Powerful Insights.
Proven Delivery.®

Business Continuity and Disaster Recovery

Trends, Considerations, & Leading Practices

November 13, 2014

Presented by:

Jon Bronson – Los Angeles
Trey MacDonald – Atlanta

protiviti®
Risk & Business Consulting.
Internal Audit.

Today's Presenters

Jon Bronson is a Managing Director in Protiviti's Los Angeles Risk Consulting practice. He has led many business continuity engagements across the country and is a subject matter specialist in developing BCM programs. Jon is a Certified Business Continuity Professional (CBCP), Certified Information Systems Auditor (CISA), and a Certified Project Management Professional (PMP). He has over 17 years of large-scale project management experience complemented by an Engineering Master's degree from the University of Southern California.

Trey MacDonald is a Director in Protiviti's Atlanta Information Technology Consulting practice. He has more than 20 years of experience in the Information Technology, Financial Services, Health Care, Risk Management and Insurance, and Energy/Utilities industries. He has worked in professional services for the last 19 years, focusing on IT Strategy, Business Continuity Management, Infrastructure management, Data Lifecycle Management, Software Architecture, and Database Design and Administration. Trey has helped design, develop and implement optimized IT strategies, infrastructure, and disaster recovery environments for multiple clients in key industries and has served as an architect and administrator for several large scale technology environments.

protiviti®

Agenda

Business Continuity Management – The Basics

Continuity Landscape – What has changed?

Key Lessons Learned

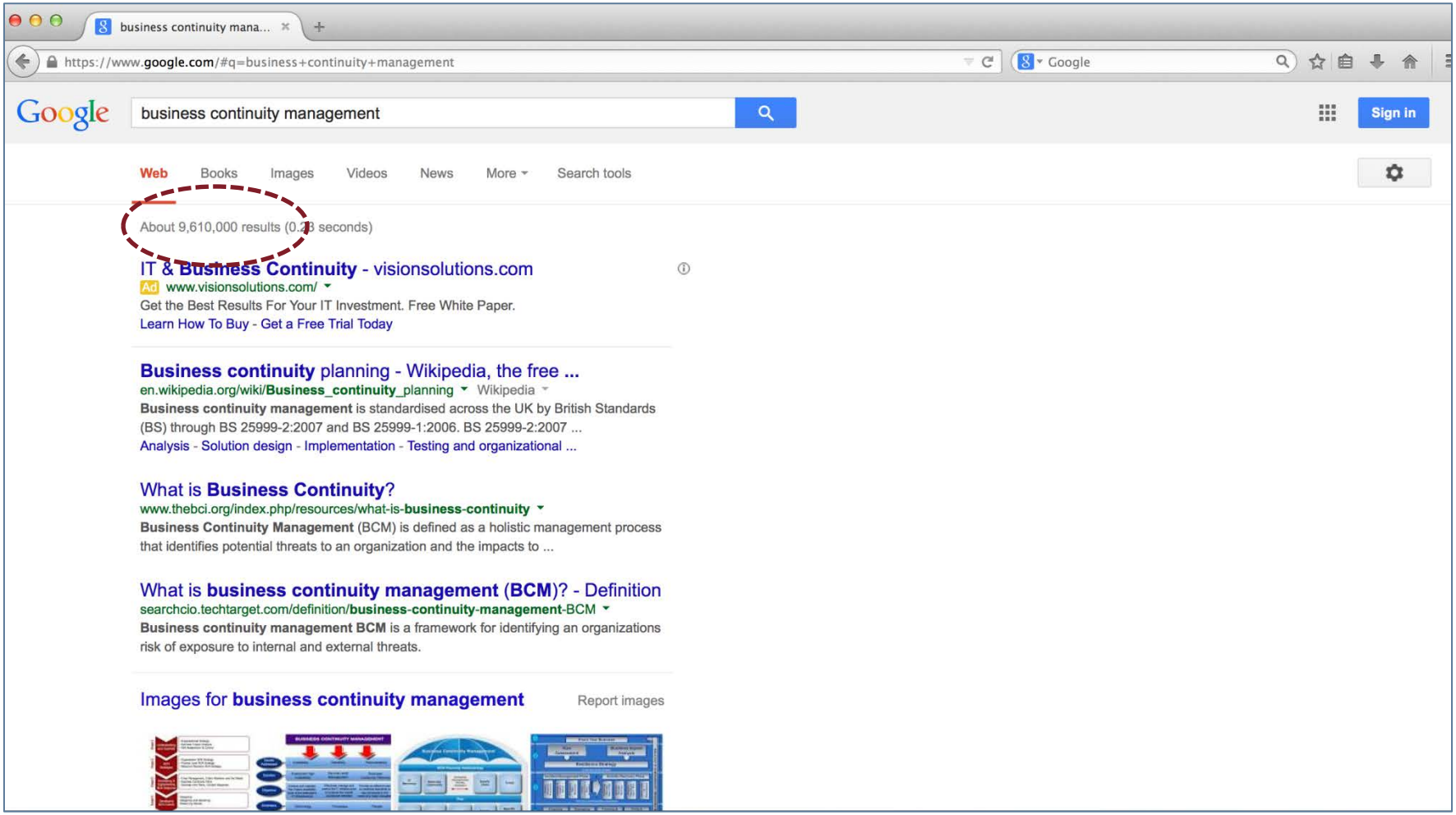
Key Program Development and Evaluation Considerations

protiviti®

Business Continuity Management
- The Basics

A Standard Approach?

A Google search on 'Business Continuity Management' returns 9,610,000 results



protiviti®

Business Continuity is…

…the development of strategies, plans and actions which provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to the enterprise.

