Business Resiliency

Business Continuity Management -

January 14, 2014
Agenda

- Key Definitions
- Risks
- Business Continuity Management Program
- BCM Capability Assessment Process
- BCM Value Proposition
- Q&A
Key Definitions: The Concept of BCM

• The capability of resuming operations after a significant unplanned event.
• Preparedness and exercise / practice are the keys to success
• Business Function Resource prioritization (dependencies analysis) based on impacts to:
  o **Technology**: data center contents destruction, software malfunction, technology provider outage
  o **Facilities**: earthquake, fire, flood, wind damage, municipal utilities outage, terrorism, political strife
  o **People**: pandemic, political strife, terrorism threat, labor action, impact from natural / man-made event
  o **Key Third Parties**: technology, financial, personnel, transportation and maintenance service provider outage
• Aligned to Enterprise-wide Risk Management and overall business strategies.
Key Definitions: BCM Elements

Business Continuity Management
Process of identifying, preventing, preparing and responding for events that may disrupt business activities.

Crisis Management
Command and control over the response to make critical decision and drive communications both internal and external.

Contingency Plan
All hazard plans for specific response to catastrophic events.

Emergency Response
Immediate first response activities to protect lives and limit damage.

Business Continuity
Continuity of critical business functions at an acceptable level during an incident.

Disaster Recovery
Restoration of business services and systems (IT and Data) during an incident.
Risks: Why is BCM Relevant Today

- Stakeholder and Board concerns about the level of preparedness
- Concentration of critical functions in fewer locations
- Negative brand and reputational impact
- Investors want to feel confident
- Reduced workforces / ‘optimization’
- Limited capital availability
- Thinly populated and high-velocity supply chains and inventories
- Increase in frequency and severity of man made and natural disasters
- High reliance on enterprise systems (24/7)
- Mergers, acquisitions and divestitures
- Disconnect between IT recovery capabilities & business unit technology availability requirements.
- Regulatory and rating agency pressures
Risks: BCM Deployment

• Traditionally focused on emergency response for workforce management, supply chain disruptions and transportation incidents, as well as IT disaster recovery. Elements of external crisis communication are also found.
• Interruption risks that impact corporate functions are infrequently covered.
• If a recent (less then 3yrs) ‘Business Impact Analysis’ and ‘interruption Risk Assessment’ have not been performed, management likely has a low awareness of how function interruptions will impact the enterprise.
• Functions potentially needing more rapid recovery and interim interruption operational procedures include:
  • Corporate and Business Unit Management functions
  • Cash management / Payables, Payroll
  • Transportation and Logistics Management
  • Human Resources
  • Vendor management
**BCM Program: Characteristics of a BCM Program**

**Assessment and Ownership**
- Critical Asset Inventory
- Enterprise Risks/Impacts
- Program Guide
- Steering Committee

**Planning and Deployment**
- Integrated plans (ERP, BCP, DR and CMP)
- Tools for plan enablement
- Enhanced for specific events
- Easy to use and update

**Exercise / Testing**
- Progressive exercise (crawl, walk, run)
- Frequency leveraged into existing lifecycle events
- Report results (Sr Leaders)

**Training and Awareness**
- Formalized Training Easy/Simple (annual update and renewal)
- Frequent Awareness sessions
- Embedded BCM culture
Staircase Methodology® is a five-tiered approach to business continuity management that is supported by numerous tools allowing a set of services relevant to successful programs.
**BCM Program: Understand the Business**

### Initiate

**Project planning**

- Develop program governance
- Establish planning assumptions
- Establish steering committee and program team
- Develop program plan
- Plan tools and approach to meet the organizational culture and requirements

### Discovery

- Review the organization’s strategic plans
- Existing documentation reviews (policy, procedures, controls, org)
- Questionnaire and Surveys
- Interviews and Workshops (Gather data and train)
BCM Program: Risk and Business Impact Analysis

This is the key core component of the BCM process!...Quantify Risks and Impacts

Analyze

100 percent of processes – “Useful Many”

20 percent of processes – “Critical Few”

Business Profile

RAI Current Resources

What resources are required to deliver our business objectives?

- People
- Facilities
- Suppliers

Processes

What is done to deliver the products and services to meet the organizational goals?

Impacts

What are the consequences over time if the processes do not function?

Risk Appetite

Defined at an organizational level, determines acceptable levels of risk.

Recovery Resources

What is needed to recover critical processes and key functions?

MAO

(Maximum Allowable Outage)

Aggregated across the business

RTO

Recovery Time

RPO

Point of Recovery

RTA Capacity

Surveys, one-on-one meetings, facilitated sessions, executive management validation

What is the Business impact?

Critical functions

Identification of supporting technology services, vital records, facilities, personnel requirements, internal interdependencies and critical third-parties.

