Internal Auditors: Friend or Foe?

Presented by:
Troy Harris
Manager, Technology Risk Management Services
RSM McGladrey, Inc.
301-607-0248
troy.harris@rsmi.com

Agenda
- Introduction
- The Traditional BCP Audit
- A New Approach to BCP Auditing
- IA Involvement and Key Auditing Considerations
  - Project Initiation
  - Risk Assessment and Business Impact Analysis (BIA)
  - Recovery Strategies
  - Business Continuity Plan Development
  - Testing & Maintenance
- Conclusions/Wrap-up and Q&A

Introduction
Opening Thought

- The Objective of Auditing a BCP:

To assist with the management of the organization’s risks by evaluating its recovery capabilities and identifying opportunities to enhance its overall BCP Program

BCP Activities Are Coordinated With…

- Emergency Response
- Risk Management
- Security
- Insurance
- Strategic Planning
- Public Authorities
- Vendors
- Business Partners
- Customers
- Internal Audit

Management Reporting

- The BCP Program Communicates with One of Management’s Ears…
  - Deliverable Approval (BIA, Plan Components, etc.)
  - BCP Program Status (Current Capabilities and Vulnerabilities)
  - Resource Requests (Funding, Staff, etc.)
  - Endorsement Requests
- …And Internal Audit Communicates with the Other One
  - Audit Reports
  - Deficiencies and Omissions

Guess Which One is the “Good Ear”…
Auditing A Business Continuity Plan

- BCPs Are Typically Audited Quantitatively Using Checklists

<table>
<thead>
<tr>
<th>Recovery and Restoration Procedures</th>
<th>5</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>All key critical systems have been identified.</td>
<td>No omissions were identified.</td>
<td>2</td>
</tr>
<tr>
<td>Formal contingency plans exist for each identified critical system.</td>
<td>Plans developed but not complete.</td>
<td>2</td>
</tr>
<tr>
<td>Formal contingency plans exist for each identified critical process.</td>
<td>Plans developed but not complete.</td>
<td>2</td>
</tr>
<tr>
<td>Formal high impact recovery stages have been identified.</td>
<td>Not documented.</td>
<td>2</td>
</tr>
<tr>
<td>Alternate procedures have been developed for performing critical business functions during the unavailability of required systems and/or other resources.</td>
<td>Few alternate procedures have been documented.</td>
<td>2</td>
</tr>
</tbody>
</table>

- To Truly Evaluate an Organization’s Recovery Capabilities, the BCP Program Must be **Qualitatively** Evaluated

The Traditional BCP Audit

Internal Auditors - Foe

- Isolated Involvement in the BCP Program
- Limited Knowledge of the Program’s Background
  - Roles/Responsibilities
  - Priorities
  - Strategies
  - Challenges
- Minimal Knowledge of BCP Concepts
- Rigid/Inflexible; Unreceptive to Input ("Independent")
- Concentrate Specifically on IA’s Objectives
The Traditional BCP Audit

- Point-in-Time Audit of the BCP Manual or a Single BCP Event
- Utilizes a Checklist Based on one or More Industry Standards
  - Standard(s) Selected by Internal Audit
  - Minimal Consideration of the Organization’s BCP Requirements
- Quantitative and Objective
  - No True Analysis of Recovery Capabilities
  - Components are Noted as Present or Missing; Possibly “Partial”

The Traditional BCP Audit - Deliverables

- Report of Included Elements and Notable Omissions
  - Is It There or Not?
  - Omissions Represent Action/Remediation List
  - Possibly Summarized with a “Score” or “Grade”
- Narrative Audit Summary
  - Minimal Evaluation of BCP Effectiveness or Impact on Recovery Capabilities
  - Simple Conclusions Based on Checklist Findings
  - No Analysis of the Reasons Behind the Omissions, etc.