1 Crisis Management Plan

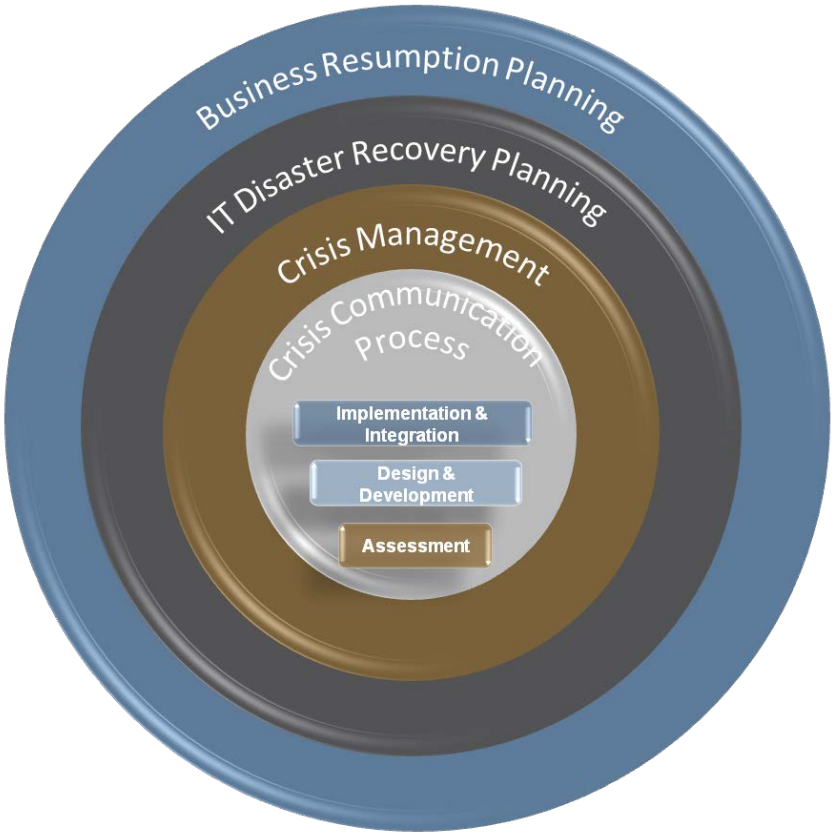
The crisis management plan provides the key communication mechanisms necessary to ensure employee safety, provide initial information and direction, and organize ongoing actions.

2 Disaster Recovery Plan (IT)

The disaster recovery plan typically refers to the plans in place to restore essential Information Technology (IT) systems and applications that enable critical business processes.

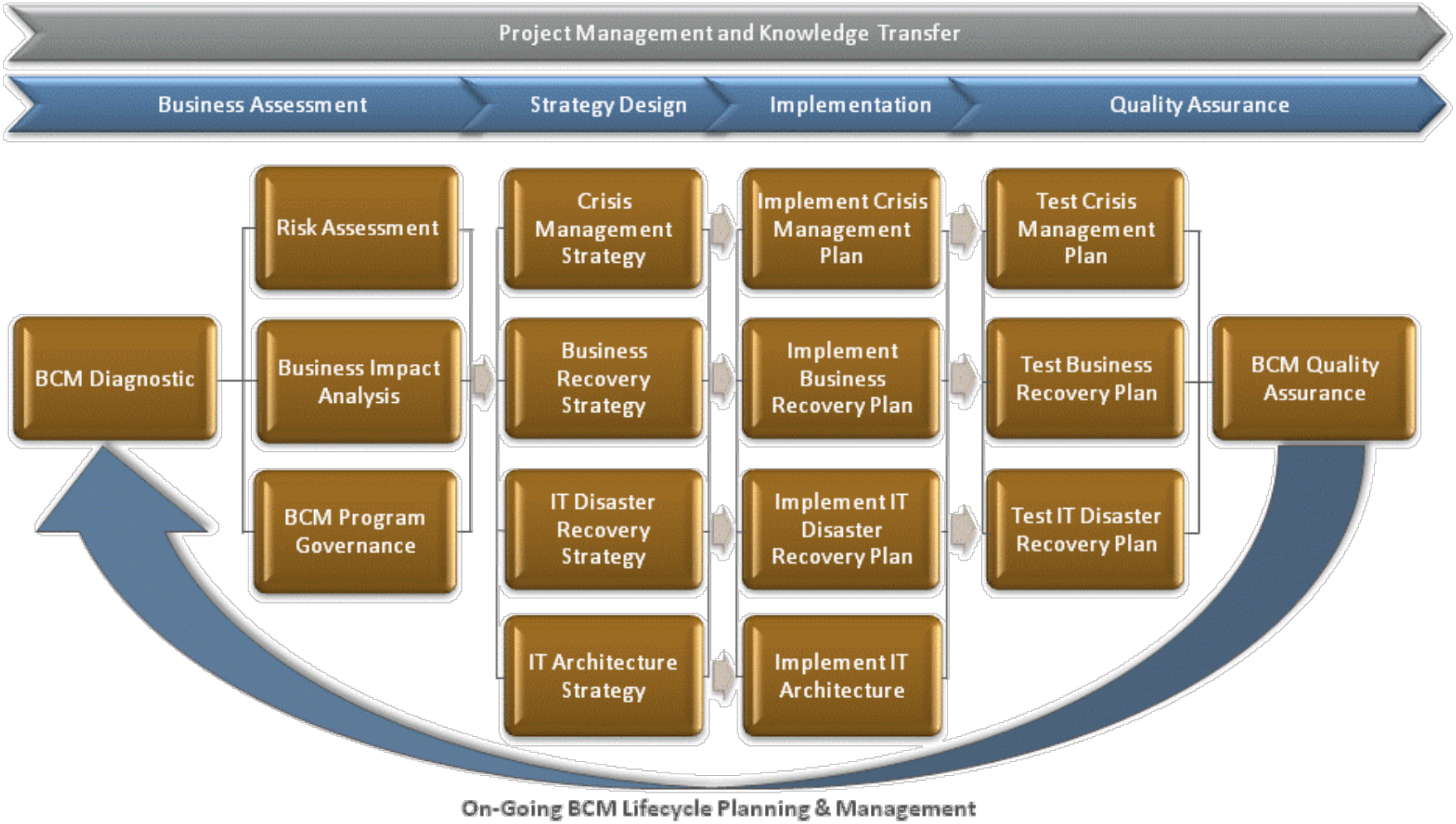
3 Business Resumption Plan

The business resumption plans are specific to each critical business function and articulate the specific steps necessary to enable the respective process (e.g. payroll).



protiviti®

Business Continuity Management Methodology



protiviti®

A Standard Approach?

Another standard approach would be regulation-based and relying on the response to the different regulations for addressing the issue of business continuity

ISO 22301 – Business continuity management systems

ISO 27031 – Guidelines for information and communication technology readiness for business continuity

CobiT v5 – Control Objectives for Info & Tech

FFIEC – Federal Financial Institutions Examination Council

FRB – Federal Reserve Board

HIPAA – Health Ins. Portability and Acct. Act

FERC – Federal Energy Regulatory Comm.

DRII – Disaster Recovery Inst. International

FEMA – Federal Emergency Mgmt Assoc.

