Business Continuity in Healthcare

Cynthia Simeone, CBCP, PMP
Director Business Resilience
Catholic Health Initiatives

Scott Ream
President
Virtual Corporation
Session Speakers

• Cynthia Simeone, CBCP, PMP
  – Business resilience veteran with credentials developing and managing business continuity, disaster recovery, and emergency management programs supporting Fortune 100 financial services, insurance, pharmaceutical, manufacturing and now, healthcare.
  
  Personal Disclaimer - My presentation is in no way an endorsement of any particular product or company

• Scott Ream
  – Mr. Ream co-founded Virtual Corporation in 1994 to assist organizations with implementation of sustainable business continuity programs. He authored the Business Continuity Maturity Model® now recognized worldwide as a standard for assessing BC program maturity.
Today’s Topic

• Hospitals and many healthcare organizations fulfill a central role in disaster response
• They must possess robust emergency management plans that address the many mitigation, preparedness and response phases of the disaster management cycle
• It requires an approach that prioritizes essential services, identifies threats to those services and develops strategies to ensure those same essential services are sustained
• Attendees will learn how to migrate from an Emergency-Centric program to a Business Resilient model to insure healthcare service and business continuity
Today’s Agenda

• Overview of Catholic Health Initiatives
• Healthcare Regulatory Landscape
• Healthcare Response to Regulatory Landscape
• Business Resilience Program Controls
• Program Maturity Progression
• Performing Maturity Assessment
• Business Resilience Program
• BR Annual Cycle
• Keys to Success
Catholic Health Initiatives Overview

• National nonprofit health organization with headquarters in Englewood, CO

• Faith-based system operating in 19 states including
  – 76 hospitals including 21 critical-access facilities and six other rural hospitals that are the sole community providers of health care
  – 40 long-term care, assisted- and residential-living facilities
  – Two community health-services organizations
  – Two accredited nursing colleges; and
  – 46 home health agencies

• Approximately 70,000 employees
Catholic Health Initiatives Overview
cont.

- CHI is the nation's second-largest Catholic health care system in the Nation
  - $13.8 billion in assets
  - $9.6 billion in total annual operating revenues
  - $612 million in charity care and community benefit, including services for the poor, free clinics, education and research
  - $9.6 billion in total annual operating revenues
Catholic Health Initiatives Strategic Initiatives

• CHI’s 2012-2016 strategic plan is built upon four core Strategies:
  – People: CHI will cultivate and advance a ministry culture that forms, supports, and develops the necessary talent to become a leader in health care practice and outcomes.
  – Quality: CHI will be recognized as a national leader in innovative care models, person-centered care and healthy communities.
  – Stewardship: CHI will focus resources and invest to innovate and excel in improving the health of the communities it serves.
  – Growth: CHI will grow and diversify its health ministry to develop the systems of care required to improve the health of the people and communities it serves.
Catholic Health Initiatives Key Goals

• Advancing personal and community health beyond traditional acute care focus
  – 65% of net patient service revenue from other than hospital inpatient care
  – Achievement of community-defined and sustainable violence reduction goals

• **Physician Alignment/Full Health Care Delivery Network**
  – OneCare is Catholic Health Initiatives’ $1.5 billion system-wide program to transform health care delivery and advance patient care by creating a shared, electronic health record for each CHI patient

• “OneCare is a patient care initiative, supported by technology” (Kevin Lofton, President and CEO)
Healthcare Landscape
Regulatory Landscape for Healthcare

Regulations for Disaster Recovery in Healthcare are presented as recommendations defined by:

- Privacy Act of 1974
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Occupational Safety and Heath Administration (OSHA) Standards
- Cardholder Information Security Program (CISP) of 2001
- Joint Commission Accreditation
Regulatory Landscape for Healthcare cont.

