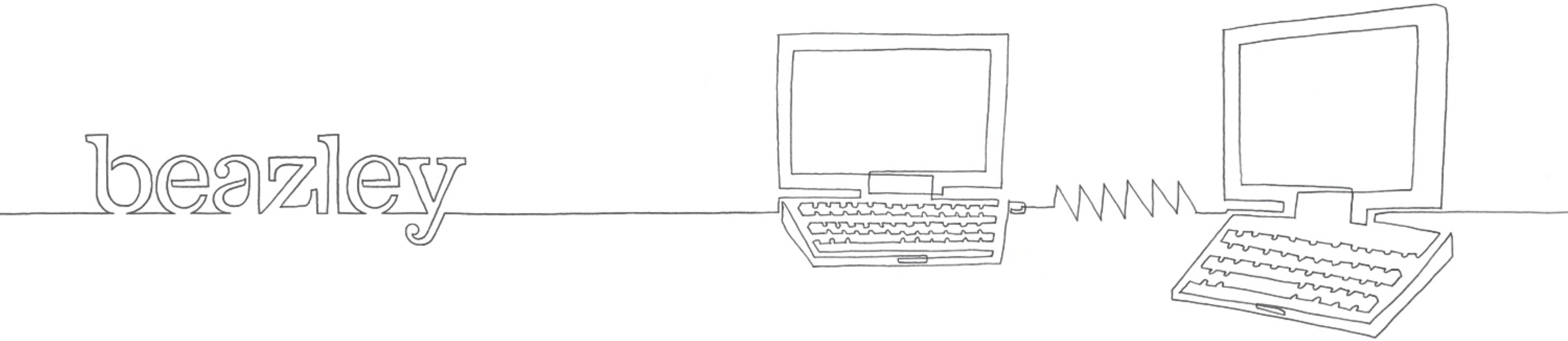
Basics of Business Continuity Planning

For Financial Institutions

December 4, 2019



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 FINANCIAL INSTITUTIONS

December 4, 2019

RSM

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

- BCP Overview
- FFIEC BCP Guidance
- RSM’s 5-Phase BCP Methodology
- Questions & Answers/Open Discussion
- Conclusions/Wrap-up

BCP 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 (DR) Plans
  - Business Resumption Plans
  - Pandemic Response Plans

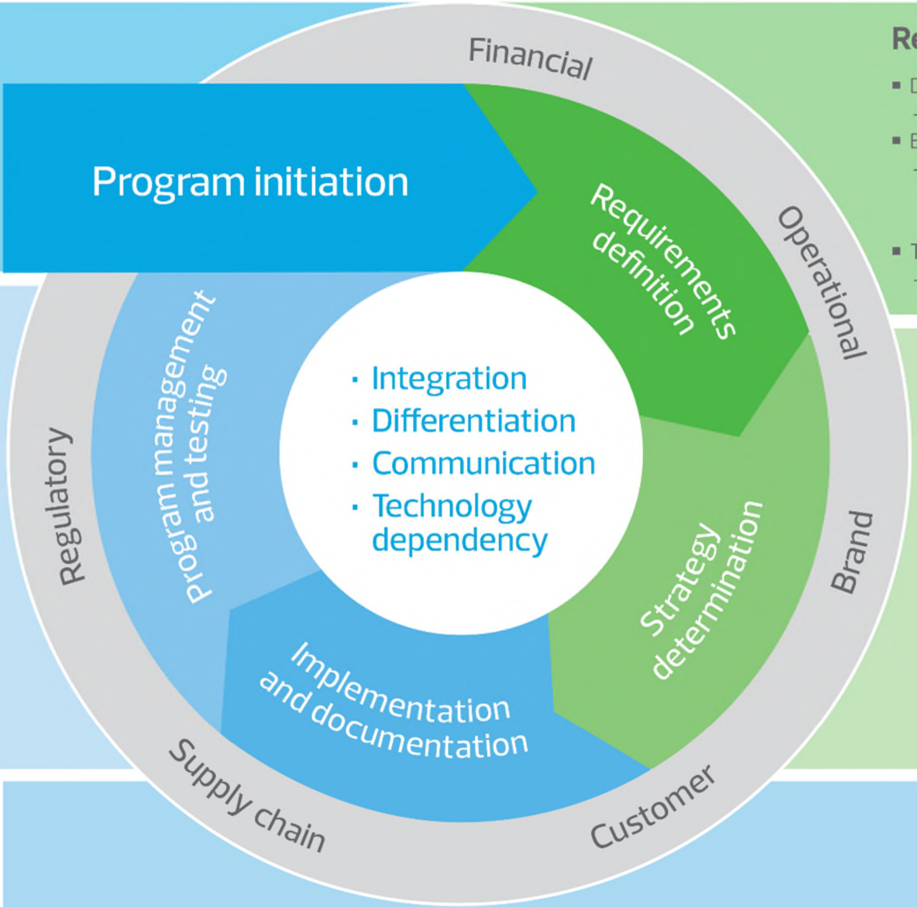
- Other Risk Management Initiatives:
  - Emergency Response Plans
  - Incident Response Plans/Incident Action Plans
  - Information Security Programs
  - Physical Security Programs
  - Compliance Programs
  - Insurance Programs
  - Staff Succession Plans

*Relative positioning may vary

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
  - Recovery coordinated from department level to the organization level
  - Designated teams for recovery coordination, IT restoration, etc.

RSM’s Business Continuity Planning Methodology



Program Initiation

- Business continuity plan (BCP) policy or charter
- BCP roles and responsibilities
- BCP document/plan management
- Executive support and prioritization

Requirements definition

- Disaster risk assessment
  - Threats and mitigation
- Business impact analysis
  - Drivers, recovery time objectives (RTOs) and recovery point objectives (RPOs)
- Technical impact analysis
  - System dependencies

Program management and testing

- Recovery exercises
  - Tabletops, functional, simulations
- Training and awareness
- Governance

Strategy determination

- Gap analysis
  - Process vs. capability
- IT disaster recovery considerations
  - Primary site improvements
- Alternate work locations
- Resource and vendor strategies

Implementation and documentation

- IT DR plans
  - Application and infrastructure documents
  - Recovery sequence
- Business continuity plans
- Incident/crisis management plans
- Failback considerations

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

FFIEC BCP GUIDANCE

FFIEC BCP Handbook

- High-level guidance on best practices and regulatory requirements for a sound planning program
- Follows closely with industry best practices
- Aligns with the methodologies developed by RSM, Disaster Recovery Institute International (DRII), and other industry sources
- Supplemented by interagency statements
- Latest revision: November 2019

FFIEC BCP Handbook – Key Focus Areas

- Enterprisewide continuity planning
- Management oversight and support – including formal and documented Board approval
- Business impact analysis (BIA) and disaster risk assessment (DRA)
- Strategic risk management
    - Adequate risk reduction strategies and recovery strategies
    - Integration with other processes-System Development Life Cycle (SDLC), audit, training, etc.

