IT Risk Management: Disaster Recovery and Business Continuity

Agenda – Purpose of Presentation

- Describe the Concept of Business Resiliency
- Define Business Continuity
- Define Business Impact Analysis
- Define Disaster Recovery
- Identify the Connections between these topics
- Recognize Supervisory Considerations

Definition Of A Disaster

A sudden calamitous event bringing great damage, loss, or destruction; *broadly* **:** a sudden or great misfortune or failure <the party was a *disaster*>

Source Merriam-Webster

What Does A Disaster Look Like?

A/C Failure
Acid Leak
Bomb Blast
Burst Pipe
Cable Cut
Chemical Spill
CO Fire
Condensation
Corrupted Data
Diesel Generator
Earthquake
Electrical Problem
Epidemic
Explosion
Fire
Flood
Hacker
Halon Discharge
Human Error
Hurricane
HVAC Failure
HW Error
Ice Storm
Lighting
Low Voltage
Network Failure
PCB Contamination
Power Outage
Power Surge
Programmer Error
Relocation Delay
Rodent
Roof Cave In
Sabotage
Shredded Data
Smoke Damage
Snow Storm
Sprinkler Discharge
Static Electricity
Strike Action
Supplier Failure
SW Error
Terrorism
Toilet Overflow
Tornado
Train Derailment
UPS Failure
Vandalism
Virus
Volcano
Water (Various)
Wind Storm

Resiliency Planning

- Business Continuity Planning
  - Takes an enterprise wide approach
  - Considers people, process, vendors, etc.
  - Is supported by a Business Impact Analysis
  - Is complimented by a Disaster Recovery Plan

- Business Impact Analysis
  - What are business critical operations
  - What is the business expectation for resumption
  - What is feasible given third party and IT capabilities

- Disaster Recovery Plan
  - What are the expectations and reality of recovering IT systems
  - How will IT systems be brought back after a disaster/system failure
  - What are the expectations of third party IT vendors

Business Resiliency

- Institution's overall plans to resume operations after a disaster
- Ability to quickly, effectively, and seamlessly react, respond, and recover business operations.
- Includes both system and operations (people)

Business Resiliency, cont.

- Key elements of a corporate level plan:
  - Management continuity - defining key roles and alternate responsibility
  - Continuity of operations - high level analysis of key operations, people and locations
  - Specific details - who does what, when, where and how

Business Resiliency, cont.

- Key issues to consider prior to a disaster:
  - Where are records stored and how can they be accessed
  - How can data security be maintained at alternate sites (i.e. secure off-premises dial-in)
  - Alternates sites - location, capacity, business line usage
  - Necessary contracts with third party vendors - data storage and procurement, alternate facilities (if an external vendor is used), storage of cash/notes, insurance
  - Small bank - naming of a re-opening team

Business Resiliency, cont.

- Business line plans - key elements
  - Each department have a business continuity coordinator who develops the plan based on a business impact analysis
  - Plan elements will be based on the identified risks
  - Building evacuation at a minimum - more critical operations - detailed back-up plan
  - Plan revised annually or when major changes occur in the business

Business Resiliency, cont.

- Key elements in a business line plan:
  - Evacuation and emergency procedures
  - Procedures to notify internal and external contacts
  - Alternate recovery site activation procedures
  - Business recovery procedures - details and priorities - includes timeframe for recovery (2-4 hours, one day, one week)
  - Details on resource requirements
  - Testing of all plans at least annually

Regulatory Guidance - Sound Practices Paper

- Issued by: U.S. Regulatory Agencies
- Date of Issuance - April 8, 2003
- Purpose - strengthen the resilience of the U.S. financial system
- Three significant post-September 11 business continuity objectives:
  - “Rapid recovery and timely resumption of critical operations following a wide-scale disruption;
  - Rapid recovery and timely resumption of critical operations following the loss or inaccessibility of staff in at least one major operating location;
  - A high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible.”

Regulatory Guidance - Sound Practices Paper, cont.

- Paper applies to:
  - core clearing and settlement organizations and
  - firms that play significant roles in critical financial markets (settles at least 5% of transactions in a specific market)
- Key settlement activities include:
  - completing pending large-value payments,
  - clearing and settling material pending transactions,
  - meeting material end-of-day funding and collateral obligations,
  - managing material open firm and customer risk positions, reconciling the day's records, and safeguarding firm and customer assets,
  - carrying out all related support functions

Regulatory Guidance - Sound Practices Paper, cont.

- Four sound practices for impacted organizations - applies to both data centers and business lines1
  - identify applicable clearing and settlement activities;
  - determine appropriate recovery and resumption objectives (e.g. - amount of time in which the business will recover after a wide scale disruption);
  - maintain sufficient geographically disbursed resources to meet objectives - critical businesses may operate simultaneously from several sites;
  - routinely use or test recovery and resumption
  - 1 Core clearing and settlement organizations should achieve these objectives by end of 2004; critical firms in specific markets within three years of the publication of this paper - Apr. 2006

Risk Assessment

- Identify threat scenarios
- Identify threat analysis
- Identify threat probability
- Perform gap analysis

Risk Management

- The organization's Risk Management Program is:
- Based on your risk assessment
- Documented in a written program
- Reviewed and approved annually
- Disseminated to financial institution employees
- Must be properly managed when outsourced to a Third-party
- Defines conditions of the BCP implementation
- Flexible
- Focused on specific threats not events
- Developed by valid assumptions and analysis
- Effective in mitigating the Rick of the institution

Board and Management Responsibilities

- The approval of:
  - Policy
  - Implementation Oversight
  - Review and Approval
  - Employee Resources (training and availability)
  - Reviews the BCP Testing Program and results
  - Reviews any Updates to the BCP Process

BIA - Business Impact Analysis

- Assessment and prioritization.
- Identification of business disruption.
- Identification of the legal and regulatory requirements.
- Estimation of maximum allowable downtime
- Estimation of Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

Monitoring And Testing

- Incorporation of the BIA and risk assessment into the BCP and testing program;
- Development testing program
- Assignment of responsibilities
- Completion of testing
- Evaluation
- Assessment
- Revision control.

BCP And DR Realities

- Testing is the only way:
  - To determine if your SLA's are achievable
  - To determine if your BCP plan is feasible
- It always costs more than you plan
- It always takes longer to bring your system back online in the midst of a disaster
- It's a high-stress event. Mistakes will occur.
- Are you prepared for the "Smoking Hole?"

DR-BCP-BIA Considerations

- Service Level Agreement Accuracy
- Key Person Risk
- Restoration Capacity
- Staff Movement and Loss
- Alignment of Business Expectations and IT Capabilities

BCP DR Options

- Type of DR Site – Cold, Warm, Hot
- Replication of data
- Bandwidth capacity planning
- Cloud solution vs. in-house support

Business Resumption

- Do you have a plan for moving services back to your original location after the disaster?
- Have you budgeted for the cost of moving back to your primary site?

Supervisory Considerations

- The existence of a plan is not enough. You must verify that:
  - Plans match the business model of the organization
  - Board, management, and staff understand their roles and responsibilities within the plan
  - Testing is performed periodically
  - Plans are reflective of the current operating environment: all new systems are considered