Health Insurance Portability and Accountability Act (HIPAA) - Privacy and Security Rules; (164.308(a)(7)

- The Contingency Plan standard includes five implementation specifications.
- Data Backup Plan (Required)
  - “Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.”
- Disaster Recovery Plan (Required)
  - “Establish (and implement as needed) procedures to restore any loss of data.”
- Emergency Mode Operation Plan (Required)
  - “Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.”
- Testing and Revision Procedures (Addressable)
  - “Implement procedures for periodic testing and revision of contingency plans.”
- Applications and Data Criticality Analysis (Addressable)
  - “Assess the relative criticality of specific applications and data in support of other contingency plan components.”
Joint Commission

• The majority of “testing” initiatives is around fire safety, power and emergency operations and response that includes these statements:

• Emergency response exercises incorporate likely disaster scenarios that allow the critical access hospital and/or hospital to evaluate its handling of communications, resources and assets, security, staff, utilities, and patients.

• The critical access hospital's and/or hospital’s plan for managing interruptions to electronic information processes is tested for effectiveness according to time frames defined by the organization.
Program Maturity Progression

Risk Reduction
Benefit to Organization

Level 1
Initial
- Ad-hoc processes
- Inadequate risk insights
- Inconsistent control

Level 2
Repeatable
- Governance structure, program charter and policy
- Practices in place
- Risk awareness and commitment to improve

Level 3
Defined
- Systemic, Repeatable and Ongoing program
- Well-defined Policy, Controls and Process based on baseline and risk profile
- Can demonstrate compliance
- Well-defined metrics to measure effectiveness
- Risk improvement over time

Level 4
Managed
- Meet defined customer service objectives
- Predictable cost for sustainable operations
- Active management and significant reduction of risk
- Adoption across entire enterprise
- Business decisions influenced by trends and metrics
- Program covers new and emerging risks (mobile, virtualization etc.)
- Risk treatment plan with mitigation and remediation executed through several iterations

Level 5
Optimized
- Optimize cost efficiency and control effectiveness
- Process evolution and continuous improvement tightly linked to changing business context
- Mature metrics, policies and controls – industry leader position
- Successful compliance and other business risk measures
- Use security as a competitive advantage
Typical Healthcare Organization’s Response to Regulatory Landscape

• Reactive Program
  – Focused on Emergency Response
  – Limited understanding of risk, risk tolerance and risk mitigation
  – Activities for improvement driven by audit remediation
  – No Enterprise Business Continuity/Disaster Recovery Policies or Standards
  – “Disaster Recovery” focused on technical recovery of systems without understanding of criticality and/or prioritization or consistency of information
  – Just-in-Time supply practices
Recommended Healthcare Business Resilience Landscape

• **Defined** Business Resilience Program

  – Incorporates the full spectrum of risk identification, risk mitigation strategies and risk response tools for the enterprise
    - Executive Leadership Governance/Oversight
    - Published Policy Statements and Supporting Standards
    - Business-driven Risk Assessment Toolkit
      - Hazard Vulnerability Assessment/Risk Assessment
      - Business Impact Analysis
      - Recovery Capability Risk Assessment

  – Incorporates a comprehensive Emergency Management/Business Continuity/Disaster Recovery Program
    - Standardized BCP/DR Documentation Templates
    - Training Strategy
    - Exercising Standards and Schedule

  – Integrates a Communications and Awareness Program
    - Customized/branded internal website
    - Subject matter experts to aid with local adoption

  – Integrates enterprise change
    - Business or Environmental Changes
    - Incident and Root Cause Analysis
    - Maturity Goals
Recommended Healthcare Business Resilience Landscape cont.

