

Business Continuity Planning / Disaster Recovery Planning Discussion

CityPlace Conference Center
Dallas, TX

June 11, 2009

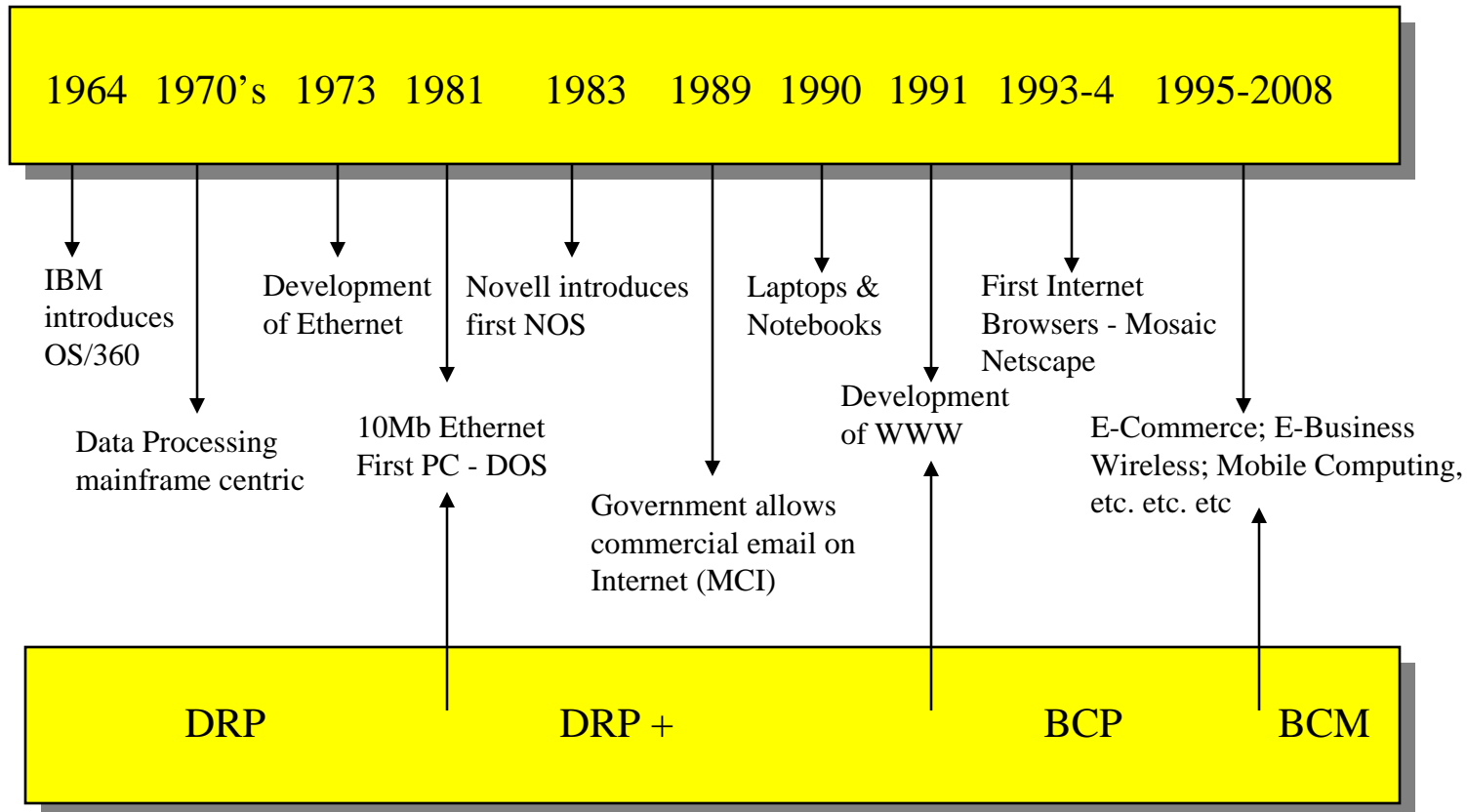
Rick Link, CISA, CISSP, CISM, CGEIT
ISACA North Texas Chapter President

Meeting Agenda



1. Evolution of DRP and BCP
2. Key Definitions for DRP and BCP
3. Key Objectives for an Organization
4. DRP and BCP Process Commonalities
 - A. Planning;
 - B. Risk Assessment & Business Impact Analysis;
 - C. Developing Plan Strategies & Developing The Plan;
 - D. Plan Testing & Maintenance; and
 - E. Awareness & Training.
5. Best Practices
6. Glossary

Evolution of BCM



Definitions



- **Disaster**

- A sudden, unplanned calamitous event causing great damage or loss.
- Any event that creates an inability on an organization's part to provide critical business functions for some predetermined period of time.
- In the business environment, any event that creates an inability on an organization's part to provide the critical business functions for some predetermined period of time.
- The period when company management decides to divert from normal production responses and exercises its disaster recovery plan. Typically signifies the beginning of a move from a primary to an alternate location.
- **SIMILAR TERMS: Business Interruption; Outage; Catastrophe.**

Definitions (cont'd)



