The Business Continuity Maturity Continuum

Nick Benvenuto & Brian Zawada
Protiviti Inc.
Agenda

- Terminology
- Risk Management Infrastructure Discussion
- A Proposed Continuity Maturity Continuum
- Where Are You?
- Where Does Management Want to Be?
- Value Proposition or Risk, By Level
- Action Steps to “Move Up”
  - And the effort involved in moving up
- How Is IT DR Different?
- Discussion

“How much continuity is right for our organization?”
…the development of strategies, plans and actions which provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to the enterprise.

BCM = Crisis Management + Business Resumption Planning + IT Disaster Recovery Planning
Introducing Two Frameworks

• Risk Management Infrastructure
  – A framework to describe elements of a risk management process
  – Value: In a comprehensive manner, identifies the key components of a process. In terms of business continuity, demonstrates this process is significantly more than a documented plan.

• Capability Maturity Continuum
  – A framework used to capture process-specific performance characteristics, as well as the action steps necessary to achieve this level of performance, in order to assess and communicate the degree to which a company has adopted best practices relative to other organizations
  – Value: Helps management identify current state capability for a given process, as well as characteristics of a desired future state, using a common framework that crosses multiple risk management disciplines
Business Continuity Risk Management Infrastructure

- Contract Terms and Conditions with Suppliers
- Customer Service Level Agreements
- Governance Documentation
  - Process Accountability
  - Recurring Activities
  - Documentation Standards
  - Strategy Testing
  - Training & Awareness
  - Plan Maintenance
- Emergency Response
- Crisis Mgmt
- Crisis Communications
- Business Resumption Planning
- IT DR Planning
- Business Impact Analysis
- Risk Assessment
- Business Continuity Strategy Testing
- Training & Awareness
- Supplier Risk Mgmt
- Audit Committee Oversight
- Executive Mgmt Sponsorship
- Business Continuity Coordinator
- Crisis Mgmt Team
- Business Recovery Coordinators
- IT DR Coordinators
- Recovery Teams
- Internal Audit Oversight
- Industry / Governmental Oversight
- Risk Assessment Conclusions (Likelihood and Vulnerability)
- Business Impact Analysis Conclusions (Recovery Objectives)
- Strategy Design Options
- Strategy Cost-Benefit Analysis
- Strategy Test Results
- Diagnostic and Benchmarking Conclusions
- Business Continuity Governance Design and Data Gathering
- Risk Assessment
- Business Impact Analysis
- Strategy Design
- Plan Documentation
- Plan Validation
- Knowledge Transfer & Implementation
- Documentation Repository
- Plan Documentation Software
- Risk Assessment Conclusions
- Business Impact Analysis Conclusions
- Hardware for IT DR Purposes
- Backup / Replication Software (IT DR Only)
### BCM Capability Maturity Continuum