NIST – Nat'l Inst. of Standards & Tech

NFPA – Nat'l Fire Protection Agency

	ISO 22301	ISO 27031	CobiT	FFIEC	FRB	HIPAA	FERC	DRII
Institute a process that includes crisis management, business resumption planning and IT disaster recovery	✓	✓	✓	✓				✓
Assess current mitigating controls	✓	✓		✓		✓		✓
Review service level agreements between the organization and its external partners	✓	✓	✓	✓	✓	✓		✓
Define standard methods for documenting response, recovery and restoration procedures, communication plans.	✓	✓	✓	✓			✓	✓
Utilize numerous types of testing approaches	✓	✓	✓	✓				✓
Audit the BCM process on a periodic basis	✓	✓	✓	✓	✓	✓	✓	✓

protiviti®

Continuity Landscape
- What has changed?

Events in the last 6 months…

When would you like to schedule your disaster…?

- ***Flooding in Serbia, Bosnia, Paraguay, Herzegovina & Croatia.***
- ***Measles Outbreak – Somalia***

- ***Earthquake – Mexico/Guatemala (Chiapas State)***
- ***Chikungunya & Dengue Outbreak – El Salvador***

- ***Floods – Cameroon, Serbia, India***
- ***Volcano – Philippines***

April	May	June	July	August	September

- ***Flash Floods and Landslides – Afghanistan***
- ***Volcano Erupt – Ubinas, Peru***
- ***Wild Fire – Chile***

- ***Flooding & Landslides – Philippines.***
- ***Floods – Sri Lanka***

- ***Earthquake – Longtoushan (China)***
- ***Cholera Outbreak – Ghana***

West Africa: Ebola Outbreak - 2014

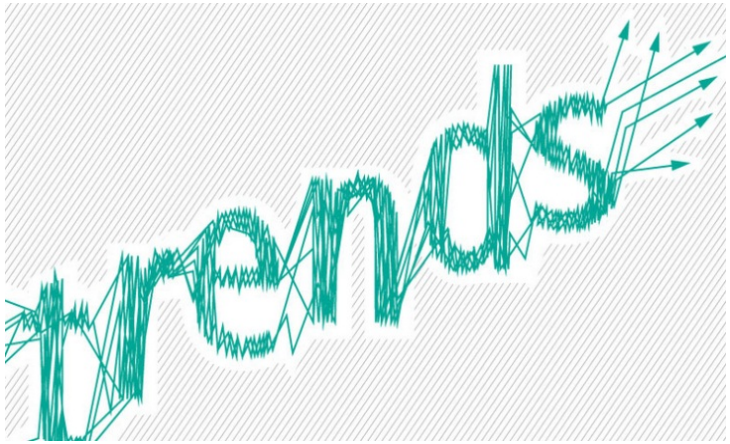
In March 2014, a rapidly evolving outbreak of Ebola hemorrhagic fever started in Guinea. The outbreak subsequently spread to Sierra Leone, Liberia, Nigeria and Senegal. On 1 Aug, WHO and the government of Sierra Leone, Guinea and Liberia launched a joint US$ 100 million response plan as part of an intensified international, regional and national campaign to bring the outbreak under control.

Source: Reliefweb

protiviti®

Business Continuity Planning (BCP) Trends & Considerations

- *Ownership of BCP*
- *“Right-sized” level of documentation*
- *Plan Integration*
- *Technology Considerations*
- *Vendor Management*

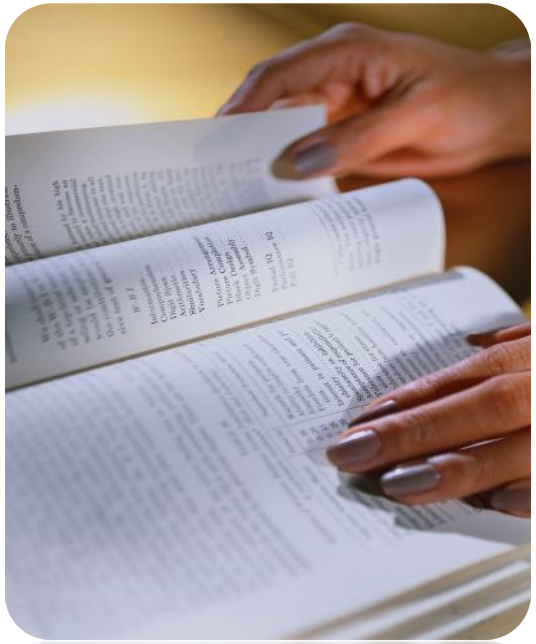


protiviti®

BCP Trends & Considerations

Ownership of BCP

- Clearly defined enterprise authority and responsibility v. custodianship of individual recovery activities
- Visibility and knowledge of the entire business – approached and managed from a business risk perspective
- Too often, BCP lies with the IT department
- Owned by someone with responsibilities for business operations with direct alignment to enterprise risk management

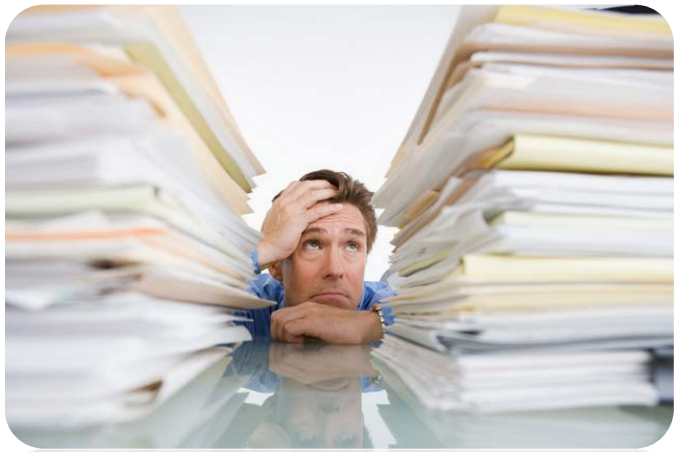


protiviti®

BCP Trends & Considerations

"Right-sized" level of documentation

- Determine the level of knowledge you want to assume is in place when you document your business recovery procedures
- For more technical processes, documentation should enable the activity to be executed by resources not normally engaged in the activity
- Action-oriented and flexible
- Document decision "triggers" for executive personnel
- Provide for viable operation of critical functions



protiviti®

BCP Trends & Considerations

Plan Integration

- Includes Crisis Management, Business Resumption, and IT Disaster Recovery
- Requires linkage and alignment between components of the plan through a comprehensive and consistent definition of “recovery strategy”
- Consistency in format and approach facilitates plan integration and execution

protiviti®

BCP Trends & Considerations

Technology Considerations

- Changes in technology architecture should be incorporated into the recovery strategy and subsequent recovery plans
  - Cloud architecture may enable alternative IT environments that streamline recovery plans and reduce reliance on traditional recovery site models.
- "XaaS" models need to be understood and defined in the business analysis to ensure recovery plans are viable
- Utilize cloud services as appropriate to house and communicate recovery plans
- Internal and external communication can be facilitated through "social media" channels

protiviti®

BCP Trends & Considerations

Vendor Management

- Define 3rd parties that are critical to business operation during the impact analysis and risk assessment
- Implement a vendor management program to:
  - Document external party roles, activities and related controls
  - Align recovery objectives
  - Validate recovery capabilities

protiviti®

Key Lessons Learned

Communication

- ***Communication is critical to effective disaster response***
  - Review the communication plan
  - Determine how employees will be provided with information when land lines and cell towers are down or overloaded
  - Include an employee call-in line to a location remote from the disaster and test the operation of the call-in process
  - Pre-determine employee meeting points
  - Define how you will communicate with stakeholders when all communication systems are down
- ***A good plan includes frequent and scheduled status updates to the media and employees***
  - Designated media spokespeople should be adequately trained