- **Managed Business Resilience Program**
  - Provides solutions that are responsive to mitigating business risks supported by people, process and technology
  - Meets defined customer service objectives
  - Includes active management and significant reduction of risk
  - Fosters cooperative enterprise relationships within individual MBOs to enhance deployment and adoption of standardized plans, processes and tools across enterprise
Business Resilience Program Controls

• CobiT v4 – [High Level Control Objective DS4] Controls have been defined to ensure continuous service by building resilience into automated solutions and developing, maintaining and testing IT continuity plans
• HiTrust Controls
  – Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information
  – Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
  – A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance
  – Business continuity plans shall be tested and updated regularly, at a minimum annually, to ensure that they are up to date and effective
Program Maturity Progression

- Compliance is viewed as a process rather than a point in time event.
- Vulnerability avoidance is accomplished through the implementation of appropriate Business Resilience controls at each MBO and Clinic:

**Business Resilience Controls**

- **Reactive**
  - Emergency Response
  - Respond to Audits

- **Compliant**
  - Annual Exercising
  - Annual Business Impact Analysis
  - Annual Risk Assessments
  - Training and Awareness
  - Documented Policies and Standards

- **Proactive**
  - 3rd Party Assessment
  - Continuity Planning
  - Annual Capabilities Risk Assessment
  - Threat Surveillance

- **Optimized**
  - Supply Chain Management
  - Comprehensive Change Management Program

Maturity / Complexity vs. Risk Reduction
What is the Business Continuity Maturity Model®?

- A tool that provides a standardized assessment approach
- The model defines how an organization evolves through maturing levels of competency at implementing BC as a sustainable practice
- The model consists of:
  - Six ‘Maturity Levels’
  - Eight ‘Corporate Competencies’ each with
    - Associated Criteria Categories & Descriptors
    - Associated Performance Requirements
Why create a BC maturity model?

• The Business Continuity Maturity Model® was developed to:
  – Answer the following questions for senior mgmt:
    • Where are we now?
    • Where do we ultimately want to be?
    • Where should we be next?
  – Achieve executive “buy-in” to implement and/or sustain a Business Continuity program
Why create a BC maturity model?

• The Business Continuity Maturity Model® was developed to:
  – Generate consistent data from which meaningful benchmark analyses can be drawn:
    • Establish standard means of scoring BC program implementations
    • Develop historical databank tagged in meaningful ways, e.g., by industry, by region, by company size, etc.
    • Generate awareness that business continuity program effectiveness can be quantified
Why create a BC maturity model?

• The Business Continuity Maturity Model® was developed to:
  – Provide a diagnostic tool for objective evaluation of BC program effectiveness
    • Generate consistent and repeatable measurements of the current “state-of-preparedness”
    • Conduct accurate and reliable analyses to identify gaps in BC program implementation
    • Propose demonstrable and justifiable actions to maximize program effectiveness and resource utilization
Business Continuity Maturity Model®

Increasing Business Continuity Competency Maturity

<table>
<thead>
<tr>
<th>Maturity Model Levels</th>
<th>Level 1 Self-Governed</th>
<th>Level 2 Supported Self-Governed</th>
<th>Level 3 Centrally Governed</th>
<th>Level 4 Enterprise Awakening</th>
<th>Level 5 Planned Growth</th>
<th>Level 6 Synergistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Athlete Analogy</td>
<td>Able to Crawl</td>
<td>Able to Walk</td>
<td>Able to Run</td>
<td>“Fit” Runner</td>
<td>Competitive Runner</td>
<td>Olympic Runner</td>
</tr>
<tr>
<td>Comparative Model</td>
<td>Organization “At Risk”</td>
<td>“Competent” Performer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A 6-level maturity model that describes how an organization evolves in implementing integrated business continuity as a sustainable practice ...
**Business Continuity Maturity Model®**

### Increasing Business Continuity Competency Maturity

<table>
<thead>
<tr>
<th>Maturity Model Levels</th>
<th>Level 1: Self-Governed</th>
<th>Level 2: Supported Self-Governed</th>
<th>Level 3: Centrally Governed</th>
<th>Level 4: Enterprise Awakening</th>
<th>Level 5: Planned Growth</th>
<th>Level 6: Synergistic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Able to Crawl</td>
<td>Able to Walk</td>
<td>Able to Run</td>
<td>“Fit” Runner</td>
<td>Competitive Runner</td>
<td>Olympic Runner</td>
</tr>
<tr>
<td>Corporate Competencies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organization “At Risk”</td>
<td>“Competent” Performer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“Best of Breed”</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...defining categories at each Maturity Level...

