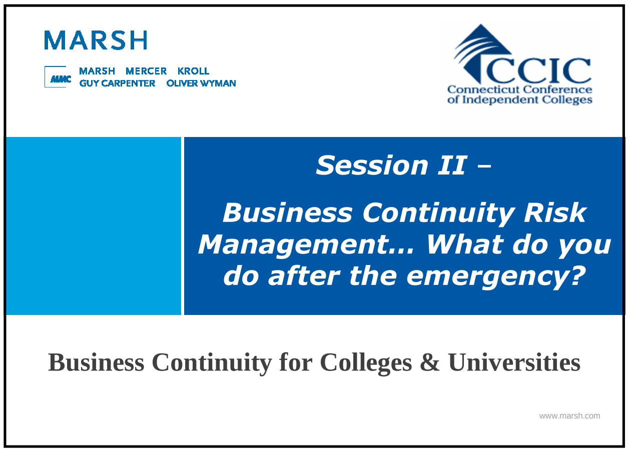


MARSH

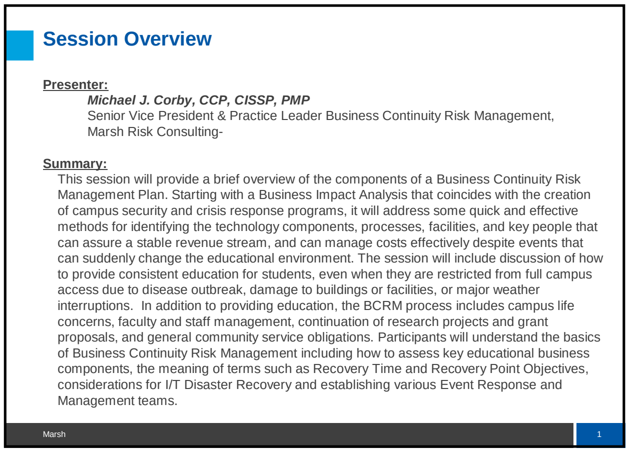
MMC MARSH MERCER KROLL GUY CARPENTER OLIVER WYMAN

CCIC Connecticut Conference of Independent Colleges

Session II – Business Continuity Risk Management… What do you do after the emergency?

Business Continuity for Colleges & Universities

www.marsh.com



Session Overview

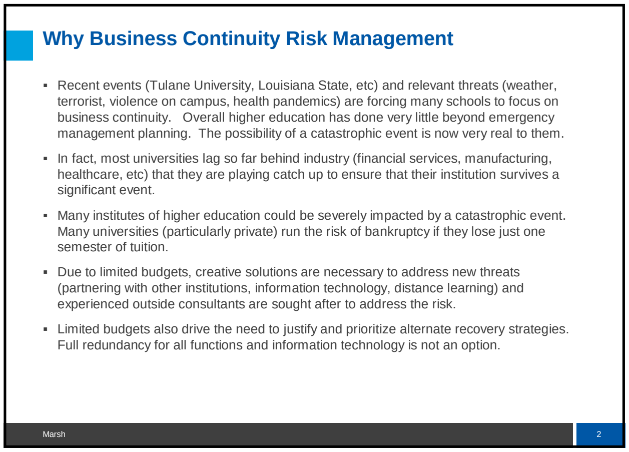
Presenter:

Michael J. Corby, CCP, CISSP, PMP
Senior Vice President & Practice Leader Business Continuity Risk Management,
Marsh Risk Consulting-

Summary:

This session will provide a brief overview of the components of a Business Continuity Risk Management Plan. Starting with a Business Impact Analysis that coincides with the creation of campus security and crisis response programs, it will address some quick and effective methods for identifying the technology components, processes, facilities, and key people that can assure a stable revenue stream, and can manage costs effectively despite events that can suddenly change the educational environment. The session will include discussion of how to provide consistent education for students, even when they are restricted from full campus access due to disease outbreak, damage to buildings or facilities, or major weather interruptions. In addition to providing education, the BCRM process includes campus life concerns, faculty and staff management, continuation of research projects and grant proposals, and general community service obligations. Participants will understand the basics of Business Continuity Risk Management including how to assess key educational business components, the meaning of terms such as Recovery Time and Recovery Point Objectives, considerations for I/T Disaster Recovery and establishing various Event Response and Management teams.

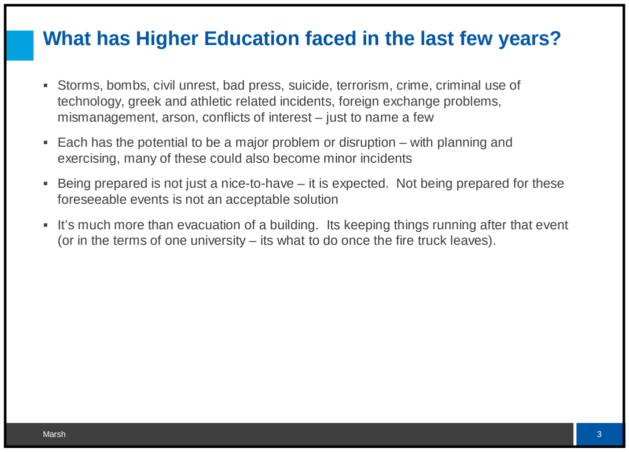
Marsh 1



Why Business Continuity Risk Management

- Recent events (Tulane University, Louisiana State, etc) and relevant threats (weather, terrorist, violence on campus, health pandemics) are forcing many schools to focus on business continuity. Overall higher education has done very little beyond emergency management planning. The possibility of a catastrophic event is now very real to them.
- In fact, most universities lag so far behind industry (financial services, manufacturing, healthcare, etc) that they are playing catch up to ensure that their institution survives a significant event.
- Many institutes of higher education could be severely impacted by a catastrophic event. Many universities (particularly private) run the risk of bankruptcy if they lose just one semester of tuition.
- Due to limited budgets, creative solutions are necessary to address new threats (partnering with other institutions, information technology, distance learning) and experienced outside consultants are sought after to address the risk.
- Limited budgets also drive the need to justify and prioritize alternate recovery strategies. Full redundancy for all functions and information technology is not an option.

Marsh 2



What has Higher Education faced in the last few years?

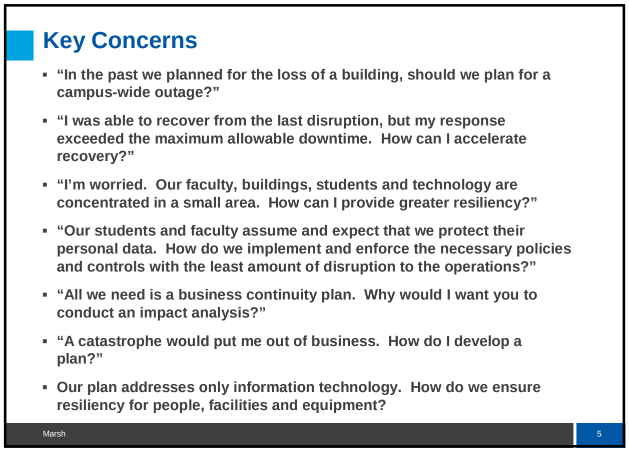
- Storms, bombs, civil unrest, bad press, suicide, terrorism, crime, criminal use of technology, greek and athletic related incidents, foreign exchange problems, mismanagement, arson, conflicts of interest – just to name a few
- Each has the potential to be a major problem or disruption – with planning and exercising, many of these could also become minor incidents
- Being prepared is not just a nice-to-have – it is expected. Not being prepared for these foreseeable events is not an acceptable solution
- It's much more than evacuation of a building. Its keeping things running after that event (or in the terms of one university – its what to do once the fire truck leaves).

Marsh 3

Are you Prepared to Respond?

What would be the impact on your Institution?

