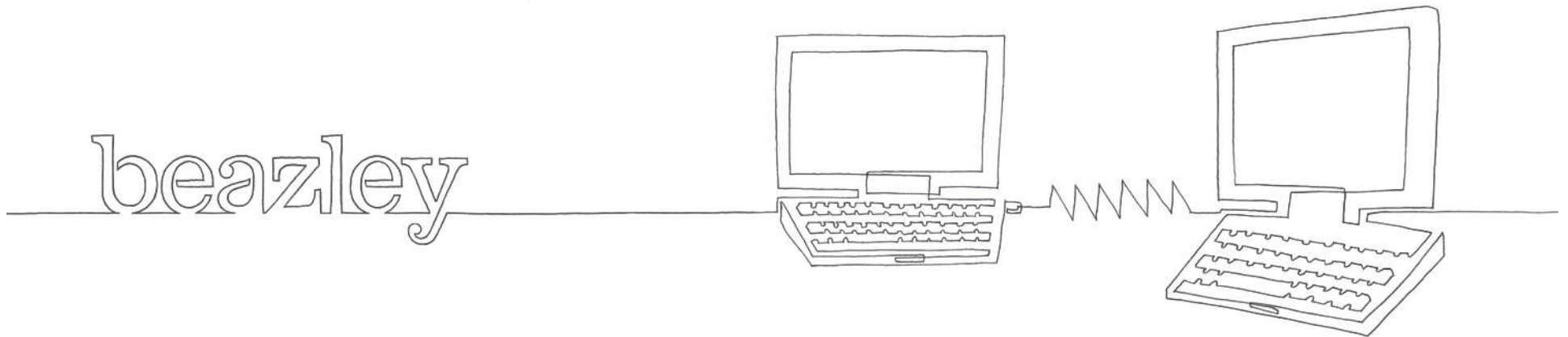


Business Continuity Planning For Small Business

March 12, 2020



Beazley Breach Response (BBR) Services workshop program

- Basics of Business Continuity Planning
- Eligibility for other workshops
- To learn more
 - Visit the **Workshops** page by clicking on Services on *beazleybreachsolutions.com*
 - Email *bbrservices@beazley.com*

BUSINESS CONTINUITY PLANNING FOR SMALL BUSINESS



March 12, 2020

Today's Presenter



Troy Harris

Senior Director, Risk Consulting

- 16 years in RSM's national Business Continuity Planning consulting practice
- Over 20 years of BCP experience
 - Experienced in both information technology (IT) disaster recovery planning and operations/business resumption planning
 - Served as both an internal recovery coordinator and an external BCP consultant
 - Experienced working with a wide variety of industries in both the public and private sectors
- Certified Business Continuity Professional (CBCP)
- Regular presenter at both local and national seminars and conferences

Agenda

- Business Continuity Planning Overview
- RSM's 5-Phase BCP Methodology
 - Program Initiation
 - Requirements Definition
 - Strategy Determination
 - Implementation and Documentation
 - Program Management and Testing
- Pandemic Planning
- Question & Answer
- Conclusions/Wrap-up

BUSINESS CONTINUITY PLANNING OVERVIEW

Business Continuity Plan (BCP) Definition

- Documented and formal arrangements for resuming critical 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 organization
 - Operations require essential resources, including technical systems
 - Recovery process must be efficient and organized

