Assessing Residual Risk ($R^2$)

Why Residual Risk Could Cost Me My Job
Sponsored by BCMMetrics™

November 2016
MHA CONSULTING, INC.

KEY FACTS

17
Years in operation.

15
Average years industry experience.

CAPABLE
Comprehensive suite of services.

GLOBAL
Diverse, global client base.

SAAS
Compliance and risk tools.

• 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.

• Services include Business Continuity, Crisis Management, Disaster Recovery, IT Best Practices and Physical Security.

• SAAS tools include BCM Compliance and Residual Risk.

SENIOR LEADER

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

### SERVICES
- Early Warning
- LifeLock
- AMGen
- CVS Health
- McKesson
- Transperfect
- Hewlett Packard Enterprise

### HEALTHCARE
- Covidien
- NuVasive
- Phoenix Children's Hospital
- OhioHealth
- Scottsdale Healthcare

### EDUCATION
- ASU
- Maricopa Community Colleges
- Johnson & Wales University
- Providence College
- The Catholic University of America

### FINANCIAL INSTITUTIONS
- American Express
- PenFed Credit Union
- City National Bank
- Charles Schwab
- Charles Schwab Bank

### CONSUMER PRODUCTS
- BJ's
- Ratner Companies
- Guitar Center
- GameStop
- Mutual of Omaha
- Health Alliance
- Copper Point Mutual Insurance Company

### INSURANCE
- Federated Insurance
- Blue Cross Blue Shield of Arizona
- York
- SkyWest

### TRAVEL & ENTERTAINMENT
- MGM Resorts International
- Harrah's Entertainment Group
- Regal Entertainment Group

### GOVERNMENT/UTILITY
- City of Tempe, Arizona
- PNM
- CAP
- NASA
## COMPREHENSIVE SOLUTIONS PRACTICES

### ASSESS THE CURRENT ENVIRONMENT
- Current State Assessment
- Business Impact Analysis
- Threat & Risk Assessment
- BCMMETRICS™ Compliance Confidence (C2)
- BCMMETRICS™ Residual Risk (R2)

### RECOVERY STRATEGIES/SOLUTIONS
- Business Recovery Strategies
- Data Center Recovery Strategies

### RESPONSE & RECOVERY PLANS
- Crisis Management
- Business Recovery
- IT Disaster Recovery

### EXERCISES
- Training & Awareness
- Mock Disaster Exercises
- Plan Functional Walkthroughs
- Alternate Worksite Exercises

### MAINTAIN & IMPROVE
- Update Recovery Plans
- Update Current State Assessment
- Update Business Impact Analysis & Threat Assessment
THE CLASS

ASSESS

BCM PROGRAM
RESIDUAL RISK

• Discuss BCM Compliance and Residual Risk
• Learn about the impact of understanding Residual Risk in your BCM Program
• Develop the process to assess Residual Risk
• Discuss next steps after assessing Residual Risk

PROVIDE

CLEAR PICTURE
OF THE KEY COMPONENTS OF RESIDUAL RISK AND ITS APPLICATION IN YOUR PROGRAM

• Risk Tolerance
• Inherent Risk Factor
• Threat Landscape
• Mitigating Controls
THE CLASS

ASSESS

BCM PROGRAM
TRADITIONAL APPROACH

• Documentation
• Audit driven
• No clear ROI
• Compliance with industry standards

ASSESS

NEXT EVOLUTION
USE RESIDUAL RISK AWARENESS AND MEASUREMENT TO ENSURE RECOVERABILITY

• Quantitatively identify pockets of inherent risk
• Determine magnitude of Residual Risk
• Evaluate potential ways to minimize Residual Risk
• Target efforts to minimize significant risk
• Focus time, money, and other resources where most needed
THE BIG PICTURE

Risk

Resilience

Maturity

Compliance

Readiness
DEFINITIONS

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 RISK.

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)
WHAT IS RESIDUAL RISK?

- 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.
Residual Risk analysis provides management with a quantitative evaluation to best determine where they need to target efforts to minimize major risk – or where they may be exceeding the recovery needs of the business and wasting valuable time, money and resources.

Today's business environment requires BCM practitioners to optimize money, time and resources while minimizing risk and providing the highest level of recoverability.

In a perfect world, you want to have the lowest possible residual risk for your most critical business units and Information Technology to minimize the potential for significant impact to your organization in the event of a disruption.