#### Definition

<table>
<thead>
<tr>
<th>Process Maturity</th>
<th>Characteristics of Capability</th>
<th>Method of Achievement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Optimizing</strong></td>
<td>Business continuity management is a competitive advantage. Management &quot;advertises&quot; the existence of the business continuity process internally and externally with customers. Continuity-related service level agreements, associated with uptime, performance and continuity, are utilized to drive efficiencies internally and build strategic relationships with customers.</td>
<td>Comprehensive, organization-wide business continuity strategies are aligned with strategic objectives and customer expectations. BCM operates as a core business function, chartered with clear accountability and responsibility. Regular BCP testing and maintenance occurs. Personnel are well trained regarding their roles and responsibilities. Metrics are collected and managed to ensure continuity-related service level agreements are met.</td>
</tr>
<tr>
<td><strong>Managed</strong></td>
<td>In addition to a customer focus and the desire to minimize financial loss and reputation impairment, management addresses regulatory compliance through the design of solutions with characteristics mandated by industry and governmental organizations. Specific compliance categories include data protection, financial reporting process continuity, strategy testing and plan maintenance processes.</td>
<td>Business continuity strategies address core business functions, information technology assets and supply chain relationships. Management fully supports this effort. The organization’s business continuity management process, to include crisis management, crisis communications, business resumption planning and IT disaster recovery planning, operates as a single function. The BCM process reflects the current business and technology environment.</td>
</tr>
<tr>
<td><strong>Defined</strong></td>
<td>Business functions and IT assets supporting the delivery of products and services, as well as customer service, are protected from long-term business interruptions. Customer expectations regarding product and service delivery have been taken into account. Testing and training limitations may result in isolated recovery issues, often taking the form of recovery capacity constraints and missed recovery objectives.</td>
<td>A formal business continuity strategy has been designed and deployed. A risk assessment has been performed to identify and assess continuity risks. A business impact analysis (BIA) has been performed, but there are no processes to keep it current. Testing is infrequent or fails to address all aspects of the continuity process. Plan maintenance activities have not occurred in over twelve months. Metrics for key BCP tasks require refinement.</td>
</tr>
<tr>
<td><strong>Repeatable</strong></td>
<td>Management relies on untested or under-tested continuity-related processes to manage the effects of business interruptions. IT asset recovery is often the most mature aspect of the continuity process, although some organizations emphasize either crisis management or business resumption planning. Employees have limited knowledge regarding their roles during recovery, potentially impacting the likelihood of a successful response effort.</td>
<td>The organization’s business continuity strategy addresses crisis management, business resumption or IT disaster recovery. Continuity processes are designed and developed separately and lack integration. A high-level risk assessment and/or business impact analysis has been performed. Although some continuity-related processes exist, plan maintenance and testing procedures have not been implemented.</td>
</tr>
<tr>
<td><strong>Ad Hoc</strong></td>
<td>Significant risk of continuity-related impacts are present. Business interruptions, ranging from isolated infrastructure failures through regional events, have the potential to cause serious financial harm and/or reputational impairment. The organization relies on “force majeure” clauses to minimize contractual violations.</td>
<td>BCP goals and expectations were derived without a risk assessment or business impact analysis. Business continuity strategies are characterized as ad hoc; a formal documented plan does not exist. Business continuity accountability and responsibility remain unassigned. Business continuity testing and training and awareness processes have not been designed. The organization lacks confidence in its ability to survive following a business interruption.</td>
</tr>
</tbody>
</table>
Business continuity management is a competitive advantage. Management "advertises" the existence of the business continuity process internally and externally with customers. Continuity-related service level agreements, associated with uptime, performance and continuity, are utilized to drive efficiencies internally and build strategic relationships with customers.

In addition to a customer focus and the desire to minimize financial loss and reputation impairment, management addresses regulatory compliance through the design of solutions with characteristics mandated by industry and governmental organizations. Specific compliance categories include data protection, financial reporting process continuity, strategy testing and plan maintenance processes.

Business functions and IT assets supporting the delivery of products and services, as well as customer service, are protected from long-term business interruptions. Customer expectations regarding product and service delivery have been taken into account. Testing and training limitations may result in isolated recovery issues, often taking the form of recovery capacity constraints and missed recovery objectives.

Significant risk of continuity-related impacts are present. Business interruptions, ranging from isolated infrastructure failures through regional events, have the potential to cause serious financial harm and/or reputational impairment. The organization relies on "force majeure" clauses to minimize contractual violations.

Business continuity strategies address core business functions, information technology assets and supply chain relationships. Management fully supports this effort. The organization’s business continuity management process, to include crisis management, crisis communications, business resumption planning and IT disaster recovery planning, operates as a single function. The BCM process reflects the current business and technology environment.

A formal business continuity strategy has been designed and deployed. A risk assessment has been performed to identify and assess continuity risks. A business impact analysis (BIA) has been performed, but there are no processes to keep it current. Testing is infrequent or fails to address all aspects of the continuity process. Plan maintenance activities have not occurred in over twelve months. Metrics for key BCP tasks require refinement.

The organization’s business continuity strategy addresses crisis management, business resumption or IT disaster recovery. Continuity processes are designed and developed separately and lack integration. A high-level risk assessment and/or business impact analysis has been performed, but there are no processes to keep it current. Testing is infrequent or fails to address all aspects of the continuity process. Plan maintenance activities have not occurred in over twelve months. Metrics for key BCP tasks require refinement.

Continuity processes are designed and developed separately and lack integration. A high-level risk assessment and/or business impact analysis has been performed, but there are no processes to keep it current. Testing is infrequent or fails to address all aspects of the continuity process. Plan maintenance activities have not occurred in over twelve months. Metrics for key BCP tasks require refinement.