Marsh 4



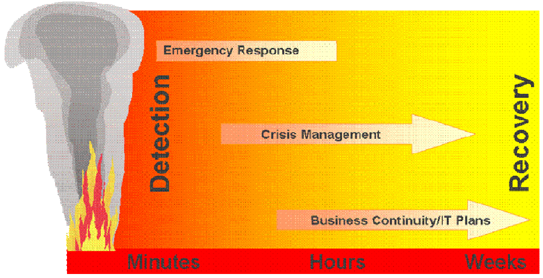
Key Concerns

- **"In the past we planned for the loss of a building, should we plan for a campus-wide outage?"**
- **"I was able to recover from the last disruption, but my response exceeded the maximum allowable downtime. How can I accelerate recovery?"**
- **"I'm worried. Our faculty, buildings, students and technology are concentrated in a small area. How can I provide greater resiliency?"**
- **"Our students and faculty assume and expect that we protect their personal data. How do we implement and enforce the necessary policies and controls with the least amount of disruption to the operations?"**
- **"All we need is a business continuity plan. Why would I want you to conduct an impact analysis?"**
- **"A catastrophe would put me out of business. How do I develop a plan?"**
- **Our plan addresses only information technology. How do we ensure resiliency for people, facilities and equipment?**

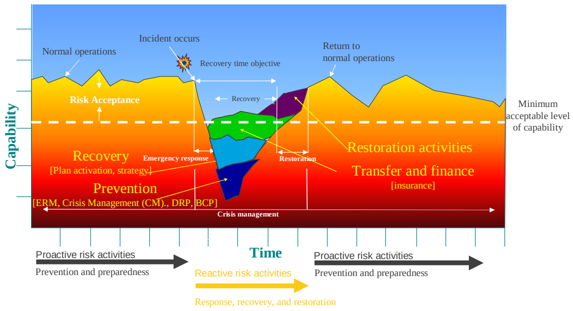
Marsh 5

Business Continuity Program

Three Important Components

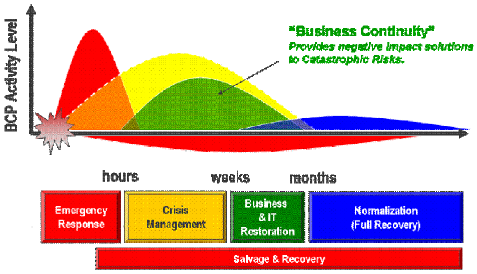


Graphical Representation of Emergency Response Elements



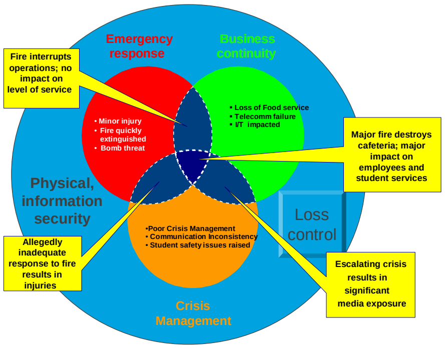
Putting Response Protocols in Perspective

The Intensity Levels of the Individual Response Protocols



Purpose:
Why are we concerned about
Business Continuity?

An Integrated Program



Fire interrupts operations; no impact on level of service

Major fire destroys cafeteria; major impact on employees and student services

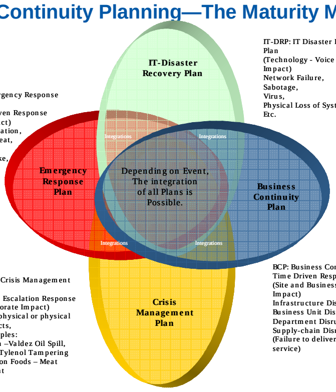
Allegedly inadequate response to fire results in injuries

Escalating crisis results in significant media exposure

Business Continuity Planning—The Maturity Model

ERP: Emergency Response Plan
Event Driven Response
(Site Impact)
Contamination,
Bomb-threat,
Fire,
Earthquake,
Wind,
Etc.

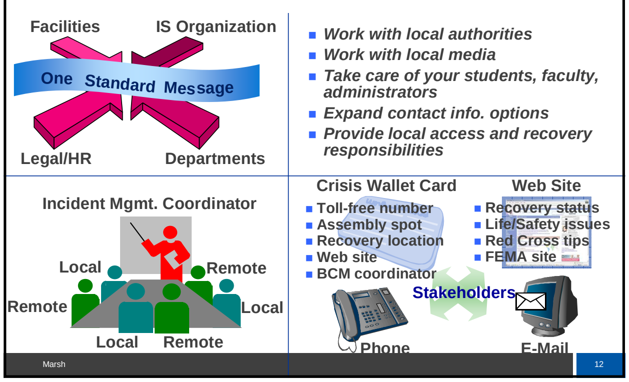
IT-DRP: IT Disaster Recovery Plan
(Technology - Voice & Data Impact)
Network Failure,
Sabotage,
Virus,
Physical Loss of Systems,
Etc.



CMP: Crisis Management Plan
Event Escalation Response
(Corporate Impact)
Non-physical or physical impacts,
Examples:
Exxon –Valdez Oil Spill,
J&J – Tylenol Tampering
Hudson Foods – Meat Threat

BCP: Business Continuity
Time Driven Response
(Site and Business and Image Impact)
Infrastructure Disruptions,
Business Unit Disruptions,
Department Disruptions
Supply-chain Disruptions
(Failure to deliver product or service)

Incident Management Communications



- *Work with local authorities*
- *Work with local media*
- *Take care of your students, faculty, administrators*
- *Expand contact info. options*
- *Provide local access and recovery responsibilities*

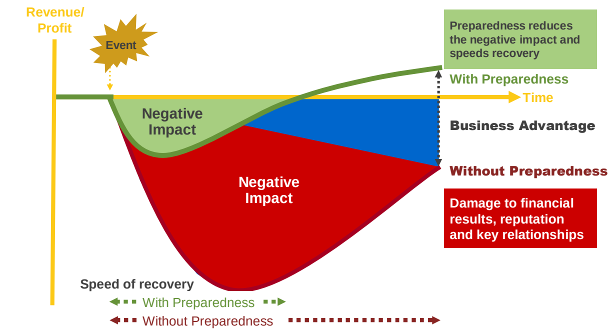
Crisis Wallet Card

- Toll-free number
- Assembly spot
- Recovery location
- Web site
- BCM coordinator

Web Site

- Recovery status
- Life/Safety issues
- Red Cross tips
- FEMA site

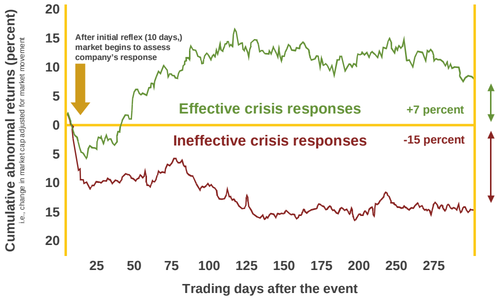
The Impact on Finances (Revenue Loss)



Preparedness reduces the negative impact and speeds recovery

Damage to financial results, reputation and key relationships

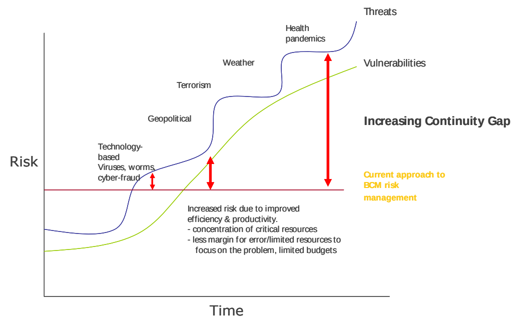
The Impact on Reputation (Shareholder Value)



Source: "The Impact of Catastrophes on Shareholder Value," Rory F. Knight & Deborah J. Pretty, Templeton College, University of Oxford, p. 3.

The Gap is Widening

Staying the same means going backwards



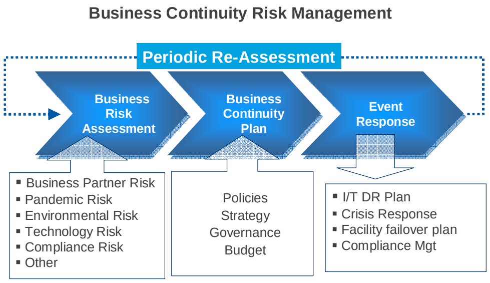
Increased risk due to improved efficiency & productivity.
- concentration of critical resources
- less margin for error/limited resources to focus on the problem, limited budgets

Definition:
What is Business Continuity Risk Management?

