

EVALUATING YOUR BCP: BEYOND CHECKLISTS AND WALKTHROUGHS

Troy Harris, Senior Director
RSM US LLP

Business Continuity Planners Of The Carolinas

November 16, 2017

Agenda

- Introduction
- Program Initiation and Management
- Disaster Risk Assessment (DRA)
- Business Impact Analysis (BIA)
- Recovery Strategies
- Business Continuity Plan (BCP)
- Testing
- Conclusions/Wrap-up
- Question & Answer/Open Discussion

INTRODUCTION

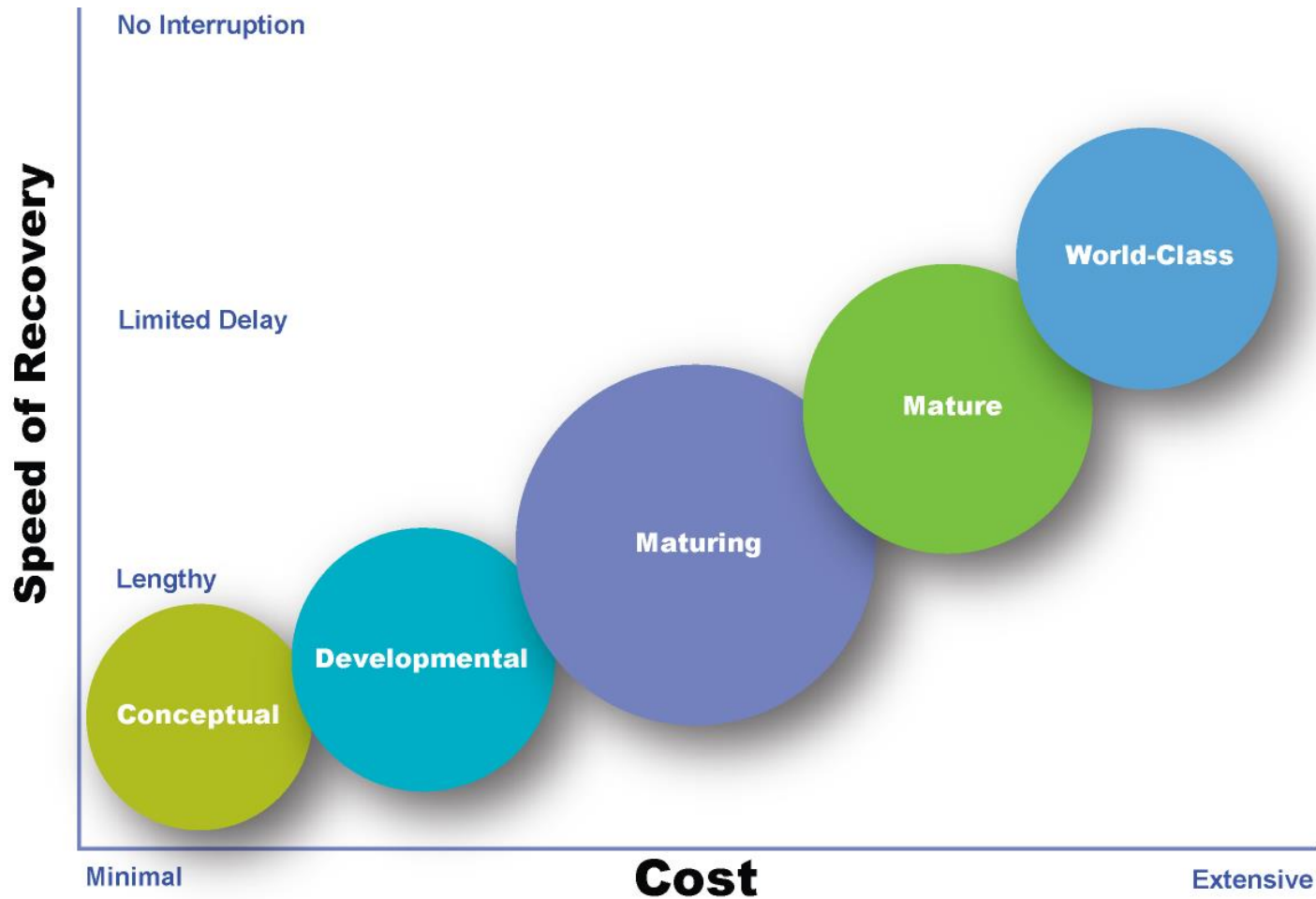
Traditional BCP Evaluation Methods

- BCP Assessments
 - Is the scope defined?
 - Are recovery time objectives (RTOs) identified?
 - Have Team Leaders been assigned?
- BCP Testing
 - Call List Tests
 - Departmental Walkthrough Exercises
 - Backup Tape Restorations