BCP vs. Broader Risk Management*

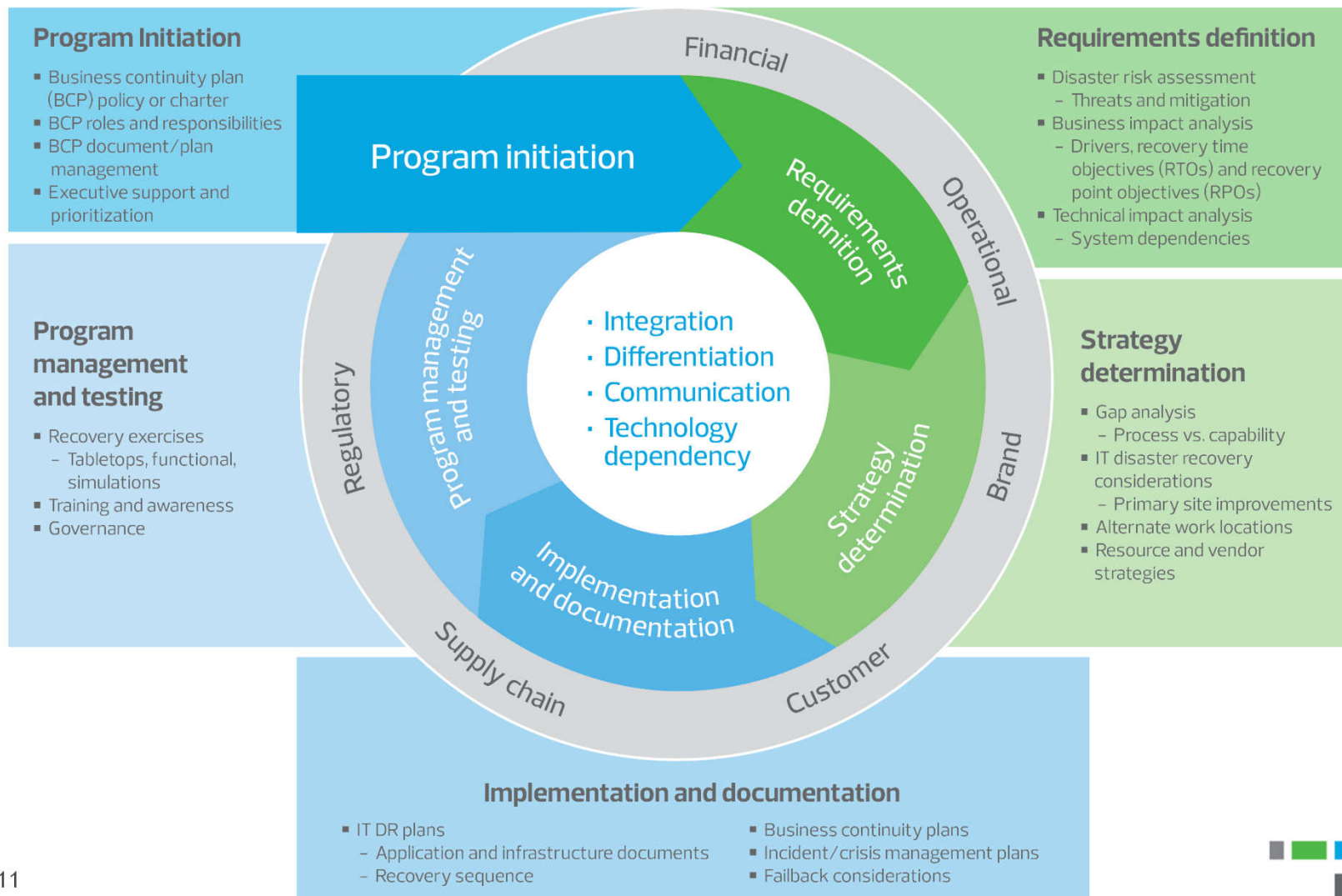
- Business Continuity Planning Elements:
 - Crisis Management Plans/Crisis Communication Plans
 - IT Disaster Recovery Plans
 - Business Resumption Plans
 - Pandemic Response Plans
- Other Risk Management Initiatives:
 - Emergency Response Plans
 - Incident Response Plans/Incident Action Plans
 - Information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

Basic BCP Concepts

- Functions and systems must be inventoried and prioritized for recovery
- BCPs should primarily address your aggregate risks and scenarios
- Recovery processes should leverage pre-established strategies for key requirements
- The organization's BCP is a collection of multiple "recovery playbooks"
 - Individual teams (departments) have their own "recovery playbooks" for reference following a disaster
 - Designated teams for recovery coordination, IT restoration, etc.