The higher the residual risk, the bigger the opportunity for a greater impact in event of a disruption.
EXAMPLE – TODDLER RESIDUAL RISK

TODDLER RISK
WE HAVE A TODDLER AT HOME AND WE NEED TO IDENTIFY THE RESIDUAL RISK BEFORE LEAVING HIM HOME WITHOUT US.

• Concern – Our toddler being injured or harmed at home.
• Inherent Risk – What is the risk for toddler harm/injury?
• Risk Tolerance – What level of risk are we willing to accept?
• Identify Potential Mitigating Controls
  o Home Camera System
  o Baby-Proof Doors
  o Covered Electrical Outlets
  o Pool Fence
  o Babysitter

RESIDUAL RISK
THE BASIC CALCULATION INCLUDES THE FOLLOWING STEPS:

Step 1 – What is the inherent risk for potential harm?
Step 2 – What is the maximum risk tolerance we will accept?
Step 3 – What is the state of our mitigating controls?
Step 4 – What is our residual risk?
  • Determine state of our mitigating controls
  • Subtract mitigating control state from our Risk Tolerance
  • The remainder is the minimum score controls must meet
  • We are either within tolerance or outside of tolerance
Step 5 - Now what do we do?
  • Which controls will we fully implement? Outsource?
  • Which controls will we leave as is and accept the risk?
  • What other controls could minimize remaining risk?
**EXAMPLE – TODDLER RESIDUAL RISK**

<table>
<thead>
<tr>
<th>Inherent Risk</th>
<th>Low=(1)</th>
<th>Medium=(3)</th>
<th>High=(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toddler Injury/Harm at Home</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maximum Risk Tolerance</th>
<th>Low - (10%)</th>
<th>Moderate -(20%)</th>
<th>High - (25%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Willingness to Accept Risk</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maximum Risk Tolerance</th>
<th>Inherent Risk</th>
<th>Risk Tolerance</th>
<th>Max Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherent Risk * Risk Tolerance</td>
<td>5</td>
<td>10%</td>
<td>0.50</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mitigating Controls</th>
<th>Low = 1</th>
<th>Moderate = 3</th>
<th>High = 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Camera System</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Home Baby Proofed</td>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Pool Fence</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baby Sitter</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hazardous Chemicals Contained</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insect Spraying</td>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Mitigating Control State**

<table>
<thead>
<tr>
<th>What is Our Remaining Residual Risk?</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherent Risk - Max Risk Tolerance</td>
<td>5</td>
<td>0.50</td>
<td>4.5</td>
</tr>
<tr>
<td>Mitigating Control State</td>
<td></td>
<td></td>
<td>3.2</td>
</tr>
<tr>
<td>In or Out of Tolerance</td>
<td></td>
<td></td>
<td>1.3</td>
</tr>
</tbody>
</table>

**Note:** Our controls do not match our tolerance.
• **Risk Acceptance**: Risk acceptance does not reduce any effects; however, it is still considered a strategy. This strategy is a common choice when the cost of other risk management options, such as avoidance or limitation, may outweigh the cost of the risk itself. A company that doesn’t want to spend a lot of money on avoiding risks that do not have a high possibility of occurring will use the risk acceptance strategy.

• **Risk Avoidance**: Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. Risk avoidance is usually the most expensive of all risk mitigation options.

• **Risk Limitation**: Risk limitation is the most common risk management strategy used by businesses. This strategy limits a company’s exposure by taking some action. It is a strategy employing a bit of risk acceptance along with a bit of risk avoidance or a combination of both.

• **Risk Transference**: Risk transference involves handing risk off to a willing third party. For example, numerous companies outsource certain operations such as customer service, payroll services, etc. This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on their core competencies.

WHAT ARE OUR RESIDUAL RISK OPTIONS?

WHAT ARE OUR OPTIONS

BASED ON THE REMAINING RESIDUAL RISK?
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 “bulletproof” and “capable” each plan is within your portfolio of critical plans.

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

CRITERIA

Criticality Factor (CF)
The level of impact of the business unit or system/app to the organization. This is based on the RTO.

Threat Landscape (TL)
The potential for threats/risks in the environment in which the business unit or system/app resides.

Inherent Risk Factor (RF)
The combination of the criticality factor and threat landscape.

Risk Tolerance (RT)
The level of risk we are willing to accept before controls are considered.

