The Business Continuity Management Risk Index (BCM-RI)
The Comprehensive Program Metric

Michael Kadar, MBCP, CISSP

© 2014, MK Continuity & Availability LLC
Questions

• How can we demonstrate the overall value of the business continuity management (BCM) program to executive management?
• How can we establish the measurement criteria necessary to quantify risk tolerance?
• Does reporting the number of BCPs developed, reviewed, and exercised assist executive management with making informed risk management decisions?
• How can we quantitatively measure current risk levels that can be compared with established risk tolerances?
• How can we report this to management in order to drive both risk management and BCM initiatives?
Objectives

• Provide a framework for developing and effectively implementing the business continuity management risk index (BCM-RI) for your organization.

• You will learn how the BCM-RI can be used to measure the overall risk/preparedness level of each business unit, each department, each subsidiary, and the entire organization.

• You will see how gap analyses can be performed to effectively compare BCM-RI levels to risk tolerance levels previously defined by management.

• Finally, you will learn how the BCM-RI can be expanded to develop risk indices for use by enterprise risk management and business resilience management programs.
Overview

• Prerequisites for Management Support
• Risk vs. Preparedness
• Business Continuity Management - Risk Index
• Composite Metrics
• BCM-RI Development
• BCM-RI Scoring System
• BCM-RI & Risk Tolerance
• BCM-RI Reporting
• Additional Risk Indices & Resilience
“Hello. I've seen you around. What group are you with?”

“Business Continuity Management.”

“Who? What does your group do?”

“We develop and exercise plans to assure the organization is prepared for crises.”

“What is our current level of preparedness and what is the preparedness goal?”

“(insert your answer here).”
Executive Support Prerequisites

There are two key prerequisites for getting executive support:

1. **Visibility**: Senior management is aware the BCM Program exists.

2. **Interest**: Senior management has reasons to be interested in BCM Program deliverables.

Then it becomes easier to get ...

Acceptance/Buy-In: Senior management has reasons to give approvals and support the BCM Program with requested resources.
In Chinese philosophy, the concept of "yin and yang", is used to describe how seemingly opposite or contrary forces are interconnected, interdependent, and how they give rise to each other as they interrelate to one another. This concept applies to:

- **Risk**
- **Preparedness**
Preparedness and Risk are not opposites. They are aspects of the same thing.

It is difficult to see one without the other – IF one really looks.
Actually

• Executive management sees, understands, and has concerns about risk-related issues much more than preparedness issues.

• In many cases, preparedness issues are almost invisible along with their relationship to risk management, leading to loss of interest in preparedness and BCM.
There are two key prerequisites for getting executive support:

1. **Visibility**: Senior management is aware the BCM Program exists

2. **Interest**: Senior management has reasons to be interested in BCM Program deliverables.

Then it becomes easier to get ...

**Acceptance/Buy-In**: Senior management has reasons to give approvals and support the BCM Program with requested resources
Which is Your BCM Modus Operandi?

Do you **push** preparedness onto organizations?

Or

Do organizations **pull** or request preparedness?

Ideally, this is executive management.
Is it working well?

It’s about as easy as pushing a rope!

How do you get them to pull?

Give them something they want – a way to measure ‘BCM Risk’
• Even if you have metrics, does executive management really care:
  – how many BCPs exist
  – which groups have them, and
  – when they were last reviewed or exercised? What do such statistics really mean to them and their concerns?
• Perhaps they have higher level interests – perhaps they might be more interested in the performance of the BCM ‘forest’ rather than the ‘trees’.
“37% say they don't measure the performance of their program. ... Most of the performance metrics are self-referencing and not related to the business. If we want to raise the profile of BCM and get executive-level buy-in, then we need to measure the value contribution of BCM programs, not just program performance.”

- Lee Glendon, Head of Research and Advocacy, BCI

2011-2012 Continuity Insights and KPMG LLP Global Business Continuity Management (BCM) Program Benchmark Study
Analogy: BCM Trees vs. Forest

• The TREES are your metrics:
  – Number of BCPs
  – Which groups have BCPs
  – Risk assessments, BIAs reviewed on-time
  – BCPs reviewed or exercised on-time
  – BCP teams trained on-time
  – Awareness sessions completed.

