

EVALUATING YOUR BCP: BEYOND CHECKLISTS AND WALKTHROUGHS

Troy Harris, Senior Director
RSM US LLP



Houston IA
8th Annual Conference
April 3, 2017 • NRG Center



Agenda

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

BUSINESS CONTINUITY PLANNING OVERVIEW

Business Continuity Plan (BCP) – Definition

- 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

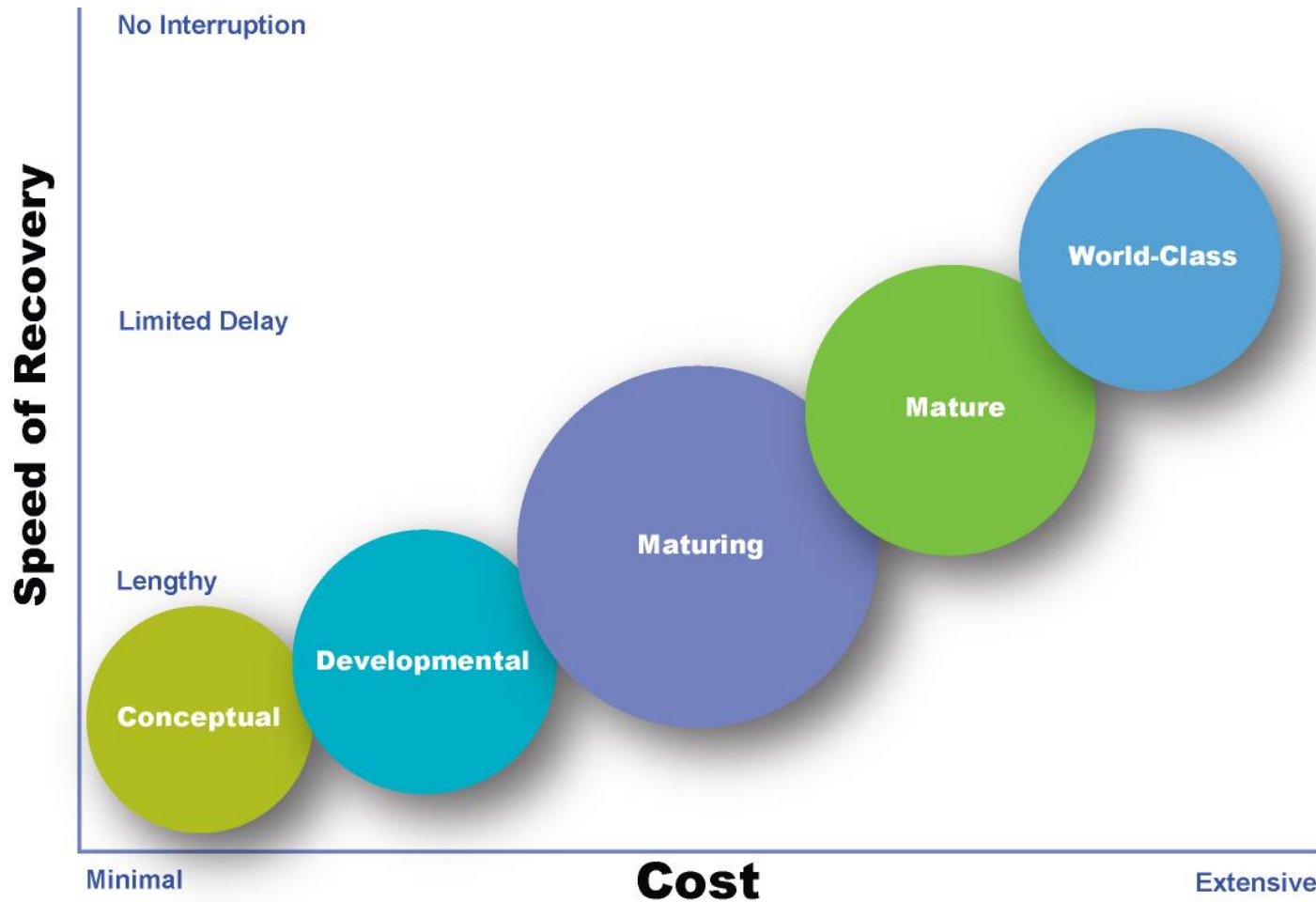
BCP vs. Broader Risk Management

- 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