Business Continuity Programs

- An organization's ability to foresee, prevent, respond, and manage adverse risk and events
- A seamless solution so employees can focus on delivering services
- An approach that is:
  - Risk-aligned with the organizational goals
  - Balanced with both corporate needs and service locations
  - Standards based and validated
  - Program planning for ongoing preparedness
  - Sustainable through a maturity-model
  - Potentially self-funding

Business Continuity Solutions are designed to focus on existing plans…

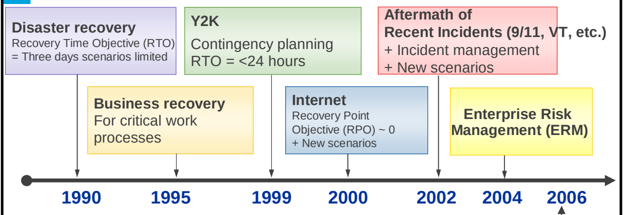


- Business Partner Risk
- Pandemic Risk
- Environmental Risk
- Technology Risk
- Compliance Risk
- Other

Policies
Strategy
Governance
Budget

- I/T DR Plan
- Crisis Response
- Facility failover plan
- Compliance Mgt

Business Continuity Management Evolution

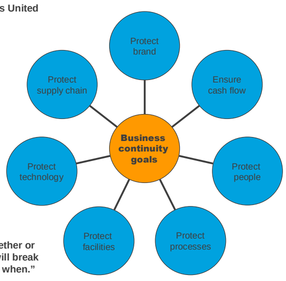

Disaster recovery
Recovery Time Objective (RTO) = Three days scenarios limited
Y2K
Contingency planning RTO = <24 hours
Aftermath of Recent Incidents (9/11, VT, etc.)
+ Incident management
+ New scenarios
Business recovery For critical work processes
Internet
Recovery Point Objective (RPO) ~ 0
+ New scenarios
Enterprise Risk Management (ERM)
1990
1995
1999
2000
2002
2004
2006

- Reduce and document incident costs
- Integrate across business units
- Scale from minor incidents to large events
- Work with emergency services
- Meet safety & regulatory requirements
- Integrate with enterprise risk management
- Maximize insurance returns
- Manage nondisaster Information Technology (IT) incidents

High availability and incident management

2008 - Business Continuity is all About Building a Dependable Revenue Stream

"E.coli outbreak hits United States."



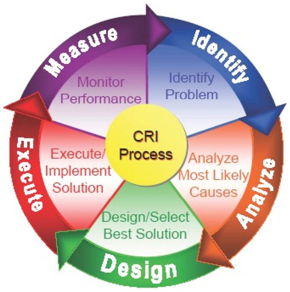
"Americans fear not getting paid after disaster."

"41 percent of businesses impacted by a disaster in New York said it cost them more than $100,000 a day"

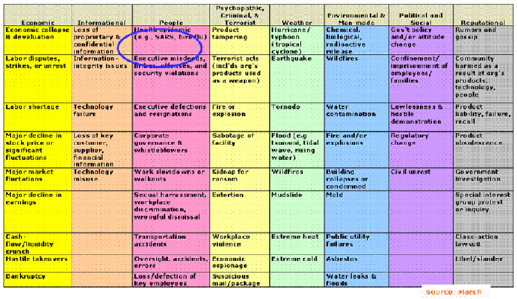
"It is not a question whether or not the next Pandemic will break out, it is just a question when."

Source: globalcontinuity.com

The Methodology is a Cycle of Continuous Improvement



A threat-based catastrophic planning approach has shown to be inefficient and difficult to achieve.



Economic	Informational	People	Psychopathic, Criminal, & Terrorist	Weather	Environmental & Man-made	Political and Social	Reputational
Economic collapse & devaluation	Loss of proprietary & confidential information	Health epidemic (e.g., SARS, bird flu)	Product tampering	Hurricane/ typhoon (tropical cyclone)	Chemical, biological, radioactive release	Gov't policy and/or attitude change	Rumors and gossip
Labor disputes, strikes, or unrest	Information-integrity issues	Executive misdeeds, bribes, offenses, and security violations	Terrorist acts (incl'ds org's products used as a weapon)	Earthquake	Wildfires	Confinement/ imprisonment of employees/ families	Community harmed as a result of org's products, technology, people
Labor shortage	Technology failure	Executive defections and resignations	Fire or explosion	Tornado	Water contamination	Lawlessness & hostile demonstration	Product liability, failure, recall
Major decline in stock price or significant fluctuations	Loss of key customer, supplier, financial information	Corporate governance & whistleblowers	Sabotage of facility	Flood (e.g tsunami, tidal wave, rising water)	Fire and/or explosions	Regulatory change	Product obsolescence
Major market fluctations	Technology misuse	Work slowdowns or walkouts	Kidnap for ransom	Wildfires	Building collapses or condemned	Civil unrest	Government investigation
Major decline in earnings		Sexual harrassment, workplace discrimination, wrongful dismissal	Extortion	Mudslide	Mold		Special interest group protest or inquiry
Cash-flow/liquidity crunch		Transportation accidents	Workplace violence	Extreme heat	Public utility failures		Class-action lawsuit
Hostile takeovers		Oversight, accidents, errors	Economic espionage	Extreme cold	Asbestos		Libel/slander
Bankruptcy		Loss/defection of key employees	Suspicious mail/package		Water leaks & floods		

Source: Marsh

Best Practice: an "IMPACT"- (versus a threat) - based approach

Assume the resource is either unavailable for >30 days and/or, worst case, destroyed.

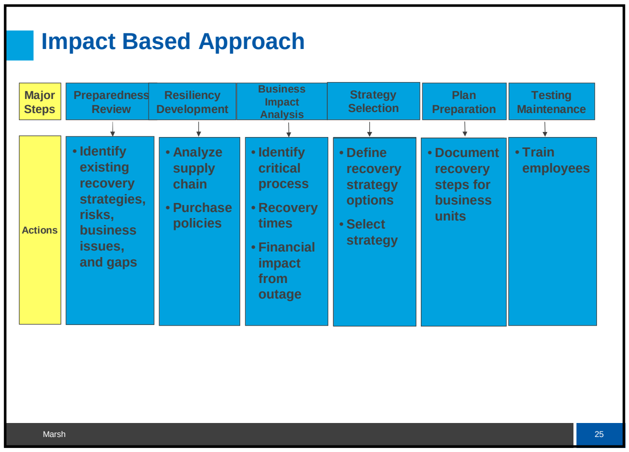
Resources Impacted

Assumption	People (students, faculty, administrators contractors, support functions)	Technology & Processing (data processing networks)	Physical (facilities, libraries, materials, equipment)	Relationships & Interdependencies
Unavailable and/or inaccessible for an extended period of time	Pandemic – 40% of internal and 40% of external work force Three orders of succession	Inability to gain access to service/ install software.	Building quarantined, civil unrest damage to facility and vital records Inability to gain access to equipment for service	Sole source, critical infrastructure, supplier severely affected
Destroyed or perished	Pandemic – 10% to 15% perish Three orders of succession	Wide-scale civil unrest and looting, destroy facilities Key electronic records destroyed.	Wide-scale civil unrest and looting destroys facilities Key documentation destroyed	Prospective students, granting agencies, alumni loose confidence, withdraw support

Get Started by Focusing on Impacts

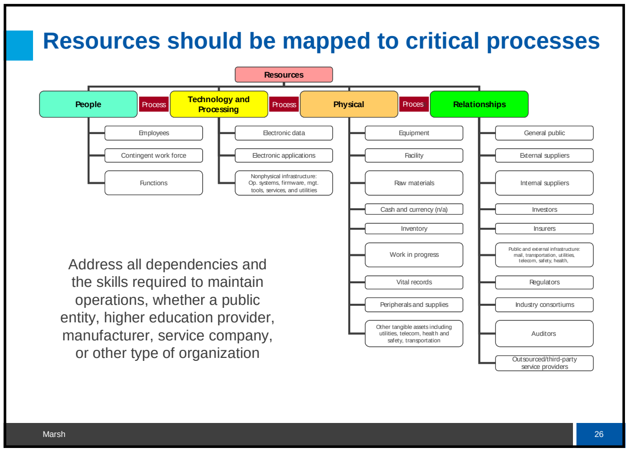
Identify where key elements of your revenue are “At Ris

- STOP chasing threats – you could exhaust your resources looking for ways to mitigate or preventing each one
- START thinking about impacts –when they happen, they all have some impact on your organization
- PROTECT your organization by focusing on where the impacts would be most severe - you need to determine what parts of your organization are most critical and “at-risk”, then figure out ways to protect them