- **Disaster Recovery Plan:**

- The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption.
- The technological aspect of business continuity planning. Focuses primarily on the recovery of infrastructure needed to support the continued operations of critical business functions or processes.
- The plan is designed to assist in restoring the key IT processes within the stated disaster recovery goals.
- **SIMILAR TERMS: Contingency Planning; Business Resumption Planning; Corporate Contingency Planning; Business Interruption Planning; Disaster Preparedness.**

Definitions (cont'd)



- **Business Continuity Plan: (BCP)**
 - Process of developing advanced arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change.
 - Focuses on the resumption or continued operations of critical business functions or processes.
 - **SIMILAR TERMS: Contingency Plan; Resumption Plan; Enterprise Plan**

Corporate & Technology Trends



- **Corporate**

- **Board and Management Accountability**
- Mergers & Acquisitions / Globalization
- Process Sourcing & Supply Chain Dependency
- **Regulatory Pressures**
- Resource Constraints
- Increased Service Demands
- Availability Requirements
 - Online Transactions / Internet
 - Self-Service Tools: ATMs / Kiosks
 - Customer Relationship Management (CRM)

- **Technology**

- IT Sourcing
- Data Center Availability
- **Data & Records Management**
- Mobility (PDAs / Auto Call Notification)
- Availability versus Recoverability
 - Recovery Time Objective (RTO)
 - Recovery Point Objective (RPO)
 - Maximum Tolerable Outage (MTO)
 - Service Delivery Objective (SDO)

Challenges



- Executive Commentary on DRP and BCP
 - “We have a hot site...”
 - “We have business interruption insurance...”
 - “We are not a bank...”
 - **“We have never, ever had a failure...”**
 - “We are not in a <hurricane, earthquake, tornado> zone...”
 - “When we did have a failure, everyone worked together and responded perfectly...”

Value Proposition



- **Protects your most valuable asset – Human Capital.**
- Encourages the ongoing viability of your organization and continual process improvement.
- **Manages the dilution of brand, reputation and market share.**
- Uphold “Prudent Man” concept and allows for executive due diligence.
- **Provides a formalized risk-based, auditable and repeatable process.**

Key Objectives



1. Limit magnitude of loss.
2. Minimize extent of interruption.
3. Limit severity.
4. Define alternatives for continuing critical functions.
5. Establish in advance a plan for recovery and restoration of business operations.
6. Train personnel.
7. Minimize decision making during a crisis.
8. Establish policy for continuous review and maintenance.
9. Establish policy for integration of Business Continuity with the Enterprise Strategic planning process.

Business Continuity Process



- **Many organizations champion and/or develop their own methodologies.**
- **DRII – Disaster Recovery Institute International (www.drii.org) supports a methodology comprised of 10 core practices:**
 1. Project Initiation and Management;
 2. Risk Evaluation and Control;
 3. Business Impact Analysis;
 4. Developing Business Continuity Strategies;
 5. Emergency Response and Operations;
 6. Developing and implementing Business Continuity Plans;
 7. Awareness and Training;
 8. Maintaining and Exercising Business Continuity Plans;
 9. Public Relations and Crisis Management; and
 10. Coordination with Public Authorities.

Business Continuity Process (cont'd)



Business Continuity Institute (www.thebci.org) supports a methodology comprised of six core stages.

1. Understanding Your Business

- ✓ Business Impact Analysis & Risk Assessment.

2. Business Continuity Management Strategies

3. Develop and Implement Business Continuity Response

- ✓ Business Continuity Plans.
- ✓ Resource Recovery Solutions and Plans.
- ✓ Crisis Management Plans.

4. Building and Embedding a Continuity Culture

- ✓ Culture and Awareness Program & Training Program.

5. Exercise Maintenance and Audit

6. Program Management

- ✓ Project Management & Policy.

Link to Enterprise Risk



At the highest level, there are four things that can be done with Risk:

| | | | |
|-----------------|---------------|-------------|---------------|
| Mitigate | Insure | Plan | Accept |
|-----------------|---------------|-------------|---------------|

Types of Risk to be Considered:

| <u>Compliance</u> | <u>Financial</u> | <u>Operational</u> | <u>Strategic</u> | <u>Technical</u> |
|--------------------------|-----------------------|--------------------|------------------|------------------------|
| Contractual | Lost/Deferred Revenue | People | Market Share | Cybercrime |
| Regulatory | Opportunity | Production | Partnerships | E-Business |
| Service Level Agreements | Shareholder Equity | Supply Chain | Reputation | Infrastructure Failure |

All sound DRP and BCP methodologies have a core set of common factors, which are needed in order to be successful, as follows:

- A. Planning;
- B. Risk Assessment & Business Impact Analysis;
- C. Developing Plan Strategies & Developing The Plan;
- D. Plan Testing & Maintenance; and
- E. Awareness & Training.

All sound DRP and BCP methodologies have a core set of common factors, which are needed in order to be successful, as follows:

A.Planning

A. Planning – Process Commonalities



DRP and BCP is an ongoing process that must be supported by a team effort. While one individual may have ownership of the process, it requires the commitment of the organization to be successful.

