Protecting Information Assets
- Week 8 -

Business Continuity and Disaster Recovery Planning
MIS5206 Week 8

- Lecture: BCP/DRP
- Mid-term Review
- Test Taking Tip
- Quiz
- Next week – guest lecturer
Reading

- Vacca Chapter 36

- ISACA Assignments:
  
  - ISACA Assignment 2: “What Every IT Auditor Should Know About Backup and Recovery”
Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)

• **Operating disruptions can occur with or without warning**
• **Results may be predictable or unanticipated**
• **It is important that the mission of the enterprise is sustained during any emergency**

• **The first priority is always the safety of the people:** Employees, Service and Support Staff and Visitors
**Business Continuity - versus - Disaster Recovery**

**Business Continuity Plan (BCP)**

Provides procedures for sustaining mission/business operations while recovering from a significant disruption caused by a natural or human-induced disaster.

**Disaster Recovery Planning (DRP)**

Provides procedures for relocating critical information systems operations to an alternative location after a significant disruption caused by a natural or human-induced disaster.
Business Continuity Plan includes...

Many plans:
1. Continuity of operations plan
2. Disaster recovery plan
3. Business resumption plan

May also include:
4. Continuity of IT support plan
5. Crisis communications plan
6. Incident response plan
7. Transportation plan
8. Occupant emergency plan
9. Evacuation and emergency relocation plan
Business Continuity Management

• The Business Continuity Plan (BCP) is developed to help assure the organization’s ability to maintain, resume, and recover the business
  *It is not just about recovering information technology capabilities*

• Planning focuses on the entire enterprise’s mission critical infrastructure
  1. People
  2. Processes
  3. Technology

• Thorough business impact analysis (BIA) and risk assessment form the foundation of an effective Business Continuity Plan

• BCP effectiveness can only be validated through testing and practical application

• At a minimum the BCP should be updated annually to reflect and respond to changes in the organization’s priorities, resources/capabilities, and risks - including its IT service provider(s)
Business Continuity Management (BCM)

An important and big topic:

– How to maintain the continued operation of the business’ processes?
Business Continuity Management (BCM)

**Prerequisite:** Good documented models of the business’ processes, broken down into a series of hierarchical layers of sub-processes, sub-sub processes...

1. Business processes
2. Resources needed to run processes
3. Threats, vulnerabilities and risks
4. Business Impact Analysis (BIA)
5. Develop recovery strategies
6. Plan, design and implement recovery plans
7. Testing
   - Maintenance (update), Awareness, Training (practice)

... Repeat
BCM: Meta processes of large enterprises

There may be 5 or 10 high-level business processes (“meta-processes”), for example:

1. Develop product offerings
2. Bring product offerings to market
3. Acquire customer orders
4. Fulfill customer orders
5. Manage and administer the business
   • For example has 6 sub-processes...

Each process can be decomposed into a further level of detailed sub-processes
   • some run in parallel
   • some in sequence...

BCM: Top-down business process analysis

Also known as: Structured decomposition

If there are 10 ‘Level-1’ processes, each of which can be decomposed into 10 sub-processes at the next level of detail, which in-turn each of which can be decomposed into 10 sub-sub-processes at the next level of detail...

...the total # of processes in the model can grow exponentially

Organizations that achieve this level of detail have an excellent model for understanding their business and business continuity management

A professional automated tool is used to:
• Support this analysis
• Store the details
• Keep the model up to date
• Delegate process ownership at each level of detail to those with operational responsibility

Business Continuity Management Process

Step 1

• Identify and map business processes
• Assess the business impact of loss of each business process
• Classify and rank the business processes into 3 or 4 groups

1. **Critical** – Loss of this process will destroy the business
2. **Severe** – Loss will cause persistent, severe damage to the business
3. **Significant** (optional) – Loss will cause significant damage
4. **Other** – Damage caused by loss of this process can be absorbed

BIA – Business Impact Analysis

Step 2

- Select each Critical and Severe process
- Analyze all sub-processes
  - Down to single functional steps to discover all the process and functional components needed to keep this high-level process in continuous operation

Methodology

1. Identify mission-critical work processes to support
2. Analyze “as-is” work processes
   – Identify users
   – Document work processes
   – BIA
3. Prioritize work processes for supported
4. Train users, test
5. Measure and analyze performance (Metrics!)
6. Make improvements
Work processes to support

Service requests and utility maintenance management work orders

– City’s Public Works Department
– 4 Divisions (230 employees)
  » Operations
  » Transportation
  » Sewer
  » Water
Service Request / Work Order
Computerized Maintenance Management System (CMMS)
Business Process Modeling

A collection of Swim Lane models document the work processes of each DPW Division.