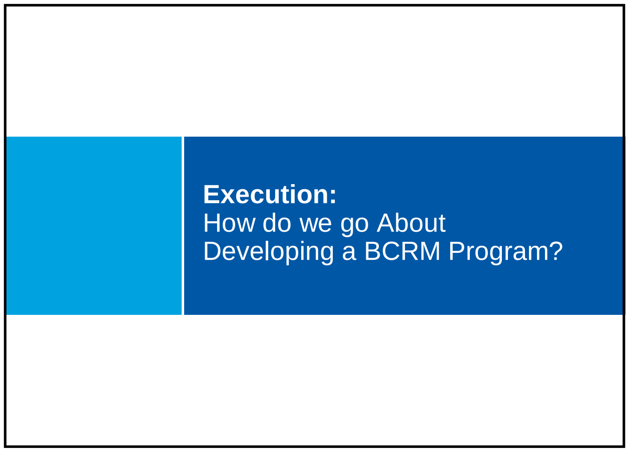
Impact Based Approach

Major Steps	Preparedness Review	Resiliency Development	Business Impact Analysis	Strategy Selection	Plan Preparation	Testing Maintenance
Actions	• Identify existing recovery strategies, risks, business issues, and gaps	• Analyze supply chain • Purchase policies	• Identify critical process • Recovery times • Financial impact from outage	• Define recovery strategy options • Select strategy	• Document recovery steps for business units	• Train employees



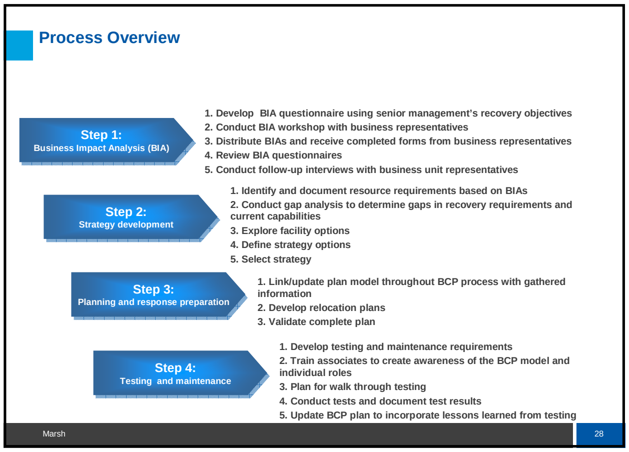
Resources should be mapped to critical processes

Address all dependencies and the skills required to maintain operations, whether a public entity, higher education provider, manufacturer, service company, or other type of organization



Execution:

How do we go About Developing a BCRM Program?



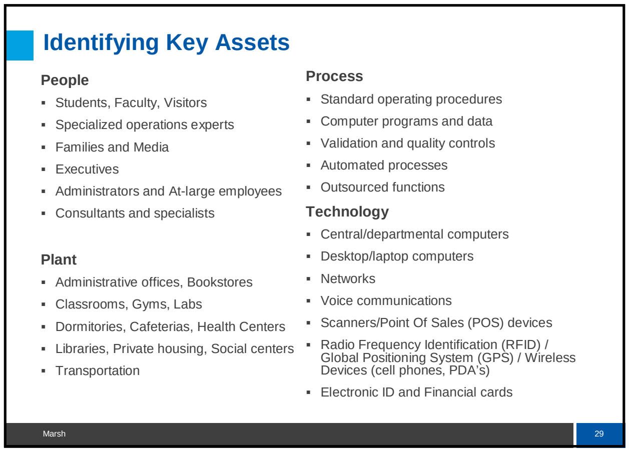
Process Overview

1. Develop BIA questionnaire using senior management’s recovery objectives
2. Conduct BIA workshop with business representatives
3. Distribute BIAs and receive completed forms from business representatives
4. Review BIA questionnaires
5. Conduct follow-up interviews with business unit representatives

1. Identify and document resource requirements based on BIAs
2. Conduct gap analysis to determine gaps in recovery requirements and current capabilities
3. Explore facility options
4. Define strategy options
5. Select strategy

1. Link/update plan model throughout BCP process with gathered information
2. Develop relocation plans
3. Validate complete plan

1. Develop testing and maintenance requirements
2. Train associates to create awareness of the BCP model and individual roles
3. Plan for walk through testing
4. Conduct tests and document test results
5. Update BCP plan to incorporate lessons learned from testing



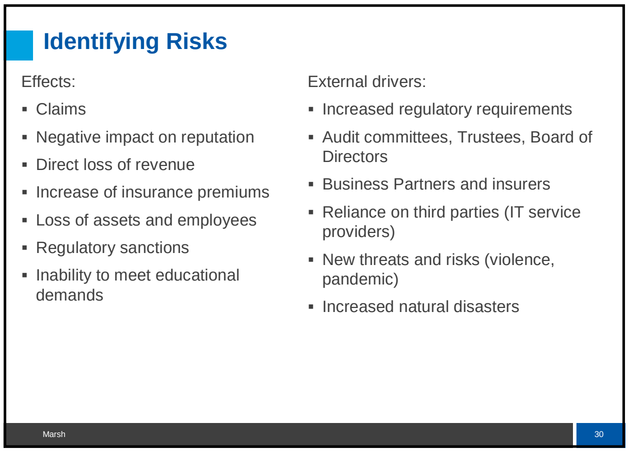
Identifying Key Assets

People
- Students, Faculty, Visitors
- Specialized operations experts
- Families and Media
- Executives
- Administrators and At-large employees
- Consultants and specialists

Plant
- Administrative offices, Bookstores
- Classrooms, Gyms, Labs
- Dormitories, Cafeterias, Health Centers
- Libraries, Private housing, Social centers
- Transportation

Process
- Standard operating procedures
- Computer programs and data
- Validation and quality controls
- Automated processes
- Outsourced functions

Technology
- Central/departmental computers
- Desktop/laptop computers
- Networks
- Voice communications
- Scanners/Point Of Sales (POS) devices
- Radio Frequency Identification (RFID) / Global Positioning System (GPS) / Wireless Devices (cell phones, PDA’s)
- Electronic ID and Financial cards



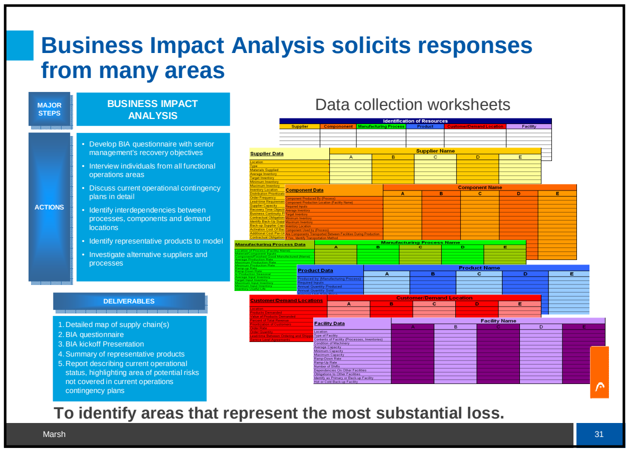
Identifying Risks

Effects:

- Claims
- Negative impact on reputation
- Direct loss of revenue
- Increase of insurance premiums
- Loss of assets and employees
- Regulatory sanctions
- Inability to meet educational demands

External drivers:

- Increased regulatory requirements
- Audit committees, Trustees, Board of Directors
- Business Partners and insurers
- Reliance on third parties (IT service providers)
- New threats and risks (violence, pandemic)
- Increased natural disasters