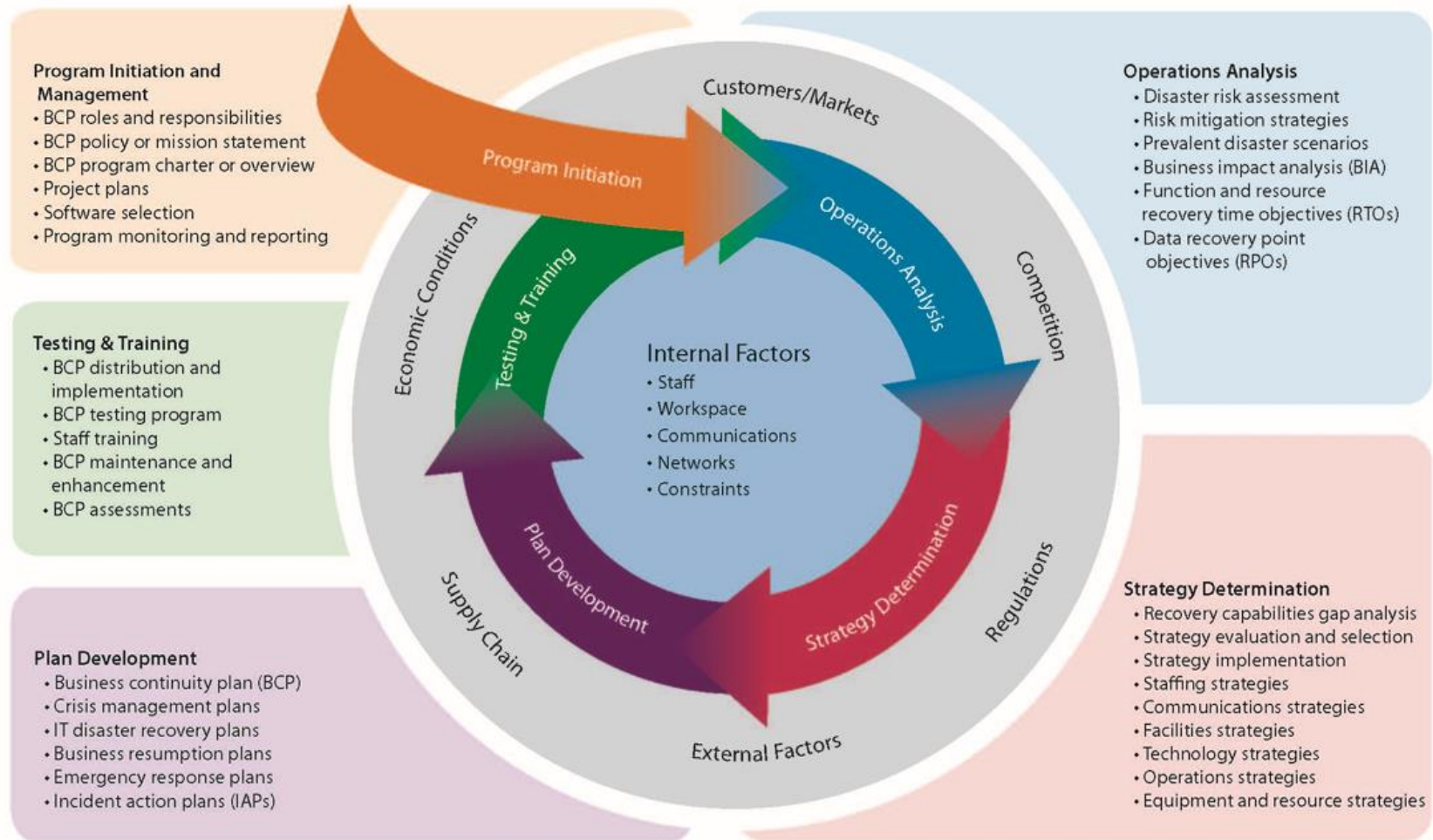
Enhanced BCP Evaluation Methods

- BCP Assessments
 - Qualitative Analysis
 - Involves a Combination of Reviews/Audits that Examine the Entire BCP Program and the Underlying Methodology, not Just the Documentation
 - “Connects the Dots”
- BCP Testing
 - Clear Objectives and Realistic Scenarios
 - Variations and Rotations
 - Thoroughly Planned, Executed, and Reported