100 percent of processes – “Useful Many”

20 percent of processes – “Critical Few”
# BCM Program: Determine Recovery Solutions

## Strategize

### Recovery strategy development

- Identity recovery capability gaps
- Integrate and finalize recovery requirements
- Recommend risk mitigation measures
- Review and assess current strategies
- Identify and price recovery strategy alternatives
- Evaluate recovery vendors if needed
- Quantify critical resources by function and develop recovery timeline
- Quantify and qualify appropriate recovery options
- Management checkpoint – review options and select recovery strategy
- Develop implementation procedures for selected strategy
**BCM Program: Design and Build the Program and Plans**

## Development

<table>
<thead>
<tr>
<th>Plan and Recovery Capability Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Establish planning assumptions</td>
</tr>
<tr>
<td>• Determine plan tools and approach to meet the organization’s requirements</td>
</tr>
<tr>
<td>• Document plans and procedures for organization or individual business processes</td>
</tr>
<tr>
<td>• Develop emergency action and crisis management procedures</td>
</tr>
<tr>
<td>• Develop recovery and communications plans (IT and Business)</td>
</tr>
<tr>
<td>• Develop migration procedures (IT and Business)</td>
</tr>
<tr>
<td>• Develop operational procedures (IT and Business)</td>
</tr>
<tr>
<td>• Document recovery team procedures (IT and Business)</td>
</tr>
<tr>
<td>• Identify assessment and change triggers</td>
</tr>
<tr>
<td>• Develop recovery plan testing strategy</td>
</tr>
<tr>
<td>• Develop training strategy, procedures and plan</td>
</tr>
<tr>
<td>• Management checkpoint</td>
</tr>
</tbody>
</table>
**BCM Program: Operate and sustain the BCM Program**

**Maintain**

### Implementation and Exercise Testing

- Facilitate implementation
- Embed and Integrate BCM into end-to-end program management
- Develop and conduct testing, training, and maintenance processes and tools
- Conduct simulations and plan enactment
- Revise and validate BCPs/DRPs/CMPs
- Develop maintenance processes to support plans and capabilities
- Periodic program assessment, benchmarking and maturity ranking

**Table Top**

- Building understanding
- Confirm strategy and plan components

**Component**

- Test that strategy components and plan elements work individually

**Simulation**

- Practice real-time responses
- Test actual strategies
- Build confidence
**BCM Capability Assessment Process**

Our operational preparedness reviews benchmark against BCM leading practices

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>No designated sponsor</td>
<td>Steering committee exists</td>
<td>Program sponsorship</td>
<td>BC program policies and standards documented</td>
<td>A culture of business resiliency exists and is embedded in the day-to-day operations.</td>
</tr>
<tr>
<td>No risk assessment / BIA</td>
<td>Risk assessment / BIA</td>
<td>Assessments</td>
<td>Importance of BC is applied to external parties</td>
<td></td>
</tr>
<tr>
<td>RTOs not been identified</td>
<td>Application RTOs defined</td>
<td>Business RTO and Application RTA optimized</td>
<td>Robust testing performed throughout the year including tests with key vendors and ad-hoc/surprise tests</td>
<td></td>
</tr>
<tr>
<td>Business recovery strategies not documented</td>
<td>Limited documentation</td>
<td>Framework for recovery &amp; restoration established</td>
<td>Change management, risk management, SDLC and training programs have BCM compliance gates</td>
<td></td>
</tr>
<tr>
<td>No maintenance or testing,</td>
<td>Limited BCM vs IT needs and capabilities</td>
<td>Critical dependencies</td>
<td>System is in place to maintain employee competency for performing recovery responsibilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Limited program testing</td>
<td>Documentation not be validated for all plans (EAP, CMP, BCP)</td>
<td>Senior management reviews the program at pre-determined intervals against defined metrics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Training procedures in place and documented</td>
<td>Testing occurs with communications tools to be used during recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Objective program review occurs periodically</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Level 1**: No designated sponsor, no risk assessment / BIA, RTOs not been identified, business recovery strategies not documented, no maintenance or testing.
- **Level 2**: Steering committee exists, risk assessment / BIA, application RTOs defined, limited documentation, limited BCM vs IT needs and capabilities, limited program testing, training procedures in place and documented.
- **Level 3**: Program sponsorship, assessments, business RTO and application RTA optimized, framework for recovery & restoration established, critical dependencies, documentation not be validated for all plans (EAP, CMP, BCP), testing occurs with communications tools to be used during recovery, objective program review occurs periodically.
- **Level 4**: BC program policies and standards documented, detailed business impacts and risks, quantified, fully documented plans up-to-date with dependencies (internal and external), detailed plans for failover and failback of all critical systems are developed, employees aware of program and involved in drills to successfully demonstrate recovery within stated RTOs, pre-defined maintenance triggers in place and followed for automatic plan updates, formal test schedule.
- **Level 5**: A culture of business resiliency exists and is embedded in the day-to-day operations, importance of BC is applied to external parties, robust testing performed throughout the year including tests with key vendors and ad-hoc/surprise tests, change management, risk management, SDLC and training programs have BCM compliance gates, system is in place to maintain employee competency for performing recovery responsibilities, senior management reviews the program at pre-determined intervals against defined metrics.
**BCM Value Proposition**

- Reduces the impact of business interruptions through careful advance planning on key services and processes through the identification of “mission critical” business processes and supporting resources (cost-effective and practical).
- Ensures rapid availability of management decision-making capabilities and communication.
- Balances recovery strategy options between real estate costs and physical diversity protection - cost-benefit balance addresses competing technical and business priorities (objective approach).
- Reduces risk of potential loss of customers, brand reputation, revenue and assets.
- Potentially enhanced risk profile with insurance carriers, affecting: Property, BI, CBI, Extra Expense, D&O, E&O coverage/premiums.
- Reduced risk and improvement of recovery times.