MITIGATING CONTROLS

Business Impact Analysis

Recovery Strategy

Recovery Exercises

Recovery Plan

Recovery Team

Third Party Supplier Risk

INDUSTRY STANDARDS, BEST PRACTICES AND COMMON SENSE
GETTING STARTED

WHAT INFO DO I NEED TO BEGIN THE RESIDUAL RISK ASSESSMENT?

- List of Business and IT Recovery Time Objectives (RTOs)
- Understanding of the Threat Landscape (TL)
- Management’s Risk Tolerance (RT)
- Acceptance of Mitigating Controls and their Weighting
- Criteria for Assessing Mitigating Control Competencies

WHAT ACCESS DO I NEED TO COMPLETE THE RESIDUAL RISK ASSESSMENT?

- Business and IT Recovery Plans Being Evaluated
- Subject Matter Experts (SMEs) for the Recovery Plans
Identify your organizational RTO Categories:
- RTO 0 – 12 Hours or Less
- RTO 1 – 24 Hours or Less
- RTO 2 – 48 Hours or Less
- RTO 3 – 5 Days or Less
- RTO 4 – > 5 Days

We use Recovery Time Objectives (RTOs) to establish the Criticality Factor component of the Inherent Risk Factor (RF) of the business or IT recovery plan being evaluated. RTOs take impacts (dollar and non-dollar) to the organization and level of relative criticality into account.

Assign
IMPACT LEVEL TO EACH RTO

Each RTO category has a level of potential business impact associated with it. The shorter the RTO, the greater the impact and vice versa. Assign a business impact level to each RTO category:
- 1 = Insignificant (no pain)
- 2 = Minimal (minimal pain)
- 3 = Moderate (we start to feel some pain)
- 4 = Critical (we are really hurting)
- 5 = Catastrophic (we could die)
STEP 1 – IDENTIFY INHERENT RISK FACTOR (RF)

Identify

THREAT LANDSCAPES

• Identify the Threat Landscape (TL) based on the potential for a threat of impact to a business unit or IT recovery plan. You should refer to your Threat & Risk Assessments. Consider the following types of events:
  o Natural
  o Man-Made
  o Technological

Assign

THREAT PROBABILITY LEVELS

• Assign Threat Landscape Score Ranking and Definition based on the environment or environments in which the business unit or system/application operates:
  o High (5) – High potential for threat impacts
  o Medium (3.5) – Moderate potential for threat impacts
  o Low (1) – Low potential for threat impacts

• Example: Threats to my business unit are a lot different if we operate out of downtown NYC versus Boise, Idaho, or if my system/app stores highly confidential information that has high value to hackers.
Global Call Center business unit resides downtown in major metropolitan business area that has a high potential for natural and man-made threats.

- Business unit provides around the clock information services critical to government agencies operating domestically and internationally.
- The RTO of the business is RTO 0 – 12 Hours or Less, along with its supporting systems and applications.
- The Criticality Factor is 5 and the Threat Landscape is 5; the Inherent Risk Factor is 25.

Inherent Risk Factor Score Range, Based on Criticality Factor * Threat Landscape:
- 20 to 25 = High Inherent Risk
- 12 to 17.5 = Moderate Inherent Risk
- <12 = Low Inherent Risk

Business Units or Systems/Apps with Moderate to High Inherent Risk Factors should be considered for Residual Risk analysis.

The higher the score, the greater inherent risk based on impact and potential threats.
• Now, we need to identify what Management’s Risk Tolerance is for varying ranges of Inherent Risk. This will be your hardest job.

• Definition: Risk Tolerance is the level of risk that an organization is prepared to accept in pursuit of its objectives, and before action is deemed necessary to reduce the risk (Wikipedia).

