

IDA



FAS Annual Conference Business Continuity Planning Presentation

September 11, 2004

Cheryl Heslip MBCI - CIBC
&
Des O'Callaghan FBCI - CDS

Outline

- BCP Overview - definitions
- BCP Essentials
- Business Impact Analysis
- Plan Development
- Crisis Management
- Plan Testing, Maintenance & Audit
- BCP Trends
- Questions

Definition

A planning **PROCESS** encompassing a **DOCUMENTED** description of the **ACTIONS** to be taken, **RESOURCES** to be used, and **PROCEDURES** to be followed, before, during and after a **BUSINESS INTERRUPTION**

Business Interruption

- An event that limits the ability to continue business functions normally
 - can include a “collateral” event
- Restricted access to facilities
- Interrupted operation of technology and / or related support infrastructure
- Unavailability of staff

Examples of Business Interruption

- Computer system failure
- Telephone system failure
- Facility closure
- Chemical incident
- Loss of staff due to epidemic illness (SARS-type threat)
- Fire
- Flood
- Tornado, hurricane, earthquake
- Severe weather - e.g. ice storm
- Bomb threat
- Terrorist attack

BCP Essentials

- Top Management “buy-in”
- Top-down and bottom up commitment
- Formal BCP Policy and accountability
- Well defined process
- Dedicated resources
- Strategy and methodology
- Standard and consistent planning tools, techniques and guidelines

Business Impact Analysis

- BIA is a formal and structured process to evaluate business risk, measured in the potential impact of a worst case scenario interruption in which staff, facilities, technology or data are inaccessible
 - identifies key processes / functions to be maintained
 - defines minimum process requirements for survival
 - establishes recovery timeframes
 - Maximum Acceptable Outage / Recovery Time Objective
 - prioritizes the sequence of recovery
 - quantifies critical resource requirements

Business Impact Analysis cont'd.

- Assess potential failure impacts:
 - loss of customers / business
 - damage to reputation / image / brand
 - lost revenue / increased cost
 - legal / regulatory exposures
 - loss of physical assets
- Gather data / analyze / validate / report
- Repeat annually or at time of significant change

Exposure Minimization

- Armed with an understanding of risk to your assets, evaluate current mitigation practices for:
 - personnel - safe environment
 - building and infrastructure protection
 - technology and equipment
 - information assets
- Implement additional mitigation strategies to lower risk, protect assets and operations

BC Planning - A Definition

- Preparing an executable and testable action plan to follow in case of disruption to normal operations:
 - to ensure critical business functions continue
 - to restore normal operations as quickly as possible
- Include:
 - Emergency Response - incl. notification and escalation
 - Teams, with defined roles and responsibilities
 - Internal and external contacts
 - Locations - for assembly, command, recovery
 - Resource requirements

Critical Resources

- People
- Facilities
- Technology
 - hardware and software
 - telecommunications - voice and data
- Vital records - electronic and hard copy
- Vendors / service providers

Crisis Management

- Strategic decisions / authority / priority setting
- Cross-functional team
 - Human Resources
 - Facilities
 - Technical Services
 - Administration - Security, Insurance, Legal, Finance, Procurement, Records Management
- Crisis Communications
 - employees, media, clients / stakeholders

Testing Plans to Confirm:

- Accuracy, completeness and viability
- Capabilities of personnel executing the plan
- Integrity of data (records off-site and current)
- Recovery time frames
- Continuity strategies meet business requirements
- Ability to meet legal / regulatory requirements
- Testing can be both passive and active

Untested plan = unproven capability

Ongoing Plan Maintenance

- Plans must continue to accurately reflect realistic procedures and staff assignments
- Maintenance supports ongoing viability of continuity capability through change
- Ensures employees have current plans
- Sample maintenance model:
 - monthly names and number updates
 - quarterly plan reviews and updates
 - semi-annual or annual testing