• The FOREST is what these metrics holistically measure: Preparedness or Risk Level.
• What does management care about? BCM? Hardly.
• Part of management’s concerns involve the management of risk.
• Most organizations have had risk management groups for decades. More recently we have seen the emergence of Enterprise Risk Management (ERM). Why?
• Risk management is a key BOD and senior management concern.
Perspective: Preparedness or Risk? The Preparedness/Risk Continuum

What will attain management visibility and interest?

High Preparedness.

Low Risk

Low Preparedness

High Risk.

What is the current Risk or Preparedness Level?
The Business Continuity Management Risk Index

The current Risk Level is the BCM-RI

High Preparedness → Low Risk

Low Preparedness → High Risk

What is the current Risk or Preparedness Level?
Definitions & You

• **Operational Risk** is the risk of loss or reputational damage resulting from inadequate or failed internal processes, people and systems or from external events
  – How does your organization define, identify, measure, and use risk levels to manage risk?

• **Risk Tolerance** is the capacity to accept or absorb risk
  – How does your organization define, identify, measure, and use risk tolerance to manage risk?
When considering risk or risk tolerance, is management thinking in terms of preparedness or Preparedness Tolerance?

What is management’s Risk Tolerance?
Quantify BCM Risk Tolerance

• The deliverables of BCM are controls and safeguards that manage risk.
• To quantify “BCM risk tolerance” we must define, then quantify “BCM risk”.
• BUT FIRST, how does your ERM organization determine, define, and measure risk levels and risk tolerance targets?
• Review BCM-RI development, definitions, criteria, etc. with ERM to assure it is an acceptable measure of risk.
**BCM Risk**

- Generally and simply, BCM Risk can be defined by the readiness/preparedness – or lack of preparedness – of the organization to recover.

- Specifically, BCM Risk is defined by the probability a particular threat/scenario will occur, the probability it will result in loss (vulnerability), and the impact of that loss.

- Now - how do we quantify BCM Risk or preparedness?

- Show management a key deliverable of BCM is increased preparedness or decreased risk.
Risk Management

High Preparedness
Low Risk

Low Preparedness
High Risk

Preparedness (controls)
- RA, BIA
- Plans, Teams, Resources
- Reviews, Training, Exercises.

Risk
- Threats
- Vulnerabilities
- Impacts
Measure Risk or Preparedness

What is Risk?

• Risk = T x V x I (product of Threat, Vulnerability, Impact).

• What Controls are you using to manage/decrease Risks?
  – Controls that decrease Threat Occurrence (likelihood)
  – Controls that decrease Vulnerability (loss likelihood)
  – Controls that decrease Impact (losses).

• Measure Levels of: Threat occurrence, Vulnerability, Actual Impacts.

• Composite Measure: Average of Risk Levels for relevant Threats?

• What should BCM be measuring: Risk? Preparedness?
Measure Risk or **Preparedness**

What is Preparedness?

- **preparedness** *noun*: The quality or state of being prepared, especially military readiness for combat.

- We can measure Preparedness by measuring the organization’s success in fulfilling the **requirements** of being prepared or ready.

- Through the implementation of BCM programs we have subjected the organization to the **process** of being prepared or ready.

- So, what are the components of the ‘process of BCM’?
Components of BCM

• The components of BCM are defined in:

• Example ‘BCM Process’: DRII Professional Practices
  – Program Initiation and Management
  – Risk Evaluation and Control
  – Business Impact Analysis
  – Business Continuity Strategies
  – Emergency Preparedness and Response
  – Business Continuity Plans
  – Awareness and Training Program
  – Business Continuity Plan Exercise, Audit, and Maintenance
  – Crisis Communications
  – Coordination with External Agencies.

• Assumption: We can measure Preparedness by measuring the organization’s success in fulfilling the requirements of the BCM program.