---

*Continuity Insights*

2012 MANAGEMENT CONFERENCE
Business Continuity Maturity Model®

Increasing Business Continuity Competency Maturity

... containing measurable criteria within each cell.

<table>
<thead>
<tr>
<th>Maturity Model Levels</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
<th>Level 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Governed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Self-Governed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Centrally Governed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Awakening</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planned Growth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Synergetic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Corporate Competencies**

Attributes of an Organization at Each Maturity Level

Criteria: ‘Descriptors’ defining a corporate competency at a specific maturity level.

**BC Program Content**

Attributes of Each BC Discipline at Each Maturity level

Criteria: “Performance Requirements” defining a program discipline at a specific maturity level.
Business Continuity Maturity Model®

Increasing Business Continuity Competency Maturity

Corporate Competencies

Each Corporate Competency categorizes a set of measurable attributes that collectively are required to create and sustain an integrated business continuity program.
**Leadership**

The commitment and understanding demonstrated by executive management regarding the implementation of an enterprise-wide business continuity program. The degree to which the “business case” (justification) has been articulated and understood.
**Resource Commitment**

The application of sufficient, properly trained and supported personnel, financial and other resources to ensure the sustainability of the BC Program.
Business Continuity Maturity Model®

Increasing Business Continuity Competency Maturity

Metrics

The development and regular reporting of quantifiable criteria used to monitor the BC Program performance. The establishment of a baseline and on-going tracking of established business continuity competency goals.
### Business Continuity Maturity Model®

**Increasing Business Continuity Competency Maturity**

<table>
<thead>
<tr>
<th>Maturity Model Levels</th>
<th>LEVEL 1</th>
<th>LEVEL 2 Competency Model</th>
<th>LEVEL 3</th>
<th>LEVEL 4</th>
<th>LEVEL 5</th>
<th>LEVEL 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>BC Program Structure</td>
<td>Ready</td>
<td>Agile Business Continuity</td>
<td>Mature</td>
<td>Optimized</td>
<td>Fusion</td>
<td>Best-in-Class</td>
</tr>
<tr>
<td>Corporate Competencies</td>
<td>Ready</td>
<td>Agile Business Continuity</td>
<td>Mature</td>
<td>Optimized</td>
<td>Fusion</td>
<td>Best-in-Class</td>
</tr>
<tr>
<td>Attributes of an Organization at Each Maturity Level</td>
<td>Able to Crawl</td>
<td>Able to Walk</td>
<td>Able to Run</td>
<td>&quot;IT&quot; Runner</td>
<td>Competitive Runner</td>
<td>Olympic Runner</td>
</tr>
<tr>
<td>Resource Commitment Matrix</td>
<td>&quot;At Risk&quot;</td>
<td>&quot;Coordinated Performer&quot;</td>
<td>&quot;Best of Breed&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### BC Program Structure

The scale and appropriateness of the business continuity program implemented across the enterprise. The degree to which the BC Program matches the articulated business case.
## Business Continuity Maturity Model®

### Increasing Business Continuity Competency Maturity

<table>
<thead>
<tr>
<th>Maturity Model Levels</th>
<th>Level 1: Basic</th>
<th>Level 2: Supported</th>
<th>Level 3: Resilient</th>
<th>Level 4: Advanced</th>
<th>Level 5: Strategic</th>
<th>Level 6: Culture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Competencies</td>
<td>Able to Speak</td>
<td>Able to Listen</td>
<td>Able to Run</td>
<td>T-1 “Runner”</td>
<td>Competitive Runner</td>
<td>Olympic Runner</td>
</tr>
<tr>
<td>BC Awareness</td>
<td>Organization “At Risk”</td>
<td>“Competent” Performer</td>
<td>“Best of Breed”</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### BC Awareness

The breadth and depth of business continuity conceptual awareness throughout all staff levels of the organization.
Business Continuity Maturity Model®