- **Define BCP vs. DRP for clear understanding by all.**
- Identify Project Sponsors and Leadership.
 - ✓ Defining objectives, policies, critical success factors, scope.
 - ✓ Identifying legal and regulatory requirements.
- Define standard terms and assumptions.
- Develop a Project Plan and Budget.
 - ✓ Hard costs and soft costs such as equipment, personnel resources, facilities, etc.

All sound DRP and BCP methodologies have a core set of common factors, which are needed in order to be successful, as follows:

B. Risk Assessment & Business Impact Analysis

B. Risk Assessment – Process Commonalities



- Process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls.
- Identify the following:
 - Risk – Exposure to loss, injury, danger; potential for loss (qualitative or quantitative).
 - Threats – Event that can cause a risk to become an actual loss (natural or man-made).
 - Vulnerabilities – Exposure to an event that can cause actual loss.

B. Risk Assessment – Process Commonalities (cont'd)



- Quantitative Risk:
 - Assigns a value to the risk.
 - Identifies cost of a particular effect, incident or phenomenon.
 - Can be state in an ALE (Annualized Loss Exposure or Expectancy).
 - **Objective (i.e., Hard Money).**
- Qualitative Risk:
 - Intangible effects caused by a particular incident.
 - Descriptive – Usually relates a cause with an effect.
 - **Subjective (i.e., Soft Money).**

B. Risk Assessment – Process Commonalities (cont'd)



- Consider threats and vulnerabilities for all critical assets
 - People;
 - Buildings and Facilities;
 - Computer Equipment (PCs, Servers, mainframes, etc.);
 - Telecom Equipment (PBX's);
 - Communication equipment (Routers, Switches, CSU / DSU etc.);
 - Inventory and Materials;
 - Production & Plant Equipment;
 - Critical Data;
 - Critical Computer Applications;
 - Operating Systems and Databases;
 - Environmental (Power, HVAC, Physical Security); and
 - Internal & External Customers & Users.

B. Risk Assessment – Process Commonalities (cont'd)



Types of Threats

– Natural:

- ✓ Flood & Other water based incidents
- ✓ Earthquakes
- ✓ Hurricane, Tornadoes, Monsoons
- ✓ Thunders, Hail and Ice storms
- ✓ Lightning and Electrical storms
- ✓ Snow and Winter storms
- ✓ Volcanic eruptions, ash fall out
- ✓ Large natural fires & smoke residues
- ✓ Epidemics

– Man Made:

- ✓ Political
- ✓ Fires
- ✓ Flood due to equipment, pipes, sprinklers etc.
- ✓ Explosions
- ✓ Hazardous / toxic material spills, contamination, access denial

B. Risk Assessment – Process Commonalities (cont'd)



- Annualize Loss Exposure: formula for assigning a dollar value for one event / risk, where no length of time is involved.
 - Risk (R) = Frequency (f) * Exposure (e)
 - ✓ $R = f * e$
 - Frequency is the number of times per year the event could occur.
 - Exposure is the cost assigned to one instance of the event.
- Example – Power Failure
 - Frequency – 10 times per year.
 - Exposure:
 - ✓ \$1,000 for Department
 - ✓ \$200 for Department B
 - $10 * 1,000 = \$10,000$
 - $10 * 200 = \$2,000$ produces a total ALE = \$12,000

B. Risk Assessment – Process Commonalities (cont'd)



- Identify Existing Controls:
 - Process or device that mitigates effect of a threat
 - Reduces effects, but cannot prevent occurrence
- Physical Controls
 - Fire suppression / sprinkler systems
 - Access control systems
 - Security guards
- Procedural Controls
 - Hiring and termination policies
 - Clean desk policy
 - Document receipting
- Logical Controls
 - Data storage protection
 - Protection afforded assets by location in relation to threat

B. Risk Assessment – Process Commonalities (cont'd)



- Evaluate the effectiveness of existing controls:
 - Deter the threat
 - Lessen the loss
 - Ability to deter or reduce multiple risks
- Improve the effectiveness of controls:
 - Implementing layers of protection where possible
 - Training
 - Documentation
 - Enforcement

B. Business Impact Analysis – Process Commonalities



- Identify the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts. Establish critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be set.
- * The BIA should quantify, where possible, the loss impact from both a business interruption (number of days) and a financial standpoint.
- Assess potential Impacts of Outage or Disruption.
- * Typically, the Finance Department should provide the number of transactions per day, week, and month and the dollar amounts however, you do need to go search and find this information...