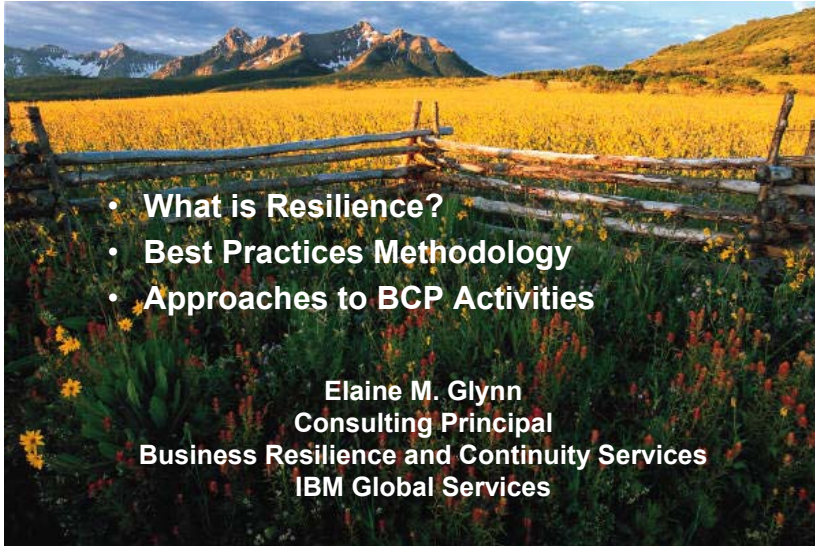
Plan Auditing

- Auditors can evaluate planning strategies and approaches, as well as the effectiveness of plans
 - does the methodology used to develop plans and capabilities meet industry best practices?
 - is the plan maintenance discipline and frequency appropriate for the organization?
 - has the plan been suitably exercised, with test results documented and deficiencies acted upon?

Business Continuity Trends

- Increasing regulatory pressure
- Rapid technology change will continue
- Continuity capability will be a competitive edge
- Zero data loss will become the norm
- People issues will keep rising in importance
- More emphasis on end-to-end processes
- Acceptance of need for ready alternate sites
- Disruptive events **will** occur (When not If)

The Next 30 minutes.....




- **What is Resilience?**
- **Best Practices Methodology**
- **Approaches to BCP Activities**

Elaine M. Glynn
Consulting Principal
Business Resilience and Continuity Services
IBM Global Services

How dynamic is your organization?

Resilience is about . . .

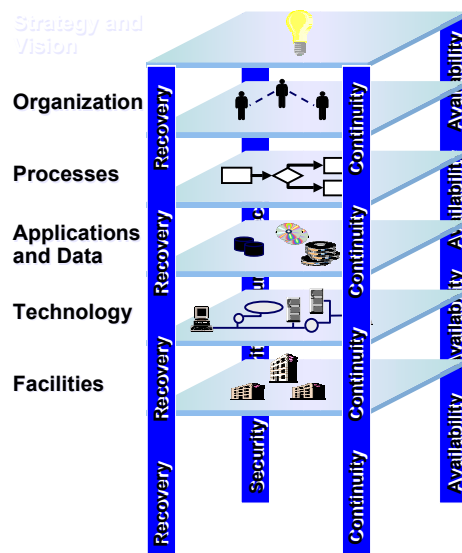
- 
- ◆ **Protecting the enterprise**
 - ◆ **The ability to recover and adapt**
 - ◆ **Enabling proactive/preemptive management**
 - ◆ **Effective management of complexity**
 - ◆ **Rapid exploitation of opportunities**
 - ◆ **Increasing competitive advantage**

How would your CEO respond to these questions?

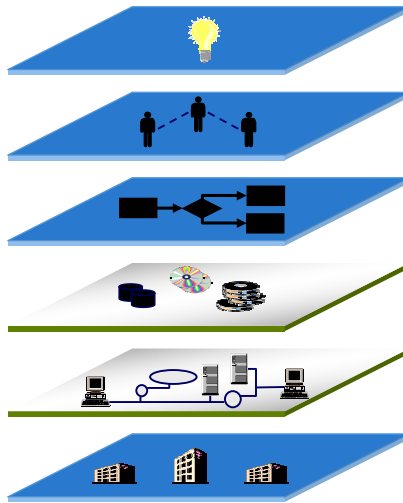


- **Strategic:** Does your firm acknowledge information based risk as an element of it's corporate risk management policy?
- **Operational:** How does your firm identify, quantify and manage these risks?
- **Reputation:** What are the risks to your brand, your reputation, your financial stability?
- **Regulatory:** Is your firm in compliance with regulatory requirements?
- **Financial:** Can you quantify the financial exposures associated with interruptions to your critical business processes?
- **Information:** Is your information secure from breach and protected from disaster?