Business Continuity Planning Maturity Model



RSM's Business Continuity Planning Methodology



PROGRAM INITIATION AND MANAGEMENT

BCP Policy/Charter

- Clear and definitive
- Appropriate for the organization
- Follows internal standards
- Appropriate scope and content
- Formally approved and adopted
- Disseminated and enforced
- Reviewed and updated

BCP Policy/Charter continued

- Scope, objectives, and assumptions
- Roles and responsibilities
- General approach/methodology
- Timeline and budget
- Testing and maintenance programs
- Training and awareness program
- Monitoring and reporting processes

BCP Definition (Sample)

- Documented and formal arrangements for resuming critical business operations in a timely manner following a disaster or other disruption
 - “Timely” may equal “Immediate”
 - Degraded operations may suffice temporarily
 - Focus is on sustaining the business
 - Business operations require essential resources
 - Recovery process must be efficient and organized

BCP vs. Broader Risk Management (Sample)

- Business Continuity Planning Elements:
 - Crisis Management Plans/Crisis Communication Plans
 - IT Disaster Recovery Plans
 - Business Resumption Plans
 - Pandemic Response Plans
- Other Risk Management Initiatives:
 - Emergency Response Plans
 - Incident Response Plans/Incident Action Plans
 - Information Security Programs
 - Physical Security Programs
 - Compliance Programs
 - Insurance Programs
 - Staff Succession Plans

BCP Roles and Responsibilities

- BCP Roles
 - Executive Sponsor
 - Steering Committee
 - Business Continuity Coordinator and/or Administrator(s)
 - Recovery Teams
 - Evaluators/Auditors
 - Liaisons

BCP Repository

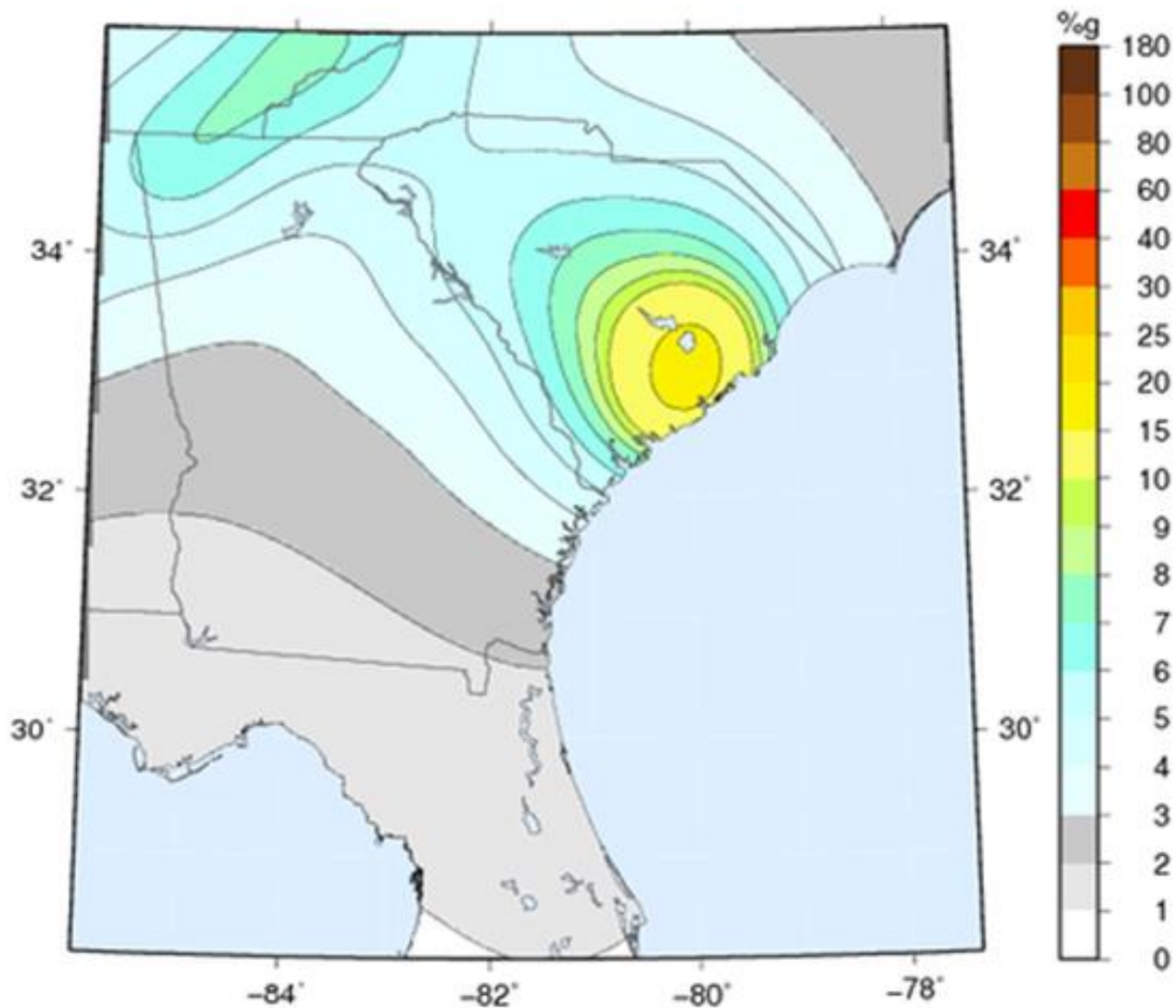
- Logical and intuitive organization
- Effective version control
- Data maintenance and external synchronization
- “Secure but accessible”
- Intuitive and usable (well-received)
- Efficient and proper use of features, templates, etc.