B. Business Impact Analysis – Process Commonalities (cont'd)

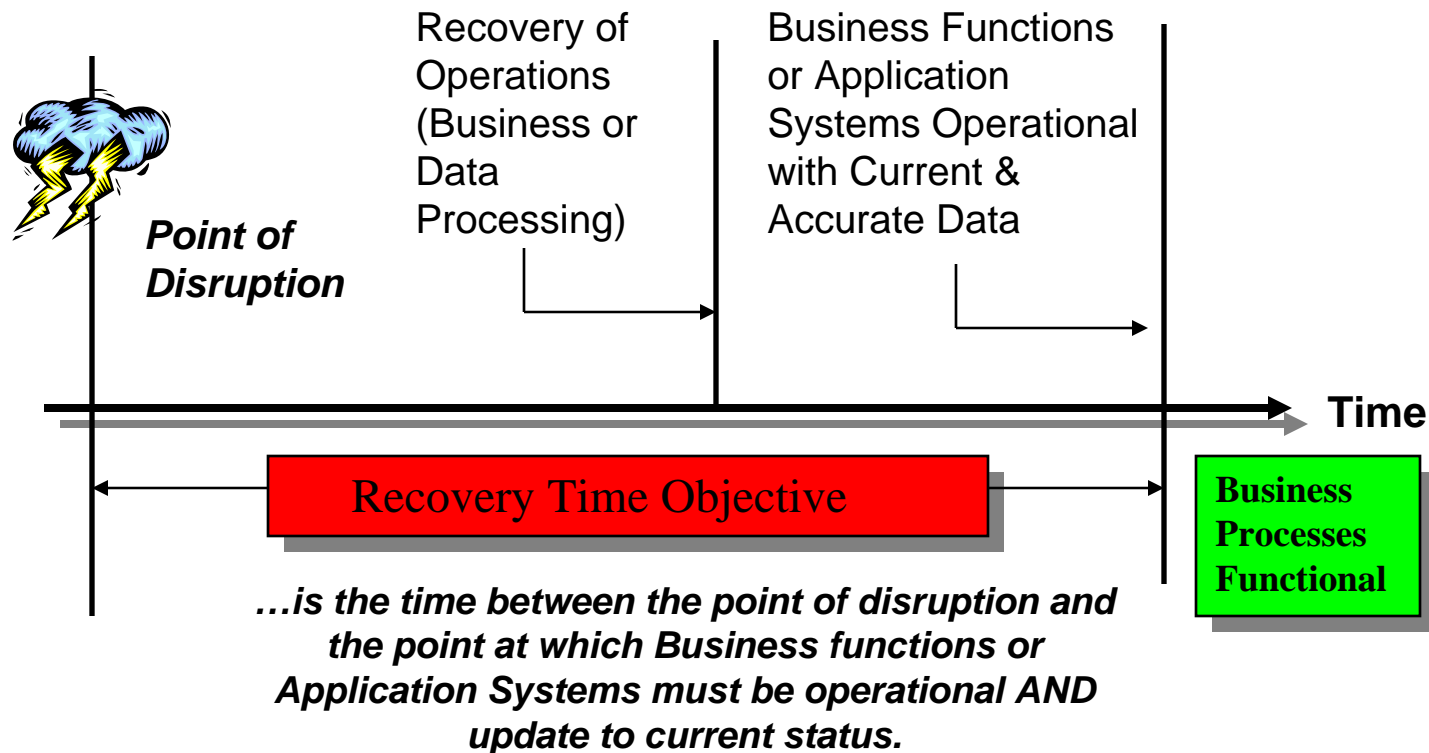


- For each major business unit within the organization you will perform the following:
 - Identify those business components or activities that if interrupted or unavailable for a determined period of time could significantly jeopardize the operation of the organization.
 - ✓ Critical business functions
 - ✓ Infrastructure
 - ✓ Applications
 - ✓ Critical or vital records
 - ✓ Personnel
 - ✓ Critical services internal and external
 - ✓ Vendors
 - Determine Required Recovery Time Objectives

B. Business Impact Analysis – Process Commonalities (cont'd)

Recovery Time Objective

The time within which the Business Functions or Application Systems must be Restored to Acceptable Levels of Operational Capability to Minimize the Impact of an Outage



B. Business Impact Analysis – Process Commonalities (cont'd)



- Data Collection:
 - Questionnaire / Interviews / Facilitated Sessions.
 - Recommend a combination of Interviews and questionnaire.
 - Validate, Validate, Validate...

- Type of Information:
 - Manual Procedures;
 - Alternative Processes;
 - Documentation;
 - Time Criticality, longest period can be with out;
 - Dependencies;
 - Special needs, forms, equipment, etc.;
 - Critical applications, systems, infrastructure etc.;
 - Critical time periods, Month end closes, year ends etc.;
 - Legal, regulatory, contractual requirements; and
 - Impacts over increasing periods of time.

B. Business Impact Analysis – Process Commonalities (cont'd)



- Data Analysis
 - Determine Quantitative Impact, including:
 - ✓ Losses identified in quantities, percentages, factors of standard that can be described in monetary terms.
 - ✓ Financial:
 - Sales
 - Market Share
 - Penalties
 - Extra Expenses incurred
 - ✓ Organization Related:
 - Assets
 - Revenue
 - Income

B. Business Impact Analysis – Process Commonalities (cont'd)



Determine Quantitative Impact

Stated another way the Potential Actual or Order of Magnitude of Loss

Example:

| | US Dollars |
|---------------|--------------------------|
| Critical | $500,001 \leq 1,000,000$ |
| Significant | $100,001 \leq 500,000$ |
| Moderate | $50,001 \leq 100,000$ |
| Minimal | $10,001 \leq 50,000$ |
| Insignificant | $0 \leq 10,000$ |