FFIEC BCP Handbook – Key Focus Areas continued

- Ongoing testing and maintenance programs
  - Including logging (documentation) of activities and the associated results
- IT disaster recovery and increased IT complexity
- Integration with third-party service providers
- Consideration of security

FFIEC BCP Handbook – “Recent” Additions

- Pandemic Response Planning
- Tiered regulatory assessment
- Increased emphasis on previous guidance
    - Board and Senior Management involvement
    - Cyclical planning process
    - Business Impact Analysis (BIA)
- Comprehensive assessment of third-party risks
- Failure of primary DR/BCP strategies and plans
    - Supplemental measures, such as Sheltered Harbor

RSM’S 5-PHASE BCP METHODOLOGY

PROGRAM INITIATION

RSM

RSM’s Business Continuity Planning Methodology

Program Initiation

- Business continuity plan (BCP) policy or charter
- BCP roles and responsibilities
- BCP document/plan management
- Executive support and prioritization

Requirements definition

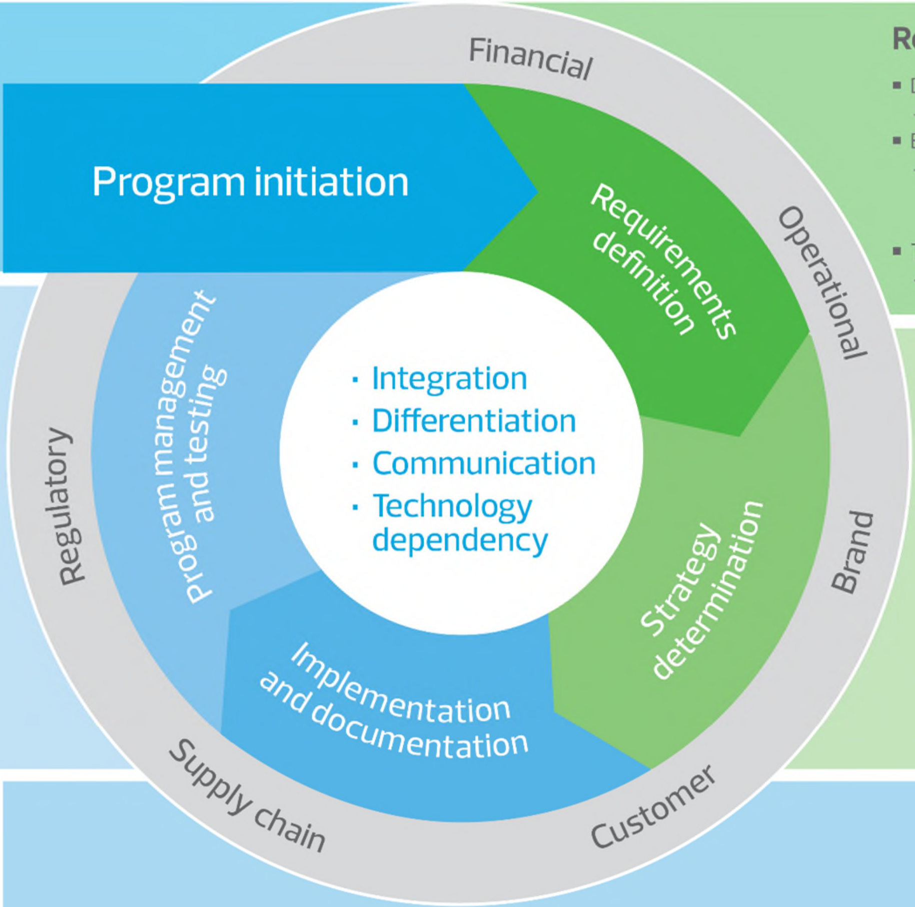
- Disaster risk assessment
  - Threats and mitigation
- Business impact analysis
  - Drivers, recovery time objectives (RTOs) and recovery point objectives (RPOs)
- Technical impact analysis
  - System dependencies

Program management and testing

- Recovery exercises
  - Tabletops, functional, simulations
- Training and awareness
- Governance

Strategy determination

- Gap analysis
  - Process vs. capability
- IT disaster recovery considerations
  - Primary site improvements
- Alternate work locations
- Resource and vendor strategies



Implementation and documentation

- IT DR plans
  - Application and infrastructure documents
  - Recovery sequence
- Business continuity plans
- Incident/crisis management plans
- Failback considerations

BCP Policy and/or Charter

- Concise, but clear and definitive
- Formally approved and properly adopted
- Regularly reviewed and updated
- Suggested topics:
  - Scope, objectives, and assumptions
  - Roles and responsibilities with clear accountability
  - General approach/methodology
  - Timeline and budget
  - Ongoing planning processes

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

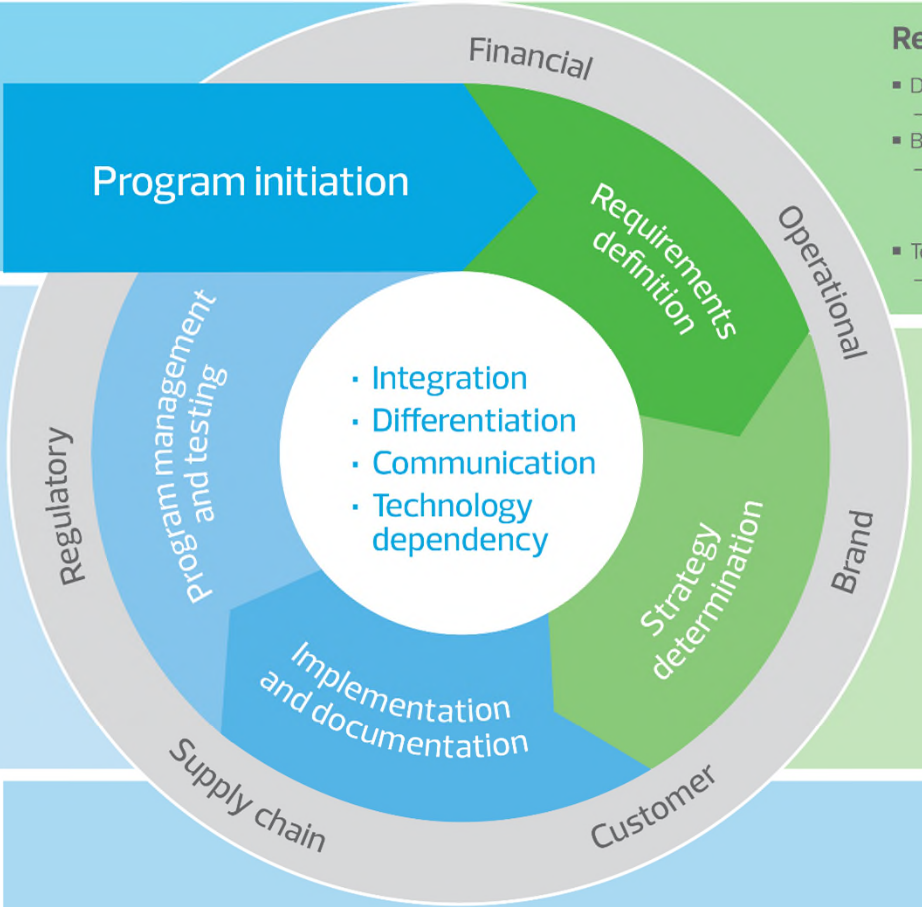
BCP Software Tools

- Specialized tools for developing, maintaining and storing your BCP(s) and other related materials
- Support consistent and effective planning
- Relational databases to support data collection and maintenance
- Specialized user interfaces and output reporting
- User security, external interfaces, expanded features, etc.