Sewer Work processes
Business Process Modeling

Water work processes
Operations work processes
Business Continuity Management Process

Step 3

- For each sub-process or function identified in Step 2:
  - What resources are needed
  - How much of each resource is needed
  - People
  - Information and communications technology
  - Equipment
  - Raw materials
  - Accommodations
  - Communications
  - ...

BIA goals:

- Identify the most critical business functions necessary for the survival of the company
- Identify the necessary resources for those critical functions
- Calculate:
  - **Recover time objective (RTO):** Maximum acceptable amount of downtime the company can endure for each resource
  - **Recovery point objective (RPO):** Maximum acceptable amount of data loss (measured in time, but implies # of data records)
  - **Interruption window:** Maximum period of time organization can wait from point of failure to critical services/applications restoration
  - **Service delivery objective (SDO):** Level of services to be reached during the alternative process mode until the normal situation is restored
  - **Maximum tolerable outage (MTO):** Maximum time the organization can support processing in alternative mode
Business Continuity Management Process

Step 4

• For each resource identified in Step 3, what is the high-level threat scenarios put that resource at risk?

• Focus on effects, not cause

### Inventory of Work Processes and Staff needed from a Single DPW Division

<table>
<thead>
<tr>
<th>Sewer Division</th>
<th>Sewer Collection</th>
<th>Street &amp; Sewer</th>
<th>CSO System Supervisor</th>
<th>Chief Construction Inspector</th>
<th>Sewer Inspector</th>
<th>Construction Inspector</th>
<th>Complaint Person</th>
<th>CCTV Crew</th>
</tr>
</thead>
<tbody>
<tr>
<td>Street Repair</td>
<td>Laterals and Sewer Mains, Install (City)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Laterals and Sewer Mains, Install (Contractor)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Laterals and Sewer Mains, Repair</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Manhole, Repair &amp; Replace</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Catch Basins, New</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Catch Basins, Repair &amp; Replace</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Lamphole Repair &amp; Replace</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CCTV &amp; Cleaning</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CSO Cleaning &amp; Repairs</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Street Repair (cave in)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Miss Utility Stake Outs</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Understanding cross organizational workflows...

Identifying dependencies on critical paths for completing prioritized work processes

MIS 5206 Protecting Information Assets
Gaining an Understanding of Staff Needed to Support Mission Critical Work

<table>
<thead>
<tr>
<th>Water Divisions</th>
<th>Operations Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meters</td>
<td></td>
</tr>
<tr>
<td>Water Quality</td>
<td></td>
</tr>
<tr>
<td>Sewer Collection</td>
<td></td>
</tr>
</tbody>
</table>

DPW work is often supported by staff of a number of DPW Divisions, other City offices, and outside agencies.

MIS 5206 Protecting Information Assets
Business Process Analysis Results in an Integrated Overview of how DPW Work is Coordinated
Business Continuity Management Process

Step 5

• For each resource/scenario combination
  – Are the current resources provided with sufficient resilience for the overall business to withstand the impacts of the scenario?
• Are there any single points of failure?
Step 6

- What additional resource protection is needed to provide the required level of resource resilience so the overall business can withstand the threat scenarios?
- For example:
  - Preventive measures to avoid the threats materializing
  - Containment measures to limit the damage
  - Redundancy of resources to avoid single points of failure and to provide fallback capacity
  - Incident management plans including (DRP!)
  - Recovery plans to resume business following an incident
  - Training and awareness
Disaster Recovery Planning

- Establish a planning group
- Establish priorities for applications, data and networks
- Develop recovery strategies
- Prepare inventory and documentation of the plan
- Develop verification criteria and procedures
- Implement the plan
Disaster Recovery Plan

- **Primary facility recovery and backup sites:** If primary site is destroyed, where should processing take place
- **People:** Human resources is the resource that is most forgotten about
- **Hardware:** Replacement time requirements, SLAs from suppliers, dangers of legacy, and/or proprietary devices
- **Software:** Necessary applications, and supporting utilities and operating systems for production
- **Data:** If not fault-tolerant (e.g. mirroring), will need to load backed up data to restore processing
- **Communication to different entities after a disaster:** Employees, customers, stock holders, suppliers, media
- **Security:** Protecting against looting and fraudulent activities after a disaster
- **Legal responsibilities**
- **Employees' responsibilities to families:** May need to tend to their families instead of helping the company get back on its feet
Disaster recovery time targets

Disaster recovery must be achieved within critical deadlines

– Need for careful analysis
  • Of business needs for recovery of services
  • Time-criticality of various information services