The Traditional BCP Audit - Results

- List of Omissions to be Added to the BCP
  - Not Necessarily Deficiencies to be Addressed
  - Mandated Timelines to Complete the Additions
  - Additions May Detract from Strategic BCP Objectives
- Management and Organizational Visibility of Omissions
  - Certainly Not Positive Publicity for the BCP Program
  - Diminishes Confidence and Incentive to Participate
- More Work for the BCP Coordinator and Core Team
A New Approach to BCP Auditing

Internal Auditors - Friend

• Active Participant in all Aspects of the BCP Process
• Understands the Background, History, and Objectives of the BCP Program
• Knowledgeable of BCP Concepts and Proficient with Basic Disaster and Business Recovery Techniques
• Collaborative Attitude
• Seeks to Contribute to the Organization’s Risk Mitigation and Recovery Capabilities

A New Approach to BCP Auditing

• Ongoing Evaluation of the Organization’s Recovery Capabilities

• Audit Criteria Designed/Customized for the Organization
  – Derived from a Combination of Standards
  – Reflects the Organization’s BCP Requirements and Objectives

• Qualitative and Subjective
  – Components are Analyzed for Adequacy and Effectiveness
  – Examines Methodologies, Techniques, Processes, Resources, etc.
A New Approach to BCP Auditing - Deliverables

- Informative Checklists
  - Criteria Accurately Reflects The Goals of the BCP Program
  - Supplemented with Detailed Comments
  - Omissions and Other Findings Reflect (Potential) Deficiencies

- Narrative Sections
  - Executive Summary of Findings and Rational Conclusions
  - Evaluation of Deficiencies and the Related Implications
  - Analysis of “Cause and Effect” with Viable Recommendations

A New Approach to BCP Auditing - Results

- Renewed Endorsement of the Overall BCP Initiative
- Approval of Individual Activities
- Management Intervention
- Revised BCP Program Priorities/Management Direction
- Revised BIA Priorities
- Resource Adjustments
- Additional Reporting & Monitoring

IA Involvement
and
Key Auditing Considerations
Project Initiation

IA Involvement - Project Initiation
• Development of Program Charter
• Creation of BCP Policy
• Definition of Project Scope, Objectives, and Assumptions
• Establishment of Roles and Responsibilities
• Creation of Program Budget
• Organization of Steering Committee
• Participation on Steering Committee
• Organizational Announcement(s)

Key Auditing Considerations
• Is There An Enterprise-Wide Commitment to Risk Mitigation and Business Continuity Planning?
• Does the BCP Initiative Have Appropriate Visibility & Backing?
• Is the BCP Policy Effective?
• Are the Scope, Objectives, and Assumptions Appropriate?
Key Auditing Considerations continued

- Are the Methodology Standards Effective and Useful?
- Are Roles/Responsibilities Adequate and Appropriate?
- Is BCP Awareness Effectively Promoted?
- Is the BCP Repository (i.e., Software) Efficient and Useful?

Risk Assessment And Business Impact Analysis (BIA)

IA Involvement - Risk Assessment

- Identification of Risk Factors to be Examined
- Evaluation of Risk Factors
- Weighting of Risk Factors
- Analysis of Remediation Efforts
- Recommendation of Remediation Activities
IA Involvement - BIA
• Identification of Impacts to be Evaluated
• Identification of Core Business Functions and Primary Systems/Resources
• Creation of Rating Thresholds
• Evaluation of Disruption Impacts
• Assignment of RTO, RPOs, and Recovery Priorities

Key Auditing Considerations
• Were All Potential Risks Considered?
• What Were the Sources of the Collected Information?
• Were Risk Factors Accurately Evaluated?
  – Risk Prevalence
  – Anticipated Impact (Magnitude & Duration)
• Were Current and Potential Risk Mitigation Measures Accurately Evaluated?
  – Prevention
  – Preparation (Minimize Impact & Facilitate Recovery)