Increasing Business Continuity Competency Maturity

**External Coordination**

Coordination of business continuity issues and requirements with external community including customers, vendors, government regulatory bodies, unions, local 1st responders. Insure that critical supply chain partners have in place adequate BC Programs of their own.
Business Continuity Maturity Model®

Increasing Business Continuity Competency Maturity

Program Pervasiveness

The level of business continuity coordination between departments, functions and business units. The degree to which business continuity considerations have been incorporated in other business initiatives / programs.
Business Continuity Maturity Model®

### Increasing Business Continuity Competency Maturity

<table>
<thead>
<tr>
<th>Maturity Model Levels</th>
<th>LEVEL 1</th>
<th>LEVEL 2</th>
<th>LEVEL 3</th>
<th>LEVEL 4</th>
<th>LEVEL 5</th>
<th>LEVEL 6</th>
<th>LEVEL 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Competencies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Attributes of an Organisation at Each Maturity Level**:
  - Level 1: Ability to Cope
  - Level 2: Ability to Work
  - Level 3: Ability to Run
  - Level 4: "Fit" Runner
  - Level 5: Competitive Runner
  - Level 6: Olympic Runner

### BC Program Content

#### BC Program Content

Each of the four BC program disciplines categorizes a set of attributes of increasing capability as stand alone disciplines (maturity levels 1-3) and as part of an integrated BC program (maturity levels 4-6).
How to conduct a self-assessment workshop?

- This is an intuitive self-assessment process depending on the collective opinion of those participating at the time the self-assessment is completed.
- The self-assessment facilitators will encourage discussion amongst participants to resolve conflicts and reach consensus answer which is documented “live” and on-screen so that all workshop participants can see the answer agreed upon.
- We will document all assumptions we make as we progress through the self-assessment.
- We will produce the initial ‘scorecard’ at the end of today’s workshop.
During the workshop, we will discuss each Descriptor and reach mutual agreement on what percentage complete it is.

**STEP ONE**
Review each ‘Descriptor’ from the BCMM® and answer each with question: “What % complete is this descriptor?

**BC PROGRAM STRUCTURE**

<table>
<thead>
<tr>
<th>Performance Requirements</th>
<th>% Complete</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategy/Culture/Goals</strong></td>
<td>25</td>
<td>Not significantly linked to any of these at present</td>
</tr>
<tr>
<td>Dept/BUs BCM activities in sync with relevant portions of Enterprise strategy, culture, and goals</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organizational Design</strong></td>
<td>50</td>
<td>many plans have dependencies documented - more to be don</td>
</tr>
<tr>
<td>Identification of key internal linkages and working agreements</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Roles &amp; Responsibilities</strong></td>
<td>50</td>
<td>Some groups working hard independently. Others asking for help. Others still not yet taken full ownership.</td>
</tr>
<tr>
<td>Dept/BUs staff has responsibility for BCM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overlapping roles may occur</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td><strong>Policies &amp; Process</strong></td>
<td>50</td>
<td>All followed standard M&amp;T - not all plans took full advantage of these methods and tools</td>
</tr>
<tr>
<td>Active Dept/BUs have formulated policies, standards, &amp; practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Enterprise policy for BCM exists</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**STEP TWO:** In the Notes, we will describe why any descriptor is not currently at 100% complete.

The Support Team will guide the participants through each descriptor.
Scorecard and findings document will be prepared from the workshop data that describes gaps and strengths of current BC planning environment as well as all recommended actions.