Source: www.disastersrus.org/katrina/ACP_Hurricane_Katrina_Observations.pdf

protiviti®

Decision Hierarchy

- ***Avoid delay in critical decisions with a defined decision hierarchy***
  - A well defined command and control structure is essential to effective decision making
  - Define command and control and give them the authority to act
  - Emphasize that businesses, families, and individuals must be decisive and personally responsible when responding to emergencies

Source: www.disastersrus.org/katrina/ACP_Hurricane_Katrina_Observations.pdf

protiviti®

Its Not Just IT!

- ***Not an "IT only" venture. Distinct teams are needed for system recovery and business resumption:***
  - The recovery of the network or telecommunications requires:
    - Key members of the IT department
    - Any vendors servicing the company
  - To resume operation of processes requires:
    - Thoroughly examined business processes
    - Effective prioritization of what needs to be restored first and which customers need service first

protiviti®

Keep Your Plans Up-to-Date

- ***Create an iterative process for plan maintenance.***
  - When writing and revising plans, involve subject matter experts from each area to ask the relevant questions:
    - What resources are needed?
    - Who initiates and approves resources?
  - Emphasize that business continuity must be an organization-wide effort
    - Come together on a periodic basis to ensure the business continuity plan is up to date and accurately reflects the risk profile of the organization
  - Develop a “right-sized” plan - Less emphasis on the volume of documentation and more emphasis on training employees

Source: www.disastersrus.org/katrina/ACP_Hurricane_Katrina_Observations.pdf

protiviti®

Business Continuity Management – Key Program Development and Evaluation Considerations

Key BCM Program Components

A BCM development framework has six key program elements that reflect the key elements of strategic and tactical planning. These program elements include:

Executive Management Support & Sponsorship	**Executive Management Support & Sponsorship** addresses BCM policy and standards development, executive oversight of risk identification, prioritization, program funding, and operational accountability for strategic and tactical planning.
Risk Assessment & Business Impact Analysis	**Risk Assessment & Business Impact Analysis** involves definition of risk management objectives that represent business driven requirements; also determines process criticalities and recovery priorities.
Business Continuity Strategy Design	**Business Continuity Strategy** is driven by business requirements and defines the methods by which the organization meets established recovery objectives; also ensures proper alignment between business functions, core IT assets and other business dependencies.
Plan Development & Strategy Implementation	**Plan Development & Strategy Implementation** involves implementing plans and procedures that enable strategy execution, and ensure a viable and workable operational recovery capability.
Training & Awareness	**Training & Awareness** reviews current awareness and training methods that will prepare key management and staff for responding to disruptive events.
Testing & Plan Maintenance	**Testing & Plan Maintenance** involves validating existing capabilities to respond to disruptive events, including exercising the ability to relocate and recover operations to designated alternate operating facilities.

protiviti®

Executive Management Support & Sponsorship

Effective Governance is enabled by BCM policy and standards, executive oversight of risk identification and prioritization, necessary funding, and clear operational accountabilities.

Objectives	• Confirm that an oversight process exists that aligns strategic business objectives with BCM risk management investments. • Ensure that BCM program purpose, scope, objectives, and fundamental operational responsibilities are clearly defined.
Leading Practices	• BCM policy outlines the purpose, scope, objectives and fundamental management responsibilities for developing an operational program. • Standards outline enterprise requirements for strategic and tactical BCM planning (i.e., addressing people, process and technology requirements). • BCM steering committee is established, either as a standalone entity or reporting to an executive-level risk management committee, to oversee initiatives. • Membership of the BCM steering committee reflects broad executive representation from finance, operations, administration, legal, information systems, human resources and other key business areas. • A budget is established centrally and is approved by the BCM steering committee to address risk management and operational recovery requirements. • Operational responsibilities for BCM are clearly defined, assigned and acknowledged.

protiviti®

Risk Assessment & Business Impact Analysis (BIA)