But, aren’t these just ‘metrics’?
Composite Metrics

• Yes they’re “Metrics”, but do they indicate ‘Preparedness’?
• We need to condense them to represent composite metrics that better indicate Preparedness

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment:</td>
<td>Threats/scenarios of concern, adequacy/update of existing controls, addition of new controls</td>
<td>RA quality &amp; dates, controls implemented</td>
</tr>
<tr>
<td>Business Impact Analysis:</td>
<td>Essential processes (Mission Essential Functions), RTO, RPO, Critical Time Period, recovery operations level, interdependencies, recovery resources</td>
<td>BIA quality &amp; dates, review dates</td>
</tr>
<tr>
<td>Recovery Strategy:</td>
<td>Recovery strategies for each scenario, ability to serve as RA controls and meet BIA requirements</td>
<td>Strategy quality, review dates</td>
</tr>
</tbody>
</table>
**Composite Metrics (cont.)**

- Another possible composite metric

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Existence of Plans:</strong></td>
<td>Essential facilities and business processes (high “Tier”) have plans</td>
<td>Plan inventory/count, compliance to standards</td>
</tr>
<tr>
<td><strong>Relevance of Plans:</strong></td>
<td>Plans address scenarios (risks) of most concern</td>
<td>Scenarios addressed</td>
</tr>
<tr>
<td><strong>Viability of Plans:</strong></td>
<td>Demonstrated in exercises</td>
<td><strong>Plan exercise dates</strong>, problems corrected</td>
</tr>
<tr>
<td><strong>Currency of Plans:</strong></td>
<td>Plans are reviewed periodically, teams are trained</td>
<td><strong>Plan review dates</strong>, training dates</td>
</tr>
</tbody>
</table>
BCM-RI Development: Phase 1

• Possible initial composite metric for a Risk Index – ‘Exercise Completion Date’.
  – Develop BCM Program Standards that requires the following before an Exercise Completion Date is assigned
    • Plan exists: The document meets a Plan Requirements Standard.
    • Review: The BIA, RA, plan document, team, and recovery resources have been evaluated using a Review Checklist based on a Plan Maintenance Standard.
    • Training: The team defined in the BCP attends training in compliance with a Plan Maintenance Standard.
    • Exercise: The plan document, team, and recovery resources have been exercised in compliance with a Plan Maintenance Standard.

• When choosing a BCM-RI measure ask yourself, “Does this composite metric indicate the level of risk (preparedness)”?
BCM-RI Development: Phase 1

• OK, we have an ‘Exercise Completion Date’ metric, now what?
• We need to develop a quantitative way to express the current level of Risk – we need a scoring system.
• Recommendation: Use a normalized system with a scale of zero (0) to one hundred (100)

High Preparedness = 100

0 = Low Preparedness

Low Risk = 0

100 = High Risk
• Assigning the BCM-RI score
  – When the Exercise Completion Date is approved by the BCM group, and if this is the business unit’s only plan, they earn a BCM-RI score of zero
    • BCM-RI = 0 (i.e. low score ~ low risk).

• But is the risk as low a few months later?
  – Plan Document: May now have outdated procedures or contact numbers.
  – Team: Someone may have left or joined the business unit.
  – Resources: Offsite copies of backup documents or data may be out-of-date, vendor services may have changed, equipment or supplies may have been removed from offsite storage.

• Need to modify the BCM-RI score to indicate increasing risk or decreasing preparedness as time passes.
Sample BCM-RI Scoring System

- Develop a system where ‘exercised’ plans have low risk scores.
- As time passes, the risk, and risk score increases automatically until it is exercised again according to a Maintenance Cycle.
- Sample scoring system:

<table>
<thead>
<tr>
<th>Plan Type</th>
<th>Plan Value (points)</th>
<th>Tier 1 Maint Cycle</th>
<th>Tier 2 Maint Cycle</th>
<th>Tier 3 Maint Cycle</th>
<th>Tier 4 Maint Cycle</th>
<th>Age 1 Mult.</th>
<th>Age 2 Mult.</th>
<th>Age 3 Mult.</th>
<th>Age 4 Mult.</th>
<th>Age 5 Mult.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCP</td>
<td>150</td>
<td>12</td>
<td>24</td>
<td>36</td>
<td>48</td>
<td>0</td>
<td>0.25</td>
<td>0.5</td>
<td>0.75</td>
<td>1.0</td>
</tr>
<tr>
<td>ERP</td>
<td>150</td>
<td>12</td>
<td>24</td>
<td>36</td>
<td>48</td>
<td>0</td>
<td>0.25</td>
<td>0.5</td>
<td>0.75</td>
<td>1.0</td>
</tr>
<tr>
<td>CMP</td>
<td>500</td>
<td>12</td>
<td>na</td>
<td>na</td>
<td>na</td>
<td>0</td>
<td>0.25</td>
<td>0.5</td>
<td>0.75</td>
<td>1.0</td>
</tr>
</tbody>
</table>