Facilitate, but do not replace, the plan development, maintenance and testing processes

REQUIREMENTS DEFINITION

RSM’s Business Continuity Planning Methodology



Program Initiation

- Business continuity plan (BCP) policy or charter
- BCP roles and responsibilities
- BCP document/plan management
- Executive support and prioritization

Requirements definition

- Disaster risk assessment
  - Threats and mitigation
- Business impact analysis
  - Drivers, recovery time objectives (RTOs) and recovery point objectives (RPOs)
- Technical impact analysis
  - System dependencies

Program management and testing

- Recovery exercises
  - Tabletops, functional, simulations
- Training and awareness
- Governance

Strategy determination

- Gap analysis
  - Process vs. capability
- IT disaster recovery considerations
  - Primary site improvements
- Alternate work locations
- Resource and vendor strategies

Implementation and documentation

- IT DR plans
  - Application and infrastructure documents
  - Recovery sequence
- Business continuity plans
- Incident/crisis management plans
- Failback considerations

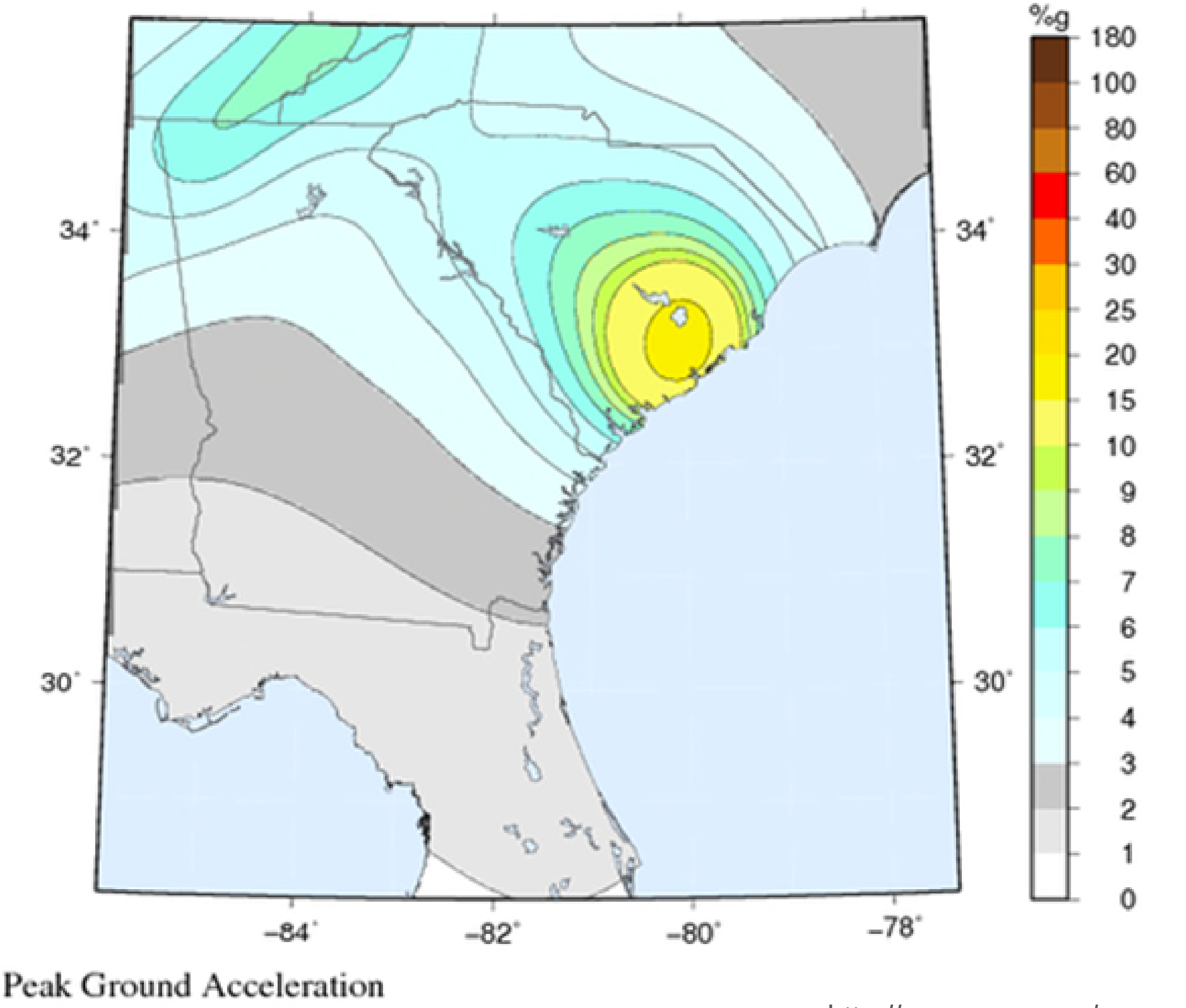
REQUIREMENTS DEFINITION

Disaster Risk Assessment (DRA)

Disaster Risk Assessment (DRA) Process

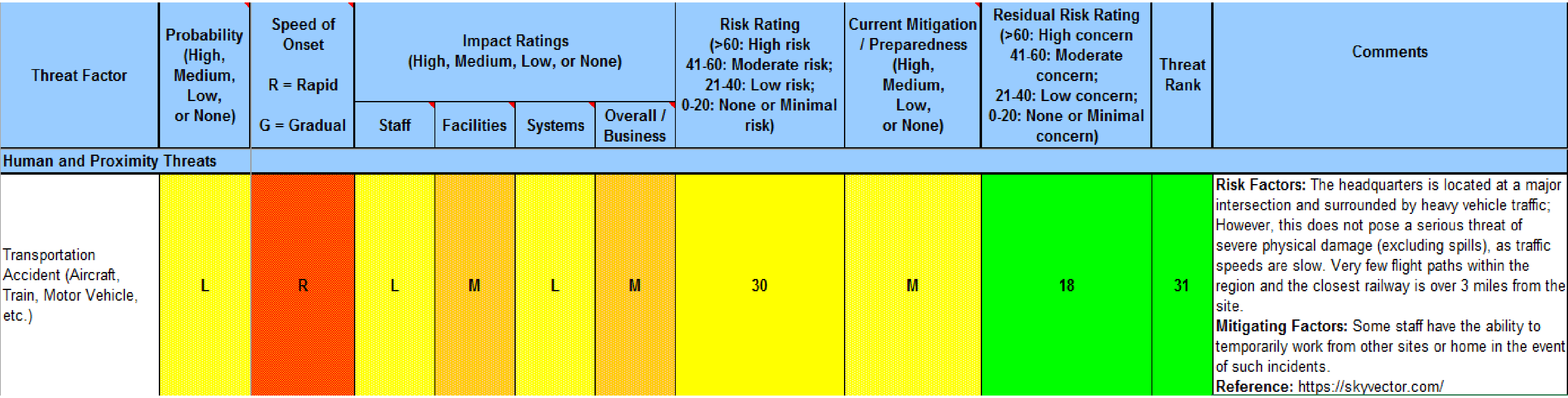
- Assemble a comprehensive library of risk factors
- Collect and analyze data from multiple sources
  - Perceptions
  - Government and industry authorities
  - Historical experiences
  - Observation
  - Other research
- Assign ratings for Probability and appropriate Impact categories
- Calculate inherent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