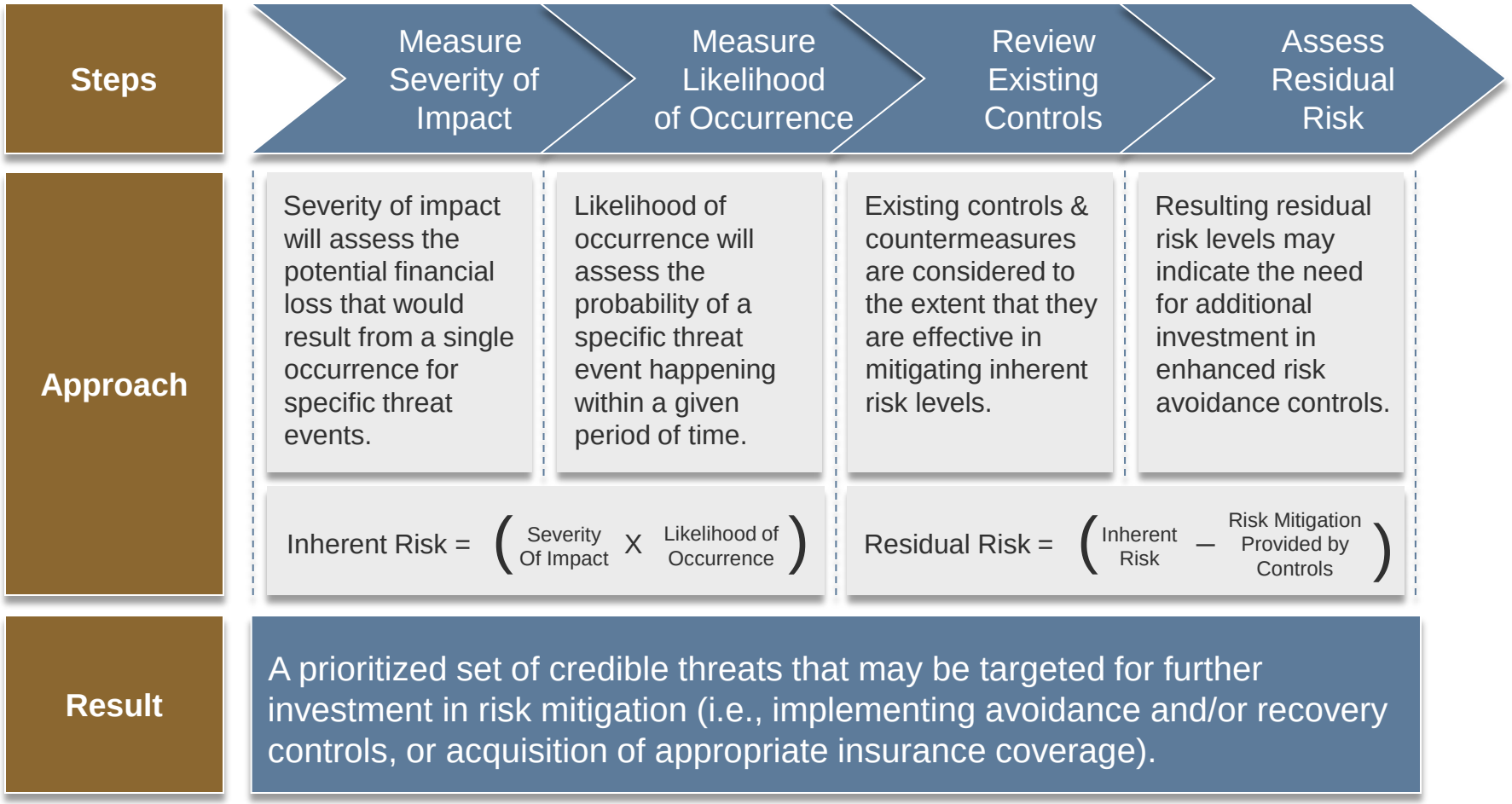
Risk Assessments and BIAs drive the definition and continued enhancement and viability of recovery strategies.

Objectives	• Confirm that credible threats are identified and prioritized for risk mitigation. • Validate that legal, regulatory, financial and operational impacts of a disruption to operations have been analyzed and recovery objectives have been appropriately determined.
Leading Practices	• Risk Assessment investigates inherent risk levels based on specific and credible threats by measuring both likelihood and severity of event occurrence. • Risk Assessment reviews mitigating controls and countermeasures applicable to each threat and estimates residual risk levels. • Risk Assessment defines a "geographic scope of disruption" as a guideline for locating alternate facilities to ensure that primary and backup locations are not simultaneously disrupted by a common threat event. • BIA assesses financial, operational and regulatory/legal impacts and management tolerances for disruption resulting from a “worst case” scenario. • BIA analytically defines recovery objectives based on measured business impacts and management tolerances for disruption. These objectives should include both requirements for recovery times and data recovery. • BIA establishes minimum operating requirements that must be restored to satisfy business needs.

protiviti®

Risk Assessment Drives Avoidance Solutions

Risk assessment in avoidance requires measurement of residual risk relative to credible threats by considering inherent risk, severity of impact, likelihood, and existing controls.



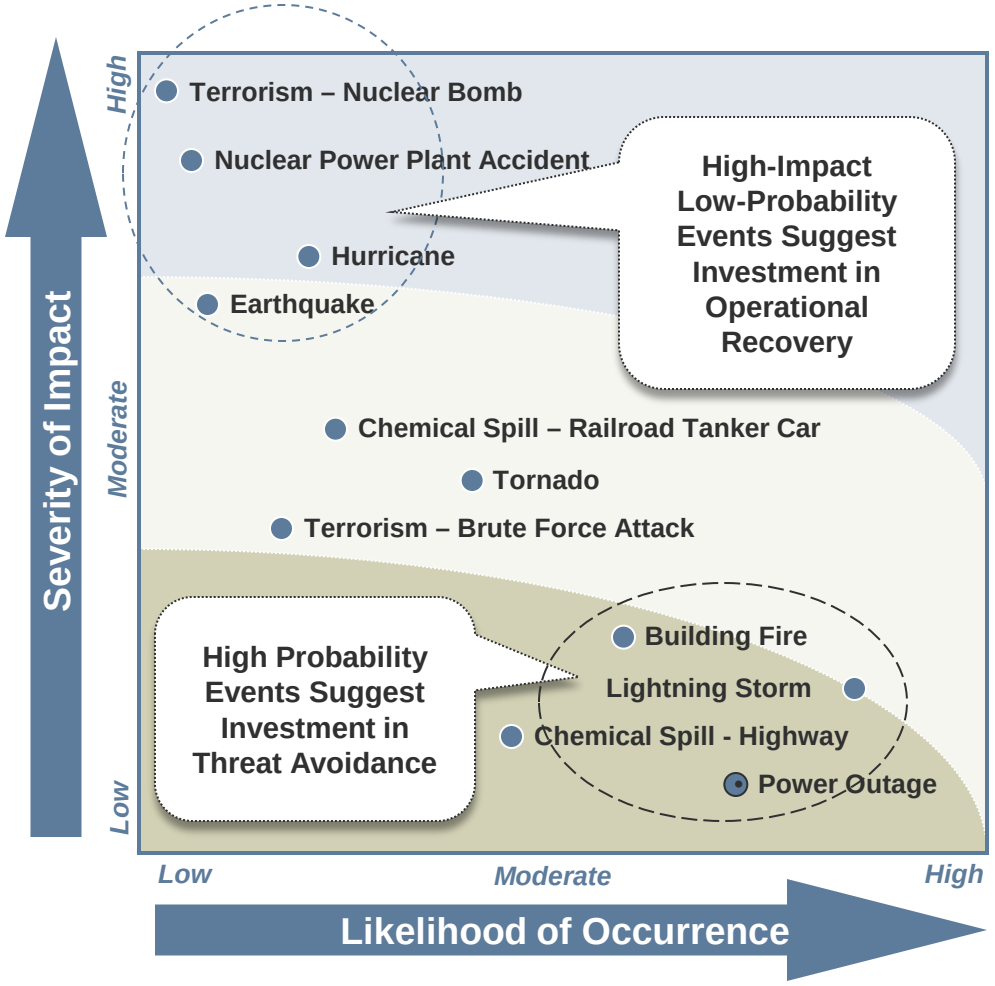
protiviti®

Measuring Risk in BCM

Risk assessment compares likelihood and severity of threat events against current risk mitigation controls to determine residual risk.