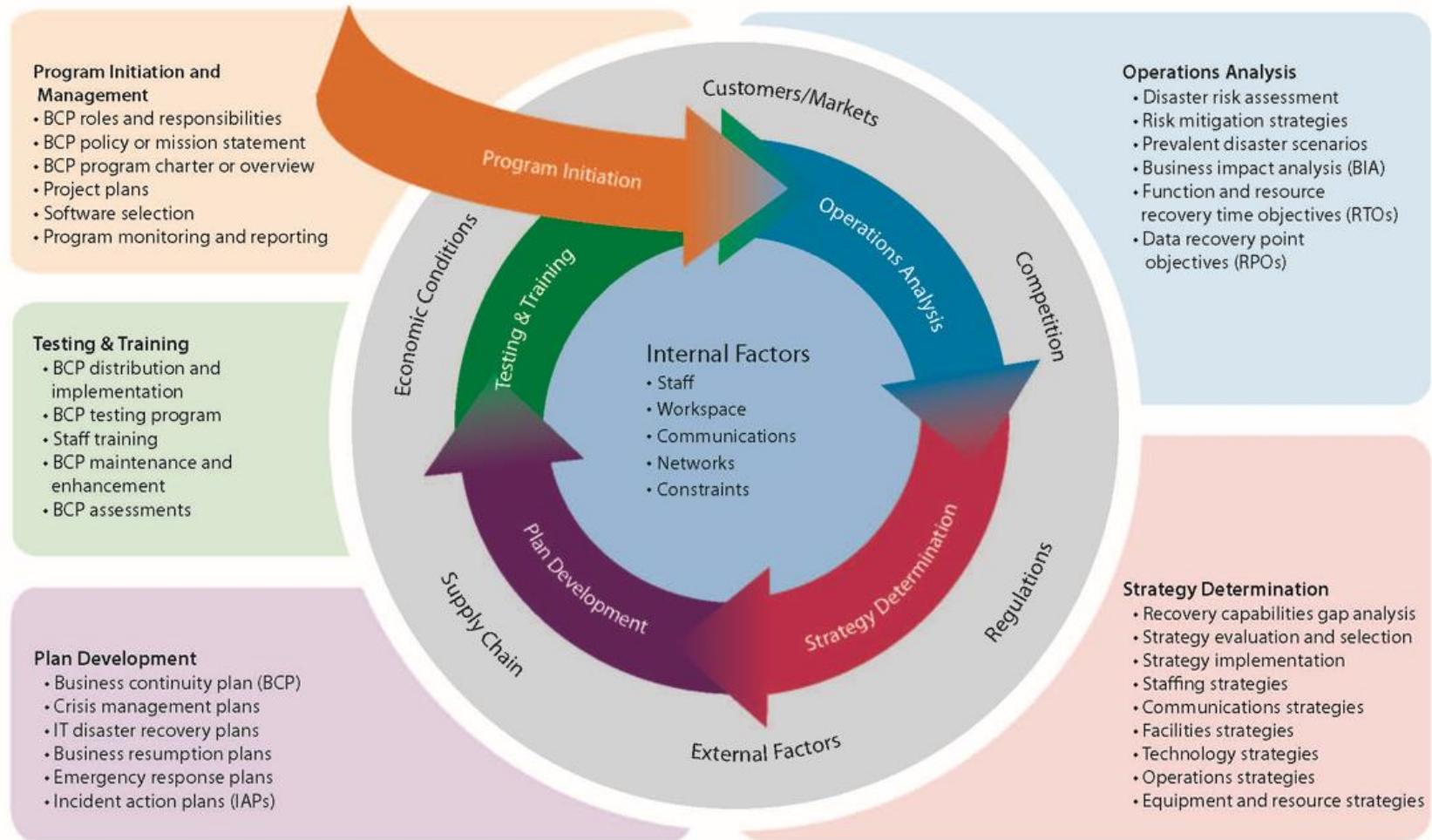
Lessons From Past Disasters

- The event may impact multiple sites simultaneously.
- Communications may suffer extended outages.
- Full staffing may not be available for the recovery.
- Hotsite demand may exceed available capacity.
- Work in process and vital records may be destroyed.
- Essential transportation may not be available.
- Supply chains may break down.
- Untested provisions are unreliable.