Custom Hazard Map



http://www.usgs.gov/

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	**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. **Mitigating Factors:** Some staff have the ability to temporarily work from other sites or home in the event of such incidents. **Reference:** https://skyvector.com/

Risk Mitigation

- Establish formal risk mitigation plans
  - Priorities correlated to risk assessment results
  - Objectives and tasks
  - Responsibilities
  - Timelines
- Monitor progress and publish status reports
- Periodically reevaluate both risks and mitigation

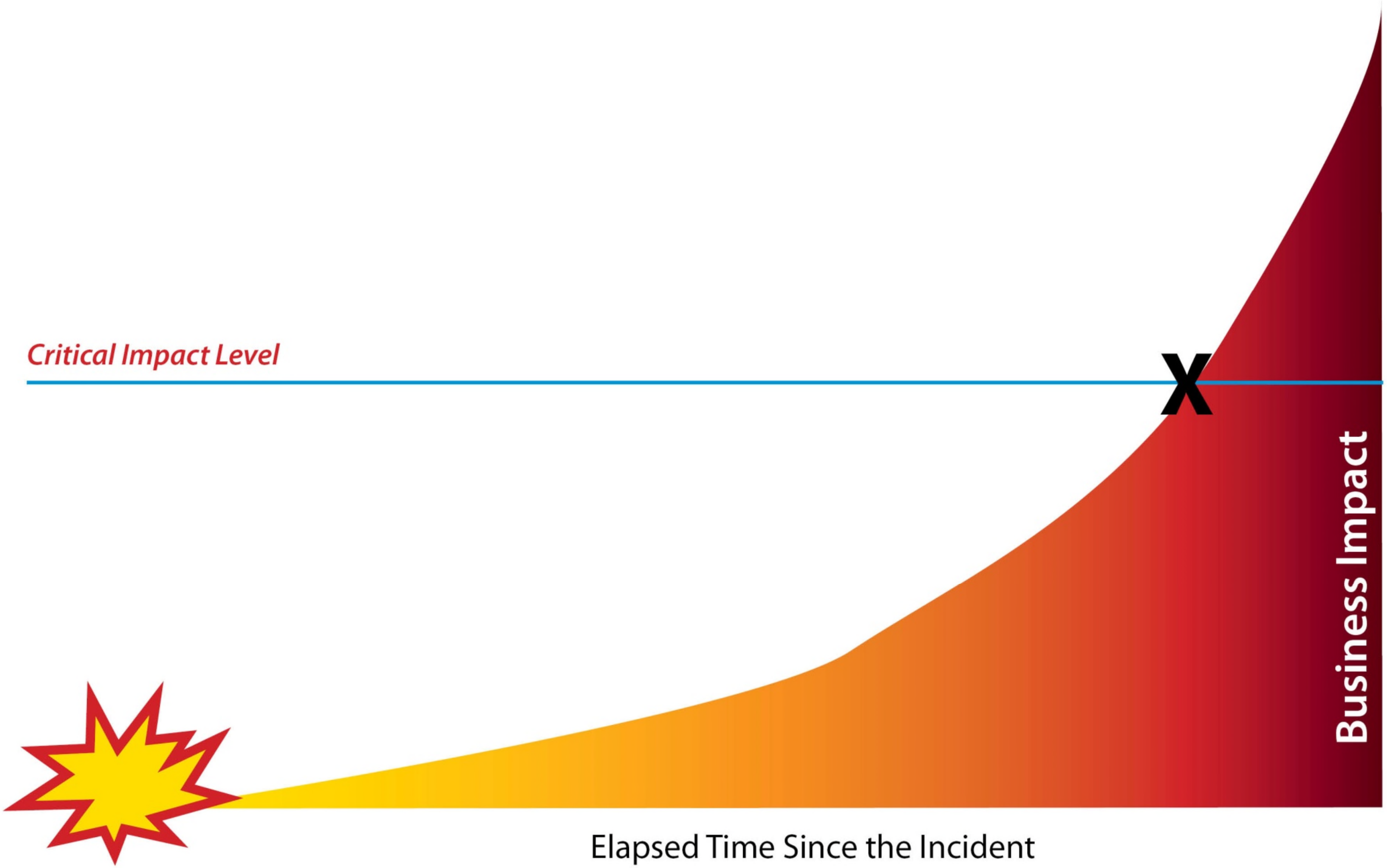
REQUIREMENTS DEFINITION

Business Impact Analysis (BIA)

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
- Identify and evaluate technical requirements

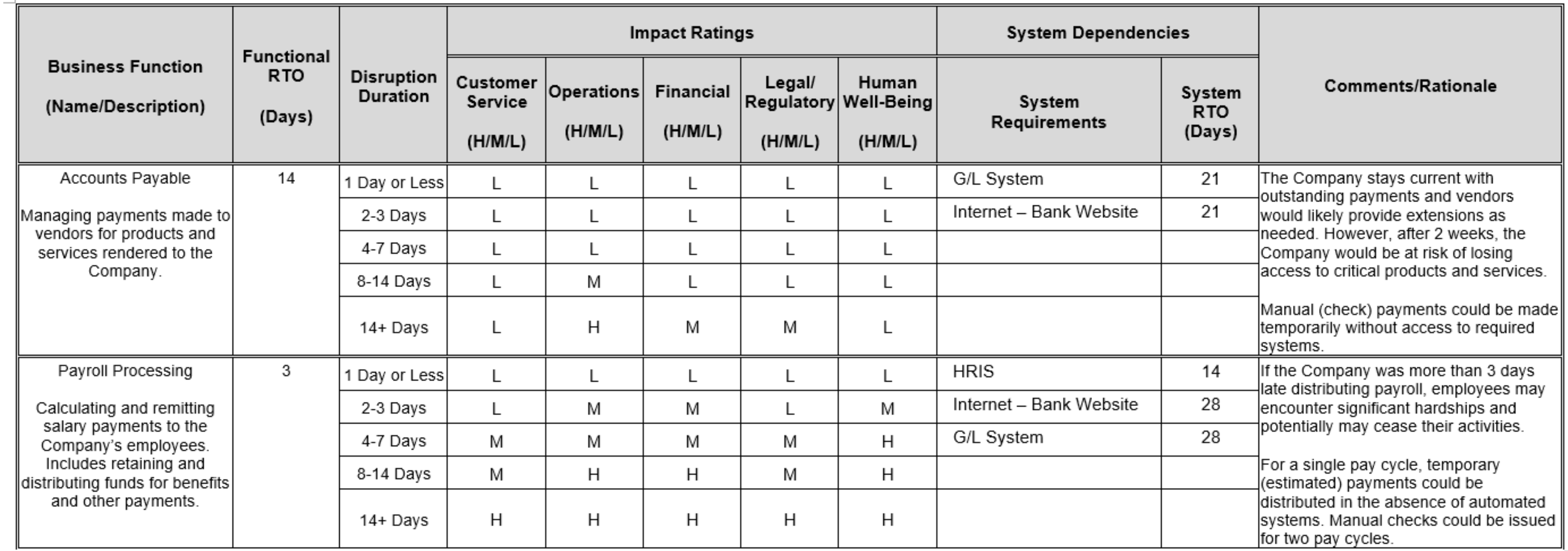
Business Impact Analysis—
Recovery Time Objective (RTO)