Business Impact Analysis solicits responses from many areas

MAJOR STEPS

BUSINESS IMPACT ANALYSIS

ACTIONS

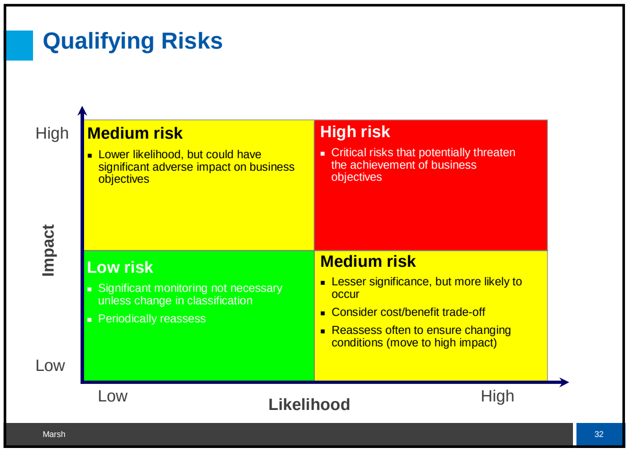
- Develop BIA questionnaire with senior management's recovery objectives
- Interview individuals from all functional operations areas
- Discuss current operational contingency plans in detail
- Identify interdependencies between processes, components and demand locations
- Identify representative products to model
- Investigate alternative suppliers and processes

DELIVERABLES

1. Detailed map of supply chain(s)
2. BIA questionnaire
3. BIA kickoff Presentation
4. Summary of representative products
5. Report describing current operational status, highlighting area of potential risks not covered in current operations contingency plans

Data collection worksheets

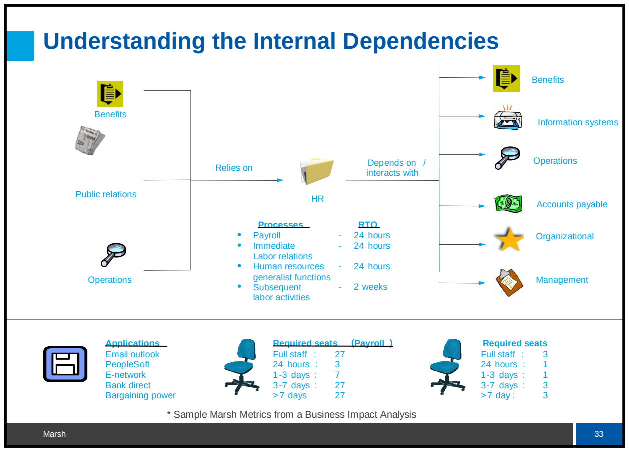
To identify areas that represent the most substantial loss.



Qualifying Risks

Impact	Low (Likelihood)	High (Likelihood)
High	**Medium risk** ▪ Lower likelihood, but could have significant adverse impact on business objectives	**High risk** ▪ Critical risks that potentially threaten the achievement of business objectives
Low	**Low risk** ▪ Significant monitoring not necessary unless change in classification ▪ Periodically reassess	**Medium risk** ▪ Lesser significance, but more likely to occur ▪ Consider cost/benefit trade-off ▪ Reassess often to ensure changing conditions (move to high impact)

Likelihood



Understanding the Internal Dependencies

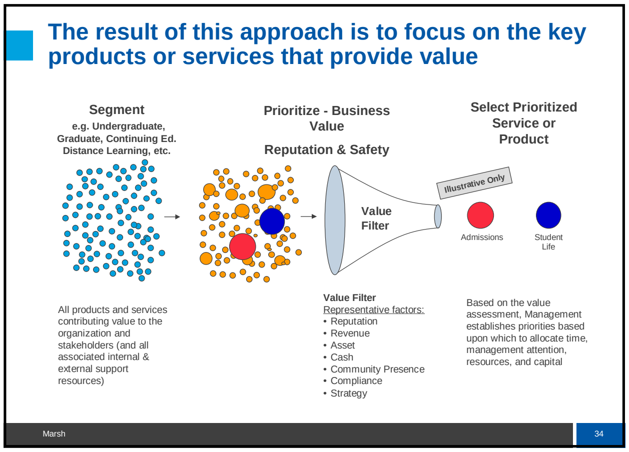
Processes		RTO
• Payroll	-	24 hours
• Immediate Labor relations	-	24 hours
• Human resources generalist functions	-	24 hours
• Subsequent labor activities	-	2 weeks

Applications
Email outlook
PeopleSoft
E-network
Bank direct
Bargaining power

Required seats (Payroll)	
Full staff :	27
24 hours :	3
1-3 days :	7
3-7 days :	27
>7 days	27

Required seats	
Full staff :	3
24 hours :	1
1-3 days :	1
3-7 days :	3
>7 day :	3

* Sample Marsh Metrics from a Business Impact Analysis



The result of this approach is to focus on the key products or services that provide value

Segment

e.g. Undergraduate, Graduate, Continuing Ed. Distance Learning, etc.

Prioritize - Business Value

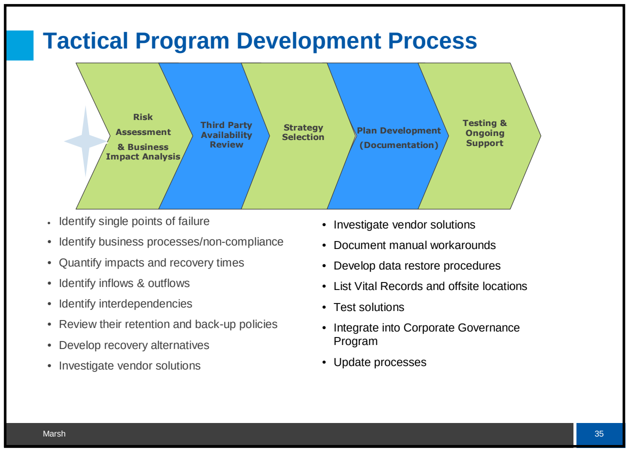
Reputation & Safety

Select Prioritized Service or Product

All products and services contributing value to the organization and stakeholders (and all associated internal & external support resources)

Value Filter
Representative factors:
- Reputation
- Revenue
- Asset
- Cash
- Community Presence
- Compliance
- Strategy

Based on the value assessment, Management establishes priorities based upon which to allocate time, management attention, resources, and capital

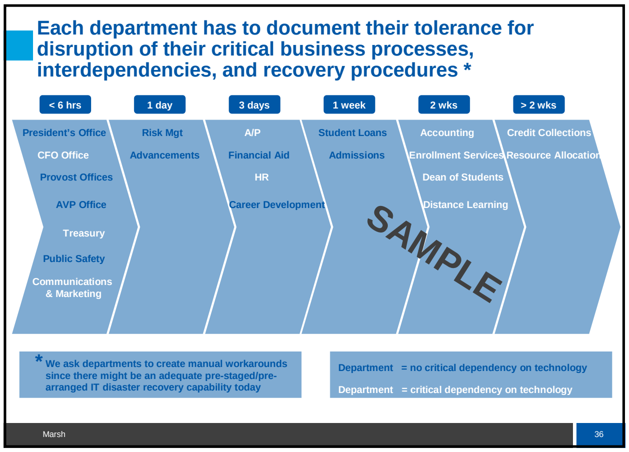


Tactical Program Development Process

Risk Assessment & Business Impact Analysis
Third Party Availability Review
Strategy Selection
Plan Development (Documentation)
Testing & Ongoing Support

- Identify single points of failure
- Identify business processes/non-compliance
- Quantify impacts and recovery times
- Identify inflows & outflows
- Identify interdependencies
- Review their retention and back-up policies
- Develop recovery alternatives
- Investigate vendor solutions

- Investigate vendor solutions
- Document manual workarounds
- Develop data restore procedures
- List Vital Records and offsite locations
- Test solutions
- Integrate into Corporate Governance Program
- Update processes



Each department has to document their tolerance for disruption of their critical business processes, interdependencies, and recovery procedures *

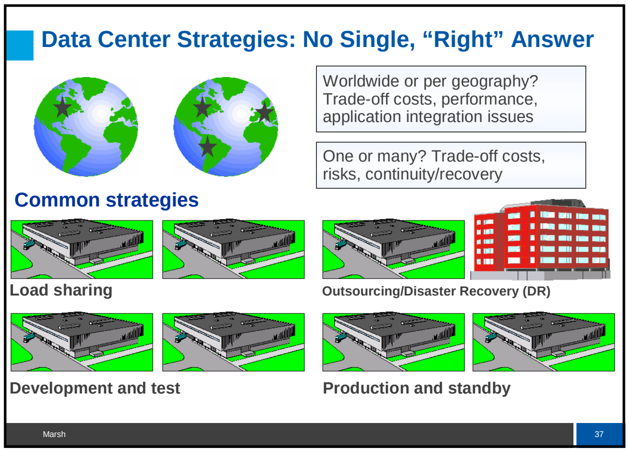
< 6 hrs	1 day	3 days	1 week	2 wks	> 2 wks
President's Office	Risk Mgt	A/P	Student Loans	Accounting	Credit Collections
CFO Office	Advancements	Financial Aid	Admissions	Enrollment Services	Resource Allocation
Provost Offices		HR		Dean of Students	
AVP Office		Career Development		Distance Learning	
Treasury					
Public Safety					
Communications & Marketing					