Business Continuity Planning Maturity Model



RSM's Business Continuity Planning Methodology



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 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

PROGRAM INITIATION AND MANAGEMENT

The BCP Policy and Related Materials

- The business continuity planning policy
 - Clear and definitive
 - Appropriate for this organization
 - Follows policy standards
 - Appropriate scope and content
 - Formally approved and adopted
 - Disseminated and enforced
 - Reviewed and updated
 - Supported by a program charter and other materials

The BCP Policy and Related Materials continued

- Program charter
 - 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

The BCP Policy and Related Materials continued

- Effective BCP standards and guidelines
 - Recovery Plan templates
 - Centralized/common information
 - Glossary of terms
 - User guides and training
- Complementary standards and guidelines
 - Standard operating procedures (SOPs)
 - Job descriptions
 - Project management standards
 - Risk monitoring and reporting
 - IT disciplines
 - Physical security, incident response, etc.

BCP Roles and Responsibilities

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

BCP Roles and Responsibilities continued

- Appropriate assignments
 - Roles (functions, authority, etc.)
 - Skill-set (experience, training, etc.)
 - Workload/capacity
- Established and monitored expectations
 - Job descriptions
 - Performance objectives and incentives
 - Performance evaluations
 - Awards and recognition

The BCP Culture

- True Management/Executive Support
- Desirable Involvement
- Effective and Broad “Initiative Introduction” & Awareness
- Collaborative Effort vs. Isolated Responsibilities
- Best Practices vs. Regulatory Compliance
- Benefits vs. Challenges
- Professional Development
- Early “Wins” vs. Long-Term Goals
- *Positioned to Succeed*

The BCP Repository

- From collections of disconnected files to highly specialized packages
 - Logical and intuitive organization
 - Effective version control
 - Data maintenance and external synchronization
 - “Secure but accessible”
 - Intuitive and usable (well-received)
 - Proper use of features, templates, etc.

Assessing Your BCP Software Package

- Tool for developing, maintaining and storing your plan(s)
- Supports planning from the BIA stage through testing and even plan activation
- Databases to support data collection and maintenance
- Specialized user interfaces to increase productivity
- Dynamic reporting of information in “manuals”
- Effective security features
- Integration of external documents and data imports
- Interfaces to other systems

