AGENDA

BCM OVERVIEW

BCM METHODOLOGY

PERSECTIVES & LESSONS LEARNED

ADDITIONAL REFERENCE MATERIALS

INTERNAL AUDIT’S ROLE IN BCM
WHO IS WILLING TO “BET” THE BUSINESS SOMETHING WON’T HAPPEN

The Facts:

• As per the joint survey report from the Business Continuity Institute and BSI on organizational threat perceptions, the leading threats rated by level of concern in 2014 were:
  – Unplanned IT and telecom outages (77% of respondents extremely concerned or concerned)
  – Data breach (73%)
  – Cyber attack (73%)

• The percentage of people showing concern for all three of these threats has increased considerably during 2014, and are significantly higher rated than the next set of threats:
  – Adverse weather (57%)
  – Interruption to utility supply (56%)
  – Security incident (53%)
VALUE THROUGH RISK MITIGATION

• Regulatory Risk
  – A growing number of corporations are held accountable by regulatory bodies to maintain tested continuity plans
  – Failure to follow plans can lead to fines and in some cases prohibit from operating or delivering products or services

• Financial Risk
  – Responding to customer demands
    ✓ Hold suppliers accountable to maintain BCPs and protect its supply chain
    ✓ Hold suppliers accountable for delivery of products or services
  – Understanding officer liability
    ✓ Directors and officers can be held liable for a company’s response to a business interruption, leading them to be more likely to enforce an effective BCM program
  – Minimizing single points of failure
    ✓ Ex. Using only one supplier and having that supplier go out of business
    ✓ Solution: Implement BCM solutions to make sure operations can be resumed quickly

• Reputation Risk
  – Protecting the company’s brand in the face of growing competition
  – Maintaining the public’s approval for the way the company handles a crisis
Drivers & Key Indicators of Need

- Corporate governance (e.g., ERM)
- Customer demands
- Experienced a recent disruption
- Regulatory requirements
- Current events and the perceived threat (e.g., single points of failure)
- Director and Officer liability
- Lack of appropriate BCM ownership
- Cannot afford downtime

Misconceptions

- Plans can prevent disasters
- The plan completes the project
- Recovery means ASAP, or immediately
- “Generic, cookie cutter” plans work
- The BCM software will create our plan

“Corporate leaders have an obligation to the stakeholders of their organizations to ensure that everything that can reasonably be done to protect the business is done.” - Gartner Group
# BUSINESS CONTINUITY MANAGEMENT

## Business Continuity Management (BCM)

The analysis and evaluation of strategies, development of approaches, testing and implementation of plans that meet an organization’s continuity needs from a people, process, and technology perspective. The BCM program should incorporate industry best practices as well as any relevant regulatory or industry-specific compliance requirements, such as HIPAA, PCI, privacy/notification laws, etc.

<table>
<thead>
<tr>
<th>Crisis Management &amp; Communications</th>
<th>Business Resumption</th>
<th>IT Disaster Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focuses on limiting the impact of an event on an organization’s people, infrastructure and essential business functions. Effective responses require proactive communication and leadership immediately following a significant disruption.</td>
<td>Focuses on the evaluation of those people, processes, technology and data that are vital to the organization's operations to mitigate business, environmental, man-made and technology risks inherent to their business by developing plans that direct personnel how to operate in a diminished capacity.</td>
<td>Links critical business processes to the IT resources needed to support them (whether internal to the organization or outsourced). Accounts for critical business process needs that rely upon key systems and data in order to execute successfully.</td>
</tr>
</tbody>
</table>
TYPICAL DISRUPTION TIMELINE

Disaster Occurs

Enterprise-wide and process-specific situation assessment performed.

Recovery procedures are enacted to respond to disaster and prepare to resume business and IT operations.

Alternative facilities are prepared to house personnel and technology as necessary

IT/Business Recovery

Continuous Communication Across the Enterprise

Operate at Alternative Facilities if Necessary

Validate Personnel Safety and Execute Crisis Communication Plan

Business processes operate below normal levels, but product is manufactured, received, sold, and shipped in some capacity.

IT Systems and Data are available in some capacity in order to support business processes

As time passes, operations return to near-normal levels.

Business Resumption

Normal Operations

Business has recovered from the disaster. Technology, facilities, or supply chain have returned to normal levels.

Business metrics may or may not return to normal.