* We ask departments to create manual workarounds since there might be an adequate pre-staged/pre-arranged IT disaster recovery capability today

Department = no critical dependency on technology

Department = critical dependency on technology

Marsh 36



Data Center Strategies: No Single, "Right" Answer

Worldwide or per geography? Trade-off costs, performance, application integration issues

One or many? Trade-off costs, risks, continuity/recovery

Common strategies

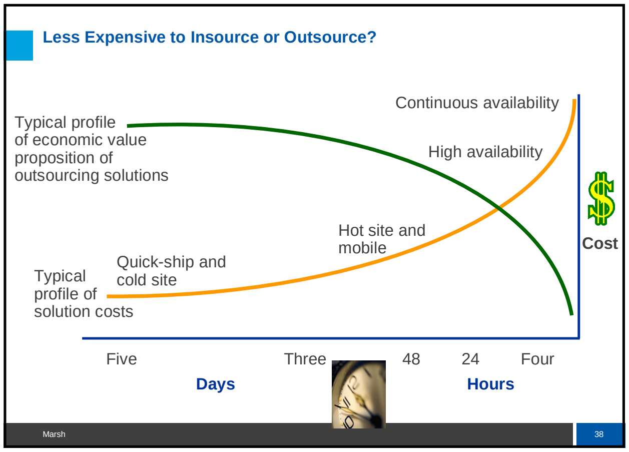
Load sharing

Outsourcing/Disaster Recovery (DR)

Development and test

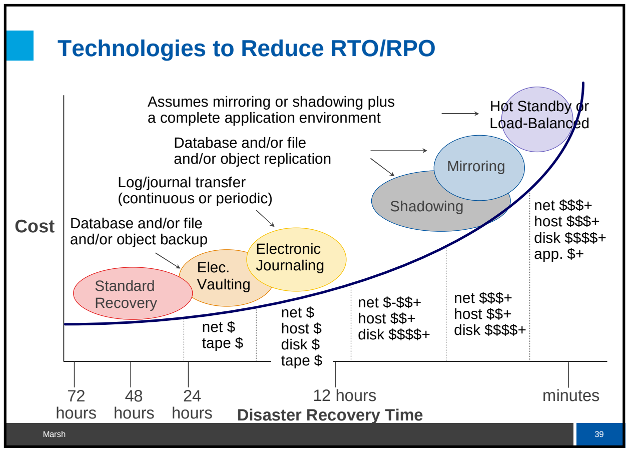
Production and standby

Marsh 37



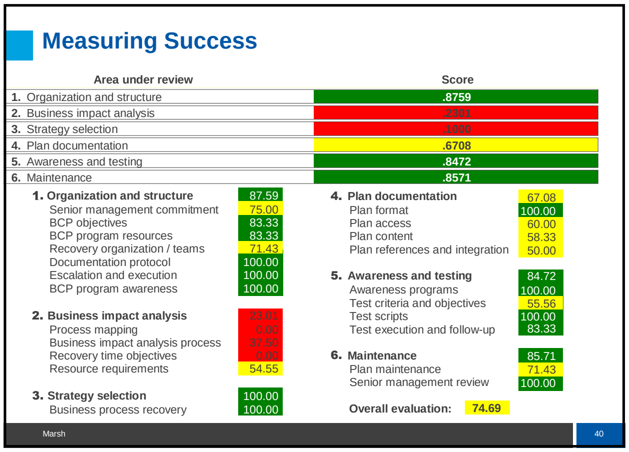
Less Expensive to Insource or Outsource?

Marsh 38



Technologies to Reduce RTO/RPO

Marsh 39



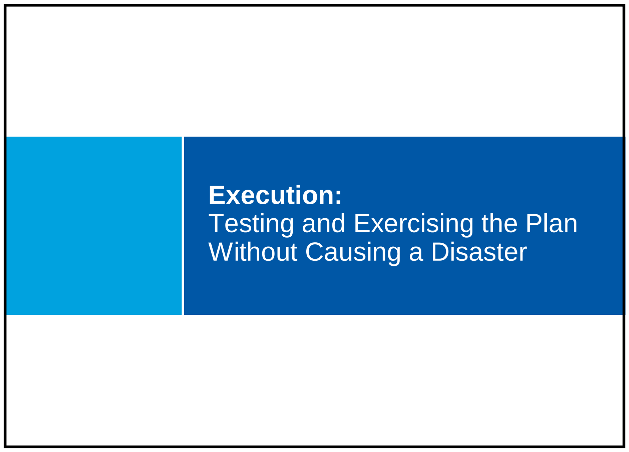
Measuring Success

Area under review	Score
1. Organization and structure	.8759
2. Business impact analysis	.2301
3. Strategy selection	.1000
4. Plan documentation	.6708
5. Awareness and testing	.8472
6. Maintenance	.8571

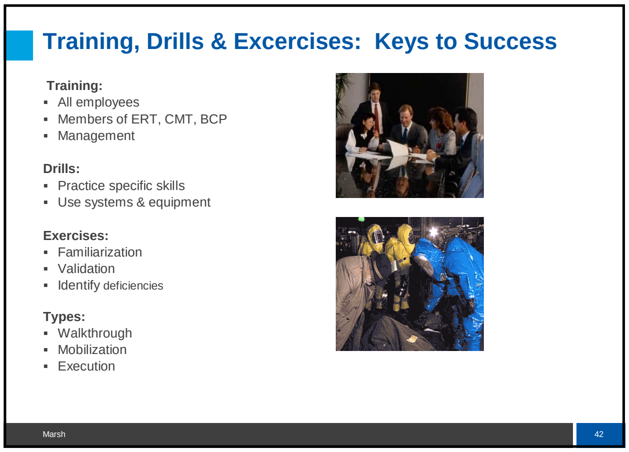
1. Organization and structure	87.59
Senior management commitment	75.00
BCP objectives	83.33
BCP program resources	83.33
Recovery organization / teams	71.43
Documentation protocol	100.00
Escalation and execution	100.00
BCP program awareness	100.00
2. Business impact analysis	23.01
Process mapping	0.00
Business impact analysis process	37.50
Recovery time objectives	0.00
Resource requirements	54.55
3. Strategy selection	100.00
Business process recovery	100.00
4. Plan documentation	67.08
Plan format	100.00
Plan access	60.00
Plan content	58.33
Plan references and integration	50.00
5. Awareness and testing	84.72
Awareness programs	100.00
Test criteria and objectives	55.56
Test scripts	100.00
Test execution and follow-up	83.33
6. Maintenance	85.71
Plan maintenance	71.43
Senior management review	100.00

Overall evaluation: 74.69

Marsh 40



Execution:
Testing and Exercising the Plan Without Causing a Disaster



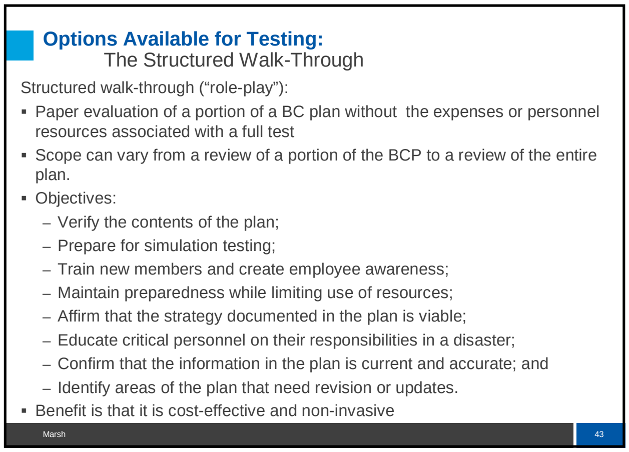
Training, Drills & Excercises: Keys to Success