Business Resilience touches all operational and infrastructure layers within an organization



The problem is viewed too narrowly...



9/11 & Black Out Lessons

- Business and IT Strategies not linked
- Roles poorly defined... no ownership, no one in command.
- Outdated, overly complicated procedures
- Processes didn't link to critical interfaces - LOB's
- Lack of standardization
- No "true" redundancy
- Supply Chain not covered
- Business Unit components not maintained.
- Change Control not linked to recovery plans

Resiliency is an iterative and on-going process.



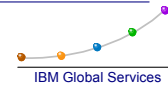
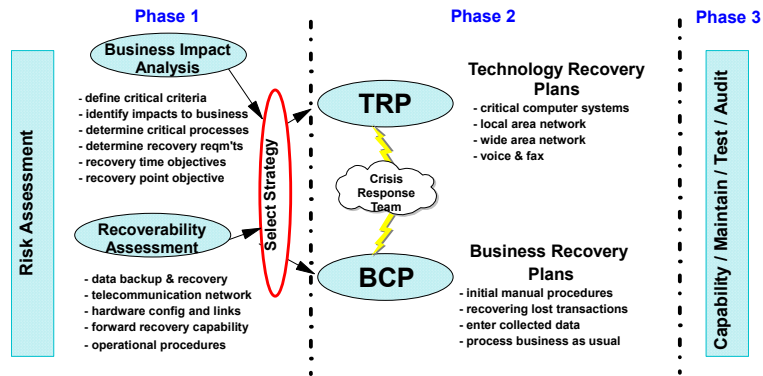
Re-evaluation Drivers include:

- * Market conditions
- * Change in desired risk position
- * Change to business model
- * Introduction of new technology
- * New government regulation

Successful Infrastructures must be flexible/dynamic and fit the business model they are intended to serve.

Successful businesses will make resiliency part of everyday operations and insure it grows and adjusts to business needs.

Methodology's can be expressed in many different ways. Business Continuity Planning activities can begin at any point within a solid BCP Methodology



Business resilience is the ability to...

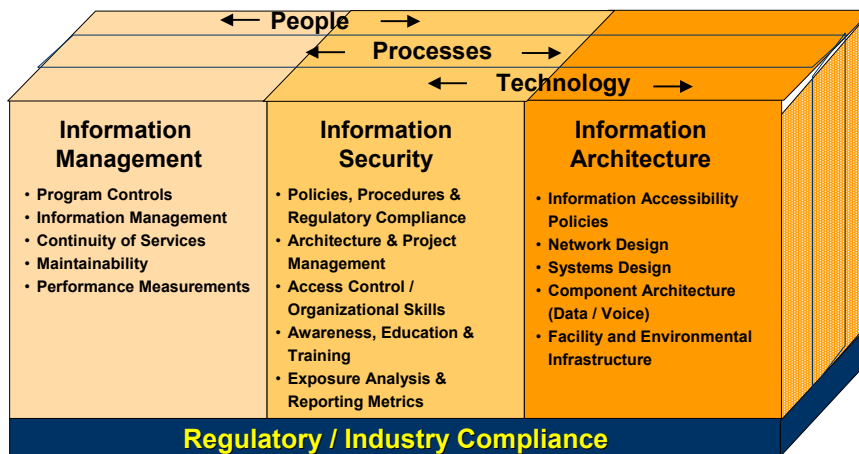
Manage information-based risks so you can rapidly adapt and respond to opportunities and threats while continuing business operations