• Identify the Risk Tolerance for the range of Inherent Risk Factor (Criticality Factor * Threat Landscape/5) levels:
  - If the Inherent Risk Factor range is 4.0 to 5.0 = Risk Tolerance Low (5%)
  - If the Inherent Risk Factor range is 3.0 to 3.9 = Risk Tolerance Moderate (10%)
  - If the Inherent Risk Factor range is <3.0 = Risk Tolerance High (20%)

• However, management can accept more risk as they see fit. You MUST tell them having a lower risk tolerance means it will take more resources (people, money, etc.) to ensure you are within tolerance.
EXAMPLE – CALL CENTER BUSINESS UNIT

<table>
<thead>
<tr>
<th>San Francisco Headquarters</th>
<th>Criticality</th>
<th>Threat Landscape</th>
<th>Risk Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherent Risk Factor</td>
<td>Risk to Business if Disrupted</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Risk Tolerance</td>
<td>Low - (5%)</td>
<td>Moderate - (10%)</td>
<td>High - (20%)</td>
</tr>
<tr>
<td>Willingness to Accept Risk</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Maximum Risk Tolerance:

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Tolerance</th>
<th>Max Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5%</td>
<td>0.25</td>
</tr>
</tbody>
</table>

INHERENT RISK FACTOR = CRITICALITY FACTOR * THREAT LANDSCAPE/5
You will need to educate management on Risk Tolerance and how the level of tolerance will impact the BCM program and its requirements.

Management will often accept more risk than you expect.

Lower Risk Tolerances require tighter controls to be in place that require more money, resources, etc., and vice versa.

Lower Threat Landscapes reduce Risk Factor scores significantly, meaning controls do not need to be at their highest.

- Identify Mitigating Controls
- Weight Mitigating Controls
- Identify Criteria to Assess Controls
- Determine Scoring for Mitigating Controls
STEP 3 – MITIGATING CONTROLS

PLAN MITIGATING CONTROLS

• Business Impact Analysis
• Recovery Strategy
• Recovery Exercises
• Recovery Plan
• Recovery Team
• Third Party Supplier Risk
• Training & Awareness

* These controls can be used to address IT recovery plans as well.

WEIGHTING & SCORING

• Each control is first weighted based on its importance to the ability to recover. Weighting for all controls must add up to 100%.
• Each control is individually scored (1 to 5) based on its level of completion and execution.
• The weight of each control is multiplied by its level of completeness and execution (1 to 5).
• The resulting scores are added together to provide a mitigating control score for the recovery plan.
STEP 3 – MITIGATING CONTROLS

ASSESSING & SCORING

MITIGATING CONTROLS

1. Poor/Non-Existent
   No Business Recovery Plan exists or is more than a year out of date.

2. Below Average
   Standard Business Recovery Plan with no specific recovery information.

3. Average
   Detailed Business Recovery Plan with specific recovery tasks.

4. Above Average
   Detailed Business Recovery Plan is complete, current and integrated with division and enterprise Business Continuity plans as required.

5. Superior
   Detailed Business Recovery Plan is complete, current, integrated and aligned with its dependent Disaster Recovery and Application Recovery Plans.
### BUSINESS UNIT EXAMPLE

#### Business Unit: Call Center

**San Francisco Headquarters**

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Criticality</th>
<th>Threat Landscape</th>
<th>Risk Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk to Business if Disrupted</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

**Risk Tolerance**

<table>
<thead>
<tr>
<th>Willingness to Accept Risk</th>
<th>Low - (5%)</th>
<th>Moderate - (10%)</th>
<th>High - (20%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Maximum Risk Tolerance**

<table>
<thead>
<tr>
<th>Risk Factor * Risk Tolerance</th>
<th>Risk Factor</th>
<th>Tolerance</th>
<th>Max Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>5%</td>
<td>0.25</td>
</tr>
</tbody>
</table>

#### Mitigating Controls

<table>
<thead>
<tr>
<th>Control</th>
<th>Weight</th>
<th>Poor = 1</th>
<th>Average = 3</th>
<th>Best Practice = 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Impact Analysis</td>
<td>10%</td>
<td></td>
<td>0.50</td>
<td></td>
</tr>
<tr>
<td>Recovery Strategy</td>
<td>30%</td>
<td>0.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Plan</td>
<td>5%</td>
<td></td>
<td>0.25</td>
<td></td>
</tr>
<tr>
<td>Recovery Team</td>
<td>10%</td>
<td></td>
<td>0.30</td>
<td></td>
</tr>
<tr>
<td>Recovery Exercise</td>
<td>35%</td>
<td>0.35</td>
<td>0.30</td>
<td></td>
</tr>
<tr>
<td>Third Party Exposure</td>
<td>10%</td>
<td></td>
<td>0.30</td>
<td></td>
</tr>
<tr>
<td>Mitigating Control State</td>
<td>100%</td>
<td></td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