Workshop data will determine strengths and gaps — it’s not about the score

<table>
<thead>
<tr>
<th></th>
<th>Self-Assessment Results</th>
<th>Maturity Model Scores</th>
<th>Aggregate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Level 1</td>
<td>Level 2</td>
<td>Level 3</td>
</tr>
<tr>
<td>Leadership</td>
<td>100%</td>
<td>100%</td>
<td>36%</td>
</tr>
<tr>
<td>Employee Awareness</td>
<td>100%</td>
<td>100%</td>
<td>16%</td>
</tr>
<tr>
<td>BC Program Structure</td>
<td>100%</td>
<td>63%</td>
<td>52%</td>
</tr>
<tr>
<td>Program Pervasiveness</td>
<td>100%</td>
<td>100%</td>
<td>17%</td>
</tr>
<tr>
<td>Metrics</td>
<td>100%</td>
<td>100%</td>
<td>16%</td>
</tr>
<tr>
<td>Resource Commitment</td>
<td>100%</td>
<td>100%</td>
<td>7%</td>
</tr>
<tr>
<td>External Coordination</td>
<td>100%</td>
<td>100%</td>
<td>45%</td>
</tr>
<tr>
<td>BC Program Content</td>
<td>100%</td>
<td>100%</td>
<td>82%</td>
</tr>
<tr>
<td>Incident Management</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Technology Recovery</td>
<td>100%</td>
<td>100%</td>
<td>80%</td>
</tr>
<tr>
<td>Security Management</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Business Recovery</td>
<td>100%</td>
<td>100%</td>
<td>48%</td>
</tr>
</tbody>
</table>

Percent Complete

| Color Legend | 0-49% | 50-89% | 100% |

Increasing Business Continuity Competency Maturity

<table>
<thead>
<tr>
<th>Maturity Model Levels</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
<th>Level 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Governed</td>
<td>Athlete</td>
<td>Ability</td>
<td>Athlete</td>
<td>Ability</td>
<td>Athlete</td>
<td>Ability</td>
</tr>
<tr>
<td>Supported Self</td>
<td>Analog</td>
<td>Ability</td>
<td>Analog</td>
<td>Ability</td>
<td>Analog</td>
<td>Ability</td>
</tr>
<tr>
<td>Centrally Governed</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
</tr>
<tr>
<td>Planned Growth</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
</tr>
<tr>
<td>Synergistic</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
<td>Ability</td>
</tr>
</tbody>
</table>

Continuity Insights

2012 Management Conference
Maturity Level 1 – Self-Governed

Little, if any business continuity planning is localized and largely “ad hoc” across the enterprise.
### Increasing Business Continuity Competency Maturity

<table>
<thead>
<tr>
<th>Maturity Model Levels</th>
<th>Level 1 Supported</th>
<th>Level 2 Self-Governed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Athlete Analogy</td>
<td>Able to Crawl</td>
<td>Able to Walk</td>
</tr>
<tr>
<td>Comparative Model</td>
<td>Organization &quot;At Risk&quot;</td>
<td>&quot;Champion&quot; Performer</td>
</tr>
<tr>
<td>Corporate Competencies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attributes of an Organization at Each Maturity Level</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>BC Program Content</th>
<th>Attributes of Each BC Discipline at Each Maturity Level</th>
</tr>
</thead>
</table>

**Maturity Level 2 – Supported Self-Governed**

Pockets of integrated business continuity underway, but remains largely siloed within specific areas of the organization.
### Increasing Business Continuity Competency Maturity

#### Maturity Model Levels

<table>
<thead>
<tr>
<th>Maturity Model Levels</th>
<th>Corporate Competencies</th>
<th>Attributes of an Organization at Each Maturity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Athlete Analogy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comparative Model</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Maturity Level 3 – Centrally Governed

Participating departments have instituted rudimentary governance program and mutually agreed upon practices. Management has begun discussing the value proposition for an integrated business continuity program.
Maturity Level 4 – Enterprise Awakening

The organization has started an appropriately scaled, sustainable integrated BC program with the goal of reaching all parts of the organization.
Maturity Level 5 – Planned Growth

All departments have created and tested their initial integrated BC plans. Plans and planning begin encompassing inter-departmental and other dependency considerations.
**Maturity Level 6 – Synergistic**

All departments have a measurably high degree of BC planning proficiency. Cross-functional planning and testing routinely practiced. The organization is widely regarded as a BC leader within their industry.
BCMM® Model Access Limits

• Access to the Model:
  – Open (http://virtual-corp.net/html/bcmm.html)
  – Controlled (http://theicor.org)

• Access to the Proprietary Model (Additional Components):
  – Controlled
  – Managed by the BC Service Center
Business Resilience Program

• *The Business Resilience program:*

• *Integrates with*
  – Incident/Emergency Management
  – Business Recovery (includes National Offices and Clinical)
  – IT Disaster Recovery

• *Aligns with*
  – Information Security Management
  – Physical Security Management
What is Integrated Business Continuity?