Training:
- All employees
- Members of ERT, CMT, BCP
- Management

Drills:
- Practice specific skills
- Use systems & equipment

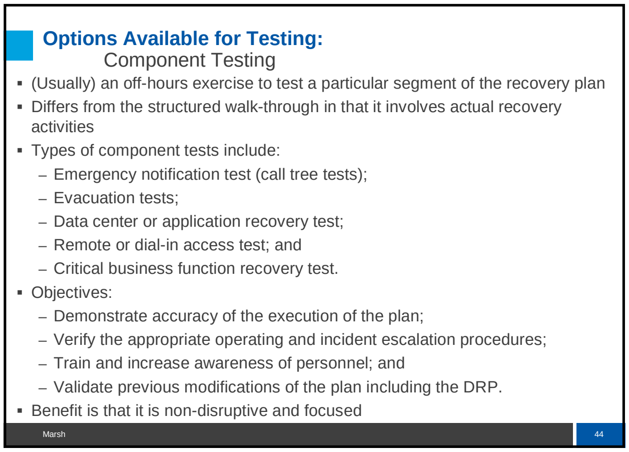
Exercises:
- Familiarization
- Validation
- Identify deficiencies

Types:
- Walkthrough
- Mobilization
- Execution



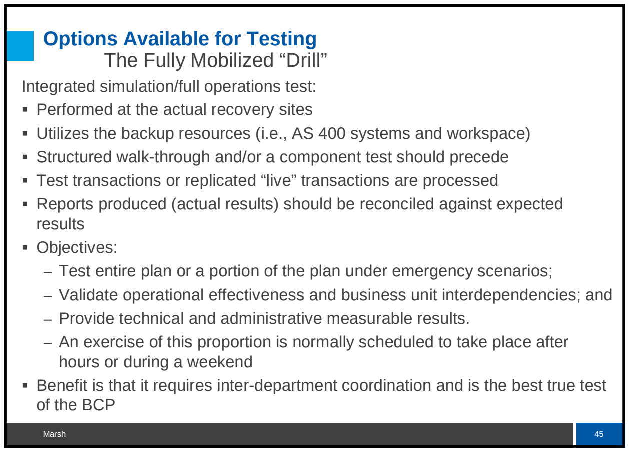
Options Available for Testing:
The Structured Walk-Through

Structured walk-through ("role-play"):
- Paper evaluation of a portion of a BC plan without the expenses or personnel resources associated with a full test
- Scope can vary from a review of a portion of the BCP to a review of the entire plan.
- Objectives:
  - Verify the contents of the plan;
  - Prepare for simulation testing;
  - Train new members and create employee awareness;
  - Maintain preparedness while limiting use of resources;
  - Affirm that the strategy documented in the plan is viable;
  - Educate critical personnel on their responsibilities in a disaster;
  - Confirm that the information in the plan is current and accurate; and
  - Identify areas of the plan that need revision or updates.
- Benefit is that it is cost-effective and non-invasive



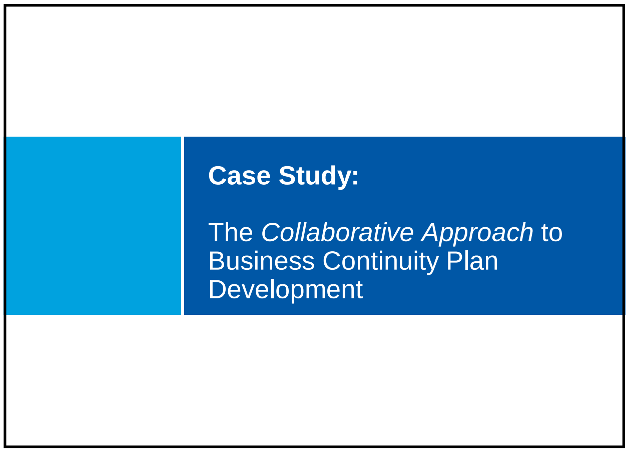
Options Available for Testing:
Component Testing

- (Usually) an off-hours exercise to test a particular segment of the recovery plan
- Differs from the structured walk-through in that it involves actual recovery activities
- Types of component tests include:
  - Emergency notification test (call tree tests);
  - Evacuation tests;
  - Data center or application recovery test;
  - Remote or dial-in access test; and
  - Critical business function recovery test.
- Objectives:
  - Demonstrate accuracy of the execution of the plan;
  - Verify the appropriate operating and incident escalation procedures;
  - Train and increase awareness of personnel; and
  - Validate previous modifications of the plan including the DRP.
- Benefit is that it is non-disruptive and focused



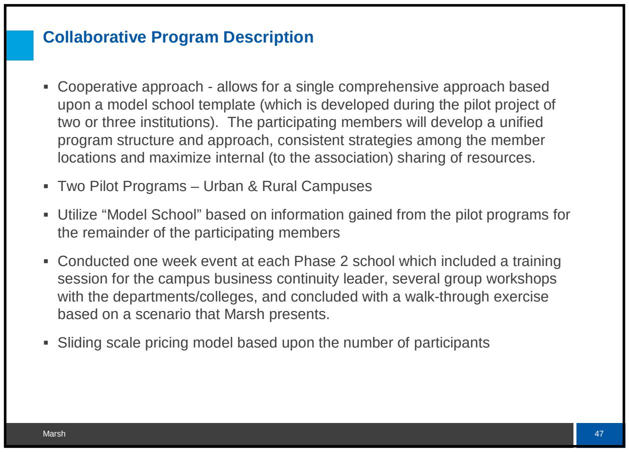
Options Available for Testing
The Fully Mobilized "Drill"

Integrated simulation/full operations test:
- Performed at the actual recovery sites
- Utilizes the backup resources (i.e., AS 400 systems and workspace)
- Structured walk-through and/or a component test should precede
- Test transactions or replicated "live" transactions are processed
- Reports produced (actual results) should be reconciled against expected results
- Objectives:
  - Test entire plan or a portion of the plan under emergency scenarios;
  - Validate operational effectiveness and business unit interdependencies; and
  - Provide technical and administrative measurable results.
  - An exercise of this proportion is normally scheduled to take place after hours or during a weekend
- Benefit is that it requires inter-department coordination and is the best true test of the BCP



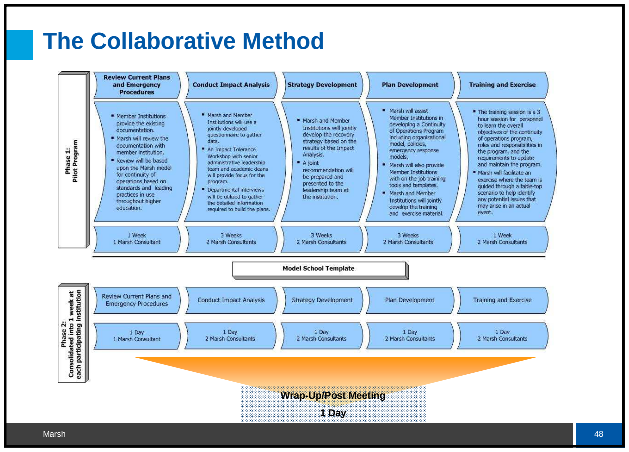
Case Study:

The *Collaborative Approach* to Business Continuity Plan Development



Collaborative Program Description

- Cooperative approach - allows for a single comprehensive approach based upon a model school template (which is developed during the pilot project of two or three institutions). The participating members will develop a unified program structure and approach, consistent strategies among the member locations and maximize internal (to the association) sharing of resources.
- Two Pilot Programs – Urban & Rural Campuses
- Utilize "Model School" based on information gained from the pilot programs for the remainder of the participating members
- Conducted one week event at each Phase 2 school which included a training session for the campus business continuity leader, several group workshops with the departments/colleges, and concluded with a walk-through exercise based on a scenario that Marsh presents.
- Sliding scale pricing model based upon the number of participants