#### What is Our Residual Risk?

<table>
<thead>
<tr>
<th>Risk Factor - Tolerance</th>
<th>Mitigating Control State</th>
<th>In or Out of Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4.75</td>
<td>2.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.75</td>
</tr>
</tbody>
</table>
## BUSINESS PROCESS OUTSOURCER

### Customer Support Operations

<table>
<thead>
<tr>
<th>Recovery Plan Name</th>
<th>Address</th>
<th>Building Name</th>
<th>Recovery Plan Owner Name</th>
<th>Executive Owner Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Support Operations</td>
<td>5555 5th Avenue Anywhere Midwest 55555 USA</td>
<td>Corporate Headquarters</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Risk Factor
- **Catastrophic**

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

### Threat Landscape
- High

### Mitigating Control Name

<table>
<thead>
<tr>
<th>Control Name</th>
<th>Score</th>
<th>State Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Impact Analysis</td>
<td>4</td>
<td>Above Average</td>
</tr>
<tr>
<td>Recovery Strategy</td>
<td>3</td>
<td>Average</td>
</tr>
<tr>
<td>Recovery Exercises</td>
<td>2</td>
<td>Below Average</td>
</tr>
<tr>
<td>Recovery Plan</td>
<td>3</td>
<td>Average</td>
</tr>
<tr>
<td>Recovery Team</td>
<td>3</td>
<td>Average</td>
</tr>
<tr>
<td>Training and Awareness</td>
<td>3</td>
<td>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>2.25</td>
<td>Outside Tolerance</td>
</tr>
</tbody>
</table>

---

2016 BCMMETRICS™
<table>
<thead>
<tr>
<th>Recovery Plan Name</th>
<th>Address</th>
<th>Building Name</th>
<th>Recovery Plan Owner Name</th>
<th>Executive Owner Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Risk Appetite/Tolerance</th>
<th>Threat Landscape</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate</td>
<td>20% - Moderate</td>
<td>Low</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mitigating Control Name</th>
<th>Score</th>
<th>State Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Impact Analysis</td>
<td>5</td>
<td>Superior/Not Applicable</td>
</tr>
<tr>
<td>Recovery Strategy</td>
<td>4</td>
<td>Above Average</td>
</tr>
<tr>
<td>Recovery Exercises</td>
<td>4</td>
<td>Above Average</td>
</tr>
<tr>
<td>Recovery Plan</td>
<td>5</td>
<td>Superior/Not Applicable</td>
</tr>
<tr>
<td>Recovery Team</td>
<td>5</td>
<td>Superior/Not Applicable</td>
</tr>
<tr>
<td>Training and Awareness</td>
<td>5</td>
<td>Superior/Not Applicable</td>
</tr>
<tr>
<td>Third Party Supplier Risk</td>
<td>4</td>
<td>Above Average</td>
</tr>
<tr>
<td>Residual Risk (RR)</td>
<td>0.00</td>
<td>Within Tolerance</td>
</tr>
</tbody>
</table>

BCMMETRICS™ 2016
SO, WHAT ARE THE NEXT STEPS?

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

• What mitigating controls have the most significant risk overall to our 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)?

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

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

THINGS TO THINK ABOUT

• We have found the most significant critical exposures are in Recovery Strategy and Recovery Exercises even for the most advanced organizations.

• Third Party Risk is still an unknown variable. Few organizations have a good knowledge of their exposure; it’s a big risk.

• Very few organizations have truly manageable R² in their programs. Many are solely focused on just getting the documentation done and lack the target - execution.

• You can significantly reduce risk by simply heightening the capability of the most important controls, from Low to Moderate.

• Perfect is the enemy of the good.

• Focus on the outcome, become target focused, and concentrate on the ability to successfully recover.
SUMMARY

• Implement BCM Compliance and Residual Risk.
• Identify where significant risks exist.
• Develop action plan to mitigate the risks.
• Address the compliance risks impacting Residual Risk.
• Stay target focused – recoverability.
UPCOMING WEBINARS

• **TESTING THE DR PLAN**, Richard Long
  – WEDNESDAY JANUARY 11, 2017 AT 11:00 A.M. PST

• **CALCULATING BCM ROI**, Michael Herrera
  – WEDNESDAY MARCH 8, 2017 AT 11:00 A.M. PST
Michael A. Herrera, CEO
MHA Consulting, Inc.
herrera@mha-it.com
www.mha-it.com
Office: (888) 689-2290
Mobile: (602) 708-1718