Business continuity strategies are designed without a risk assessment strategy. Crisis management, business resumption planning and IT disaster recovery planning occur separately. The organization lacks confidence in its ability to survive following a business interruption.
Business continuity management is a competitive advantage. Management “advertises” the existence of the business continuity process internally and externally with customers. Continuity-related service level agreements, associated with uptime, performance and continuity, are utilized to drive efficiencies internally and build strategic relationships with customers.

Business functions and IT assets supporting the delivery of products and services, as well as customer service, are protected from long-term business interruptions. Customer expectations regarding product and service delivery have been taken into account. Testing and training limitations may result in isolated recovery issues, often taking the form of recovery capacity constraints and missed recovery objectives.

Significant risk of continuity-related impacts are present. Business interruptions, ranging from isolated infrastructure failures through regional events, have the potential to cause serious financial harm and/or reputational impairment. The organization relies on “force majeure” clauses to minimize contractual violations.

In addition to a customer focus and the desire to minimize financial loss and reputation impairment, management addresses regulatory compliance through the design of solutions with characteristics mandated by industry and governmental organizations. Specific compliance categories include data protection, financial reporting process, continuity, strategy testing and plan maintenance processes.

Continuity processes are designed and developed separately and lack integration. A high-level risk assessment and/or business impact analysis has been performed. Although some continuity-related processes exist, plan maintenance and testing procedures have not been implemented.

BCP goals and expectations were derived without a risk assessment or business impact analysis. Business continuity strategies are characterized as ad hoc; a formal documented plan does not exist. Business continuity accountability and responsibility remain unassigned. Business continuity testing and training and awareness processes have not been designed. The organization lacks confidence in its ability to survive following a business interruption.
### Capability Maturity Continuum
#### Ad Hoc

#### Capability Description
- Sponsored at a Lower Level in the Organization
- Reliance on “Heroic” Measures
- Terminology Confusion
- Discussions Regarding Recovery Strategies
- Few, if any, Documented Response or Recovery Procedures

#### Value Achieved
- Initial Understanding of Constraints Involved in Executing a Recovery Strategy

#### Action Steps to Move Up
- Formal Executive Management Sponsorship
- Budget Allocation for Analysis
- Agree on Scope
• **Company A – Pharmaceutical Industry**
  – Delegated to IT Operations Without a Budget
  – Scope is Limited to Components of IT Disaster Recovery
    • Data Backed Up, Tapes Moved Off-Site
    • Reliance on Vendor to Drop Ship Servers to Another ‘Company A’ Facility
  – Safety Department Develops and Maintains Evacuation Plans
    • Some Confuse This with Business Continuity
  – Customer Service, Shared Service Functions, Manufacturing and Product Distribution Are Not Addressed
Capability Maturity Continuum
Repeatable

• Capability Description
  – Limited Executive Sponsorship
  – IT Recovery Is Maturing (or a single component of the business continuity process is maturing)
    • A Lack of Integration (silo approach)
  – BIA / Risk Assessment Completed
  – Some Limited Testing of Response Strategies
  – Some Awareness Programs

• Value Achieved
  – “One Dimensional” Program Results in Lessons Learned and In-House Skills Previously Absent
  – Foundation of an Enterprise-wide Business Continuity Process

• Action Steps to Move Up
  – Formal Executive Management Sponsorship
  – Budget Allocation for More Inclusive Analysis
  – Expansion of Scope
An Example – Repeatable

Company R – Manufacturing Industry

- The CFO Sponsored An Initiative to Address the Accounting and Finance Department Based on Auditor Guidance (Sarbanes-Oxley Section 404)
  - The CIO Implemented a Separate Program 18 Months Ago; No Coordination Between the Two Programs
- Both the CFO and CIO Completed Business Impact Analyses and Limited-Scope Risk Assessments
  - Gaps and Differing Conclusions Based on Respondents
- Workplace Recovery Strategies in Place for Some Corporate Shared Services Functions; Hot-Site Contract in Place for Critical IT Assets
- Some Limited Testing (Boardroom Style Testing)
  - Mid-Level Management Participation in Response Walkthroughs
- Training and Awareness Programs Limited to Industry Conferences Participation (Continuity Insights Conference)
- Plant-level Plans are Absent, with the Exception of Fire, Evacuation and Hazardous Materials Handling Procedures
- Multiple Single Points of Failure in the Supply Chain; No Plans for Backup Suppliers
Capability Maturity Continuum Defined