Months

Tiering/prioritizing ensures cost-effective mitigation.
BCM-RI: Single Plan Example

A Tier 1 business unit was assigned an ‘Exercise Completion Date’ of 5/22/13 by the BCP Program Office which calculated their score

\[
\text{BCM-RI} = \frac{(\text{Plan Value} \times \text{Age Mult.})}{\text{Total Plan Values}} \times 100.
\]

\[
\begin{align*}
\text{BCM-RI} &= \frac{(150 \times 0)}{150} \times 100 = 0 \text{ for 5/23 to 11/22} \\
\text{BCM-RI} &= \frac{(150 \times 0.25)}{150} \times 100 = 25 \text{ for 11/23 to 5/22/14} \\
\text{BCM-RI} &= \frac{(150 \times 0.50)}{150} \times 100 = 50 \text{ for 5/23/14 to 11/22/14} \\
\text{BCM-RI} &= \frac{(150 \times 0.75)}{150} \times 100 = 75 \text{ for 11/23/14 to 5/22/15} \\
\text{BCM-RI} &= \frac{(150 \times 1.0)}{150} \times 100 = 100 \text{ after 5/23/15}
\end{align*}
\]

<table>
<thead>
<tr>
<th>Business Unit or Facility Tiers</th>
<th>Plan Age Multipliers (6 mos. Each)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Plan Type</th>
<th>Plan Value</th>
<th>Tier 1 Maintain Cycle</th>
<th>Tier 2 Maintain Cycle</th>
<th>Tier 3 Maintain Cycle</th>
<th>Tier 4 Maintain Cycle</th>
<th>Age 1 Mult.</th>
<th>Age 2 Mult.</th>
<th>Age 3 Mult.</th>
<th>Age 4 Mult.</th>
<th>Age 5 Mult.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCP</td>
<td>150</td>
<td>12</td>
<td>24</td>
<td>36</td>
<td>48</td>
<td>0</td>
<td>0.25</td>
<td>0.5</td>
<td>0.75</td>
<td>1.0</td>
</tr>
</tbody>
</table>
**BCM-RI and Risk Tolerance**

- Organization with a **Tier 1 BU** (12 month cycle) and a **Tier 2 BU** (24 month cycle), each with a BCP

Corporate Risk Tolerance = 25 max.

<table>
<thead>
<tr>
<th>Plan</th>
<th>May ’12</th>
<th>Aug. ’12</th>
<th>Nov. 12</th>
<th>Feb. 12</th>
<th>2nd Year</th>
<th>3rd Year</th>
<th>4th Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCP T1 Activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BCP T1 BCM-RI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Reporting by Organization

Corporate BCM-RI = (Org 1 \text{RI} \times \text{Org1 \% of All Plans}) + 
\hspace{1cm} (\text{Org 2 RI} \times \text{Org2 \% of All Plans}) + ..... 

<table>
<thead>
<tr>
<th>Organization</th>
<th>BCM-RI</th>
<th># of Plans</th>
<th>% of All Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply Chain</td>
<td>12</td>
<td>8</td>
<td>4%</td>
</tr>
<tr>
<td>Human Resources</td>
<td>9</td>
<td>11</td>
<td>5%</td>
</tr>
<tr>
<td>Information Technology</td>
<td>31</td>
<td>104</td>
<td>50%</td>
</tr>
<tr>
<td>Operations</td>
<td>48</td>
<td>87</td>
<td>41%</td>
</tr>
<tr>
<td>CORPORATE</td>
<td>36</td>
<td>210</td>
<td>100%</td>
</tr>
</tbody>
</table>

Corporate BCM-RI = (12 \times 4\%) + (9 \times 5\%) + (31 \times 50\%) + (48 \times 41\%) = 36

If the Risk Tolerance level is 25, is this company’s \textbf{Current Risk Level} acceptable?
Is this company \textbf{prepared}?
Reporting by Tier/Criticality

- Example of how the BCM-RI can show where to direct BCM resources more cost effectively

<table>
<thead>
<tr>
<th>Tier</th>
<th>BCM-RI</th>
<th># of Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>47</td>
<td>19</td>
</tr>
<tr>
<td>2</td>
<td>34</td>
<td>31</td>
</tr>
<tr>
<td>3</td>
<td>23</td>
<td>58</td>
</tr>
<tr>
<td>4</td>
<td>20</td>
<td>102</td>
</tr>
</tbody>
</table>

Risk Tolerance = 25

- Highlights not enough focus on more critical business units and facilities.
ERM’s ‘Risk Categories?’