Key Auditing Considerations continued
• Were All Potential Impacts Examined?
  – Direct and Indirect
  – Tangible and Intangible
  – Inordinate Recovery Expenses
  – Recoverable Impacts
• What Information was Collected for Analysis?
• Were Impacts Accurately Identified?
• Are RTO/RPO/Recovery Priority Assignments Appropriate?
• Are the BIA Results Reflected in the BCP?
Recovery Strategies

IA Involvement - Recovery Strategies

• Definition of Recovery Strategy Requirements
• Identification/Evaluation/Selection of Potential Solutions
• Identification/Evaluation/Selection of Individual Recovery Strategies (Particular Productions, Vendors, etc.)
• Implementation Planning
• Testing and Monitoring

Key Auditing Considerations

• Based on the Results of the BIA, What Categories of Recovery Strategies Does the Organization Require?
• What Requirements are Associated with Each Strategy Category?
• What are the Relative Priorities of the Different Strategies?
• What Evaluation/Selection Methodology Was Used?
Key Auditing Considerations continued

- Were All Viable Options Considered?
- Were the Selected Strategies Fully Implemented?
- Do the Recovery Strategies Meet the Corresponding Objectives/Requirements?
- How are the Recovery Strategies Monitored and Evaluated?

Business Continuity Plan Development

IA Involvement - BCP Development

- Creation of BCP Organization Structure/Teams
- Definition of Activation Criteria and Escalation Processes
- Team/Departmental Plan Development
- Definition of Resource Requirements
- Manual Design/Organization
- Integration of BIA Results
Key Auditing Considerations

- Is the BCP Organization Structure Clear and Appropriate?
- Is the BCP Manual Organized in a Clear and Logical Manner?
- Are Key Recovery Processes Documented and Effective?
- Are Administrative Sections Appropriate?

Key Auditing Considerations continued

- Are Functional and Resource Resumption/Restoration Provisions in Compliance with Defined RTOs/RPOs?
- Are Task Lists Concise but Thorough, and Accurate?
- Are Resource Requirements Clearly Defined?
- Is Adequate Reference Information Readily Available?

Testing & Maintenance
IA Involvement - Testing & Maintenance

- Creation of Test Schedule
- Selection of Test Scope/Objectives/Participation/Scenario
- Observation/Evaluation of Test & Reporting of Test Results
- Creation of Maintenance Schedule
- Monitoring of Maintenance Activities
- Confirmation of Plan Distribution and Disposition
- BCP Program Status Reporting

Key Auditing Considerations

- Are Tests Thorough and Valid?
- Is Test Participation Appropriate?
- Were Test Objectives Accomplished?
- How Are Identified Deficiencies to be Addressed?
- When Will Deficiencies be Retested?
- What Additional Provisions Require Testing?

Key Auditing Considerations continued

- Is the Maintenance Schedule Adequate?
- Is the BCP Maintained According to the Schedule?
- Is the BCP Also Maintained Based on Triggering Events?
- Is the BCP Maintenance Comprehensive?
- How is Participation Facilitated and Monitored/Enforced?
- Are Appropriate Version Control and Distribution Processes Utilized?
Key Auditing Considerations continued

- Are Awareness and Education Efforts Appropriate and Effective?
- Is the BCP Program Appropriately Integrated with Complementary Initiatives?
- Who Monitors the Status of the BCP Program?
- How Are They Kept Informed of the BCP Program Status?
- What Are The Results of the BCP Program Monitoring/Reporting?

Conclusions/Wrap-up and Q&A

Final Thoughts

- The BCP Manual is Only One Component of an Overall Business Continuity Program
- To Evaluate an Organization’s Ability to Respond to, and Recover From, a Disaster, Internal Auditors Must Understand the Entire BCP Process and Examine All Components of the BCP Program
- BCPs Should be Subjectivity Evaluated Based on the Organization’s Own Recovery Planning Objectives
Q&A and Open Discussion

Thank You For Your Time and Participation

Troy Harris
Manager, Technology Risk Management Services
RSM McGladrey, Inc.
301-607-0248
troy.harris@rsmi.com