Technical Requirements

- Identify the key technical applications or services that are required to perform each function
- Individually evaluate the criticality of each system
- Determine the RTO of each system *requirement*
- Validate the data loss tolerance or Recovery Point Objective (RPO) of each system

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			

See Handout 1 – BIA Matrix Template

STRATEGY DETERMINATION

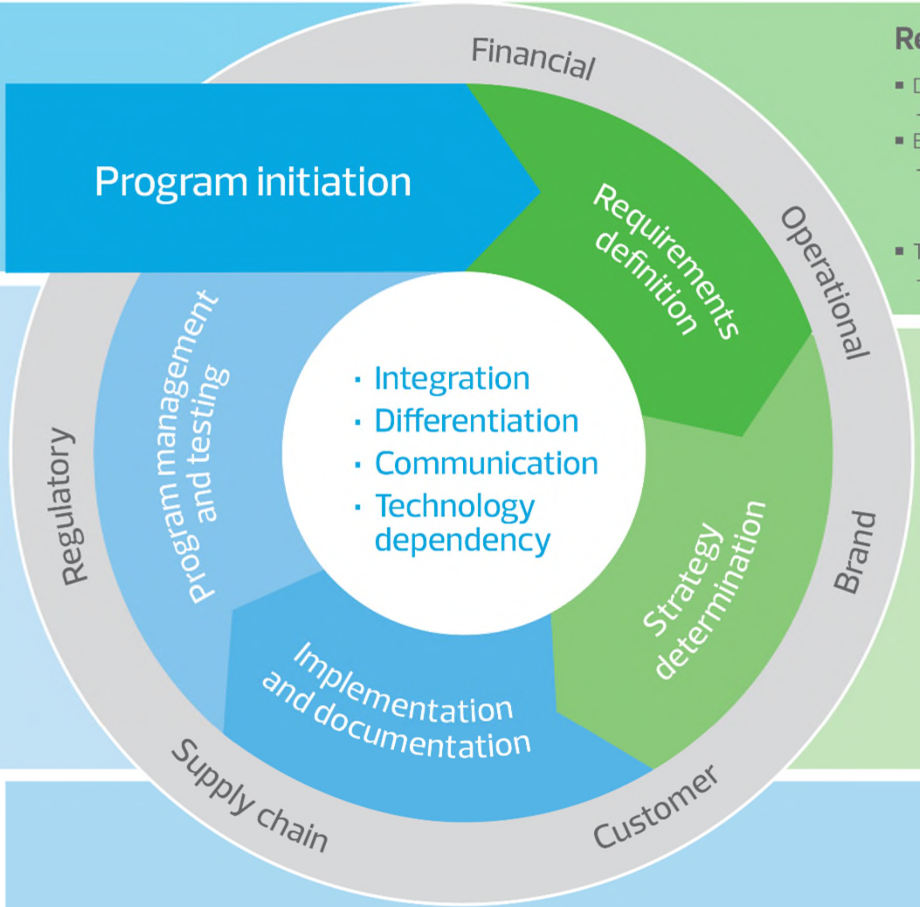
RSM’s Business Continuity Planning Methodology

Program Initiation

- Business continuity plan (BCP) policy or charter
- BCP roles and responsibilities
- BCP document/plan management
- Executive support and prioritization

Requirements definition

- Disaster risk assessment
  - Threats and mitigation
- Business impact analysis
  - Drivers, recovery time objectives (RTOs) and recovery point objectives (RPOs)
- Technical impact analysis
  - System dependencies



Strategy determination

- Gap analysis
  - Process vs. capability
- IT disaster recovery considerations
  - Primary site improvements
- Alternate work locations
- Resource and vendor strategies

Implementation and documentation

- IT DR plans
  - Application and infrastructure documents
  - Recovery sequence
- Business continuity plans
- Incident/crisis management plans
- Failback considerations

Program management and testing

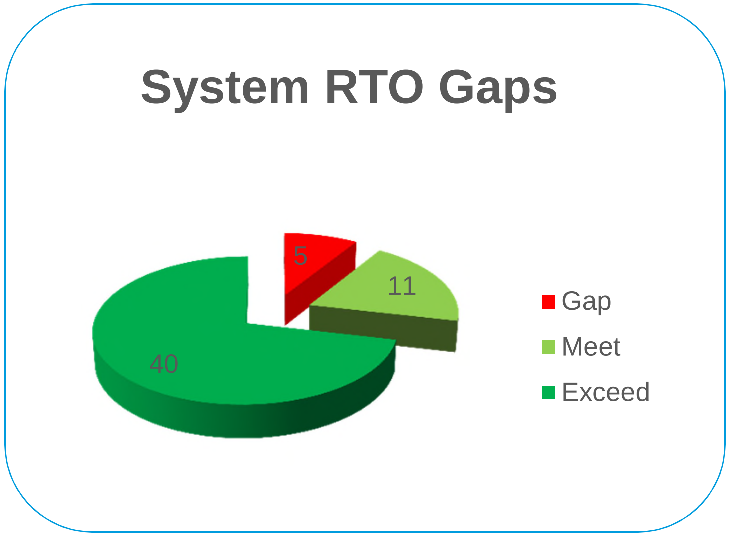
- Recovery exercises
  - Tabletops, functional, simulations
- Training and awareness
- Governance

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

Recovery Strategy Gap Analysis

- Map BIA Requirements to Current/Planned Strategies
- Determine Current/Planned Capabilities
  - Realistic/Valid Timelines
    - Timing From Initial Disruption
    - Foundation for Estimates
  - Interdependency Considerations
    - Predecessors
    - Restoration Capacity
- Include a Formal Gap Analysis
- Identify Enhancement Requirements



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

IMPLEMENTATION AND DOCUMENTATION

RSM’s Business Continuity Planning Methodology

Program Initiation

- Business continuity plan (BCP) policy or charter
- BCP roles and responsibilities
- BCP document/plan management
- Executive support and prioritization