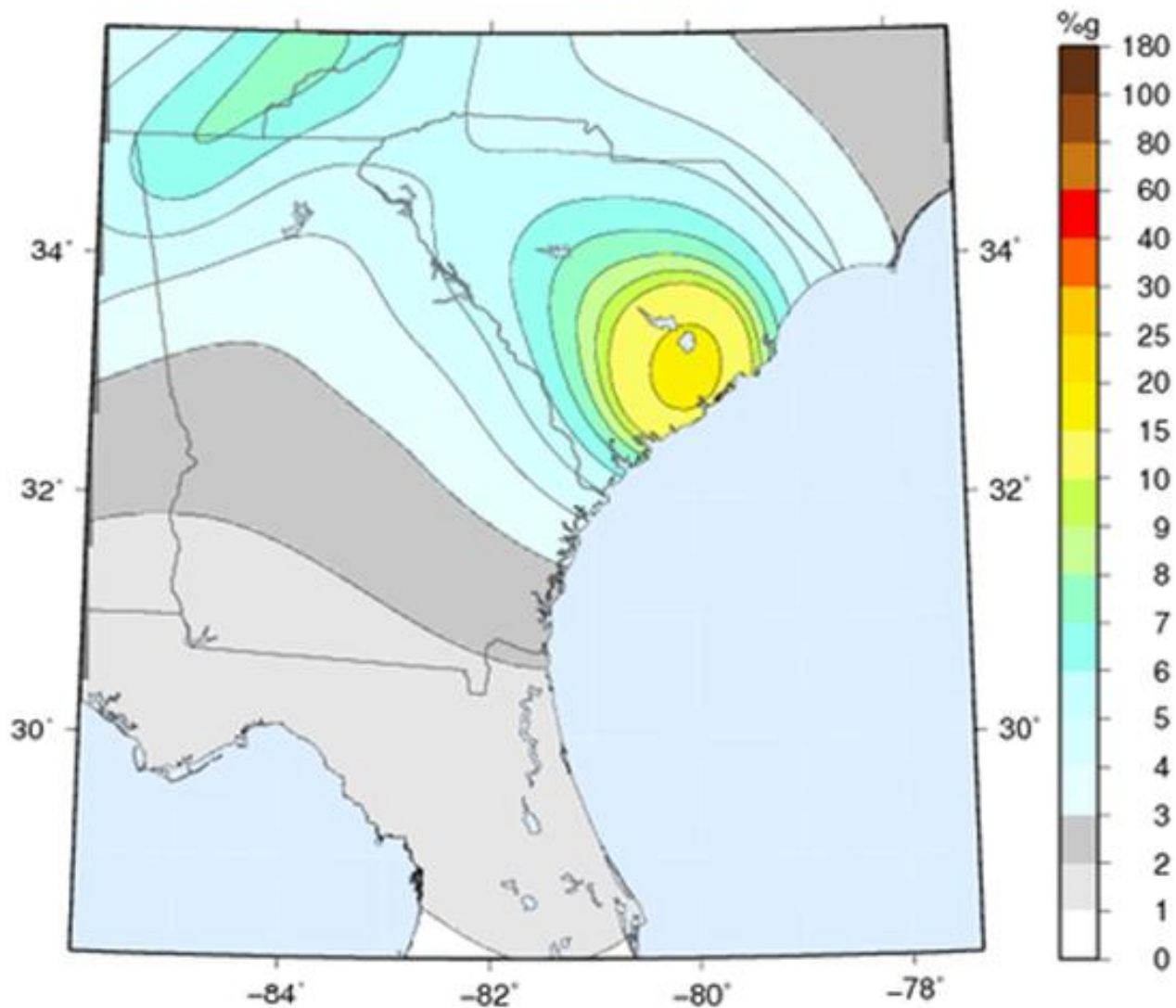
Effectively facilitates, but does not replace, the plan development, maintenance and testing processes.

DISASTER RISK ASSESSMENT AND BUSINESS IMPACT ANALYSIS (BIA)

Validating the 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



Peak Ground Acceleration

Validating the Risk Assessment Process continued

- Rating Categories
 - Probability
 - Impacts (Staff, Facilities, Systems, Overall/Business, etc.)
- Rating Values and Thresholds
 - 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