B. Business Impact Analysis – Process Commonalities (cont'd)



- Determine Qualitative Impact:
 - ✓ Losses with financial impact that cannot be quantified, must be described.
 - ✓ Intangible losses that can impact operationally but that cannot be quantified in monetary terms.
 - ✓ Quality:
 - Efficiency
 - Satisfaction
 - Control
 - ✓ Related to Relationships:
 - Intra-departmental
 - Inter-departmental
 - External Vendors / Clients / Business Partners
 - Reputation
 - Goodwill

All sound DRP and BCP methodologies have a core set of common factors, which are needed in order to be successful, as follows:

C. Developing Plan Strategies & Developing The Plan

C. Developing Plan Strategies – Process Commonalities



- Determine and guide the selection of alternative business recovery operating strategies for recovery of business and information technologies within the recovery time objectives, while maintaining the organization's critical functions.
- You should perform the following:
 - Identify / Develop available alternate strategies and their advantages and disadvantages and cost ranges.
 - Identify viable recovery strategies within business functional areas
 - Assess Strategies.
 - Perform Cost Benefit Analysis.
 - Consolidate strategies across the enterprise.
 - Obtain Business Unit Consensus on Consolidated Strategies.

C. Developing Plan Strategies – Process Commonalities (cont'd)



- **DRP and BCP Strategies, Advantages, Disadvantages, Cost**
 - Identify Requirements for **DRP and BCP** Strategies
 - ✓ Review business recovery issues from BIA
 - ✓ Review technology recovery issues for each support area
 - ✓ Review non-technology issues for each support area
 - Identify Off-Site storage requirements and Alternative facilities
 - ✓ Criteria for selection:
 - Communications Needs;
 - Contract Considerations;
 - Location and facilities;
 - Hardware / Software Support;
 - Experience;
 - Additional Services required; and
 - Plan Testing Time and Cost.

C. Developing Plan Strategies – Process Commonalities (cont'd)



- Identify Viable Recovery strategies within business functional areas:
 - ✓ Service Degradation
 - ✓ Internal Recovery (Reciprocal Agreement)
 - ✓ Commercial Recovery Centers:
 - Service Bureaus
 - Hot Sites
 - Cold Sites
 - Time Brokers
 - Buy and Replace
 - Just in time shipping
 - Warm Site
 - ✓ Combination Strategies

C. Developing Plan Strategies – Process Commonalities (cont'd)



- Assess Strategies:
 - Review each proposed strategy to ensure that it meets the following as defined during the BIA
 - ✓ Business Needs
 - ✓ Recovery Objectives
 - In addition each strategy should be reliable in terms of accessibility and availability of recovery capability
- Cost Benefit Analysis:
 - Many methods are available so use one that is:
 - ✓ Practical
 - ✓ Reliable
 - ✓ Understandable

C. Developing Plan Strategies – Process Commonalities (cont'd)



- Consolidating Strategies across the Enterprise
 - Coordination of Technology Recovery
 - Enterprise Level Crisis Management
 - Enterprise Level Media Handling
 - Centralized strategy for interfacing with local emergency organizations and facilities:
 - ✓ Police
 - ✓ Fire
 - ✓ Hospitals

C. Developing the Plan – Process Commonalities



- Design, develop and implement the Plan that provides recovery within the determined recovery time objectives.
- The Plan Design should include:
 - Plan Scope and Objective:
 - ✓ Definition of Standard Terms
 - ✓ Selecting the appropriate Methodology
 - ✓ Scope of Project itself
 - Business Recovery Organization (BRO) and responsibilities (recovery team concept):
 - ✓ BCP Planning Coordinator
 - ✓ Disaster Recovery Teams
 - ✓ Business Continuity Management Teams

C. Developing the Plan – Process Commonalities (cont'd)



- Major Plan Components:
 - ✓ Reduction
 - ✓ Response
 - ✓ Recovery and Resumption
- Scenario to Execute the Plan:
 - ✓ Guidelines for execution of full or partial plan
- Escalation, notification and plan activation:
 - ✓ Disaster Declaration Procedures
 - ✓ Mobilization procedures
 - ✓ Damage assessment concepts
 - ✓ Recovery Site Activation
- Vital records and off-site storage program:
 - ✓ What goes off-site
 - ✓ Inventory of what is off site
 - ✓ How do you get it back

C. Developing the Plan – Process Commonalities (cont'd)



- Salvage and Reclamation Procedures:
 - ✓ Document extent of damage, items destroyed, items recoverable.
 - ✓ Arrange for removal of recoverable items.
- Restoration Planning:
 - ✓ Preparations of new facility.
 - ✓ Preparations for moving into new facility.
 - ✓ Plans for cutting over from temporary site to new facility.
- Provisions for testing and maintenance of the plan:
 - ✓ Procedures for periodic and routine update of plan.
 - ✓ Procedures for periodic and routine testing of plan or plan components.



