BCM Trends, Issues, and the Future

AZ Central RIMS Chapter

January 11, 2017
MHA CONSULTING, INC.

KEY FACTS

- A 17-year proven track record of applying industry standards and best practices across a diverse pedigree of clients.
- A simple mission: Ensure the continuous operations of our client’s critical processes.
- SaaS toolset includes BCM Compliance and Residual Risk.

SENIOR LEADERSHIP

Michael A. Herrera, CBCP
Chief Executive Officer
Phoenix, Arizona
www.mha-it.com
DIVERSE, GLOBAL CLIENT BASE

<table>
<thead>
<tr>
<th>SERVICES</th>
<th>HEALTHCARE</th>
<th>EDUCATION</th>
<th>FINANCIAL INSTITUTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>EARLY WARNING Services</td>
<td>AMGEN</td>
<td>ASU</td>
<td>PENFED Credit Union</td>
</tr>
<tr>
<td>LifeLock</td>
<td>CVS Health</td>
<td>Maricopa Community Colleges</td>
<td>City National Bank</td>
</tr>
<tr>
<td>ATS</td>
<td>COVIDEN</td>
<td>NUSAIVE</td>
<td>Charles Schwab Bank</td>
</tr>
<tr>
<td>American Traffic Solutions</td>
<td>REDFLEX Traffic Systems</td>
<td></td>
<td>Desert Schools</td>
</tr>
<tr>
<td>Traffic Systems</td>
<td>McKesson</td>
<td>Phoenix Children’s Hospital</td>
<td>Fannie Mae</td>
</tr>
<tr>
<td>Transperfect</td>
<td>OhioHealth</td>
<td>Providence College</td>
<td>Square</td>
</tr>
<tr>
<td>Hewlett Packard</td>
<td>McKesson</td>
<td>Providence College</td>
<td>Mercedes-Benz Financial Services</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Scottsdale Healthcare</td>
<td>The Catholic University of America</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CONSUMER PRODUCTS</td>
<td>INSURANCE</td>
<td>TRAVEL &amp; ENTERTAINMENT</td>
<td>GOVERNMENT/UTILITY</td>
</tr>
<tr>
<td>BJ's</td>
<td>Mutual of Omaha</td>
<td>MGM Resorts</td>
<td>City of Tempe Arizona</td>
</tr>
<tr>
<td>Ratner Companies</td>
<td>Health Alliance</td>
<td>Harrah's</td>
<td>PNM</td>
</tr>
<tr>
<td>Guitar Center</td>
<td>CopperPoint</td>
<td>Regal Entertainment Group</td>
<td>CAP Central Arizona Project</td>
</tr>
<tr>
<td>GameStop</td>
<td>BlueCross BlueShield of Arizona</td>
<td>Well Resorts</td>
<td>NASA</td>
</tr>
<tr>
<td>Insight</td>
<td>York</td>
<td>SkyWest</td>
<td></td>
</tr>
<tr>
<td>Nestle</td>
<td>Henkel</td>
<td>AAA</td>
<td></td>
</tr>
<tr>
<td>Petsmart</td>
<td>ProLogic</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TriWest</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2016 MHA Consulting. All Rights Reserved.
## COMPREHENSIVE SOLUTIONS PRACTICES

<table>
<thead>
<tr>
<th>ASSESS THE CURRENT ENVIRONMENT</th>
<th>RECOVERY STRATEGIES/SOLUTIONS</th>
<th>RESPONSE &amp; RECOVERY PLANS</th>
<th>EXERCISES</th>
<th>MAINTAIN &amp; IMPROVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Current State Assessment</td>
<td>• Business Recovery Strategies</td>
<td>• Crisis Management</td>
<td>• Training &amp; Awareness</td>
<td>• Update Recovery Plans</td>
</tr>
<tr>
<td>• Business Impact Analysis</td>
<td>• Data Center Recovery Strategies</td>
<td>• Business Recovery</td>
<td>• Mock Disaster Exercises</td>
<td>• Update Current State Assessment</td>
</tr>
<tr>
<td>• Threat &amp; Risk Assessment</td>
<td></td>
<td>• IT Disaster Recovery</td>
<td>• Plan Functional Walkthroughs</td>
<td>• Update Business Impact Analysis &amp; Threat Assessment</td>
</tr>
<tr>
<td>• BCMMETRICS™ Compliance Confidence (C2)</td>
<td></td>
<td></td>
<td>• Alternate Worksite Exercises</td>
<td></td>
</tr>
<tr>
<td>• BCMMETRICS™ Residual Risk (R2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• BCMMETRICS™ BIA On-Demand (BIA^{OD})</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Business Resumption Planning:**
The process initiated to resume business operations to a level consistent with the business requirements.

**IT Disaster Recovery Planning:**
The recovery of information technology processes, systems, applications, databases, and network assets used to support critical business processes.

**Crisis Management:**
A series of actions taken to gain control of the event quickly to minimize the affects of an interruption and prepare for recovery.
Stringent legislation, regulations, and standards require comprehensive business continuity “proof of control” measures be verifiable and operational.

Hyper-vigilant, focused regulators, auditors, and customers are better prepared to evaluate your program.