RSM'S 5-PHASE BCP METHODOLOGY

RSM's Business Continuity Planning Methodology



Ongoing BCP Program

- Should encompass all facets of the BCP Program, including:
 - BCP Policy and Program Charter
 - Business Impact Analysis (BIA)
 - Disaster Risk Assessment (DRA)
 - Recovery strategies
 - BCP
 - Testing Schedule and Procedures
 - Training Schedule and Procedures

Ongoing BCP Program continued

- Activities should be performed according to an established schedule and in response to designated “triggering” events:
 - Log activities and report progress to Steering Committee, etc.
 - Respond to organizational changes, test results, audits, etc.
 - Adjust schedule and/or procedures as necessary/appropriate
- Key ongoing (scheduled) activities:
 - Exercises/Tests/Drills
 - Staff Training
 - Maintenance
 - Enhancement
 - Reviews/Audits

RSM'S 5-PHASE BCP METHODOLOGY

Phase I: Program Initiation

Phase I – Summary

- Define project schedule and project management protocols
- Formalize/confirm BCP roles
- Publish BCP policy and charter
- Establish BCP documentation repository
- Conduct kick-off call(s)/meeting(s)

BCP Roles

- Executive Sponsor
- Steering Committee
- Business Continuity Coordinator and/or Administrator(s)
- Recovery Teams
 - Team Leaders
 - Alternate Team Leaders
 - Team Members (and Alternates)
- Evaluators/Auditors
- Liaisons

RSM'S 5-PHASE BCP METHODOLOGY

Phase II: Requirements Definition

Phase II – Summary

- Disaster Risk Assessment (DRA)
 - Analyze prevalent disaster threats to determine the associated risk
 - Evaluate mitigation of your greatest risks
 - Identify supplemental risk mitigation measures
 - Define likely disaster scenarios and a worst-case situation
- Business Impact Analysis (BIA)
 - Inventory your current business functions
 - Analyze anticipated disruption impacts
 - Correlate business functions to system/resource requirements
 - Establish recovery priorities and thresholds (RTOs and RPOs)

Disaster Risk Assessment (DRA) Process

- Assemble a comprehensive library of risk factors
- Collect and analyze data from multiple sources
 - Perceptions
 - Government and industry authorities
 - Historical experiences
 - Observation
 - Other research
- Assign ratings for Probability and appropriate Impact categories
- Calculate inherent risk
- Appropriately integrate mitigation considerations
- Document conclusions *and* rationale