All sound DRP and BCP methodologies have a core set of common factors, which are needed in order to be successful, as follows:

D.Plan Testing & Maintenance

D. Plan Testing – Process Commonalities



- A program to periodically and methodically test all major components of the plan to ensure that they are functioning as designed.
- Testing provides additional benefits:
 - Verification of off-site storage arrangement and processes.
 - Ensures that recovery team procedures are correct.
 - Identifies deficiencies and weaknesses within the plan.
 - Educating and training recovery support team members.
 - Provides feedback into the plan maintenance process.
 - Demonstrates that the plan will work as effectively as possible.

D. Plan Testing – Process Commonalities (cont'd)



- The testing process should include the following:
 - Allow for periodic testing of major plan components at least semi-annually.
 - Identify scope, goals and objectives for each individual test.
 - Provide for an independent auditing of test performance.
 - Provide for a post-mortem / report of test results which are communicated to appropriate management levels.
 - Provide a feedback mechanism into the plan maintenance process.
 - Provide for the allocation of adequate resources.

D. Plan Maintenance – Process Commonalities



- Develop processes to review and maintain the currency and accuracy of the information contained within the plan, in order to ensure that the Plan will continue to meet and support the organizations changing recovery needs.
 - Maintenance timetables should be developed:
 - ✓ Entire plan should be reviewed (at least annually).
 - ✓ Contact lists should be reviewed quarterly.
 - ✓ Individual business functional area recovery procedures.
 - Distribution procedures:
 - ✓ Ensure older versions are replaced with most current versions.
 - Budgeting of required resources.

D. Plan Maintenance – Process Commonalities (cont'd)



- Identify sources of change information:
 - ✓ Exercise results.
 - ✓ Strategic Business Plans.
 - ✓ Changes in Infrastructure etc.
- Change Management processes within organization should take into account DRP and BCP.

D. Plan Maintenance – Process Commonalities (cont'd)



- Plan components to consider when reviewing or auditing a plan:
 - Revision Dates
 - Escalation Flow
 - Succession Planning
 - Test Plans
 - Test Results
 - Contact Lists
 - Home phone
 - Cell phone
 - Closest relative
 - Vendors
 - Service providers
 - Monitoring Procedures
 - Maintenance Procedures
 - Revision Control Procedures
 - Document Control Procedures
 - Team Charters

All sound DRP and BCP methodologies have a core set of common factors, which are needed in order to be successful, as follows:

E.Awareness & Training.

E. Awareness and Training – Process Commonalities



- A program to create corporate awareness and enhance the skills required to develop, implement, maintain, and execute the Plan:
 - Awareness is knowing or reality, implies that you have knowledge of something:
 - ✓ Videos / Films;
 - ✓ Newsletters;
 - ✓ Posters;
 - ✓ Promotional Items;
 - ✓ Brown-Bag Lunch Meetings; and
 - ✓ Budget and resources must be allocated.

E. Awareness and Training – Process Commonalities (cont'd)



- Training is to provide schooling using a process or method to address the following:
 - New hire orientation;
 - Outside courses;
 - Internal courses;
 - CBT (Computer Based Training); and
 - Budget and resources must be allocated.

Common Plan Mistakes



- Effort is UNDERESTIMATED
- RECOVERY REQUIREMENTS not adequately defined
- RESTORATION PROCESS not thought through
- Role of BUSINESS CONTINUITY MANAGER not recognized
- Plan not ADEQUATELY MAINTAINED
- INADEQUATE Testing
- Not achieving SENIOR MANAGEMENT buy in

Selling to Senior Management



- **Take a positive approach vs. describing impact of a variety of serious but unlikely threat events.**
- **Stress benefits to the company and its bottom line:**
 - Side benefits as a result of business impact analysis:
 - ✓ **Process re-design / optimization.**
 - ✓ **Work flow analysis.**
 - Improved lines of communication
 - Teamwork.
 - Awareness of potential impacts can lead to additional mitigation measures being identified (e.g., vulnerability of supply chain).
 - Alternative uses of recovery resources (e.g., training facility).
 - Selling point (customers, business partners).
- **Still not convinced:**
 - Fiduciary responsibility (“prudent man” rule)

Issues Influencing Planning Decisions



- Regulatory Compliance
 - HIPAA
 - GLBA
 - Homeland Security Department
 - Executive Order 13010
 - Foreign Corrupt Policies Act
 - OMB Circulars
 - Others
- Liability of the Board
- Liability of Management
- Public Image
- Competitive Advantage

Hurricane Season – Record Breaking Years!



Season Storm Records:

- 28 named storms are the most named in a single season (1993 had 21 named storms).
- 15 hurricanes are the most hurricanes in a single season (1969 had 12 hurricanes).
- 7 major hurricanes with a Category 3 or higher on the Saffir-Simpson Hurricane Scale (1950 had 8 major hurricanes).
- 3 Category 5 hurricanes (Katrina, Rita, and Wilma) are the most Cat 5 recorded in a single season.
- 7 named storms made US landfall including Arlene, Cindy, Dennis, Katrina, Rita, Tammy and Wilma (1916 and 2004 had named eight storms that made landfall).
- 5 names were retired including Dennis, Katrina, Rita, Stan and Wilma (1955, 1995, and 2004 had four names retired).
- The 2005 season was the most destructive for the US with damages estimated to be in excess of \$100 Billion.