Management is increasingly being held accountable for minimizing exposures.

Non-regulated businesses in all industries are now being required to show evidence of Business Continuity in their organization.
KEY TRENDS

TRENDS IN

BUSINESS CONTINUITY

- Lack of management emphasis.
- Let's face it, we are not prepared.
- Threat landscape is changing daily.
- Third party supplier risk.
- Budget.

- Loss of intellectual capital.
- Recovery timeframes are shorter and shorter.
- Organizations cannot lose data.
- Minimal to no testing.
- Lack of integration between Risk Management & BCM.
LET’S TAKE A QUICK SURVEY REGARDING BCM COMPLIANCE & RESIDUAL RISK

• How many of you regularly measure and assess compliance in your BCM program?
• If yes, what BCM standard or standards do you use to assess the state of compliance of your program?
• How many of you identify and measure residual risk in your program?
• How many of you routinely update management on the state of compliance and/or residual risks?

“Without data you’re just another person with an opinion.”
- W. Edwards Deming, Data Scientist
HOW CAN BETTER UNDERSTAND MY BCM RISK?

COMPLIANCE
IS BEING IN A STATE OF ACCORDANCE WITH ESTABLISHED STANDARDS, GUIDELINES AND DIRECTIVES.

Considerations
• Management Oversight
• Policies and Standards
• Methodology
• Documentation

Assesses
• Program Dimensions (Program Admin, Crisis, DR, BRP, etc.)

Output
• Levels of Compliance (Low, Moderate, High)

RESIDUAL RISK
IS THE RISK THAT REMAINS AFTER ALL EFFORTS HAVE BEEN MADE TO IDENTIFY AND ELIMINATE THE RISKS.

Considerations
• Inherent Risk
• Risk Tolerance
• Mitigating Controls
• Residual Risk

Assesses
• Individual Business and IT Recovery Plans

Output
• Areas of Residual Risk (within or outside tolerance)
BCM COMPLIANCE STANDARDS

STANDARDS IN BUSINESS CONTINUITY

- ISO 22301
- FFIEC
- NIST 800
- NFPA 1600
- SEC
- FISMA
- FINRA
- Supply Chain Resiliency Leadership Council

MEASURE COMPLIANCE IN THESE BCM DIMENSIONS

- Program Administration
- Crisis Management
- Business Recovery
- IT Disaster Recovery
- Fire & Life Safety
- Supply Chain Risk Management
- Third Party Management
BCM COMPLIANCE – THE GOOD
BCM COMPLIANCE – THE UGLY

- Program Administration: Value 22.00
- Crisis Management: Value 61.00
- Business Recovery: Value 15.00
- IT Disaster Recovery: Value 49.00
- Supply Chain Risk Management: Value 9.00
- Fire & Life Safety: Value 2.00
WHAT DO THESE SCORES TELL US?

**COMPLIANCE ASSESSMENTS**

ASSESS THE STATE OF ACCORDANCE WITH ESTABLISHED STANDARDS, GUIDELINES AND DIRECTIVES:

- Identifies Areas of Success and Opportunity
- Pinpoints Where Resources are Needed/Not Needed
- Highlights areas of Significant Risk with the GREATEST ROI for improvement
- Provides Direction for Strategic Planning, Roadmaps for Improvement, Continuous Monitoring and Resource Allocation (people, money, technology)
- Reveals Potential Areas of Residual Risk.

**NEXT STEPS**

AFTER THE COMPLIANCE ASSESSMENT TYPICALLY INCLUDE THE FOLLOWING:

- Strategic Planning
- Roadmaps for Improvement
- Resource Allocation (People, Money, etc.)
- People Assessment
- Residual Risk Analysis

**Remember** - If you can’t measure it, you can’t manage it.
COMPLIANCE LEARNINGS

BAD

USE OF COMPLIANCE MEASUREMENTS

• We continue to pass audits, so who cares?
• Why measure? We know it’s bad.
• We aren’t held to standards.
• It won’t happen to us
• How do I use the data?
Residual Risk is defined as the remaining risk after controls have been implemented and monitored and the effect of their findings considered.

Residual Risk considers the inherent risk (risk before controls) that exists prior to assessing the mitigating controls.

Identifies the Risk Tolerance or level of willingness to accept risk. Low Risk Tolerance = tighter, more stringent controls, more expense and vice versa.

Process assesses and evaluates the state of mitigating controls that are designed to mitigate effects of the inherent risk.

Determines if remaining Residual Risk is within or outside of the agreed upon Risk Tolerance based on the state of the mitigating controls.
## ASSESSING BCM RESIDUAL RISK

**THE RESIDUAL RISK PROCESS**

We calculate BCM Residual Risk ($R^2$) for critical business and IT recovery plans within a program.

The process considers Criticality Factors, Threat Landscape, Risk Tolerance and Mitigating Controls for each individual plan.

Assessing Residual Risk will identify how “bullet proof” and “capable” each plan is within your portfolio of critical plans.

**FOCUS** should be given to those business units and / or systems/aps with the highest inherent risk to the organization.