Requirements definition

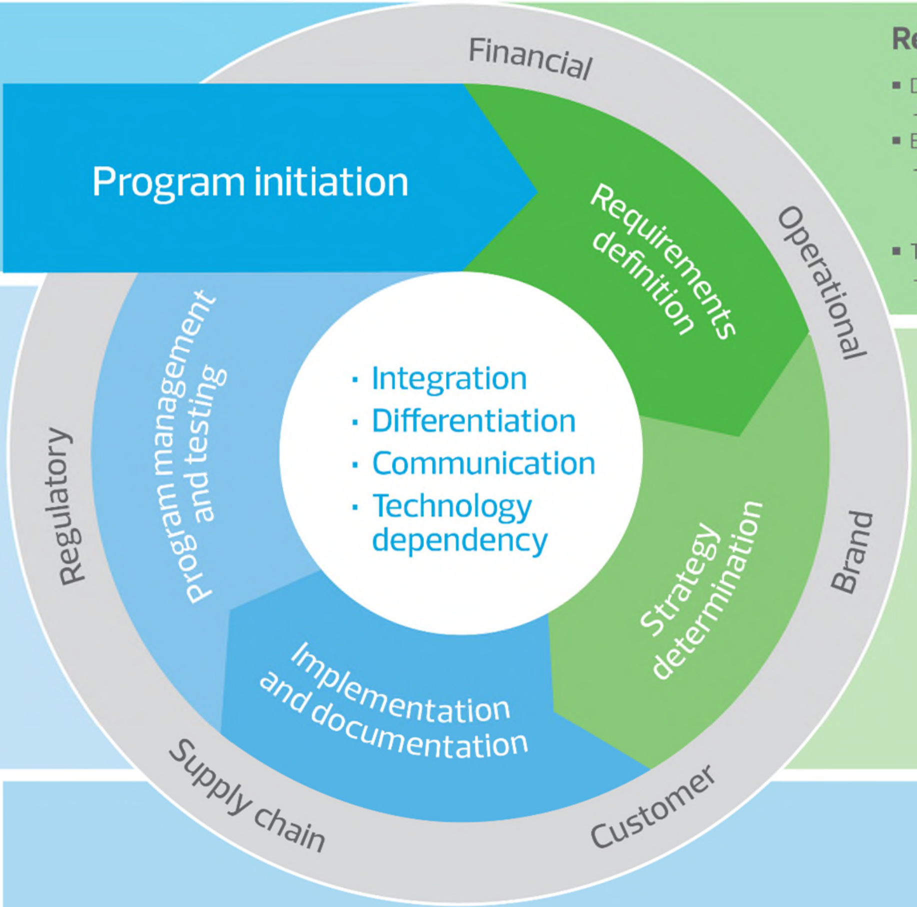
- Disaster risk assessment
  - Threats and mitigation
- Business impact analysis
  - Drivers, recovery time objectives (RTOs) and recovery point objectives (RPOs)
- Technical impact analysis
  - System dependencies

Program management and testing

- Recovery exercises
  - Tabletops, functional, simulations
- Training and awareness
- Governance

Strategy determination

- Gap analysis
  - Process vs. capability
- IT disaster recovery considerations
  - Primary site improvements
- Alternate work locations
- Resource and vendor strategies



Implementation and documentation

- IT DR plans
  - Application and infrastructure documents
  - Recovery sequence
- Business continuity plans
- Incident/crisis management plans
- Failback considerations

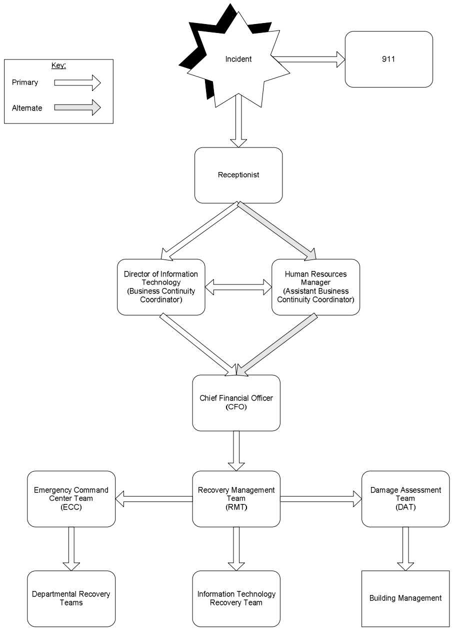
BCP Manual – Structure and Format

- Defined, consistent, and logical
- Should facilitate (or even mimic) a recovery effort
- Supported by a detailed table of contents or even chapter summaries
- Segregates administrative and overview sections from actionable recovery plans
- Includes team-specific sections/plans ("playbooks")

See Handout 2 – Sample BCP Outline

Recovery Coordination Teams

- 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:
Primary
Alternate
Incident
911
Receptionist
Director of Information Technology (Business Continuity Coordinator)
Human Resources Manager (Assistant Business Continuity Coordinator)
Chief Financial Officer (CFO)
Emergency Command Center Team (ECC)
Recovery Management Team (RMT)
Damage Assessment Team (DAT)
Departmental Recovery Teams
Information Technology Recovery Team
Building Management

Recovery Coordination Teams 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

Departmental Business Resumption Plans (BRPs)