• Capability Description
  – Thorough Analysis, Taking into Account Customer Expectations
  – Increase in Scope – Business and IT Recovery Capabilities Maturing
  – Accountability Realignment
    • No Longer 'Owned' by IT or IA
  – Improvements in Testing and Training
    • Infrequent Tests Include the Execution of Recovery Procedures
    • Periodic Training Sessions

• Value Achieved
  – Beginning to Satisfy Regulators
  – Multi-Dimensional Program Addresses Business Requirements
  – Employees Understand How to Receive Updates and Stay in Contact with Management

• Action Steps to Move Up
  – Formal Business Continuity Standards and Actions (accountability and task assignments)
  – Develop a List of Recurring Tasks (testing, training and plan maintenance functions)
Company D – Banking Industry

- CRO Sponsored Initiative
  - Vice President-level Function has Day-to-Day Responsibility (2 Analysts)
- Ongoing Initiatives Include Crisis Management, Crisis Communications, Business Resumption Planning and IT Disaster Recovery
  - IT DR Ownership Retained by IT
- Enterprise-wide Business Impact Analyses and Risk Assessments were Completed 18 Months Ago
- Each Plan is Tested Annually
  - Workplace Recovery Plans are Tested in a Boardroom Style Environment
  - IT Utilizes In-House Assets for Non-Mainframe Recovery
- Some Training and Awareness Programs Are In Place
  - Executive Management Media Handling and Crisis Communications Training
- “Magnets” were Distributed with Call Tree and Emergency Contact Numbers
- The “Regulator Relationship” Has Evolved Into Discussions Regarding Ways to Enhance Operational Effectiveness Based on Industry Best Practices
• Capability Description
  – Full Executive Management Sponsorship
  – Detailed Policies and Procedures (standards)
  – Elimination of Organizational Boundaries – One Process
  – Scope of Continuity Effort Looks Outward, Taking Supply Chain Into Account
  – Crisis Communications Process Maturing
  – Plans Remain Up-to-Date

• Value Achieved
  – Confidence
  – Employees Know What’s Expected of Them
  – Accountability
  – Efficiency
  – Customer Satisfaction

• Action Steps to Move Up
  – Alignment with Strategic Business Objectives
  – Integration with Organizational Change Management Processes
An Example – Managed

Company M – Insurance Industry

- Executive Steering Committee – CFO, COO, CIO and CRO
  - Director-level Function has Day-to-Day Responsibility, “Owns” Crisis Management, Crisis Communications, Business Resumption Planning and IT Disaster Recovery
- Enterprise-wide Business Impact Analyses and Risk Assessments were Completed 18 Months Ago
- Business Continuity Governance Program Drives Recurring Tasks, Employee Involvement and Financial Incentives
- Each Plan is Tested Semi-Annually, When Significantly Changed or If Problems Persist During Testing
  - Workplace Recovery Plans Are Tested in a Boardroom Style Environment
  - IT Utilizes In-House Assets for Non-Mainframe Recovery
- Mandatory Recovery Team Training and Awareness Programs Twice a Year
  - Executive Management Media Handling and Crisis Communications Training
- Insurance Agent and Vendor Relationships Have Been Taken Into Account When Developing Strategies and Plans
- Crisis Communications Process Maturing – Holding Statements Have Been Developed
- Plans Remain Up-to-Date – Quarterly Review of HR Records and Integration with Change Management Processes
Capability Maturity Continuum  
Optimizing

- **Capability Description**
  - Recurring Testing, Limited Artificial Assumptions
  - Formal Training Program
  - Measured Business Continuity Program – Defined Metrics and SLA’s are in Place
  - Uses Continuity Capabilities as a Competitive Advantage

- **Value Achieved**
  - Greater Confidence!
  - “What Gets Measured Gets Done!”
  - Potential Differentiator Among Competition

- **Action Steps to Move Up**
  - Review Feedback and Action Items from Testing, Business Impact Analyses and Risk Assessments
An Example – Optimizing

- **Company O – Electric Utility**
  - A Focus on the Customer Experience – On-Time Billing, Customer Service Centers and Outage Handling
  - Quarterly Executive Steering Committee Meetings to Discuss Metrics
    - Training Program Participation by Response and Recovery Team Members
    - Plans Missing Update Windows
    - Test Results versus Established Recovery Windows (to include completeness and integrity checks of business applications by end users)
    - Action Item Tracking
    - Budgetary Analysis
    - Discussions Regarding Bi-Annual Benchmarking Assessment
IT Disaster Recovery Capability Maturity Continuum