Hurricane Season – Record Breaking Years!



Individual Storm Records:

Dennis:

- Dennis became the most intense hurricane on record before August when the central pressure of 939 mb was recorded.

Emily:

- Emily eclipsed the record previously set by Dennis for lowest pressure recorded for a hurricane before August with its central pressure reached 929 mb.

Katrina:

- Katrina recorded the greatest storm Surge of 27 feet in the Mississippi from an Atlantic hurricane. The previous record was 24.6 feet in Hurricane Camille (1969).
- Katrina became the most destructive storm on record with greater than \$100 Billion damage. Hurricane Andrew (1992) had approximately \$50 Billion (normalized to 2005 dollars).
- Katrina produced a record wave height in the Gulf of Mexico of 55 feet at Buoy 040 (64 nautical miles south of Dauphin Island, AL).

Hurricane Season – Record Breaking Years!



Individual Storm Records:

Rita:

- Rita's central pressure dropped to 897 mb and was the third lowest pressure ever measured in the Atlantic Ocean.

Vince:

- Vince was the furthest north and east that a storm had ever developed in the Atlantic basin.
- Vince was the first tropical cyclone in recorded history to strike the Iberian Peninsula.

Wilma:

- Wilma had the fastest intensification ever by an Atlantic hurricane.
- Wilma had the smallest eye diameter ever measured in a hurricane – two nautical miles.

Best Practices



- Senior management's new attitude / commitment towards DRP and BCP – perception of risk has changed – new vulnerabilities / threat events recognized.
- Need business continuity as well as disaster recovery plans and not just to appease the auditors.
- Employees must be familiar with their recovery roles and responsibilities.
- Plans must be maintained current and tested.
- Common assumptions must be revisited:
 - Primary or back-up recovery resources may not be available for the recovery effort.
 - A worst case / extended scenario (e.g., one or more buildings not accessible) is possible – local exclusion zones may be enforced: need alternate sites.
 - Primary suppliers may be impacted.
 - Utilities may be unavailable.

Best Practices (cont'd)



- Must consider the impact on business partners, etc.
- Need to document recovery procedures in adequate and appropriate detail.
- Keep it simple: charts, call-trees where possible (30 seconds to read and retain a page of the recovery plan).
- Decentralize internal communications (use of web sites and wireless devices to alleviate communication jams).
- Pay attention to details (ensure names of recovery team alternates are on access lists).
- Primary recovery resources not always able to handle the stress / emotional toll and were ineffective recovery managers.

Best Practices (cont'd)



- Recovery resource allocation: some critical processes could have made do with fewer staff, while some of the processes originally considered less critical needed more staff.
- Physical location of resources: concentrated by function.
- Back-up frequently (including making copies of hard copy vital records like contracts, leases, deeds).
- Validity of the “same geographic quadrant” criteria.
- Store vital records and recovery back-ups off-site and ensure the off-site location is at least several miles from the primary location.

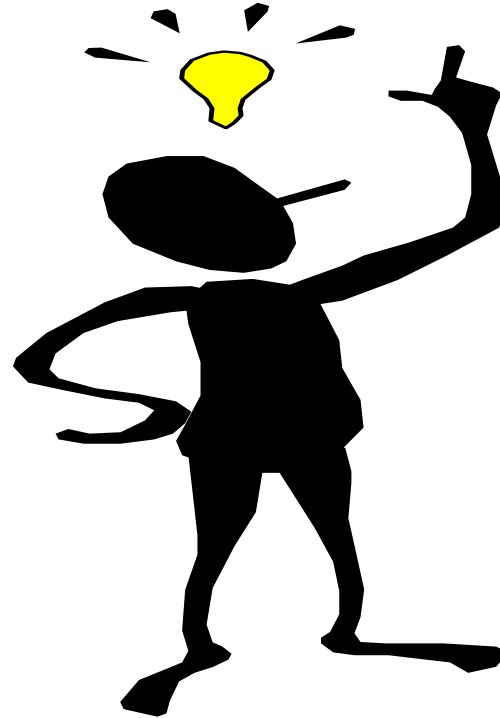
Best Practices (cont'd)



- Don't have the primary and back-up servers in the same building.
- Employees must be familiar with emergency management procedures (e.g., evacuating the building) which should include provisions for the handicapped.
- The ripple effects of a major threat event are global.

People are the most critical issue...