Threat Factor	Probability (High, Medium, Low, or None)	Impact Ratings (High, Medium, Low, or None)				Risk Rating (>=60: High risk 41-60: Moderate risk; 21-40: Low risk; 0-20: None or Minimal risk)	Current Mitigation / Preparedness (High, Medium, or Low)	Residual Risk Rating (>=60: High concern 41-60: Moderate concern; 21-40: Low concern; 0-20: None or Minimal concern)	Threat Rank
		Staff	Facilities	Systems	Overall / Business				
Natural Threats									
Wind	H	L	L	M	M	90	M	54	2
Ice	H	L	L	M	M	90	M	54	2
Tornado	L	M	H	L	L	35	L	28	10
Hurricane	L	M	M	L	L	30	L	24	11
Internal Fire	L	M	H	M	M	45	H	18	21
Internal Flooding	L	N	L	M	L	20	L	16	24
External Flooding	L	N	L	L	L	15	L	12	27
Large Snowfall	M	M	N	N	L	30	H	12	27
Heat	L	L	N	N	N	5	L	4	37
Earthquake	N	M	M	M	L	0	L	0	44
Human Threats									
Vendor / Supplier Disruption	H	N	N	M	H	75	L	60	1
Terrorism	M	H	L	N	L	50	M	30	5
Internal Sabotage	M	N	N	M	H	50	M	30	5
Data Theft: Internal	M	N	N	M	H	50	M	30	5
Unauthorized Modification of Internal Software or Hardware	M	N	N	M	H	50	M	30	5
Malicious Damage or Destruction of Software or Data	M	N	N	M	H	50	M	30	5
Explosion (Gas, Steam, etc.)	L	M	M	L	L	30	L	24	11
Improper Handling of Sensitive Data	H	N	N	N	M	30	L	24	11
Hazardous Materials/Chemical Spill	L	M	M	L	L	30	L	24	11
Building/Structure Failure	L	L	H	M	M	40	M	24	11
External Sabotage	M	N	N	M	H	50	H	20	18
Data Theft: External	M	N	N	M	H	50	H	20	18
Burglary	M	N	L	H	L	50	H	20	18
Nuclear Incident	L	M	L	N	L	20	L	16	24
Unavailability of Key Employee(s)	M	N	N	N	M	20	M	12	27
Unauthorized Modification of End Product	M	N	N	N	M	20	M	12	27
Data Entry Error	H	N	N	N	M	30	H	12	27
Water Contamination	L	M	N	N	L	15	M	9	32
Pandemic	L	M	N	N	L	15	M	9	32
Biological Incident (Anthrax, etc.)	L	M	N	N	L	15	M	9	32
Work Stoppage	L	L	N	N	L	10	M	6	36
Workplace Violence	L	M	N	N	N	10	H	4	37
Embezzlement	L	N	N	N	M	10	H	4	37
Extortion	L	N	N	N	L	5	L	4	37
Civil Unrest/Riot	L	L	N	N	N	5	M	3	42
Vandalism	L	N	L	N	N	5	M	3	42
Technical Threats									
Power Failure or Fluctuation	H	L	L	M	M	90	M	54	2
Communications (Voice or Data) Failure	M	N	N	M	M	40	M	24	11
UPS or Battery Failure	M	N	N	M	M	40	M	24	11

Validating the Risk Assessment Results

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

Evaluating the 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

Validating the 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)



Validating the 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

BIA Summary Matrix Grouped by Department

Department: Deposit Operations - Transaction Services

		----- Impact Ratings -----						
Function Name:	Function Description:	RTO (Days)		Customer Service:	Operations:	Financial:	Legal/ Regulatory:	Human Well-Being:
ATM and Debit Card Account Reconciliation	Balancing of ATM and Debit Card transactions	2/3	1 Day:	Medium	High	Low	Low	Low
			2-3 Days:	High	High	Medium	Medium	Low
			4-7 Days:	High	High	High	Medium	Medium
			8-14 Days:	High	High	High	High	Medium
			14+ Days:	High	High	High	High	Medium

Supporting Resources:

<u>Resource Name:</u>	<u>Resource RTO (Days):</u>
Item Processing System	2/3
ATM Service	2/3
Internet	2/3
Core System	2/3
Debit Card Service	1
File Server	2
Imaging System	4

Narrative Basis:

Balancing procedures aid in identifying issues, double postings, etc. An extended delay in resuming this function could lead to a substantial backlog, incorrect or outdated financial data, undetected errors, etc. Due to both the volume and value of these transactions, it would be imperative for the Bank to restore this function in less than one day following a disaster

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

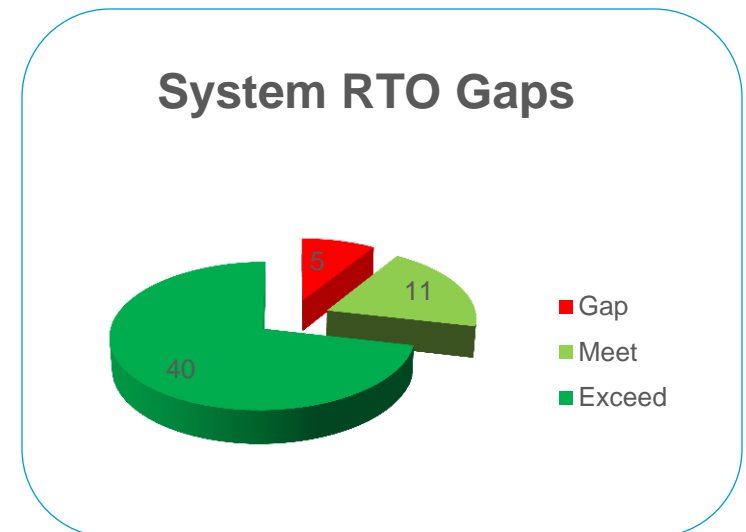
- Facilities
 - Data centers/server rooms/network closets
 - Retail locations
 - Office space
 - Specialized areas
 - Storage
 - Vaults and secure areas
- Operational workarounds and transfers
- Technical assistance and general staffing
- Crisis Management/Crisis Communication