**CRITERIA**

<table>
<thead>
<tr>
<th><strong>Criticality Factor (CF)</strong></th>
<th>The level of impact of the business unit or system/app to the organization. This is based on the RTO.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat Landscape (TI)</strong></td>
<td>The potential for threats/risks in the environment that the business unit or system/app resides in.</td>
</tr>
<tr>
<td><strong>Inherent Risk Factor (RF)</strong></td>
<td>The combination of the criticality factor and threat landscape.</td>
</tr>
<tr>
<td><strong>Risk Tolerance (RT)</strong></td>
<td>The Level of Risk We Are Willing to Accept Before Controls Are Considered</td>
</tr>
</tbody>
</table>

**MITIGATING CONTROLS**

- Business Impact Analysis
- Recovery Strategy
- Recovery Exercises
- Recovery Plan
- Recovery Team
- Third Party Supplier Risk

**INDUSTRY STANDARDS, BEST PRACTICES & COMMON SENSE**
WHERE DOES THE MAJOR RISK EXIST?

- Recovery Strategy
- Recovery Exercises
- Recovery Team
- Third Party Supplier Risk
## BUSINESS PROCESS OUTSOURCER - TECHNOLOGY

<table>
<thead>
<tr>
<th>Telephone System</th>
<th>Critical (&lt; 4 Hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Plan Name</td>
<td>Address</td>
</tr>
<tr>
<td>Switch Recovery Plan</td>
<td>7777 7th Avenue Anywhere 2 Midwest 77777 USA</td>
</tr>
<tr>
<td>Building Name</td>
<td>Recovery Plan Owner Name</td>
</tr>
<tr>
<td>Data Center 2</td>
<td></td>
</tr>
</tbody>
</table>

### Risk Factor
- Catastrophic

### Risk Appetite/Tolerance
- 10% - Low

### Threat Landscape
- High

### Mitigating Control Name
- Business Impact Analysis
- Recovery Strategy
- Recovery Exercises
- Recovery Plan
- Recovery Team
- Training and Awareness
- Third Party Supplier Risk
- Residual Risk (RR)

### Score

<table>
<thead>
<tr>
<th>Control</th>
<th>Score</th>
<th>State Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Impact Analysis</td>
<td>3</td>
<td>Average</td>
</tr>
<tr>
<td>Recovery Strategy</td>
<td>4</td>
<td>Above Average</td>
</tr>
<tr>
<td>Recovery Exercises</td>
<td>1</td>
<td>Poor/Non Existent</td>
</tr>
<tr>
<td>Recovery Plan</td>
<td>1</td>
<td>Poor/Non Existent</td>
</tr>
<tr>
<td>Recovery Team</td>
<td>1</td>
<td>Poor/Non Existent</td>
</tr>
<tr>
<td>Training and Awareness</td>
<td>2</td>
<td>Below Average</td>
</tr>
<tr>
<td>Third Party Supplier Risk</td>
<td>2</td>
<td>Below Average</td>
</tr>
<tr>
<td>Residual Risk (RR)</td>
<td>2.85</td>
<td>Outside Tolerance</td>
</tr>
</tbody>
</table>

2016 BCMMETRICS™
SO, WHAT ARE THE NEXT STEPS?

NOW WHAT DO WE DO?
NOW THAT WE HAVE AN IDEA OF WHERE OUR RESIDUAL RISK LIES, WHAT DO WE DO?

AREAS TO REVIEW
TAKE A HARD LOOK AT THESE AREAS FROM A COMPLIANCE AND RESIDUAL RISK PERSPECTIVE

- What mitigating controls have the most significant risk overall as an organization?
- Are we doing too much for some areas? Can we reduce costs?
- What can we do with the risk (transfer, mitigate, accept, etc.)?
- What is causing the failure in the mitigating controls that have the most significant exposures (e.g., resources, money, policy, standards, bad management, enforcement)?

- BCM Team
- Policies and Standards
- BIAs
- Training & Awareness
- Recovery Plans
- Recovery Strategies
- Recovery Exercises
- Third Party Supplier Risks

© 2016 MHA CONSULTING. ALL RIGHTS RESERVED.
THE ELUSIVE BCM ROI

ENTERPRISE COMPLIANCE & RESIDUAL RISK = BCM ROI
**SUMMARY**

**COMPLIANCE**  
Is being in a state of accordance with established standards, guidelines and directives.

**Considerations**  
- Management Oversight  
- Policies and Standards  
- Methodology  
- Documentation

**Assesses**  
- Program Dimensions (Program Admin, Crisis, DR, BRP, etc.)

**Output**  
- Levels of Compliance (Low, Moderate, High)

**RESIDUAL RISK**  
Is the risk that remains after all efforts have been made to identify and eliminate the risks.

**Considerations**  
- Inherent Risk  
- Risk Tolerance  
- Mitigating Controls  
- Residual Risk

**Assesses**  
- Individual Business and IT Recovery Plans

**Output**  
- Areas of Residual Risk (within or outside tolerance)
Michael A. Herrera, CEO
MHA Consulting, Inc.
herrera@mha-it.com
www.mha-it.com
Office: (888) 689-2290
Mobile: (602) 708-1718