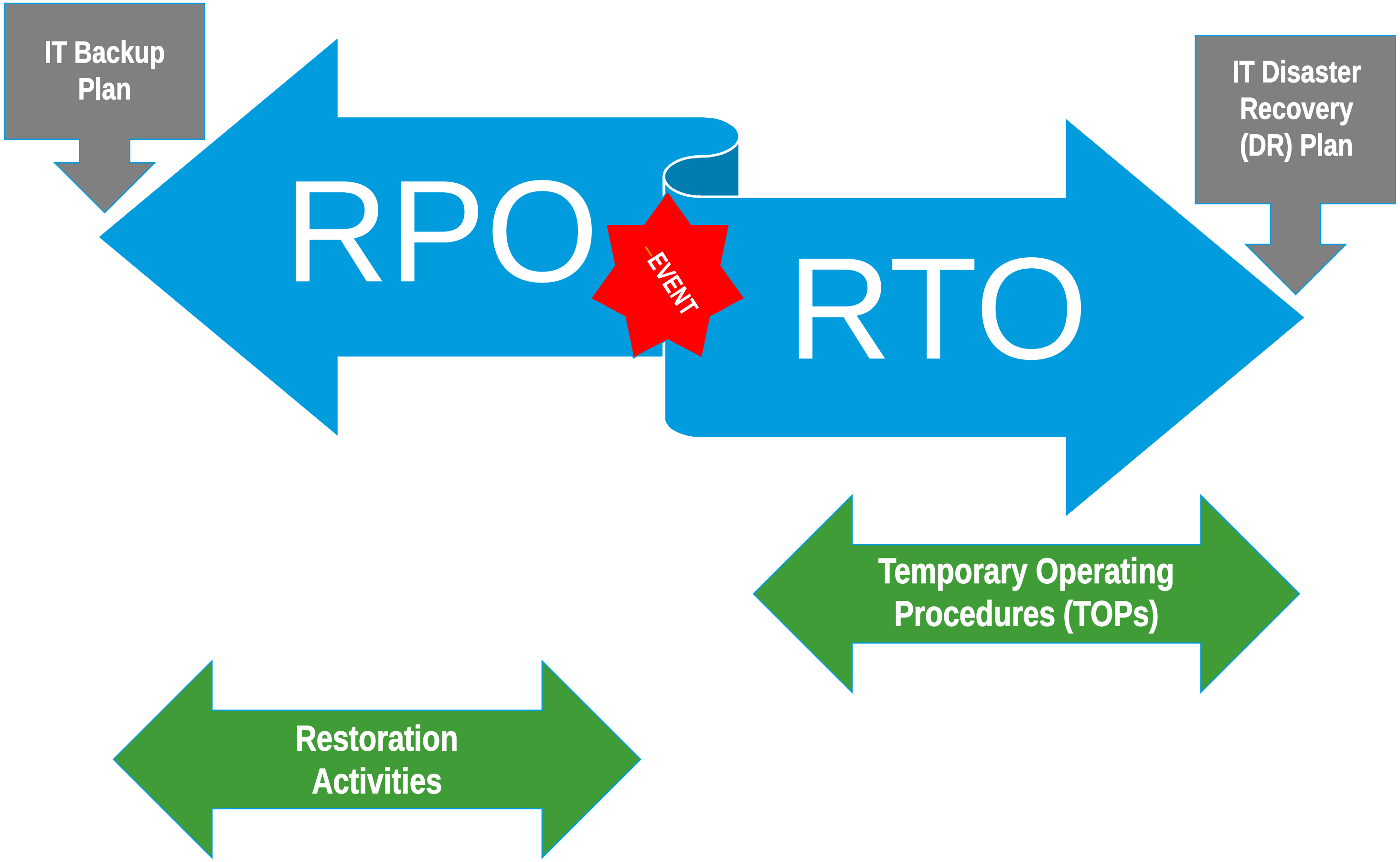
- Team/department overview
  - Ongoing (“normal”) responsibilities
  - Disaster responsibilities
- Departmental recovery strategies
  - Facilities/workspace
  - Technology
  - Personnel
  - Other
- Team assignments (including alternates)
- Business functions and priorities/RTOs
- External resource requirements (schedule)

Departmental BRPs continued

- Internal resources requirements
  - Quantity over time (schedule)
  - Source (including off-site storage)
- Administrative/common recovery tasks
- **Custom recovery tasks**
- Reference materials
  - Contact lists
  - Resource inventories
  - User manuals
  - Standard Operating Procedures (SOPs)
  - Configuration specs or parameters
  - Other
- Other miscellaneous sections, such as:
  - Interdependency diagrams
  - Vital records list

See Handout 3 – BCP Chapter Template

Custom Recovery Tasks continued


IT Backup Plan
RPO
EVENT
RTO
IT Disaster Recovery (DR) Plan
Temporary Operating Procedures (TOPs)
Restoration Activities

IT Disaster Recovery Plans (DRPs)

- Overview and scope
- Team assignments (including alternates)
- Recovery priorities and RTOs
- Recovery strategy or strategies
- Resource requirements
  - Quantity
  - Specs
  - Source
  - Location
  - Other

IT DRPs continued

- Technical restoration tasks
  - Restoration
  - Configuration
  - Validation
- Interdependencies and other considerations
- Reference materials
  - Contact lists
  - Diagrams
  - Inventories
  - Addresses and settings
  - Administration and support procedures
  - Other

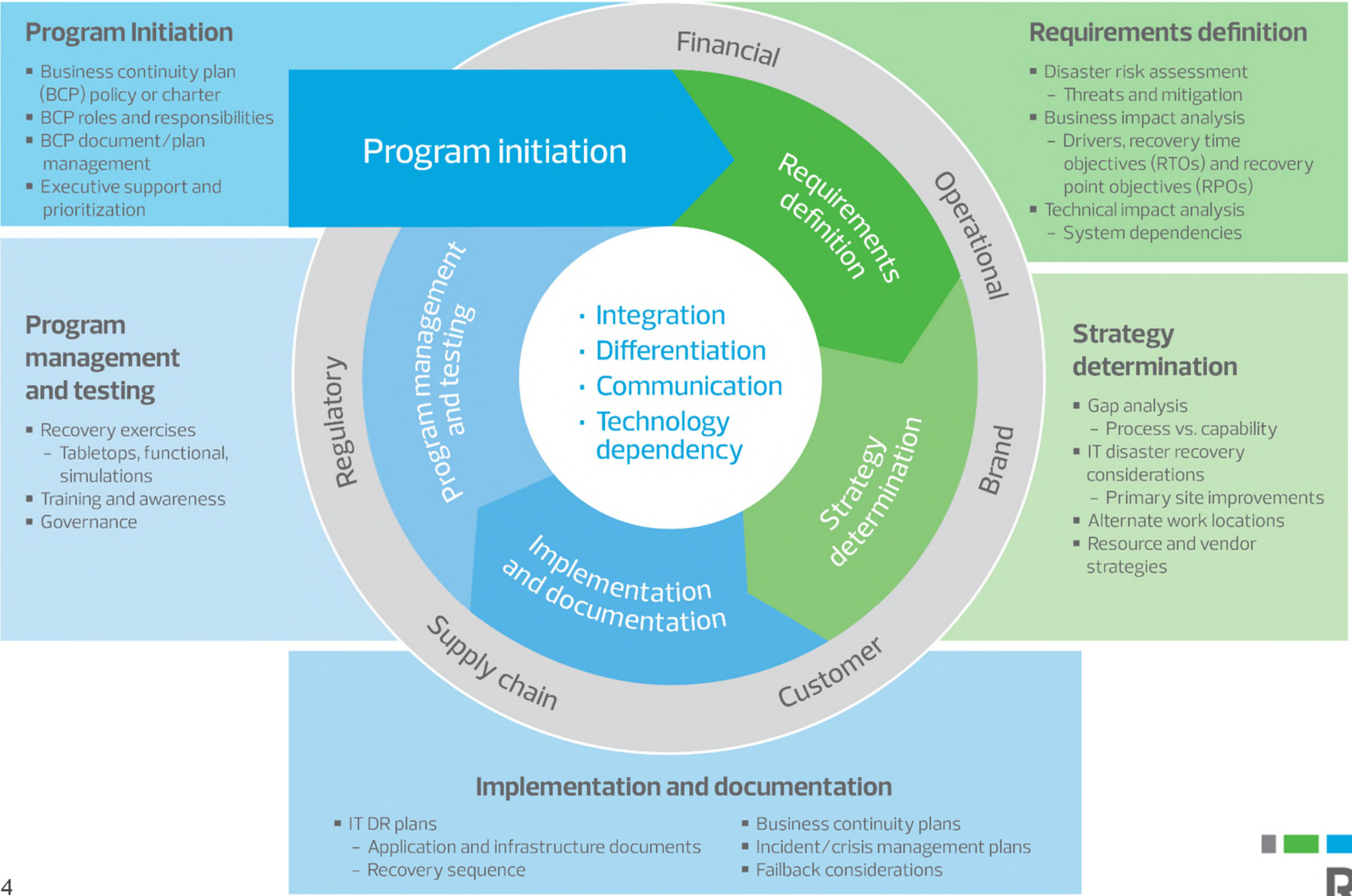
Pandemic Response Plans

"Recognized variation from traditional BCPs"