Evaluating the Recovery Strategy Gap Analysis

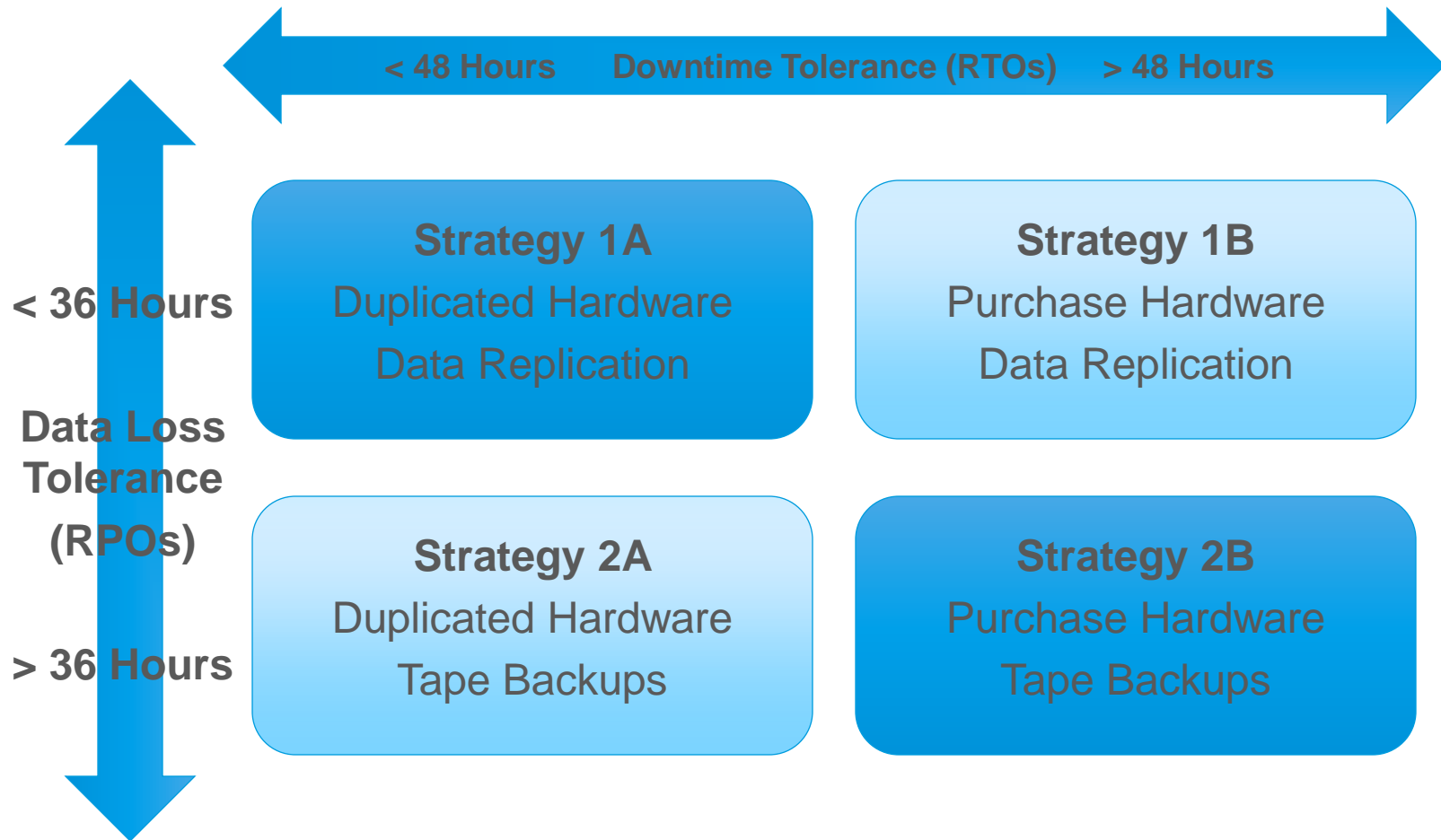
- Mapping of BIA Requirements to Current/Planned Strategies
- Determination of Current/Planned Capabilities
 - Realistic/Valid Timelines
 - Timing From Initial Disruption
 - Foundation for Estimates
 - Interdependency Considerations
 - Predecessors
 - Restoration Capacity
- Formal Gap Analysis
- Identification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