**Integrated Business continuity (BC):** The formal planning process that minimizes or eliminates the impact of events that disrupt critical clinical and business operations, functions, and services. This process integrates the following disciplines:

- Incident Management
- Technology Recovery
- Security Management
- Clinical and Business Recovery
Integrated Business Continuity
Working Together

- **Incident Management Plan**
  - Save lives and protect assets
  - Conduct damage assessment
  - Site Emergency Operations Center (EOC)
  - Command, Control, and Communications

- **Security Management Plan**
  - Physical & cyber security plans

- **Clinical & Business Recovery Plan**
  - Ensure that critical functions continue to be performed
  - Departmental Recovery Plans
  - Includes EOC communications and authorizations

- **Technology Recovery Plan**
  - Ensure critical technology assets and services are available
  - Hot site recovery
The Business Continuity Program Life Cycle

- **Capability**
  - Normal Operations
  - Minimum Acceptable Level of Capability
  - Risk Mitigation

- **Time**
  - Proactive BCM Activities (Prevention and Preparedness)
  - Reactive BCM Activities (Response, Recovery & Restoration)
  - Proactive BCM Activities (Prevention and Preparedness)

- **Events**
  - Incident Occurs
  - Recovery Time Objective (RTO)
  - Emergency Response
  - Recovery
  - Restoration
  - Return to Normal Operations

- **Contingency Planning and Crisis Management**

---

*modified U.S. DoD graphic*
Program Approach Summary

- Obtained Leadership Approval Business Resilience Program
- Established Business Resilience Awareness Communication Program
- Developed 5 year Strategic Plan
- Performed analysis on enterprise BR Management tools
  - Developed “best-in-class” HVA and BIA
  - Deployed HVA
  - Developed BIA deployment program
    - Ran Pilot
    - Rolled out to MBOs
    - Developed Application BIA
- Enhanced Emergency Management
  - Implement suitable technology and process controls for ongoing surveillance, assessment of threats and response to incidents
Our Vision - Sustainability

• Developed Standardized Plans
  – Emergency Management
  – Continuity of Operations
  – Business Continuity/Downtime Procedures
  – IT Disaster Recovery
  – Migrated reporting structure from IT Operations to IT Security

• Scheduled exercises to meet
  – Audit remediation requirements
  – Application migration requirements
  – Business Resilience Program
    • Integrated Table-Top Exercises
    • Integrated Functional Exercises

• Reported Metrics
  – Dashboard with regional activities
  – Conduct Business Resilience Maturity Survey
  – Update market program maturity dashboards
**High Level CHI BR Roadmap – Foundational Tasks Annual Realization**

<table>
<thead>
<tr>
<th>Proposed Initiatives/Activities</th>
<th>JAN</th>
<th>FEB</th>
<th>MAR</th>
<th>APR</th>
<th>MAY</th>
<th>JUNE</th>
<th>JULY</th>
<th>AUG</th>
<th>SEPT</th>
<th>OCT</th>
<th>NOV</th>
<th>DEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>BR Governance and Administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Impact Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Continuity Plans</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery Plans</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exercising</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit &amp; Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Continuity Insights 2012 MANAGEMENT CONFERENCE*
Business Resilience Program Keys to Success

• Establish preparedness and BR “culture”
• Implement practical, prudent strategies and plans that remain relevant over time
• Develop an organizational understanding of dependencies and vulnerabilities
• Establish the ability to assess emergency response, business continuity and disaster recovery capabilities
• Establish the ability to document and maintain BR program