DISASTER RISK ASSESSMENT (DRA)

Risk Assessment Process

- Comprehensive library of risk factors
- Sources of risk data
 - Perceptions
 - Government and industry authorities
 - Historical experiences
 - Observation
 - Other research
- Mitigation considerations

Custom Hazard Map



Risk Assessment Process continued

- Rating Categories
 - Probability
 - Impacts (Staff, Facilities, Systems, Overall/Business, etc.)
- Rating Values and Thresholds/Definitions
 - High Staff Impact = 3
An incident would severely impact both on-site *and* off-site (i.e., regional) staff.
 - Medium Staff Impact = 2
An incident would severely impact only on-site *or* off-site staff.
- Calculation Algorithms
 - Probability x Impact = Inherent Risk
 - Inherent Risk x Mitigation Factor = Residual Risk

Risk Assessment Results

- Thorough and accurate
- Justified
- Current
- Realistic and logical
- Documented

Risk Mitigation Efforts

- Formal risk mitigation plans
 - Objectives and tasks
 - Responsibilities
 - Timelines
 - Correlated to risk assessment results
- Monitoring and reporting
- Current status/progress
- Reevaluation of both risks and mitigation

BUSINESS IMPACT ANALYSIS (BIA)

BIA Process

- Inventory of business functions
- Information sources
 - Surveys
 - Interviews
 - Research
 - Analysis
- Impact categories
 - Financial
 - Operational
 - Customer service
 - Legal and/or regulatory issues
 - Human Well-Being
 - Other
- Tangible vs. intangible impacts
- Direct vs. indirect impacts
- Rating criteria and thresholds

Business Impact Analysis— Recovery Time Objective (RTO)



BIA Results

- Final Conclusions
 - Recovery Priorities
 - RTOs
 - Recovery Point Objectives or RPOs
 - Other
- Other Considerations
 - Recovery Costs
 - Recoverable Impacts
 - Alternates/Workarounds (resources only)
- Steering Committee/Management Adjustments

RECOVERY STRATEGIES

Recovery Strategy Coverage

- Hardware, software, and data
 - Core systems
 - Midrange systems
 - Servers
 - Desktop systems
- Voice and data communication
 - Hardware
 - Software
 - Infrastructure
 - Services
- Third-party systems and interfaces