Normal Operations

Business operates status quo.
BCM METHODOLOGY
BUSINESS CONTINUITY METHODOLOGY

An effective Business Continuity Program uses an ongoing, iterative lifecycle to facilitate the development and maintenance of strategies, plans and actions which provide protection or alternative modes of operation for those activities or business processes which if interrupted, might bring about a seriously damaging or potentially fatal loss to the enterprise.

Business Assessment

- BCM Diagnostic
  - Business Impact Analysis
  - BCM Program Governance

- Risk Assessment
- Business Impact Analysis
- BCM Program Governance

Strategy Design

- Crisis Management Strategy
- Business Recovery Strategy
- IT Disaster Recovery Strategy
- IT Architecture Strategy

Implementation

- Implement Crisis Management Plan
- Implement Business Recovery Plan
- Implement IT Disaster Recovery Plan
- Implement IT Architecture

Quality Assurance

- Test Crisis Management Plan
- Test Business Recovery Plan
- Test IT Disaster Recovery Plan
- BCM Quality Assurance

On-Going BCM Lifecycle Planning & Management
BUSINESS CONTINUITY LIFECYCLE

Leading Practices

- Identify risks that could make an organization vulnerable to business interruptions per location
- Understand the effectiveness of risk-mitigation controls
- Identify greatest risk areas (in terms of probability and impact)
- Prioritize risks and spend time only on the risks that are most likely to occur and/or have the potential to severely impact the organization

- Identify key internal and external business process and IT asset interdependencies
- Identify business process and IT assets; assess impact to losing key processes and assets and determine Recovery Time Objectives (RTO)
- Identify application-specific Recovery Point Objectives (RPO), highlighting the maximum data loss the business can afford
- Identify minimum process/system capacity requirements necessary to recover business operations to an acceptable level following an interruption

- Establish senior management sponsorship & support (e.g., through a BCM Steering Committee made up of business and IT representatives)
- Define, review, and approve BCM priorities and large capital expenditures, including additional headcount
- Share BCM costs between business and IT
BUSINESS CONTINUITY LIFECYCLE

Crisis Management Strategy

Business Recovery Strategy

IT Disaster Recovery Strategy

IT Architecture Strategy

BCM Strategy Design

Leading Practices

- Define strategies to respond to events and recover critical business functions and IT assets through analysis of risk assessment and BIA results
- Develop aggregate resource requirements
- Execute a gap analysis of resources, data/information and human capital required vs. that which is immediately available
- Develop multiple options that meet recovery requirements
- Perform a cost benefit analysis of the options developed
- Select best option through BCM governance mechanisms
BUSINESS CONTINUITY LIFECYCLE

Implement Crisis Management Plan

Implement Business Recovery Plan

Implement IT Disaster Recovery Plan

BCM Plan Implementation

Leading Practices

- Establish standardized methods to document action-oriented response and recovery procedures
- Address all major plan components, including response and recovery team responsibilities, facility and resource requirements, and detailed, systematic procedures
- Store plans in an off-site location that is accessible to personnel responsible for execution of responses and recovery procedures
- Upgrade / invest in IT architecture in a manner that aligns to strategy design
test crisis management plan

leading practices

- Design tests in a manner that covers all major components of the business continuity program and provides participants with standards to achieve
- Establish testing methods that address priority-tiered processes. Example testing procedures include:
  - Table-top
  - Alternate site
  - Communication
  - Simulation or End-to-End
- Document testing summaries after each session
- Evaluate lessons learned to identify points of refinement for the next training event and to update plan components
- Establish a training schedule for all response and recovery team members
- Establish a program maintenance schedule to ensure plan components remain up to date
PERSPECTIVES & LESSONS LEARNED
Disaster preparation and crisis response plans should be based upon worst-case scenarios and they should be routinely tested.

Business continuity planning is not an “IT only” venture. Distinct teams are needed for system recovery and business resumption.

Placing too much reliance on the availability of a small group of individuals to facilitate recovery may hinder the organization’s recovery efforts.

Disaster preparation and crisis response plans should be based upon worst-case scenarios and they should be routinely tested.

While companies may or may not be affected by a crisis event, critical suppliers and customers in the affected region may be. Therefore, companies should understand critical vendor recovery requirements and (as deemed necessary) identify multiple suppliers for critical resources needed for their processes.

Communication must be a priority for an effective business continuity response.

BCM LESSONS LEARNED

Below is a list of BCM lessons learned from company disasters and/or unplanned business disruptions.