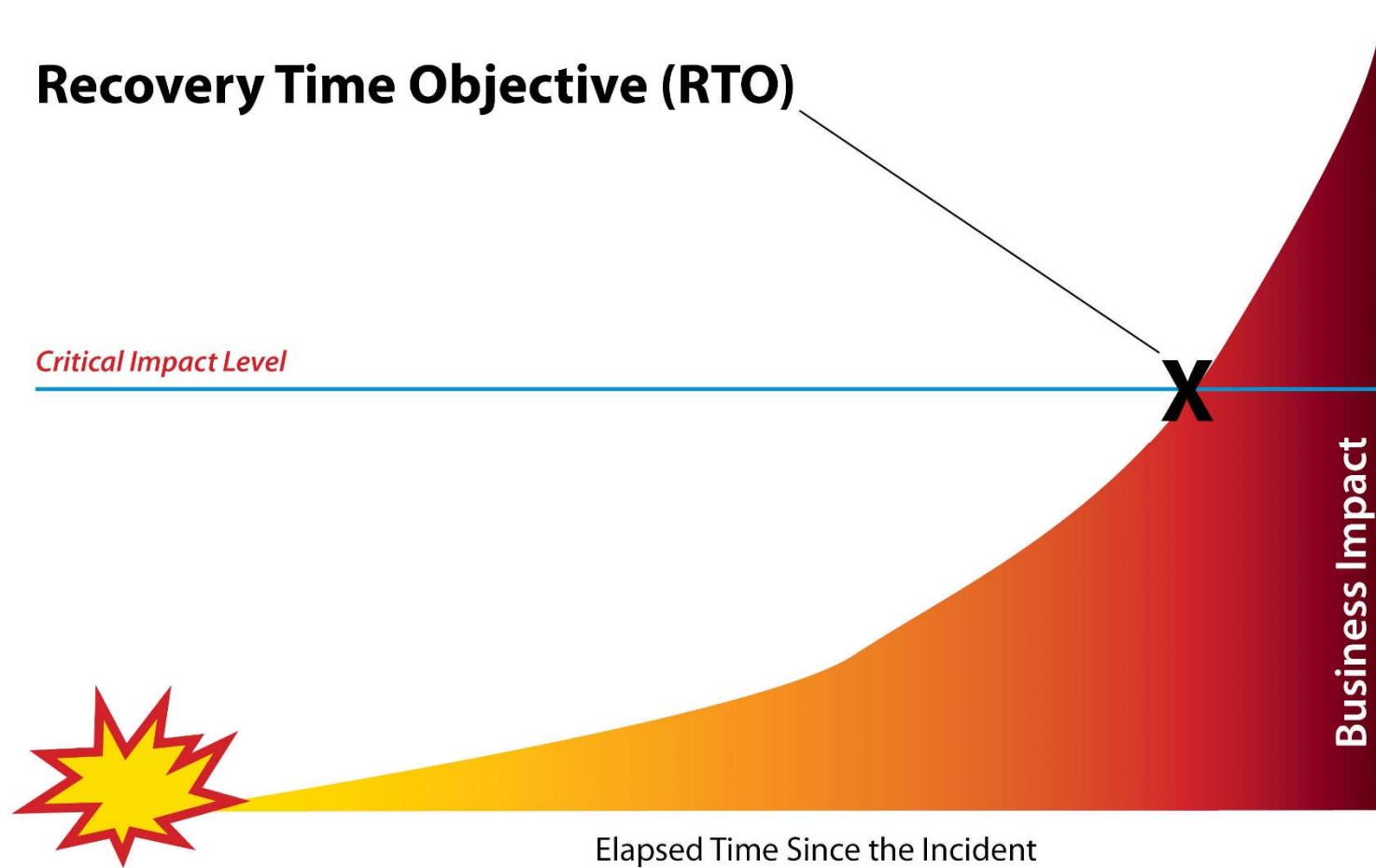
DRA Sample

Threat Factor	Probability (High, Medium, Low, or None)	Speed of Onset R = Rapid G = Gradual	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, Low, or None)	Residual Risk Rating (>60: High concern 41-60: Moderate concern; 21-40: Low concern; 0-20: None or Minimal concern)	Threat Rank	Comments
			Staff	Facilities	Systems	Overall / Business					
Human and Proximity Threats											
Transportation Accident (Aircraft, Train, Motor Vehicle, etc.)	L	R	L	M	L	M	30	M	18	31	<p>Risk Factors: The headquarters is located at a major intersection and surrounded by heavy vehicle traffic; However, this does not pose a serious threat of severe physical damage (excluding spills), as traffic speeds are slow. Very few flight paths within the region and the closest railway is over 3 miles from the site.</p> <p>Mitigating Factors: Some staff have the ability to temporarily work from other sites or home in the event of such incidents.</p> <p>Reference: https://skyvector.com/</p>

BIA Process

- Establish the BIA “framework”
 - Impact categories
 - Impact rating criteria and thresholds
- Assemble a comprehensive inventory of business functions
- Assess each function using the established framework
- Determine acceptable outage tolerance, or Recovery Time Objective (RTO)
- Identify and evaluate technical requirements, including both RTO and Recovery Point Objective (RPO)

Business Impact Analysis (BIA)