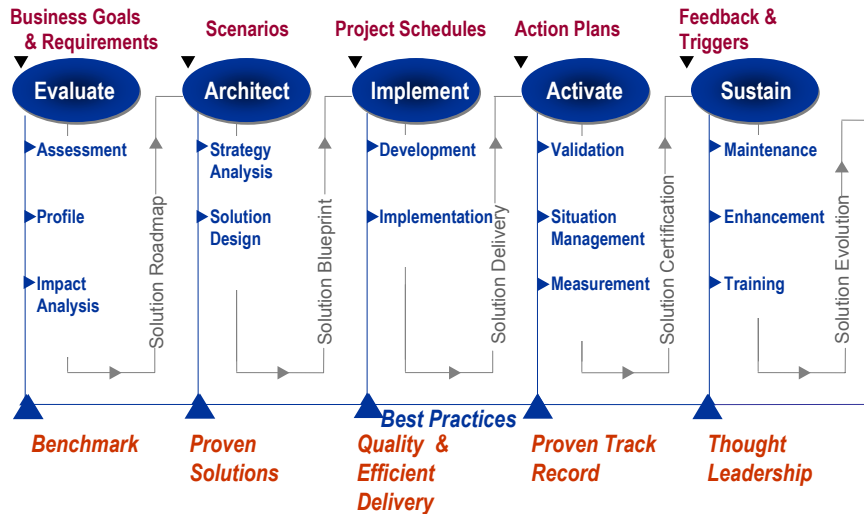
The Next 30 minutes.....



Information Availability



SunGard Availability Methodology



Key Program Components

Executive IA Program sponsorship and signoff

- Program not a project
- Senior Management, Business and IT input
- Formal signoff from all stakeholders

Understand business requirements

- Key business drivers and risks
- Financial and operational impacts
- Availability requirements and recovery timeframes
- Vital Record and Data loss tolerances
- Reliance on Partner, Vendor and other 3rd parties

Key Program Components

Effective Solution Design

- Consider Availability, Security and Recovery requirements
- Mitigate risk through resiliency
- Scenario based solution planning

Validate IA Program Capabilities

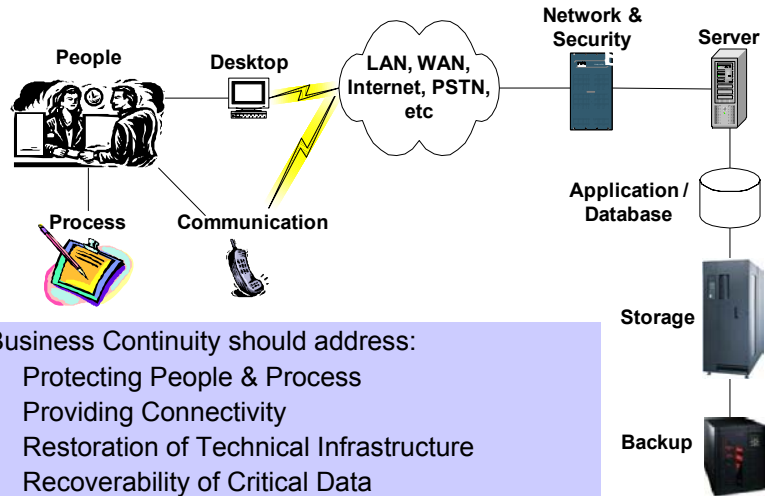
- Testing involves Senior Management, Business and IT
- Define clear business objectives and metrics for success
- Exercises should address crisis walkthroughs, manual procedures, single points of failure and data synchronization

Key Program Components

Program Sustainability

- Education and Awareness for all employees
- Address IA into new products and services
- Define and implement Change Management
- Regular reviews of business requirements, solution components and documentation

People, Process & Technology



Protecting People & Process

- Understanding Business Risks, Impacts and Drivers
- Effective Crisis Management and Communication Plans
- Developing, Testing and Maintaining Business Resumption Plans
- Revisiting Business Processes and associated Recovery Strategies

Providing Connectivity

- Keeping employees connected to:
 - Customers
 - Critical systems, applications and data
 - Other offices / business functions
 - Vendors and Partners
 - Internet
- Redundancy and Operational Resiliency
- Eliminate Single Points of Failure and Bottlenecks
- Effective Monitoring Capabilities
- Documented Network Architecture
- Documented and Tested Fail-over Procedures
- Vendor SLA with Performance Measurements