Interpretation of Risk Analysis

- Inherent risk is measured by giving consideration to both the severity and likelihood of disruptive events.
- Residual risk considers the mitigating affects of existing or enhanced avoidance controls.
- Operational recovery controls, as opposed to avoidance, are more often implemented to manage high-impact low-probability events.
- Threat events having high residual risk should be considered priorities for risk mitigation investment
- Geographic scope of disruption should be considered when identifying alternate recovery facilities for operational recovery.

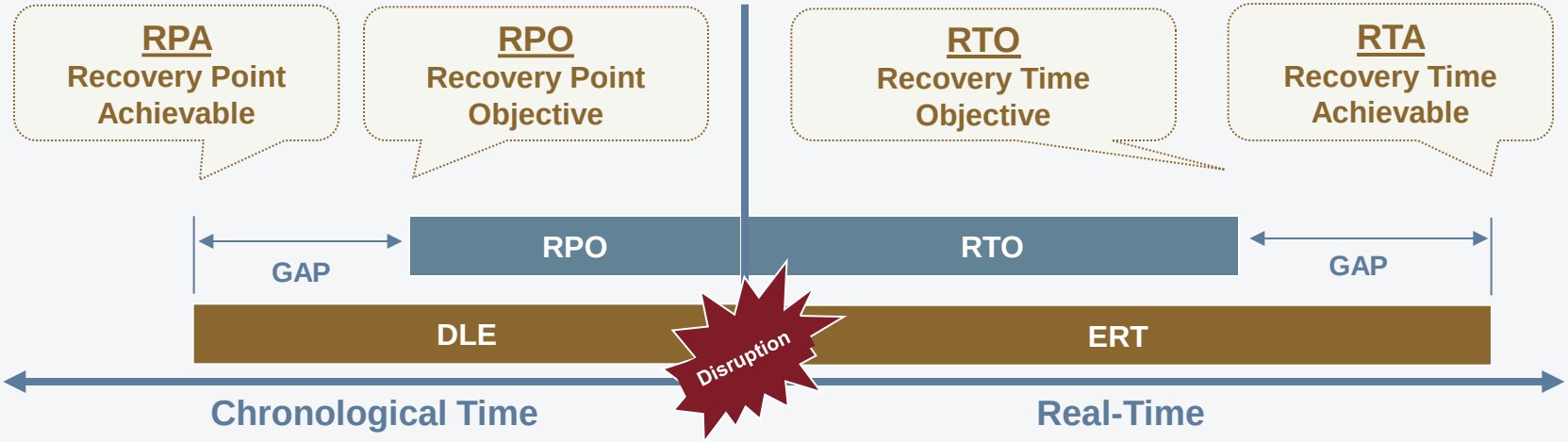


protiviti®

Business Impact Analysis – Results

The results of a BIA should provide the organization with recovery objectives. Specifically, the BIA should address:

- Recovery Time Objectives (RTO) – period of time that systems and functions need to be recovered after a disruption (basis for recovery strategies).
- Recovery Point Objectives (RPO) – point in time in which systems and data must be recovered after a disruption (basis for backup strategies).



protiviti®

Business Continuity Strategy

Business Continuity Strategy defines the methods by which the organization meets established recovery objectives.

Objectives	• Validate general BCM risk management strategy balances investment between avoidance, recovery, risk transfer and acceptance. • Confirm alignment between established recovery objectives and strategies addressing both business and IT recovery.

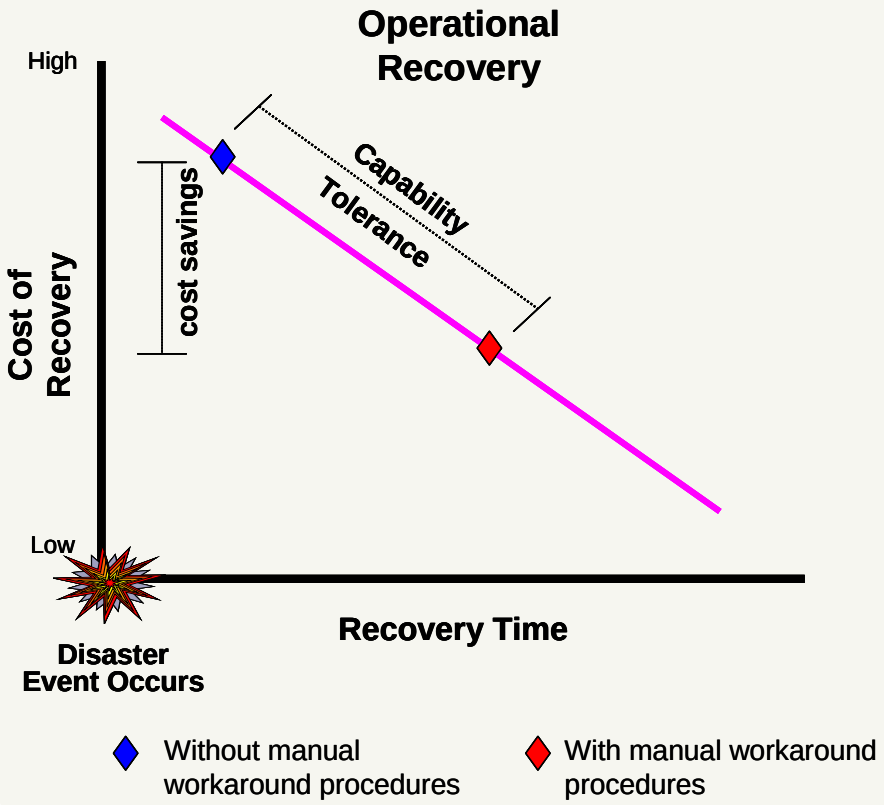
Leading Practices	• Strategy considers the likelihood and severity of disruptive threats when considering how to balance investments between avoidance and recovery.
	• Strategies have been defined to respond to events and recover critical business functions and IT assets.
	• Recovery strategies are viable and executable.
	• Strategy development addresses:
	  - Resource requirements
	  - Gap analysis of resources
	  - Consideration of multiple options
	  - Cost and benefit analysis
	• Continuity capabilities of vendors and suppliers are evaluated on a regular basis.

protiviti®

Business Continuity Strategy

What strategies should be considered?