BIA Sample

Business Function (Name/Description)	Functional RTO (Days)	Disruption Duration	Impact Ratings					System Dependencies		Comments/Rationale
			Customer Service (H/M/L)	Operations (H/M/L)	Financial (H/M/L)	Legal/ Regulatory (H/M/L)	Human Well-Being (H/M/L)	System Requirements	System RTO (Days)	
Accounts Payable Managing payments made to vendors for products and services rendered to the Company.	14	1 Day or Less	L	L	L	L	L	G/L System	21	The Company stays current with outstanding payments and vendors would likely provide extensions as needed. However, after 2 weeks, the Company would be at risk of losing access to critical products and services. Manual (check) payments could be made temporarily without access to required systems.
		2-3 Days	L	L	L	L	L	Internet – Bank Website	21	
		4-7 Days	L	L	L	L	L			
		8-14 Days	L	M	L	L	L			
		14+ Days	L	H	M	M	L			
Payroll Processing Calculating and remitting salary payments to the Company's employees. Includes retaining and distributing funds for benefits and other payments.	3	1 Day or Less	L	L	L	L	L	HRIS	14	If the Company was more than 3 days late distributing payroll, employees may encounter significant hardships and potentially may cease their activities. For a single pay cycle, temporary (estimated) payments could be distributed in the absence of automated systems. Manual checks could be issued for two pay cycles.
		2-3 Days	L	M	M	L	M	Internet – Bank Website	28	
		4-7 Days	M	M	M	M	H	G/L System	28	
		8-14 Days	M	H	H	M	H			
		14+ Days	H	H	H	H	H			

RSM'S 5-PHASE BCP METHODOLOGY

Phase III: Strategy Determination

Phase III – Summary

- Identify current recovery strategies and the corresponding recovery capabilities
- Map BIA requirements to current recovery strategies and capabilities
- Identify and prioritize recovery capabilities gaps
- Establish initiative(s) to remediate recovery gaps
- Establish and execute Vendor Continuity Management Program

Recovery Strategy Coverage Areas

- Technology
 - Hardware, software, and data
 - Voice and data communication
 - Third-party systems and interfaces
- Facilities
 - Workspace
 - Data center(s)
 - Specialized sites (secure areas, lobbies, meeting rooms, etc.)
- Specialized equipment and other resources
- Operational workarounds and transfers
- Technical assistance and general staffing
- Crisis communication

Basic Recovery Strategy Options

- Internal Resources
- Specialized Vendors/Services
- Business Partners
- Public Resources
- Acquire/Address As Needed

Vendor Continuity Management Program

- Risk-rate ALL suppliers and services-providers
 - Different than other vendor risk assessments
 - Rating based on their impact to the continuity of your operations
 - Consider criticality of product/service, portability, etc.
 - Include technology providers
- Evaluate vendor continuity capabilities based on the assigned risk rating
 - Evaluation frequency
 - Evaluation criteria
- Proactively remediate and validate deficiencies

RSM'S 5-PHASE BCP METHODOLOGY

Phase IV: Implementation and Documentation

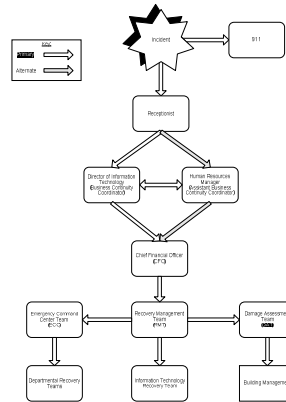
Phase IV – Summary

- Prepare actionable “playbooks” to guide the recovery process
- Document teams/roles, recovery processes and supporting information for reference following a disaster
- Properly and efficiently integrate SOPs and other reference information
- Address specialized considerations for coordinating the recovery process, restoring IT and other resources, resuming operations – and responding to pandemics or similar events

BCP “Playbooks”

- Recovery Coordination Plans (RCPs)