Definition

<table>
<thead>
<tr>
<th>Characteristics of Capability</th>
<th>Method of Achievement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Optimizing</strong></td>
<td>Disaster recovery strategies are aligned with strategic objectives and customer expectations. Disaster recovery planning operates as a core business function, chartered with clear accountability and responsibility. New technologies are proactively pursued to support continuous improvement.</td>
</tr>
<tr>
<td><strong>Managed</strong></td>
<td>Upper management (business and IT) is directly involved in the disaster recovery planning process. A strong sense of teamwork exists among the groups responsible for business continuity. Metrics are collected and managed to ensure recovery objectives are met. Technology solutions to support the recovery process are also evaluated using qualitative measures.</td>
</tr>
<tr>
<td><strong>Defined</strong></td>
<td>The organization is committed to the development of disaster recovery capabilities. A risk assessment has been performed to identify and assess IT continuity risks. A business impact analysis (BIA) has been performed to measure potential business impact from failure events, and the results are communicated to IT. Technology solutions to support the recovery process are evaluated.</td>
</tr>
<tr>
<td><strong>Repeatable</strong></td>
<td>Disaster recovery capabilities are the result of IT management commitment, with limited business support. IT management “ranked” the criticality of production systems, as a way to support recovery point objectives (RPO) and recovery time objectives (RTO). A recovery plan has been created but is under-tested. A recovery/fail over location has been prearranged. Basic technologies to support the recovery process have been implemented.</td>
</tr>
<tr>
<td><strong>Initial</strong></td>
<td>Existing recovery capabilities were planned without management support. Goals and expectations are undefined. The organization elected to identify failure scenarios and assign recovery objectives without a business impact analysis or risk assessment. Few technology solutions are introduced to support the recovery process. Recovery procedures lack detail and rely on the most experienced administrators.</td>
</tr>
</tbody>
</table>

Disaster recovery planning processes are continuously and systematically improved. Recovery-related service level agreements, associated with uptime, performance and continuity, are utilized to drive efficiencies internally and build strategic relationships. Common threats to the organization’s critical IT systems are understood and eliminated.

The overall effectiveness of the disaster recovery plan is measured and understood by upper management. In addition to recovery objectives, DR capabilities address regulatory compliance with guidelines mandated by industry and governmental organizations. Sources of individual threats to IT critical systems are understood and mitigated.

Recovery processes are standardized, documented and integrated into the organization’s disaster recovery plan. Testing and training activities are regularly scheduled and designed to validate recovery objectives. Impacts from failure events are managed in accordance with recovery objectives.

Disaster recovery planning processes have been established. However, in most cases they are designed and developed separately lacking the necessary integration with business recovery and crisis management. Failure events are recognized and corrected after they occur.

The recovery process is characterized as “ad hoc”. Specific recovery procedures are undefined and recovery capabilities depend on individual efforts and “heroic measures”. The existing process has a low probability of success following a major disaster, and even minor events such as data corruption or isolated infrastructure failures may result in crisis.
BCM vs IT DR Continuum – A Comparison

• What’s Different?
  – Nothing
  – More Tactical and Focused on Technical Support

• What’s the Same?
  – Success is Achieved Through Alignment with Business Derived Requirements
Questions and Discussion
Presenter Contact Information

- **Nicholas Benvenuto, Managing Director**  
  - Business Continuity Management Services  
  - New York, NY  
  - nicholas.benvenuto@protiviti.com  
  - (212) 603-8399

- **Brian Zawada, Associate Director**  
  - Business Continuity Management Services  
  - Cleveland, OH  
  - brian.zawada@protiviti.com  
  - (216) 696-6098
Management continues to struggle with the concept of “how much continuity is right for our organization.” Some companies favor a very basic risk management model, whereas others strive for the “Cadillac” business continuity process. Regardless of the company’s desired end-state, business continuity is an evolutionary process. A common source of executive management frustration is defining a best practices-compliant end state and focusing on hitting this target in one fluid motion over the extreme short term (as opposed to moving through maturity “toll gates” over time).

This presentation will focus on defining an industry-independent business continuity maturity continuum and key milestones and organizational characteristics associated with each. We will outline the value introduced by each maturity improvement in order to help “sell” management on improvement opportunities. We will also identify action steps to move from one maturity level to the next in the most cost-effective manner possible.