- Alternative site or business facility
- Alternate source of product
- Third-party service providers/outsourcers
- Distributed processing
- Alternative communications
- Manual procedures
- Reciprocal agreements
- Defer action
- Do nothing

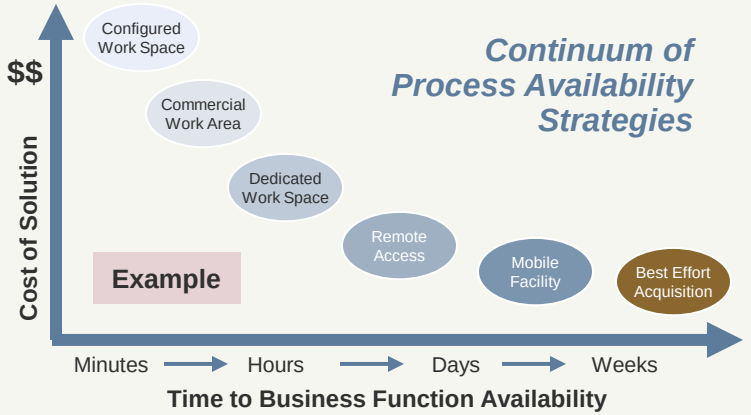


protiviti®

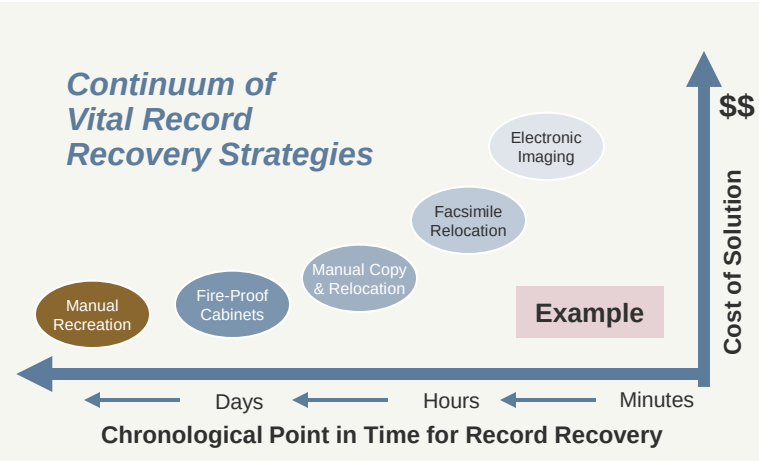
Business Recovery Objectives Drive Strategy

Strategy should combine appropriate alternatives for both availability and data/record recovery, driven by recovery objectives, to achieve a cost-effective recovery solution.

- The Recovery Time Objectives (RTO) should be used as a guideline for the selection of both process and application availability strategy.
- Implementation cost for availability strategies will typically increase as Recovery Time Achievable (RTA) is reduced.



- The Recovery Point Objective (RPO) should be used as a guideline for the selection of both vital record and electronic data recovery strategy.
- Implementation cost for data/record recovery strategies will typically increase as Recovery Point Achievable (RPA) is reduced.



protiviti®

Plan Development & Strategy Implementation

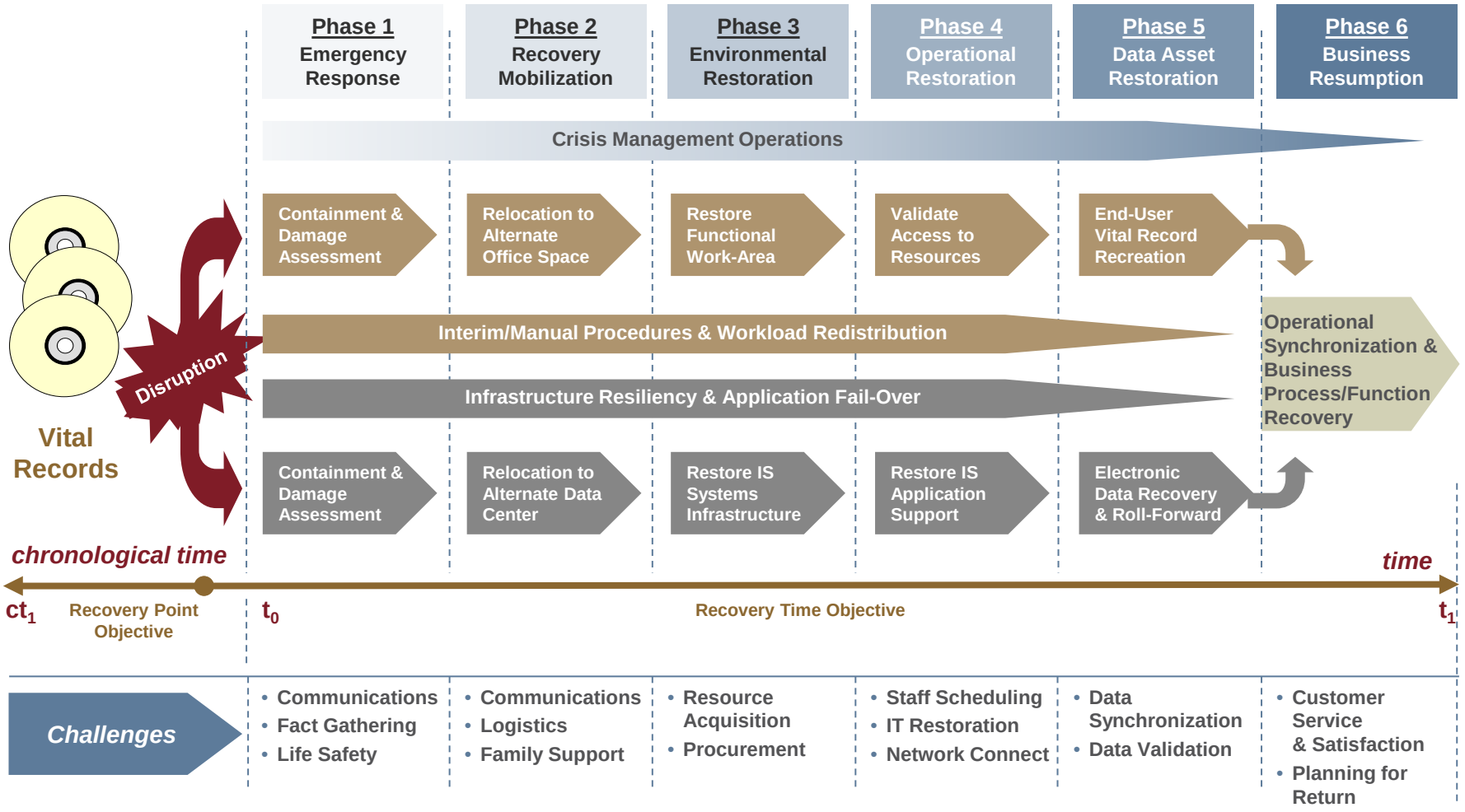
Plan Development and Strategy Implementation involves putting solutions in place that enable strategy execution, and ensure a viable and workable recovery capability.