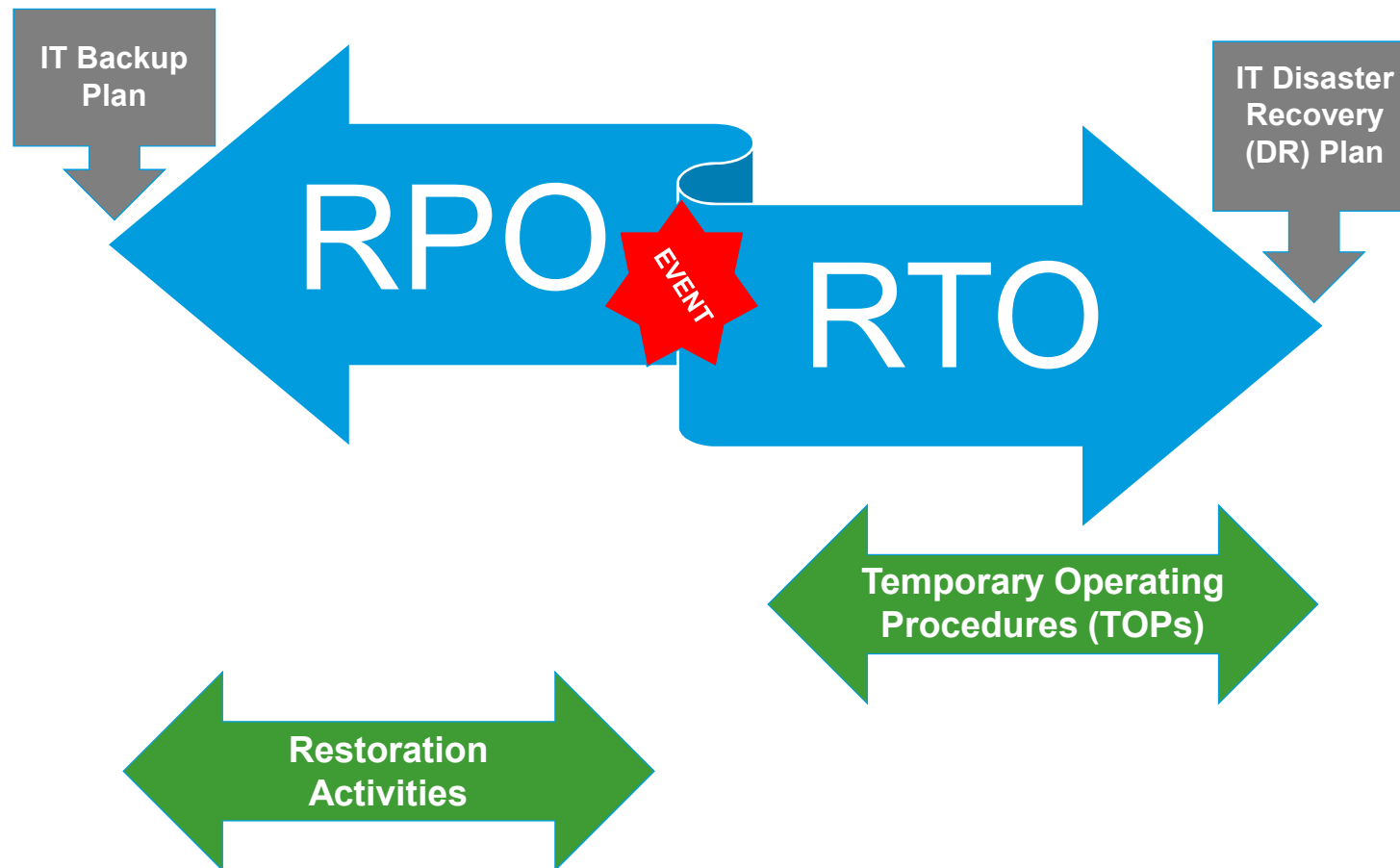
- BCP activation
- Damage assessment
- Internal and external communication
- Overall recovery coordination
- Recovery process tracking/administration



- Business Resumption Plans (BRPs)

- Team overview
- Functions and RTOs
- Team roster and roles
- Recovery strategies
- Recovery task list
- Recovery resource requirements
- Pandemic considerations
- Reference information

Recovery Tasks



BCP “Playbooks” continued

- IT Disaster Recovery Plans (DRPs)
 - Overview and scope
 - Team assignments (including alternates)
 - Recovery priorities and RTOs
 - Recovery strategy or strategies
 - Resource requirements
 - Technical restoration tasks
 - Interdependencies and other considerations
 - Reference materials