The Collaborative Method

Phase 1: Pilot Program

Review Current Plans and Emergency Procedures	Conduct Impact Analysis	Strategy Development	Plan Development	Training and Exercise
▪ Member Institutions provide the existing documentation. ▪ Marsh will review the documentation with member institution. ▪ Review will be based upon the Marsh model for continuity of operations based on standards and leading practices in use throughout higher education.	▪ Marsh and Member Institutions will use a jointly developed questionnaire to gather data. ▪ An Impact Tolerance Workshop with senior administrative leadership team and academic deans will provide focus for the program. ▪ Departmental interviews will be utilized to gather the detailed information required to build the plans.	▪ Marsh and Member Institutions will jointly develop the recovery strategy based on the results of the Impact Analysis. ▪ A joint recommendation will be prepared and presented to the leadership team at the institution.	▪ Marsh will assist Member Institutions in developing a Continuity of Operations Program including organizational model, policies, emergency response models. ▪ Marsh will also provide Member Institutions with on the job training tools and templates. ▪ Marsh and Member Institutions will jointly develop the training and exercise material.	▪ The training session is a 3 hour session for personnel to learn the overall objectives of the continuity of operations program, roles and responsibilities in the program, and the requirements to update and maintain the program. ▪ Marsh will facilitate an exercise where the team is guided through a table-top scenario to help identify any potential issues that may arise in an actual event.
1 Week 1 Marsh Consultant	3 Weeks 2 Marsh Consultants	3 Weeks 2 Marsh Consultants	3 Weeks 2 Marsh Consultants	1 Week 2 Marsh Consultants

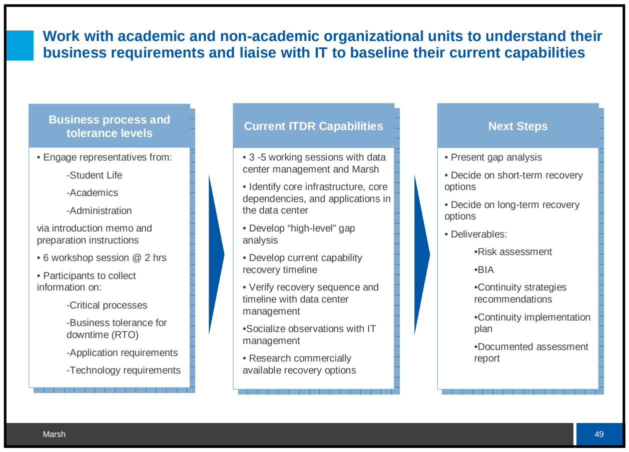
Model School Template

Phase 2: Consolidated into 1 week at each participating institution

Review Current Plans and Emergency Procedures	Conduct Impact Analysis	Strategy Development	Plan Development	Training and Exercise
1 Day 1 Marsh Consultant	1 Day 2 Marsh Consultants	1 Day 2 Marsh Consultants	1 Day 2 Marsh Consultants	1 Day 2 Marsh Consultants

Wrap-Up/Post Meeting
1 Day

Marsh 48



Work with academic and non-academic organizational units to understand their business requirements and liaise with IT to baseline their current capabilities

Business process and tolerance levels

- Engage representatives from:
  - -Student Life
  - -Academics
  - -Administration

via introduction memo and preparation instructions

- 6 workshop session @ 2 hrs
- Participants to collect information on:
  - -Critical processes
  - -Business tolerance for downtime (RTO)
  - -Application requirements
  - -Technology requirements

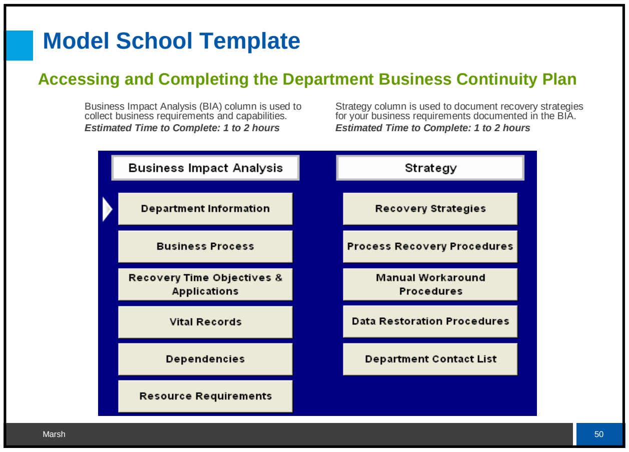
Current ITDR Capabilities

- 3 -5 working sessions with data center management and Marsh
- Identify core infrastructure, core dependencies, and applications in the data center
- Develop "high-level" gap analysis
- Develop current capability recovery timeline
- Verify recovery sequence and timeline with data center management
- •Socialize observations with IT management
- Research commercially available recovery options

Next Steps

- Present gap analysis
- Decide on short-term recovery options
- Decide on long-term recovery options
- Deliverables:
  - •Risk assessment
  - •BIA
  - •Continuity strategies recommendations
  - •Continuity implementation plan
  - •Documented assessment report

Marsh 49



Model School Template

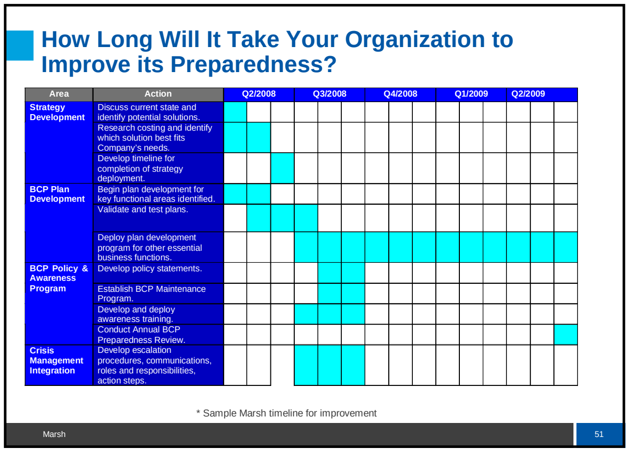
Accessing and Completing the Department Business Continuity Plan

Business Impact Analysis (BIA) column is used to collect business requirements and capabilities.
Estimated Time to Complete: 1 to 2 hours

Strategy column is used to document recovery strategies for your business requirements documented in the BIA.
Estimated Time to Complete: 1 to 2 hours

Business Impact Analysis	Strategy
Department Information	Recovery Strategies
Business Process	Process Recovery Procedures
Recovery Time Objectives & Applications	Manual Workaround Procedures
Vital Records	Data Restoration Procedures
Dependencies	Department Contact List
Resource Requirements	

Marsh 50

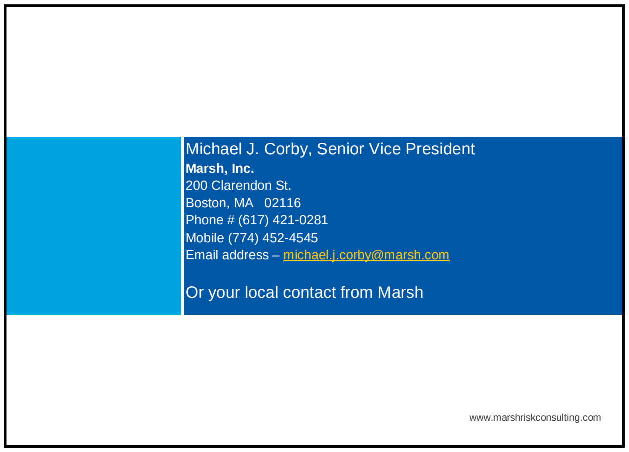


How Long Will It Take Your Organization to Improve its Preparedness?

Area	Action	Q2/2008			Q3/2008			Q4/2008			Q1/2009			Q2/2009		
Strategy Development	Discuss current state and identify potential solutions.	■														
	Research costing and identify which solution best fits Company's needs.	■	■													
	Develop timeline for completion of strategy deployment.			■												
BCP Plan Development	Begin plan development for key functional areas identified.	■	■													
	Validate and test plans.		■	■	■											
	Deploy plan development program for other essential business functions.				■	■	■	■	■	■	■	■	■	■	■	■
BCP Policy & Awareness Program	Develop policy statements.					■	■									
	Establish BCP Maintenance Program.					■	■									
	Develop and deploy awareness training.				■	■	■									
	Conduct Annual BCP Preparedness Review.															■
Crisis Management Integration	Develop escalation procedures, communications, roles and responsibilities, action steps.				■	■	■									

* Sample Marsh timeline for improvement

Marsh 51



Michael J. Corby, Senior Vice President
Marsh, Inc.
200 Clarendon St.
Boston, MA 02116
Phone # (617) 421-0281
Mobile (774) 452-4545
Email address – michael.j.corby@marsh.com

Or your local contact from Marsh

www.marshriskconsulting.com

MARSH
MMC MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN

www.marsh.com