Objectives	• Confirm the development and implementation of Crisis Management Plans, Business Recovery Plans and IT Disaster Recovery Plans. • Confirm availability of standardized documentation consisting of response and recovery procedures.
Leading Practices	• All major plan components are addressed including: response and recovery team responsibilities; facility and resource requirements; recovery procedures. • A Crisis Management Team comprised of business leaders has been identified and trained. • Procedures for communicating with employees, vendors, regulators, and business partners are identified and are actionable. • IT disaster recovery plans address technology infrastructure, including the recovery of critical IT applications and network assets (voice and data). • Business resumption plans address key business processes, including the recovery of other non-technical dependencies. • The end result should be integrated, recovery plan documentation that has been properly distributed and contains the necessary detail to recover from an interruption within the pre-defined recovery time objective.

protiviti®

Business Continuity Execution Timeline

A business continuity strategy is executed in a sequence of action-oriented recovery phases.



protiviti®

Training & Awareness

Training & awareness reviews current methods that will prepare key management and staff for responding to disruptive events and recovering and restoring operations.

Objectives	• Verify that personnel are properly trained to execute plans. • Verify that coordinators have proper skills and qualifications in BCM planning. • Verify that operations staff have appropriate emergency response training.
Leading Practices	• Personnel receive periodic awareness training in emergency communications and management escalation procedures. • Designated recovery coordinators are encouraged to obtain and retain formal BCM certification from credible BCM industry associations. • Recovery team members participate in scheduled test exercises to better understand their responsibilities for recovery execution. • Staff participation in BCM industry conferences is encouraged. • Industries that manufacture or use hazardous materials in production may have more extensive training requirements based on federal and state laws.

protiviti®

Testing & Plan Maintenance

Testing and Plan Maintenance involves validating existing capabilities to respond to disruptions by exercising the ability to recover and restore operations.

Objectives	• Confirm test schedule and lifecycle planning approach is comprehensive and effective in validating execution capabilities. • Verify that test execution issues are identified, properly documented and subsequently assigned to appropriate management for resolution. • Verify a plan maintenance schedule exists and BCM program components are regularly updated.
Leading Practices	• Crisis management, business resumption, and IT disaster recovery plans are fully and satisfactorily tested. • Testing lifecycle requirements address pre-test planning, test execution and post-test review. • Complimentary alternative methods of testing are employed (e.g., alternate site testing, table-top exercises, emergency communications testing). • Recovery test scenarios mimic actual recovery processes (i.e., testing as you would recover) and end-users participate in testing. • Testing issues are resolved in a timely manner consistent with the level of exposure they represent. • BCM program components are updated after each test and/or as needed based on changes within the company.

protiviti®

Key Points to Remember

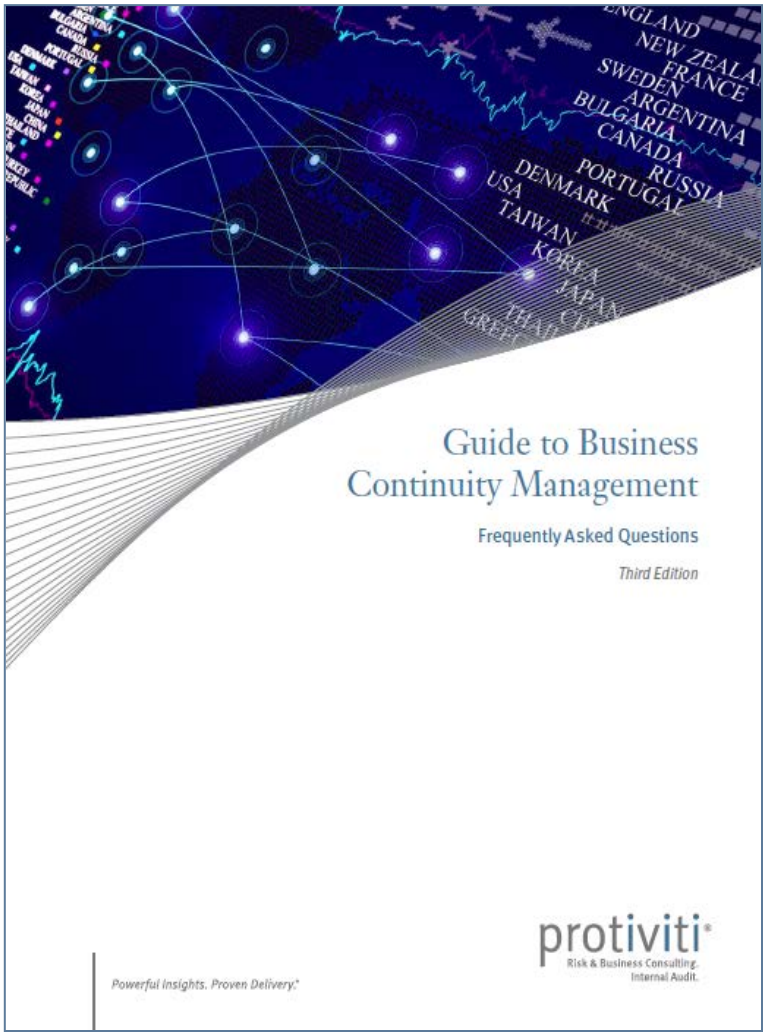
When developing a BCM program you should keep in mind the following:

- Executive Management Support and Sponsorship, if properly implemented, will make the difference between a ‘project’ and an effective business continuity program.
- Alignment of business goals with recovery strategy and executable capabilities requires periodic reassessment.
- Do not assume that the expectations of business executives regarding recovery and resumption align with IT management.
- Allocation of risk capital should reflect requirements for avoidance and recovery execution solutions.

protiviti®

Resources

Protiviti's Updated Business Continuity FAQ



Updates Include:

- Regulatory Requirements
- Industry Considerations
- Lessons Learned
- Social Media
- New Trends & Practices

Click on this link to download:
www.protiviti.com/bcm

protiviti®

Questions and Answers

Jon Bronson

Managing Director, Los Angeles, California

protiviti® Risk & Business Consulting. Internal Audit.

Phone: +1 213-327-1308

Email: jonathan.bronson@protiviti.com

Powerful Insights. Proven Delivery.®

Trey MacDonald

Director, Atlanta, Georgia

protiviti® Risk & Business Consulting. Internal Audit.

Phone: +1 404-926-4330

Email: trey.macdonald@protiviti.com

Powerful Insights. Proven Delivery.®

protiviti®

Powerful Insights.
Proven Delivery.®