RSM'S 5-PHASE BCP METHODOLOGY

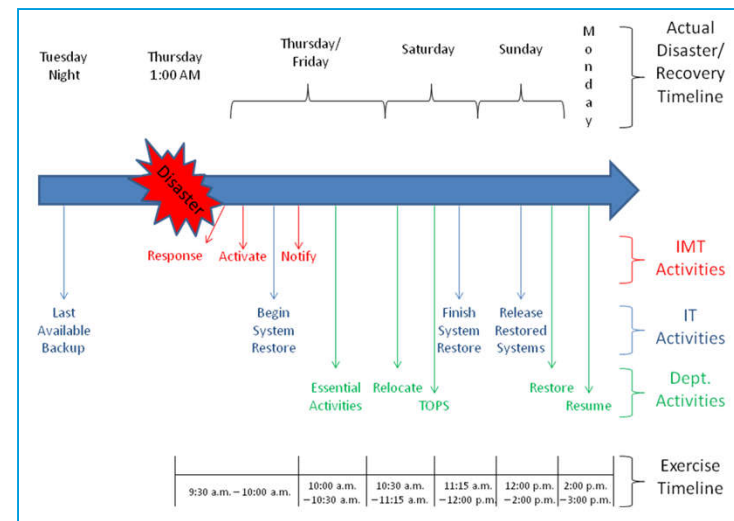
Phase V: Program Management and Testing

Phase V – Summary

- Train personnel on the overall BCP and their specific recovery roles
- Conduct varying and evolving BCP exercises
 - Verify the BCP is accurate, adequate and usable
 - Validate effectiveness of recovery strategies
 - Allow participants to experience key recovery processes and practice their roles
 - Identify weaknesses and opportunities to enhance the BCP
- Revise the BCP based on the results of the exercises

BCP Testing Program – Best Practices

- Vary test type, scope, scenario, participants, timing, etc.
- Consider realistic and unpredictable disaster circumstances
- Elevate complexity and expand scope over time
- Properly plan each event with known objectives
- Evaluate and document/report all tests and any actual activations
- Consider all tests collectively to determine BCP status and identify additional testing requirements



PANDEMIC PLANNING

Pandemic Planning

“Recognized variation from traditional BCPs”

- Little or no impact on facilities, technology, etc.
- Major impacts on staffing, customers, vendors, community, etc.
- Leverage and integrate with Crisis Management Plans, or RCTs
- Key Considerations:
 - Prevention and containment
 - Proactive monitoring
 - Escalation and de-escalation
 - Effective communication
 - Personnel (HR) policies
 - Demand variations
 - Operational priorities and scaling

Pandemic Response Plans – Objectives

- Protect your staff and customers
- Continue your critical operations
- Minimize the impact on your community, customers, employees, etc.
- Reduce the impact from inaction or bad decisions by others

Pandemic Response Plans – Skills Considerations

- Number of people available in each department, function, workgroup, etc.
- Specialized skill concentrations (including home geography)
- Internal staff with needed skills able to assist other departments
- Availability of external staff for temporary assistance
- Learning curve if new staff members are required

Pandemic Response Plan – Enterprise

- Overview
- Preemptive Measures Action Plan
 - Mitigation Framework
 - Active Measures
- Incident Management Framework
 - Incident Management Structure
 - BCP Integration
 - Communications and Coordination
 - Response Direction
- Pandemic Response Framework
 - Internal Response Levels
 - Personnel/Employment Strategy Considerations
 - Operating Strategy Considerations
 - Departmental Response

See Handout 4 – Pandemic Response Plan Template

Response Level Thresholds Examples

The following table illustrates the criteria that will be considered for both invoking and revoking each of the organization's internal response levels:

Internal Response Level	Invocation Criteria (Thresholds at which this level would be activated)	Revocation Criteria (Thresholds at which the organization would revert to the previous level)
1 (Non-pandemic Period)	<ul style="list-style-type: none"> Not Applicable (NA) 	<ul style="list-style-type: none"> Not Applicable (NA)
2	<ul style="list-style-type: none"> CDC Pandemic Severity Index established at, or increased to, Category 2 Federal government response increased to stage 3 or 4 Employees, customers and regulators inquire of the organization's preparations and plans Employee absenteeism is observed to be above average Significant infections reported locally or in the region Noticeable changes in customer demand and market conditions 	<ul style="list-style-type: none"> CDC Pandemic Severity Index decreased to Category 1 Federal government response decreased to stage 2 or lower Inquiries on pandemic preparations notably diminish Employee absenteeism returns to normal levels No new infections reported locally or in the region over a sustained period Customer demand and market conditions return to normal levels
3	<ul style="list-style-type: none"> <continued> 	<ul style="list-style-type: none"> <continued>
4	<ul style="list-style-type: none"> <continued> 	<ul style="list-style-type: none"> <continued>
5	<ul style="list-style-type: none"> <continued> 	<ul style="list-style-type: none"> <continued>

Response Level Strategies Examples

The following table illustrates the strategies that will be considered for activation at each internal response level.