Evaluating the 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



Tailored Strategies to Align with Requirements



Evaluating the Recovery Strategies

- 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

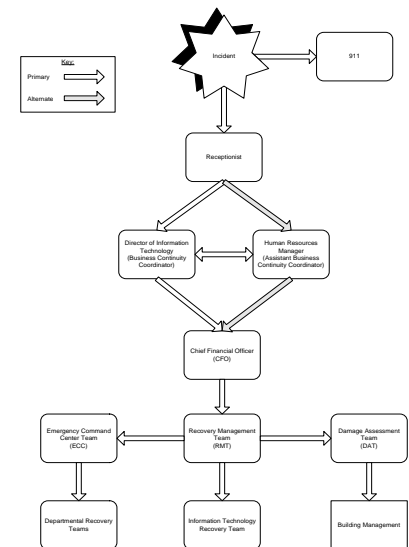
BUSINESS CONTINUITY PLAN (BCP)

The Layout and Format of the BCP Manual

- Defined and consistent
- Intuitive and logical
- Should 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
 - 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
- BCP activation



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

The 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
- External resource requirements (schedule)
- Internal resources requirements (including off-site storage inventory)
- 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

- Overview and scope
- Team assignments (including alternates)
- Recovery priorities and RTOs
- Recovery strategy or strategies
- Resource requirements (including quantity, source, etc.)
- Technical restoration tasks
- Interdependencies and other considerations
- Reference materials (contact lists, diagrams, inventories, addresses and settings, administration and support procedures, etc.)

Technical Recovery Plan Standards continued

- 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.

Plan Distribution Processes

- Control procedures
 - Who gets copies of the Plan?
 - Which portions of the Plan do they receive?
- Distribution register
 - Who currently has copies of the Plan?
 - Where are the copies stored?
 - Electronic vs. paper copies
- Acknowledgments of receipt
- Employee turnover
 - Plan retrieval and reassignment
- Plan revisions
 - Version control
 - Review/approval

TESTING

Traditional BCP Tests – Common 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

Test Types

- Checklist and call tree tests
- Departmental and integrated walkthroughs
- Alternate site simulation
- Operational simulation
- Capacity validation (“load testing”)
- Disaster recovery simulation
- Vendor activations
- Recovery coordination simulation