Recovery Strategy Coverage continued

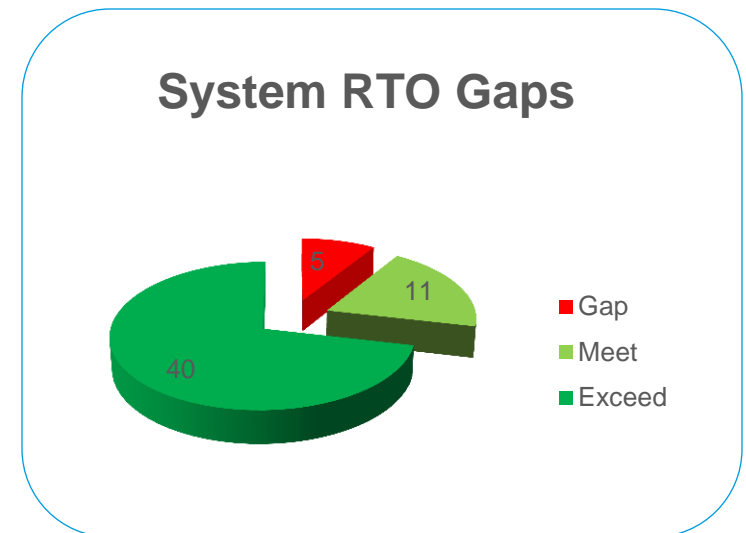
- Facilities
 - Data centers/server rooms/network closets
 - Public/retail locations
 - Office space
 - Specialized areas
 - Storage
 - Secure areas
- Operational workarounds and transfers
- Technical assistance and general staffing
- Crisis Management/Crisis Communication

Recovery Strategy Gap Analysis

- Mapping of BIA Requirements to Current/Planned Strategies
- Determination of Current/Planned Capabilities
 - Realistic/Valid Timelines
 - Timing From Initial Disruption
 - Foundation for Estimates
 - Interdependency Considerations
 - Predecessors
 - Restoration Capacity
- Formal Gap Analysis
- Identification of Enhancement Requirements

Recovery Strategy Gap Analysis continued

- Continuous monitoring for RTO and RPO compliance
- “Requirements” derived from reliable/current BIA and relevant mapping exercise
- “Capabilities” considers scaling, predecessors, dependencies, etc.
- Exceeding requirements is not necessarily ideal



Recovery Strategy Considerations

- Implementation costs
- Ongoing investment
- Disruption or inconvenience
- Scope and breadth
- Capacity
- Scenario flexibility
- Reliability
- Potential obsolescence
- Complementary vs. overlapping measures
- Other benefits and/or business drivers

BUSINESS CONTINUITY PLAN (BCP)

BCP Manual – Layout and Format

- Defined and consistent
- Intuitive and logical
- Facilitate (or even mimic) a recovery effort
- Supported by a detailed table of contents or even chapter summaries
- Described in a specialized section/chapter
- Segregates administrative and overview sections from actionable recovery plans
- Team-specific sections and plans

Key Recovery Processes

- Discovery and notification
- BCP activation
 - Broad disaster identification/detection options
 - Clear communication and escalation channels
 - Defined roles and alternates
 - Summary graphic and detailed narrative
 - Defined activation criteria
 - Correlation to other portions of the BCP

Key Recovery Processes continued

- Initial evaluation and escalation
- Damage assessment
- Internal and external communication
- Coordination with external parties
- Coordination with other internal processes
- Priority determination
- Strategy selection and allocation
- Overall recovery coordination
- Recovery process tracking and administration

Business Continuity Team Structure

- Categories of teams
 - Recovery coordination teams
 - Disaster recovery or support teams
 - Business recovery or departmental teams
- Reporting structure
- Roles and responsibilities
- Team rosters
- Authority levels and approval responsibilities
- Communication and coordination duties

Departmental Recovery Plan Standards

- Overview and responsibilities
- Departmental strategies
- Team assignments (including alternates)
- Business functions and priorities/RTOs
- Resource requirements
 - External requirements (schedule)
 - Internal requirements (including sources)
- Administrative/common recovery tasks
- **Custom recovery tasks**
- Reference materials (contact lists, SOPs, etc.)
- Other: interdependencies, vital records, etc.