Speed of recovery must be traded off against cost

– If needed, non-stop 365 day by 24-hour service can be maintained, but it pushes the cost up very high
– Business needs and justifications must be worked out in detail to plan disaster recovery
  • Remember: *The only goal is to create effective business continuity, whatever that turns out to be*
Develop Recovery Strategies

• Strategies, resources, timelines and dependencies are documented

• Approaches to “re-initiate” crucial business functions and resume on-going operations are developed and documented

• These are reviewed and confirmed (signed off) by function owners in the business as well as executives

Computer Operations

Areas of Focus:

- Sites/ Locations/ Facilities
- Computers and Infrastructure (Hardware)
- Operating Systems
- Applications and supporting utilities (software)
- Data
- Supplies
- Documentation
- Personnel
Offsite recovery alternative facilities

**Hot site:** A geographically remote facility, fully equipped and ready to power up at a moments notice

**Mobile site:** A packaged modular processing facility mounted on transportable vehicles and kept ready to be delivered and set up at a location specified on activation

**Warm site:** Less expensive alternative to hot site, includes communications components but computers are not installed – will need to be delivered and setup

**Cold site:** Less expensive than warm site, provides only the basic environment that can be outfitted with communication components and computers, though this may take from one to several weeks

**Shared site:** Least expensive arrangement (“reciprocal agreements”) with compatible companies who agree to host each other's employees and business functions in the event of a disaster

- Most risky alternative - few companies maintain extra capacity and equipment suitable to host another company's business processes
- Better than having no plan at all
## Application Systems

### Classification of Applications*

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 Mission Critical | Mission Critical to accomplishing the mission of the organization  
Can be performed only by computers  
No alternative manual processing capability exists  
Must be restored within 36 hours |
| 2 Critical | Critical in accomplishing the work of the organization  
Primarily performed by computers  
Can be performed manually for a limited time period  
Must be restored starting at 36 hours and within 5 days |
| 3 Essential | Essential in completing the work of the organization  
Performed by computers  
Can be performed manually for an extended time period  
Can be restored as early as 5 days, however it can take longer |

* From SANS
Availability of replacement software

- Operating systems, programs and utilities used during regular business must also be backed up regularly to the offsite facility.

- A program built for a particular version of an operating system, will not run if the wrong version of the operating system is installed at the offsite facility.

- Data is formatted to a particular version of a program (e.g. spreadsheet), and that version is not also updated to the backup facility, it is possible that the data will not be available for use in the time of need.
Availability of people after disaster

• Attention focused on backing up data and technology, often overlooks people and necessary skillsets for continuing the operation of the enterprise

• Employees may not be available after a disaster:
  – Death, injury, or family responsibilities
  – Business continuity committee
    • Must identify the necessary skill set for each critical task
    • Come up with back up solutions (e.g. using temp agencies or cross training individuals)
Data backup systems and redundancies

- Database shadowing
- Electronic vaulting
- Remote journaling
- Storage area network and hierarchical storage management
- Shared storage
- RAID
- Failover clustering
Plan Design & Development

• Recovery Strategies Scenarios are integrated and synchronized

• Formal Plan document is created

• Stakeholder review and sign-off on the plan
• Testing is the ONLY way that a plan can be assessed for effectiveness

• Testing can be expensive and must be prioritized with high level sponsorship

• This requires an ongoing commitment by the business as the plan must be re-assessed on a regular basis
Recovery and testing

After a disaster two teams may be assembled:

• *Salvage team*
  
  – Assesses damage and works to bring the businesses’ primary facility back on-line

• *Recovery team*

  – Coordinates bringing up the alternative site
  – To be sure everyone knows what to do, tests are conducted
    
    • Range from troubleshooting the plan by simply walking through the documents detailing the sequence of events, to actually rehearsing the plan up to the point of actual data or resource recovery at the main site.
Mechanisms that support disaster recovery services include:

- **Contingency sites**
  - Redundancy of hardware and communications lines for resilient operations

- **Data management tasks**
  - Taking appropriate backups of data and software
  - Providing backup management: labeling, indexing, storage
  - Off-site storage
  - Data recovery and restoration procedures

- **Recovery plans and procedures**

- **Incident management responsibilities**

- **Activation plans**
DRP Testing Approaches

Tests are conducted to be sure plan is good, everyone is prepared and knows what to do.