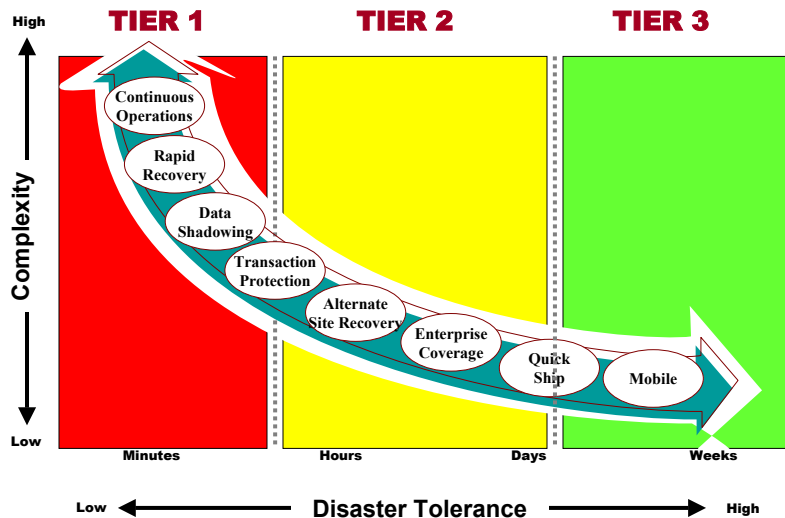
Restoration of Technical Infrastructure

- Proactive production design to address operational resiliency
- Documented and Tested IT Recovery Plans
- Incorporate Business Continuity in normal production processes (Operations, Change Management, Capacity Planning, etc.)
- Understanding of business objectives (RTO, RPO) and expectations

Recoverability of Critical Data

- Complexity due to various storage and backup environments (direct-attached, NAS, SAN, tape technology, specialized software)
- Clear understanding of storage and backup architecture
- Distinguish between dynamic (Online transactions, ERP, CRM, etc) and static (data warehousing, financial analysis, archives) data
- High Availability options required for business processes that cannot rely on dated tape restore
- Comprehensive end-user testing for application functionality and data integrity

Business Continuity - Tiered Approach



Characteristics of Tiered Solutions

Criticality	People	Network
Tier 1	<ul style="list-style-type: none"> • Run business process production in multiple locations • Dedicated alternate Workarea • Remote connectivity to IT systems 	<ul style="list-style-type: none"> • Redundant 'Live' Facilities at Alternate Site • Redundant connections to key customer, vendors & other WAN's • Dedicated equipment • No/Minimal disruptions to customers & users
Tier 2	<ul style="list-style-type: none"> • Traditional Shared Workarea • Mobile Solutions 	<ul style="list-style-type: none"> • 'Swing' critical connections ATOD • Re-establish connectivity to key customers and vendors • Reduced capabilities
Tier 3	<ul style="list-style-type: none"> • Mobile Solutions • Traditional Cold site • Address ATOD 	<ul style="list-style-type: none"> • Restore network connections on best efforts basis • Work with providers and carriers as required ATOD • Non-testable solution

Characteristics of Tiered Solutions

Criticality	Infrastructure	Data
Tier 1	<ul style="list-style-type: none"> • Dedicated Facilities, Hardware and Infrastructure • Geographical Clustering • Auto Fail-Over (Minimal Intervention) 	<ul style="list-style-type: none"> • High Availability • Hardware/SAN Mirroring • Software Replication • Database/Transaction Journaling • Multiple Vendor Involvement
Tier 2	<ul style="list-style-type: none"> • Traditional Hot Site • Quick Ship Solutions 	<ul style="list-style-type: none"> • Batch Backup • Traditional Tape Recovery • Tape Management / Storage
Tier 3	<ul style="list-style-type: none"> • Quick Ship Solutions • Mobile Solutions • Vendor Agreements • Address ATOD 	<ul style="list-style-type: none"> • Tape Backup • Static Data (data warehouse, archives, etc)

Summary

- Business Continuity Planning needs to be driven by business requirements
- Production environments (systems, applications, data, storage, backup, network, etc) need to be designed with Availability, Resiliency and Continuity in mind
- Proactive planning and operational resiliency is fundamental to Information Availability