Custom Recovery Tasks

- Unique content for each team
- Integrate with, but do not replace, Common Recovery Tasks
- Highlight variations from normal procedures
- Supported by SOPs
- Follow a consistent structure of key steps or phases:
 - Essential Activities
 - Temporary Operating Procedures (TOPs)
 - Restoration Activities
 - Resumption Activities
 - Migration Activities

Technical Recovery Plan Standards

- Logically grouped systems and resources
 - Similar platforms, recovery strategies, skill requirements, etc.
- Resources identified with defined sources
 - Hardware, software/utilities, data, telecommunications, etc.
- Defined restoration/failover steps
 - Installation, configuration, restoration, validation, support, coordination, etc.
 - Decision points, interdependencies, references to SOPs, etc.
- Key reference information
 - Production and DR environmental diagrams, look-up tables, configuration standards, vendor manuals, etc.

TESTING

Traditional BCP Tests – Characteristics

- Basic testing activities
 - Call list tests
 - Departmental walkthrough exercises
 - Backup tape restorations (“Hotsite tests”)
- Predictable arrangements
 - Defined schedule (typically annual)
 - Similar or identical objectives and scenarios
 - Consistent scope and assumptions
 - Standard list of participants

Traditional BCP Tests – Major Shortcomings

- Do not consider unpredictable nature of disasters
 - Timing
 - Impact
 - Knowledge
- Validate only certain processes, strategies, roles, interdependencies, volumes, etc.
- Testing in a vacuum

Traditional BCP Tests – Other Shortcomings

- Limited incremental training
 - Simulation of circumstances
 - Simulation of roles
- Fatigue
 - Participants
 - Evaluators
- Boring

Basic Test Schedule

- Rolling 24-month calendar
- Specific vs. approximate information
 - Timing
 - Test type
 - Participants
- Approval and commitment
- Maintained and adjusted

Enhanced Test Schedule

- Test scope and objectives to be achieved
- BCP objectives to be exercised
- Disaster scenario to be simulated
 - Type
 - Timing
 - Impact
- Participant roles
- Constraints or other variables

Testing Methodology

- Avoids repetition (scope, scenario, etc.)
- Considers realistic and unpredictable disaster circumstances
- Elevates complexity and expands scope over time
- Evaluates and documents/reports all tests and any actual activations
- Considers all tests collectively to determine BCP status and identify additional testing requirements
- Valid preparations and realistic assumptions

- Test Scope
 - Key recovery processes
 - Business functions
 - Systems and other resources
 - External dependencies
 - Participants
 - Locations
- Participants and Participation
 - Appropriate roles and levels
 - Variations
 - Engaged and knowledgeable

Disaster Scenario

- Correlated to BCP objectives and test objectives
- Realistic characteristics and circumstances
- Defined based on disaster risk assessment and relevant research
- Integrates unfolding circumstances
- Varies type, timing, impact, duration, constraints, etc.
- Clearly described/illustrated for test participants

Test Results and Actions

- Test evaluation
 - Pre-defined objectives
 - Feedback from participants, evaluators, etc.
 - Adherence to test plan
 - Adherence to BCP
- Test reporting
- Enhancement/remediation plan
 - Correlated to test results
 - Designated responsibilities
 - Defined timelines
- Monitoring and follow-up testing

CONCLUSIONS/ WRAP-UP

Key Elements of an *Effective* BCP Program

- Solid organizational commitment
- Effective risk management
- Thorough BIA
- Viable recovery strategies
- Documented recovery plan
- Effective plan deployment
- Plan testing and maintenance

Key Elements of an *Efficient* BCP Program

- Established goals and objectives
- Clear roles and responsibilities
- Defined standards, methodologies, and techniques
- Ongoing and regular collaboration
- Proficient resource utilization
- Useful and productive tools
- Formal reporting and monitoring
- Regular evaluation and constructive feedback
- Continuous refinement

Final Thoughts – BCP Assessments

- The BCP manual is only one component of an overall business continuity planning program
- To evaluate an organization's ability to respond to, and recover from, a disaster, you must understand the entire BCP process and examine all components of the BCP program
- Evaluating a BCP requires a level of subjectivity that cannot be obtained from checklists

Final Thoughts – BCP Testing


- Like disasters themselves, BCP tests should come in all shapes and sizes
- We know that untested BCPs are unreliable, and the same goes for untested BCP *components*
- To truly validate a BCP, you must test it against a collection of realistic conditions and parameters

QUESTIONS AND ANSWERS?

Thank You for Your Time

- Troy Harris
 - Senior Director, Business Continuity Planning
 - 704.844.2709
 - troy.harris@rsmus.com





This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. *The power of being understood®* is a registered trademark of RSM US LLP.

© 2017 RSM US LLP. All Rights Reserved.