- Little or no impact on facilities, technology, etc.
- Major impacts on staffing, customers, vendors, etc.
- Leverage and integrate with crisis management plans
- Consider:
  - Prevention and containment
  - Monitoring
  - Escalation and de-escalation
  - Personnel (HR) policies
  - Demand variations
  - Operational priorities and scaling

PROGRAM MANAGEMENT AND TESTING

RSM’s Business Continuity Planning Methodology



Program Initiation

- Business continuity plan (BCP) policy or charter
- BCP roles and responsibilities
- BCP document/plan management
- Executive support and prioritization

Requirements definition

- Disaster risk assessment
  - Threats and mitigation
- Business impact analysis
  - Drivers, recovery time objectives (RTOs) and recovery point objectives (RPOs)
- Technical impact analysis
  - System dependencies

Program management and testing

- Recovery exercises
  - Tabletops, functional, simulations
- Training and awareness
- Governance

Strategy determination

- Gap analysis
  - Process vs. capability
- IT disaster recovery considerations
  - Primary site improvements
- Alternate work locations
- Resource and vendor strategies

Implementation and documentation

- IT DR plans
  - Application and infrastructure documents
  - Recovery sequence
- Business continuity plans
- Incident/crisis management plans
- Failback considerations

Testing & Training – Initial Activities

- Train personnel on the overall BCP and their specific recovery roles
- Implement recovery strategies
- Perform initial testing—typically walk-through 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 Plan
- Establish an ongoing BCP program

BCP Training Program

- Key positions need to develop and maintain familiarity with their role and key BCP components
  - Document structure and navigation
  - Teams and responsibilities
  - Activation and escalation procedures
  - Recovery priorities and outage tolerances
  - Core recovery strategies
- All staff should be aware of the BCP Program and key concepts
  - New-hire training
  - Ongoing awareness initiatives
- Goal is to understand the BCP – not memorize it

BCP Testing Program – Best Practices

- Avoids repetition
  - Varies test type, scope, scenario, participants, timing, etc.
- Considers realistic and unpredictable disaster circumstances
  - Adds realism to the events
- 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

Basic Test Schedule

- Rolling 24-month calendar
- Specific vs. approximate information
  - Timing
  - Test type
  - Participants
- Gain approval and commitment
- Maintain and adjust as needed

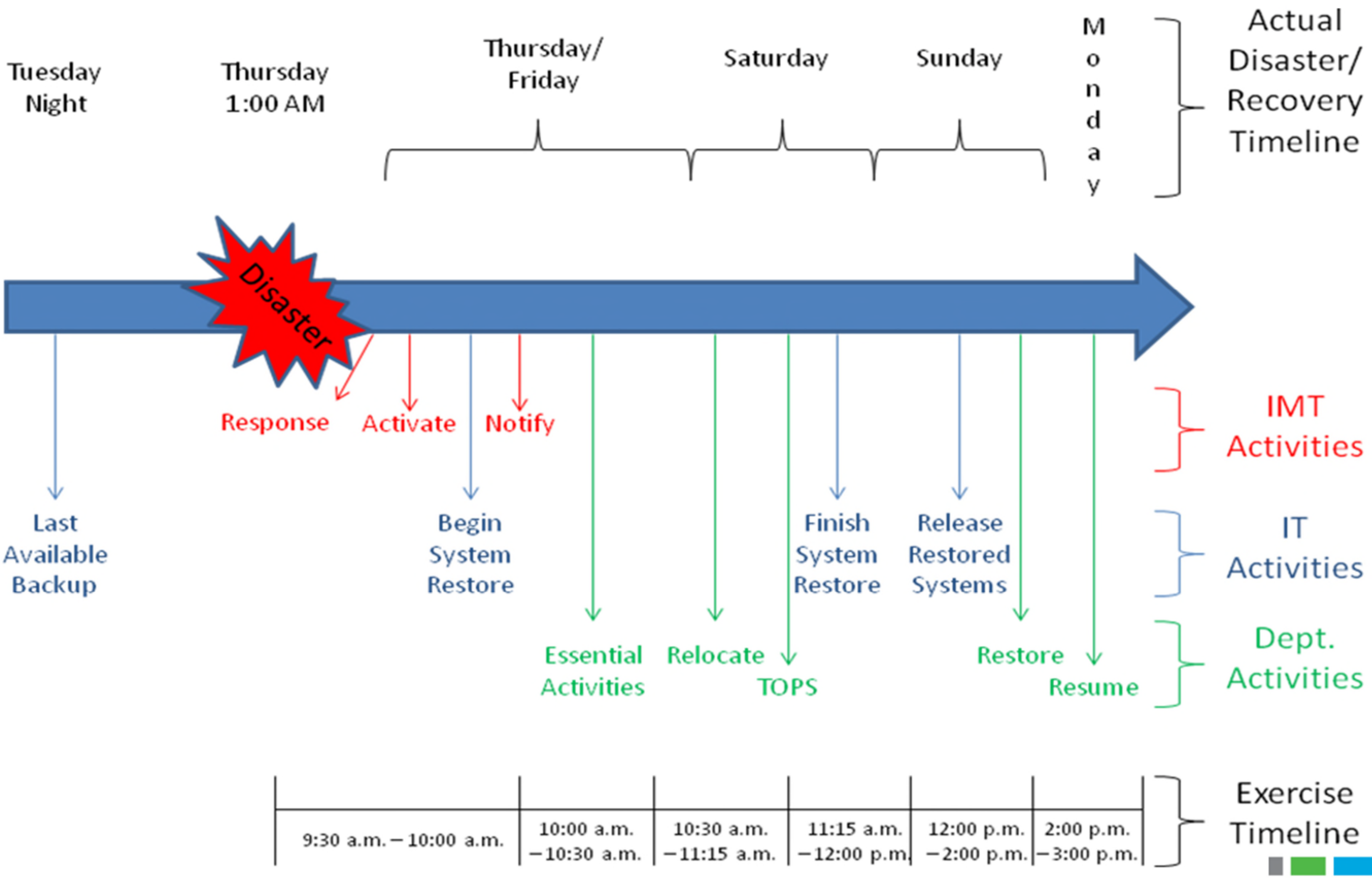
Enhanced Test Schedule

- 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

Disaster Scenario

- Correlate to BCP objectives and test objectives
- Outline realistic characteristics and circumstances
- Derive from DRA, relevant research, etc.
- Integrate unfolding circumstances
- Vary type, timing, impact, duration, constraints, etc.

Disaster Scenario – Timeline (Example)



9:30 a.m. – 10:00 a.m.	10:00 a.m. – 10:30 a.m.	10:30 a.m. – 11:15 a.m.	11:15 a.m. – 12:00 p.m.	12:00 p.m. – 2:00 p.m.	2:00 p.m. – 3:00 p.m.

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

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.

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). BZEM076_US_12/19

RSM