© 2015 Protiviti Inc.
CONFIDENTIAL: An Equal Opportunity Employer M/F/D/V. This document is for your company’s internal use only and may not be copied nor distributed to another third party.
“Typical” participants in the Planning Process:

- Executive Sponsor
- Steering Committee
- Business Continuity Coordinator
- Business Process Owners
- Information Technology
- Human Resources
- Facilities
- Security
- EHS
- Legal
- Corporate Communications
- Risk Management
- Internal Audit

…the development of a defined BCM Program is not a one-time activity, but rather a cycle that is continuously enhanced. Employees & departments from across the company are involved in the planning process.
SAMPLE BCM ROLES & RESPONSIBILITIES

Executive Committee
- Provides guidance on escalations / critical decisions; makes decisions on funding for key initiatives

BCM Steering Committee
- Sets the tone for the program; approves program scope and activities; addresses program & BCM risks as they arise; identifies items to escalate, where appropriate, to the relevant members of the Executive Committee

BCM Program Management Office
- Establish annual program plan and monitor program status; establish and communicate program requirements, deadlines, BCM approach and standards; report on progress & program risks to the BCM Steering Committee; offer guidance on Best Practices and past experience successes

BCM Project Teams
- Crisis Management
- IT Disaster Recovery
- Business Resumption
- Deliver project objectives and provide consultation on respective BCM areas, facilitate creation / maintenance of plans, plan testing, and follow-up of action items; assist BCM PMO in annual program planning

BCM Plan Officers / Coordinators
- Set the tone within their respective location / functional / process areas and establish BCM expectations; create / maintain plans (annually or upon significant changes); participate in regular plan exercises; facilitate the completion of action items from exercises
INTERNAL AUDIT’S ROLE IN BCM
INTERNAL AUDIT’S ROLE

How can Internal Auditor’s add value to the BCM process?

• **Internal “Sales Person”** – Making the case for business continuity through participation in the Risk Assessment and Business Impact Analysis.

• **Business Continuity Policy Assistance** – Assist with the development or review of initial policies and standards (in line with reasonable maturity levels and business objectives).

• **Project Management Standards** – Given IA’s role in most organizations, there is familiarity with project risk management standards that can be relevant to BCM program development / enhancement initiatives.

• **Focus** – In addition to scoping the process from a business and technology perspective, IA can assist in focusing the effort on a program development perspective. Specific attention also should be paid to the planning and execution of business continuity tests and exercises.

• **Audit the BCM program** – Review the planning process and strategies to ensure compliance. Additionally, IA can develop recommendations to address opportunities for improvement.

• **Management Communication** – Formally communicate program status and capability to management to ensure expectations are met and that the BCM program continually matures over time.
GUIDANCE FROM THE IIA

• An audit should be performed every 12 to 24 months to ensure compliance with internal policies and procedures (dependent on industry / best business practices)

• The IIA published *Global Technology Audit Guide (GTAG) 10: Business Continuity Management*, which states that BCM-related audit activity should take place “on a regular basis” and can include:
  
  − Playing a role in the organization’s planning, to include the risk assessment (it is typical for internal audit to help with an assessment of an organization’s internal and external environment).

  − Evaluating the BCP and disaster recovery plan during planning and development (internal auditors have a thorough understanding of the business and the individual function and interdependent relationships and can contribute to the BCP process).
GUIDANCE FROM THE IIA (CONT.)

- Review the proposed business continuity and disaster recovery plans for design, completeness, and overall adequacy

- During the recovery period:
  - Internal audit should monitor the effectiveness of the recovery and control of operations
  - Recommend improvements to the BCP
  - Internal audit can also provide support during the recovery activities
  - Internal auditors can assist in identifying the lessons learned from the disaster and the recovery operations

- Periodically audit the organization's BCPs/DRPs
  - Adequacy to ensure the timely resumption of operations and processes after adverse circumstances
  - Reflects the current business operating environment
BCM INTERNAL AUDIT APPROACH

- Work in a collaborative manner (Advise/Teach)
- Understand the history of BCP, management objectives and the level of maturity up front
- Understand the scope of Business Continuity
- Approach from a process perspective, as opposed to a documentation review
- Look for and assess key success factors such as repeatability, extensibility and maintainability
- Focus on the entire BCM life-cycle, ranging from standards assessments through plan testing
- Brainstorm ideas for improvement – engage the business continuity coordinators
Guide to Business Continuity Management
Frequently Asked Questions
Third Edition

Updates Include:
• Regulatory Requirements
• Industry Considerations
• Lessons Learned
• Social Media
• New Trends & Practices

Download at:
www.protiviti.com/bcm
Powerful Insights.
Proven Delivery.