>24 – 48 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Up to 1 week</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Up to 2 weeks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>First 24 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td>24 – 48 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Up to 1 week</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Up to 2 weeks</td>
<td></td>
</tr>
</tbody>
</table>
3. Business impact analysis

• Prioritize processes into time categories
  • AAA – Immediate Recovery
  • AA – Up to 4 Hours for Recovery
  • A – Same Day Recovery
  • B – Up to 1 Week for Recovery
  • C – Up to 2 Weeks for Recovery
  • D – Greater than 2 Weeks for Recovery

• Once classified, determine what mitigation or recovery strategy is appropriate and how much investment is reasonable
3. Business impact analysis

- Identify resources required to meet the Recovery Time Objectives

<table>
<thead>
<tr>
<th>Time</th>
<th>People</th>
<th>Premises</th>
<th>Technology</th>
<th>Information</th>
<th>Suppliers/Partners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First 4 hours</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-24 hours</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to 1 week</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to 2 weeks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. Business impact analysis

- BIAs will feed into your recovery strategies
- Recovery time objectives (and recovery point objectives) should be weighed against the cost of retaining the capability
  - Faster and more complete recovery generally costs more, but may be necessary
Internal Audit Involvement

Role of Internal Audit in the Business Impact Assessment (BIA)

• Independent and objective participant
• Facilitator and Collaborator

Areas of focus for Internal Auditors

• Time sensitivity, not criticality (i.e. How soon do we start to see the impact?)
• What keeps the business running and what can wait until later?
• Interdependencies of business processes and operations
4. Implement recovery organization structure

- Develop the chain-of-command
- Assign responsibility
- Build the organization structure required for execution of the BCP
- Establish command and control teams for critical areas
4. Implement recovery organization structure

- Roles and responsibilities
  - Who is the top decision maker?
  - Who is responsible for communicating with the media?
  - How and where should individuals report situations which might trigger the plan?
Internal Audit Involvement

Role of Internal Audit in the Recovery Organizational Structure

• Communication and awareness

Areas of focus for Internal Auditors

• Tone at the top

• Have responsibilities and communication channels been adequately identified and disseminated?
5. Develop Continuity Plans

- Need to pull together all the key components into a working document
- **Key components of a continuity plan include:**
  - Program administration
  - Updated contact information
  - Business impact analysis
  - Business continuity strategy
  - Business continuity tactical plans (i.e. detailed procedures, resource requirements, logistics)
  - Business contact list
  - Alternative suppliers
  - Revision history
5. Develop Continuity Plans

- Program administration
  - Scope
  - Objectives
  - Maintenance (both the program and the documents)
  - Assumptions

- Updated contact information

<table>
<thead>
<tr>
<th>Team (IT, Production, Support)</th>
<th>Member Name</th>
<th>Email</th>
<th>Work Telephone</th>
<th>Home / Cell Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. Develop Continuity Plans

- **Business Continuity Strategy**
  - Make sure to understand available alternatives, their advantages, disadvantages, cost ranges
  - Consider mitigation as a recovery strategy
  - Compare internal vs. external solutions
  - Develop both entity wide and business unit strategies
  - Ensure management is committed to developed strategy
5. Develop Continuity Plans

- Business continuity tactical plans

<table>
<thead>
<tr>
<th>Facility Shut-Down Due to Natural Hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Complete?</strong></td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
5. Develop Continuity Plans

- Business contact list

<table>
<thead>
<tr>
<th>Company</th>
<th>Contact Name</th>
<th>Emergency Telephone</th>
<th>Business Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Alternative suppliers
  - Relationships need to be cultivated in advance
  - May be constrained by cost realities of supply chain
5. Develop Continuity Plans

- Revision history

<table>
<thead>
<tr>
<th>Revision No.</th>
<th>Date</th>
<th>Description of Changes</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Role of Internal Audit in the Development of Continuity Plans

• Provide support as needed to involved parties
• Assist with the development of templates and documentation
• Enforce standards and guidelines as appropriate

Areas of focus for Internal Auditors

• Have guidelines / templates been developed and communicated to involved parties?
• Does the plan address key components such as Risk Assessment, BIA and Recovery Time Objectives?
6. Testing and maintenance

Why test the plan?

• Develop awareness across the organization
• Train employees to ensure understanding of roles
• Test the BCP to ensure feasibility and to help train on execution
• Ensure plan elements are up to date and assumptions are valid
• Identifies gaps and inefficiencies
• Highlights level of readiness
• Don’t forget training for:
  • Security staff, new hires, receptionists
6. Testing and maintenance

Where do you start? - Walk before you run

- Refresh the actual plan with participants
  - Conduct a basic verbal walk through of the plan
- Start with your own department
  - Continue expanding into larger and more complex areas of the business
  - Continually fine-tune and enhance exercises

Who is involved?