- Physical Security Risk Index
- Environmental Risk Index
- Safety Risk Index
- Information Protection Risk Index
- Information Technology Risk Index
- Supply Chain Risk Index
- Production Risk Index
- Customer Risk Index
- Financial Risk Index
- Operational Risk
- Hazard Risk
- Strategic Risk
- Reputation Risk Index

Risk Indices & Resilience
### Business Resilience

#### Business Resiliency Framework

<table>
<thead>
<tr>
<th>Objective</th>
<th>To enable the organization's preparedness and ability to recognize, react to, adapt to, and recover from unexpected HILF (Higher Impact, Lower Frequency) events.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resilience Function</td>
<td>Resilience Oversight</td>
</tr>
<tr>
<td>Organization</td>
<td>ERM: Undue Risk Exposure</td>
</tr>
<tr>
<td>Resilience Task</td>
<td>BCM Risk Index</td>
</tr>
<tr>
<td>Key Processes</td>
<td>Audit: Plan Coverage</td>
</tr>
</tbody>
</table>

#### Resilience Function

- **Objective:** To enable the organization's preparedness and ability to recognize, react to, adapt to, and recover from unexpected HILF (Higher Impact, Lower Frequency) events.

#### Organization

- **Function:** Resilience

#### Resilience Task

- **Objective:** To enable the organization's preparedness and ability to recognize, react to, adapt to, and recover from unexpected HILF (Higher Impact, Lower Frequency) events.

#### Key Processes

- **Objective:** To enable the organization's preparedness and ability to recognize, react to, adapt to, and recover from unexpected HILF (Higher Impact, Lower Frequency) events.
There are two key prerequisites for getting executive support:

1. **Visibility**: Senior management is aware the BCM Program exists

2. **Interest**: Senior management has reasons to be interested in BCM Program deliverables

Then it becomes easier to get ...

**Acceptance/Buy-In**: Senior management has reasons to give approvals and support the BCM Program with requested resources.
Summary/Action Items

Visibility

• Determine methods to align the BCM Program with ERM initiatives that have the attention of executive management.

Interest

• Identify the BCM deliverables of most interest to your executive management.
• Determine what would get executive management to want (pull) BCM deliverables.
• Learn how ERM measures/reports risk levels and risk tolerance.
• With ERM’s help determine whether your BCM Program should monitor and report ‘risk’ or ‘preparedness’.
Interest (cont.)

- Determine how your BCM Program can define and quantify BCM Risk or preparedness.
- Identify the BCM Program criteria/metrics that can be used to develop a ‘composite metric’ that quantitatively indicates the degree an organization is ‘prepared’ (is at low risk).
- Identify how a composite metric BCM-RI score can indicate increasing risk or decreasing preparedness as time passes.
- Review BCM-RI development, definitions, criteria, etc. with ERM to assure it is an acceptable measure of risk.
- Identify cost-effectiveness criteria: BU or facility Tiering, Plan/Team/Resource Maintenance Cycles.
Acceptance/Buy-In

• Determine how to use the BCM-RI:
  – To define and report the BCM risk tolerance level of operations and administrative organizations.
  – To measure and report the current BCM risk level of operations and administrative organizations.
  – As the reason for organizations to ‘pull’.
  – To perform ‘gap analyses’ (BCM risk tolerance level vs. current BCM risk level), obtain approval for gap remediation projects, and report progress to organization and executive management.
  – To represent the BCM Risk Level and/or the BCM Preparedness Level of the company/agency.
“That was easy to understand.

“Wonderful! Such dedication.”

about your next raise.”

“Actually, it’s quite common in my profession.”
Finis

Questions?
Contact Info & Reference

Michael Kadar, MBCP, CISSP  
MK Continuity & Availability LLC  
kadarsro@talkamerica.net  
248.376.5009 (cell)  
DTE Energy  
kadarm@dteenergy.com  
313.235-5515  

**************************

Book: “A Risk Management Approach to Business Continuity - Aligning Business Continuity with Corporate Governance”  
Julia Graham, David Kaye  
ISBN #1-931332-36-3