These can range from:

- Checklist review
- Tabletop exercise
- Structured walk-through
- Dry-Run tests
DRP Testing Approaches

- **Checklist review**
  - Simplest, least labor-intensive form of testing
  - Each individual has a checklist of responsibilities under the DRP
  - During testing, each individual reviews his/her checklist
  - Can be done as a group or individually

- **Tabletop exercise**
  - Test facilitator describe a specific disaster scenario
  - DRP team members verbally walk through their responses to the scenario
  - Scenarios can be disseminated at the test or in advance
DRP Testing Approaches

• **Structured walk-through**
  • More formal troubleshooting of the plan by simply walking through the documents detailing the sequence of events

• **Dry-Run tests**
  • Can be conducted on a function by function basis
  • Do not have test all functions for each cycle
  • Tests should involve actual interruptions and recoveries
  • Actually rehearsing the plan up to the point of actual data or resource recovery at the main site
Testing is necessary for all DRPs

Perform testing on the DRP periodically to ensure that the plan works and that the entire organization knows what to do in the event of a disaster.

- **Walkthrough**: Requires no disruption to the organization’s day-to-day activities. With this method, the plan is tested verbally with all of the DR Teams.
- **Simulation**: Requires no disruption to the organization’s day-to-day activities. With this method, the plan is tested in a disaster simulation, the standby facility is brought on-line to make sure that it is fully operational.
- **Parallel Testing**: Requires no disruption to the organization’s day-to-day activities. The plan is tested in the standby facility using the historical data. This data is processed to ensure the same results as the primary facility are produced.
- **Full Interruption Testing**: Requires disruption to the organization’s day-to-day activities. With this method, the plan is tested in a full disaster scenario where the primary facility is brought down and the business runs off of the standby facility alone. This method also tests whether the organization can successfully go back to the primary facility following a disaster.
Emergency response testing

Emergency response drills prepare the organization’s people to:

– Preserve life and minimize asset damage
– Reduce the chance of fraud, theft and vandalism
  • Security mechanisms usually in place may be completely disabled

By putting in place processes that:

– Identify actions taken immediately to avoid injury and loss of life
– Alert authorities and notify management
– Contain damages if possible
– Rescue critical data and equipment
Audit Focus Areas

<table>
<thead>
<tr>
<th>Areas for audit evaluation:</th>
<th>Figure 3—Possible Tests/Procedures for Backup and Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>• Review or observe backup procedures.</td>
</tr>
<tr>
<td></td>
<td>• Review documentation of a successful restore</td>
</tr>
<tr>
<td></td>
<td>(within the last year).</td>
</tr>
<tr>
<td></td>
<td>• Verify restoration personally (when risk is high</td>
</tr>
<tr>
<td></td>
<td>or restoration is an audit objective).</td>
</tr>
<tr>
<td>Site/computers/OS</td>
<td>• Review the provisions of the BCP/DRP.</td>
</tr>
<tr>
<td></td>
<td>• Review a contract (hot site, cold site, mutual</td>
</tr>
<tr>
<td></td>
<td>aid, etc.).</td>
</tr>
<tr>
<td></td>
<td>• Verify the ability to restore these aspects.</td>
</tr>
<tr>
<td>Applications</td>
<td>• Review the plan’s provisions.</td>
</tr>
<tr>
<td></td>
<td>• Review the critical applications list, including</td>
</tr>
<tr>
<td></td>
<td>ranking.</td>
</tr>
<tr>
<td></td>
<td>• Verify the ability to restore (personally, when risk</td>
</tr>
<tr>
<td></td>
<td>is high or restoration is an audit objective).</td>
</tr>
<tr>
<td></td>
<td>• Observe or inquire about the backups of application</td>
</tr>
<tr>
<td></td>
<td>software and location.</td>
</tr>
<tr>
<td>Supplies/documentation</td>
<td>• Review the plan’s provisions.</td>
</tr>
<tr>
<td></td>
<td>• Observe or inquire about the provisions and location.</td>
</tr>
<tr>
<td>Recovery team</td>
<td>• Review the plan’s provisions.</td>
</tr>
<tr>
<td></td>
<td>• Interview one or more members of the team, and ask</td>
</tr>
<tr>
<td></td>
<td>about roles and responsibilities.</td>
</tr>
<tr>
<td></td>
<td>• Gain assurance that there is provision for adequate</td>
</tr>
<tr>
<td></td>
<td>personnel for a successful restoration.</td>
</tr>
</tbody>
</table>
Test Taking Tip

Don’t Revise Your Answer
(without a very strong reason)

• Your first answer is probably the right one

• On an exam where there is no penalty for wrong answers, you are just using time that might have gone to getting another correct answer

• If you are having second thoughts, plan to come back to that question after you have completed the entire test
Quiz