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

Validating the Testing Methodology and Effectiveness

- 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

Validating the Testing Methodology and Effectiveness

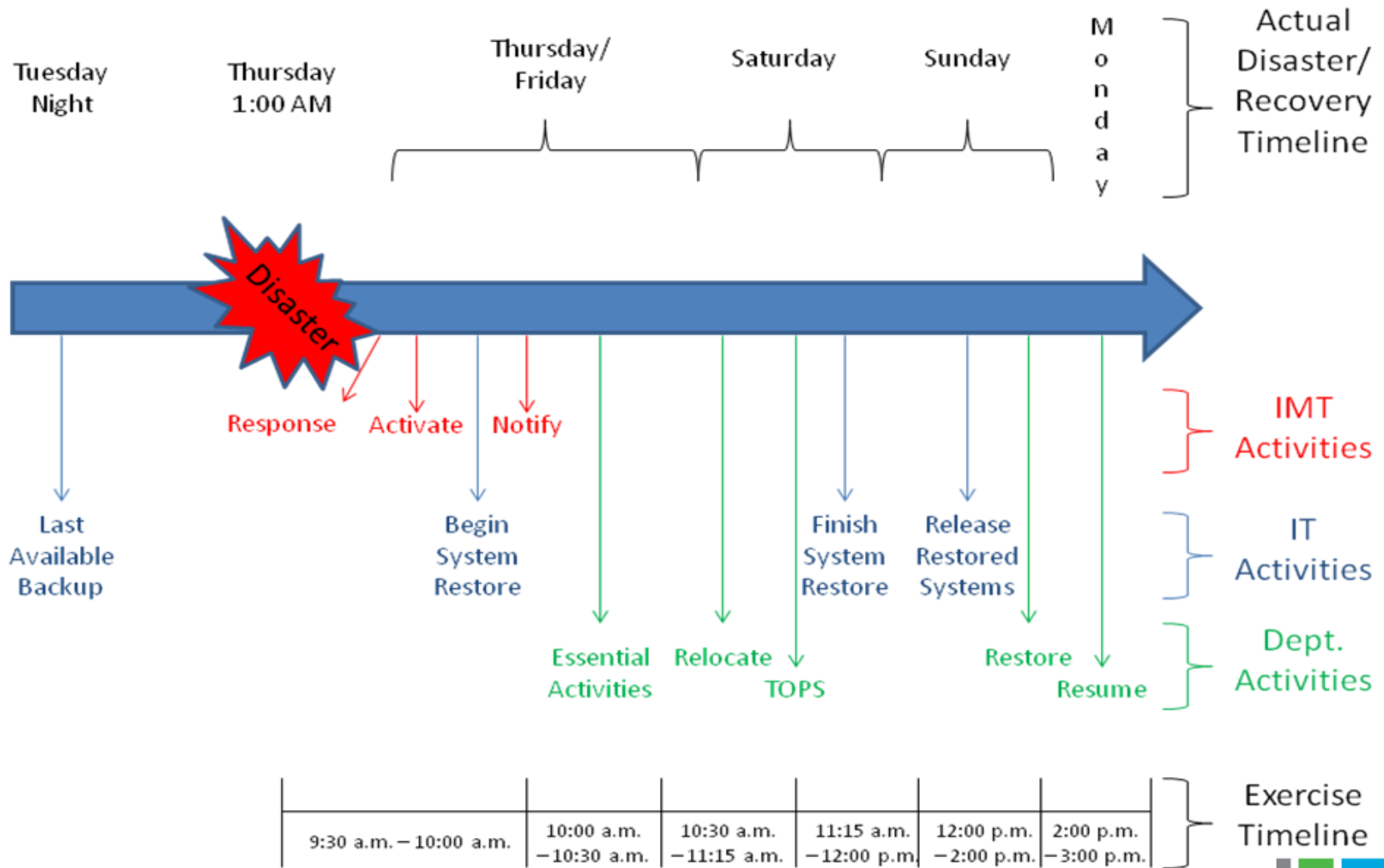
continued

- 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.

Disaster Scenario – Timeline



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
 - Management visibly endorses the risk mitigation and recovery planning initiative.
- Effective risk management
 - Disaster risks are identified and sound mitigation measures have been implemented.
- Thorough BIA
 - Disruption impacts are evaluated and recovery requirements and priorities are determined.

Key Elements of an Effective BCP Program

- Viable recovery strategies
 - Techniques for achieving critical recovery objectives are defined.
- Documented recovery plan
 - Recovery processes are defined, responsibilities assigned and reference information is documented.
- Effective plan deployment
 - The BCP is distributed to appropriate individuals.
 - Staff are trained on their roles and responsibilities.
 - Strategies are fully implemented and verified.

Key Elements of an Effective BCP Program

- Plan testing and maintenance
 - Realistic exercises are conducted to confirm plan accuracy, prepare participants to respond and identify enhancement opportunities.
 - The BCP and supporting provisions are updated on a defined schedule and whenever the organization, operation and/or environment changes.
 - BCP updates are distributed and obsolete materials are collected.
 - Participants remain knowledgeable of their role and the overall recovery process.

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 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.