- Facilitator, Scribe, Role players, Observers
- Those being tested would include anyone required to be involved in the actual business continuity plan
What needs to be planned?

What are the goals and objectives of this exercise?
• Test communication? Understand roles? Improve the plan?

What is the skill level of the team?
• Consider individual’s roles within organization and awareness of plan

What scenario will be tested?
• Consider realism and relevance of scenario

How extensive will the exercise be?
• Simple tabletop or company wide? Third Party involvement?

How will the script be developed?
• Will phones be necessary? Will video be utilized? Will volunteers be needed?
• Actions should be carried out based on what plan is in place and not what will be, maybe, someday in place

Basic rules of facilitation
• Establish and communicate rules, expectations, and assumptions
Incident Response Exercise Scenario — February 2012

Introduction to the exercise. *(Dan Steiner and Greg SJ)*

- You will receive information in various ways over the next 90 minutes.
- After you receive information, talk through your reaction: the action steps you would take, who you would communicate with, and what information you would be looking for.
- Keep your cell phone on — incoming calls are part of this exercise.
- Individuals in remote locations should have their laptops available — incoming emails are a part of this exercise.
- Your objective is to understand your role during a crisis.
- Discuss the actions you would take in contacting resources (we will not role play or actually contact them).
- You may feel overwhelmed with information at times; do your best to behave as you would in a real crisis situation. You may also feel moments of downtime; use this to let the information sink in.
- Remember the situation is intended to be as realistic, however, if some details may seem unrealistic, try to focus on the value add of the exercise.
- After the exercise is complete we will spend 30 minutes sharing our thoughts.
- TAKE ATTENDANCE / NOTE NAME TAGS — who will be the backup? Who will step up to leadership roles?

Greg will text Eric / signal with reference to STEP # at go time.

**Plan A:** Cell phone call.
**Plan B:** Eric unmutes his conference call connection and indicates verbally to the group who the call is directed to.
**Plan C:** Dan/Greg read the phone call script aloud.

**STEP #1:** A call from customer service to Joe — COO at XXX-XXX-XXXX or Jennifer SVP Operations at XXX-XXX-XXXX *(Eric):*

- Caller reports that several Platform users have made complaints of unusual activity on their account.
- Role: Customer service rep
  - Script: *Hello Joe? This is John from customer service. I have some pertinent calls to report to you. This morning our department has received multiple complaints from customers noting unusual activity in their accounts (PAUSE). Some of them have given us specifics that their email accounts linked to our accounts have spam from people in their “contacts” folder and emails of “999999” appearing from people they don’t know. Others...*
6. Testing and maintenance

Helpful Tips:

Be flexible and build in cushion
• Similar to a BCP, participants may not act as anticipated on paper
• Be prepared to introduce a new pieces of information or slow things down if the session is not running as expected

Make sure someone is documenting performance
• The facilitator should not also be responsible for notes
• Observe positives as well as opportunities

Post-op discussion
• Start with feedback from the actual scenario actors
• How was communication?
• Who was in charge?
• Who is responsible for talking with the media?
• What resources were needed but not available?
• Were the goals of the scenario accomplished?
• Get feedback from all involved to continue improving the sessions
6. Testing and maintenance

Awareness and Communication

Word of mouth can be your best advertisement
• As successful sessions are held, more teams will have interest
• Teach teams how to run their own scenarios

Be the first to reach out and collaborate
• BCP involves many teams
• Build out stronger capabilities by working with other groups

Make sure that senior leaders understand they are not alone
• Some executives may not even realize there’s a predefined plan
• Some executives may not even realize they have a team to support them

Keep the sessions updated and relevant
• As the business is exposed to new risks, update the sessions to stay relevant (i.e. social media)
Conclusions

What are the critical items I need to remember?

• Have a business continuity and disaster recovery plan
• Appoint an accountable BCP team (including a plan owner)
• Conduct a risk assessment
• Base plan on risk assessment and BIA
• Key updates should be made quarterly relative to people, technology and organization
• Ensure plan is communicated
• Test the plan at least annually
What do you think?
Share your thoughts about this presentation on Twitter using the hashtag #IIACHI

Follow us on Twitter
@IIAChicago

Not on Twitter?
Visit our Social Media booth in the Exhibit Hall to join the conversation today!