Questions & Answers



Speaker Bio & Contact Information

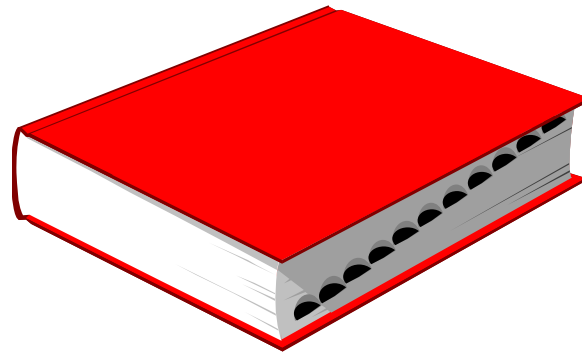


Rick Link, CISA, CISSP, CISM, CGEIT
Global Director IT Audit
Horn Murdock Cole

rick.link@acs-inc.com.com
Cell: 214-986-2786

Mr. Link has over 28 years of diversified business experience in accounting, information technology audit, information security and business continuity management. Currently responsible for global IT audit projects for ACS. Rick has been a Technology Services Practice Director at an international professional services firm. Prior to that role he was Information Security Manager at Perot Systems Corporation and a Senior IT Audit Leader at Electronic Data Systems. Mr. Link developed and implemented the Technology Risk Management Services (TRMS) service offerings for the firm which includes IT audit, security assessments and business continuity management services. He is a frequent speaker at various local, regional and national conferences discussing a variety of risk management topics and knowledgeable of various industry methodologies including COSO, ISO 17799, COBIT, ITIL, GLBA, HIPAA. He is an active member of the ISACA and a past board member several times. Mr. Link is a CISA, a CISSP, and a CISM and holds a BBA, Accounting from Sam Houston State University. He resides in Plano, TX with his wife and three daughters.

Glossary



DRP and BCP Terms



- **Alternate Site:** A back-up location where critical business functions and computer processing are recovered in the event of a disaster.
- **Business Continuity Management (BCM):** An “umbrella” term covering both disaster recovery planning and business continuity / resumption planning.
- **Business Disruption:** Any event, anticipated or not, that interrupts the normal course of business operations.
- **Business Impact Analysis (BIA):** The process of identifying the business processes critical to the profitability and survival of the organization's operations.
- **Business Resumption Planning:** The operational (i.e., business unit) piece of Business Continuity Planning.

Terms (cont'd)



- **Cold-site:** A cold-site (a.k.a. shell site) is a data center without the hardware (e.g., electrical and telecom wiring, fire detection/suppression and environmental control systems, controlled access). Cold-sites are commercially available or may be maintained internally.
- **Continuity Plan:** Arrangements, procedures, and resources held in readiness for use in the event of a disaster to minimize and manage operational impact and financial loss, re-enable mission critical business functions, and ensure regulatory compliance.
- **Critical Business Function:** A logical group of business processes that meet a business need and that, if not performed, would have an unacceptable operational, financial, and/or regulatory impact upon the business.

Terms (cont'd)



- **Disaster:** An unplanned or unexpected event that causes an unacceptable disruption of one or more business processes or support functions for an unacceptable period of time, causing significant operational, financial, and/or regulatory impact on the business.
- **Disaster Recovery Planning:** The technological (e.g., IT) piece of Business Continuity Planning: the advance planning and preparations necessary to minimize loss and ensure continuity of critical business functions.
- **Drop Ship (a.k.a. quick ship):** A recovery option/contractual agreement by which vendors ship equipment at time of disaster to predetermined customer site(s). Equipment is generally available within 72 hours of the customer declaring a disaster.

Terms (cont'd)



- High Availability: Keeping data and systems available for users 24x7.
- Hot-site: A fully equipped 7x24 data center with an existing voice and data network infrastructure which is available and configured to customer requirements within hours of declaring a disaster.
- Mobile Recovery Site: A trailer equipped with hardware, peripherals, and electrical and network hook-ups which a recovery vendor ships to a previously designated customer recovery site, where it is hooked up to existing telecom lines and power supply.
- Portable Shell Site: An environmentally protected and readied structure that can be transported to a disaster site.

Terms (cont'd)



- **Reciprocal Agreement:** An agreement between organizations with compatible computer configurations and potential excess capacity. Both organizations must be able/willing to give up space and/or processing time in the event of a disaster.
- **Recovery Plan:** Detailed procedures and actions taken to recover critical business functions.
- **Recovery Point Objective (RPO or RPT):** The point in time to which data is restored in order to resume processing transactions.
- **Recovery Strategy:** Alternative operating methods for facilities and systems in the event of a disaster.

Terms (cont'd)



- **Recovery Time Objective (RTO):** The time frame by which critical business functions must be recovered. In other words, it is the maximum allowable downtime.
- **Recovery Simulation Test (a.k.a. full recovery test):** A test of recovery procedures under conditions approximating a specific disaster scenario. This exercise requires the simulated recovery of critical business functions across an organization. It is the closest thing to an actual disaster. The full recovery test provides a level of confidence in the ability to recover in an actual disaster.
- **Risk Assessment / Analysis:** The process of identifying and minimizing exposure to an organization's probable threat events
- **Temporary Operating Procedures:** Predetermined procedures that streamline operations at time of disaster while maintaining acceptable levels of control and auditability.

Terms (cont'd)



- Threat: An event which can cause a disaster and disrupt critical business functions. Threats can be natural (fire, flood, tornado, earthquake), or man-made (sabotage, computer virus, human error), or technological (power outage, telecom failure, equipment failure, software bug).
- Warm-site: An alternate processing site which is only partially equipped.