Internal Response Level	Personnel/Employment Policies	Operating Practices
1 (Non-pandemic Period)	<ul style="list-style-type: none"> Not Applicable (NA) 	<ul style="list-style-type: none"> Not Applicable (NA)
2	<ul style="list-style-type: none"> Publish potential policy adjustments to staff members without implementing such changes Launch health awareness and pandemic education campaigns 	<ul style="list-style-type: none"> Issue statements and awareness initiatives to customers, business partners, etc. Review, revise and validate pandemic preparations Prepare for suspension of less critical functions
3	<ul style="list-style-type: none"> Issue temporary adjustments to basic employment policies such as sick leave, vacation allowance, etc. Confirm possible alternate roles for each position and title Increase telecommuting practices Confirm/revise corporate and employee insurance coverage 	<ul style="list-style-type: none"> Review cross-training and workflow continuity arrangements Suspend least critical functions as needed Divert functions to home-office or outside parties, as feasible
4	<ul style="list-style-type: none"> <continued> 	<ul style="list-style-type: none"> <continued>
5	<ul style="list-style-type: none"> <continued> 	<ul style="list-style-type: none"> <continued>

BRPs – Pandemic Considerations Examples

1. Pandemic Impacts and Minimum Response Level to Suspend

Function Name	Personal Interaction/On-Site Requirements	Unique Skills and/or Authorities	Volume/Demand Changes	Operating Cost Changes	Vendor/Supplier Dependence	Minimum Response Level to Suspend
New Client Provisioning	Medium	Low	Medium	Medium	Medium	4
Marketing and Product Development	None	None	Low	None	Low	3

2. Alternate Staffing Options and Remote Processing Capabilities

Function Name	Primary Staff	Alternate Staff	Remote Processing Capabilities	Remote Processing Considerations
New Client Provisioning	•	•	<ul style="list-style-type: none"> Function can be partially performed remotely, but in-person interaction is key to obtaining some customers. 	<ul style="list-style-type: none"> Remote access to internal systems would be required. Remote access to external systems would be required. Remote interaction with Corporate and/or customers may be required. During a pandemic situation, prospective customers are more likely to forego in-person meetings. Account applications and other materials would have to be transported among personnel for authorization, or electronic distribution and approval processes would have to be adopted.
Marketing and Product Development	•	•	<ul style="list-style-type: none"> Function can entirely be performed remotely. 	<ul style="list-style-type: none"> Remote access to internal systems would be required. Remote access to external systems would be required. Remote interaction with Corporate and/or other departments may be required.

QUESTIONS AND ANSWERS?

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 continued

- Viable recovery strategies
 - Techniques for achieving critical recovery objectives are defined and fully implemented
- Documented recovery plan
 - Recovery processes are defined, responsibilities assigned and reference information is available
- Effective plan deployment
 - The current plan is distributed to appropriate individuals
 - Obsolete materials are collected
 - Participants remain knowledgeable of their role and the overall recovery process

Key Elements of an *Effective* BCP Program continued

- Plan testing and maintenance
 - Realistic exercises are conducted to confirm plan accuracy, prepare participants to respond and identify enhancement opportunities
 - The plan is updated on a defined schedule and whenever the organization, operation and/or environment changes

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

RSM US LLP

One South Wacker Drive, Suite 800
Chicago, IL 60606
312.634.3400

+00 (1) 800 274 3978
www.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.

© 2020 RSM US LLP. All Rights Reserved.

Disclaimer

The descriptions contained in this communication are for preliminary informational purposes only and should not be taken as legal advice. The product is available on an admitted basis in some but not all US jurisdictions through Beazley Insurance Company, Inc., and is available on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd's. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: 0G55497). Further information and disclosures can be found on our website www.beazley.com. BZEM093_US_03/20.

