Disaster Recovery/Business Continuity Planning

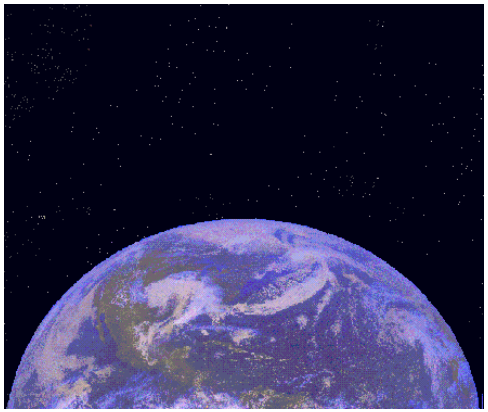
Lunchtime Seminar

3 June 2004

Debby Dix CISSP, CBCP

Overview

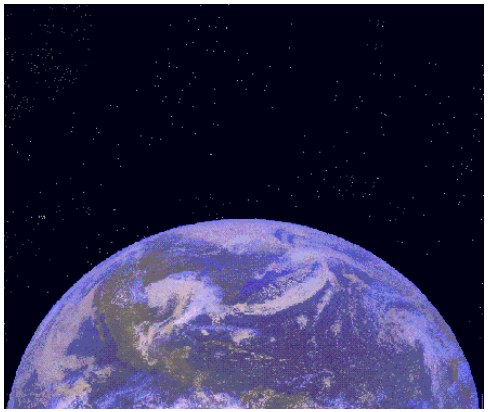
- Basic Terminology
- Are there differences between Contingency Planning, Disaster Recovery, Continuity of Operations Planning, and Business Continuity Planning? If so, what are they?
- Common perceptions, assumptions, and myths
- What's the real story? Dispelling those myths
- Where are we in the process?
- What about OSO's Plans?



Terminology

- **Recovery Point Objective (RPO) – The point in time to which data must be restored in order to resume processing transactions. RPO is the basis on which a data protection strategy is developed.**

- **Recovery Time Objective (RTO) – The maximum acceptable delay time by which a function must be restored…period from the disaster declaration to the recovery of the critical function.**



What's the Difference?

- Disaster Recovery (DR)
  - Focuses on what to do AFTER something bad has happened
  - Primarily IT focused
  - Reactive
- TS2000 Contingency Planning
  - DOC-mandated software designed to incorporate security and contingency planning into one place
- NOAA Continuity of Operations Planning (COOP) Template
  - Focuses most specifically on high-level strategies, orders of succession and the "first 30 days"

What's the Difference?

- **Business Continuity Plan (BCP)**
  - **More proactive**
  - **Includes operational entities and their functions rather than just IT**
  - **Attempts to ensure critical functions and systems REMAIN operational, or are at least restored within an acceptable predefined period of time (Recovery Time Objective)**
  - **Attempts to define point in time to which the clock is "re-set" (Recovery Point Objective)**
  - **More comprehensive than either TS2000CP or the NOAA COOP Template.**
  - **Provides activity checklists and step-by-step guidance**

Perceptions, Assumptions, and Myths

- Only large organizations/offices need a plan, and it only needs to address IT
- It isn't worth the time, effort, and expense
- Once a plan is written, you can relax. The task is over
- The bigger the better
- If I say my functions are not critical, then what I do won't be considered important (job security?????)
- Plans need to be developed to address all anticipated scenarios

Perceptions, Assumptions, and Myths (cont')

- This planning stuff is all just a waste of time and will only be worth the effort should a disaster happen. And what are the chances of that?

- It's vital to ALWAYS "pass" BCP tests to prove to management that staff knows what they're doing

The Truth - Dispelling those Perceptions, Assumptions, and Myths

- Everyone needs a plan – though your plan may be to just backup files and should something happen, just buy new and start over

- It's more expensive to lose everything and be shut down should something happen! And then there's the cost of damage to reputation (and possible Congressional funding)!!

- The plan is obsolete once put to "paper". Constant updates and maintenance are required. You can't recover on "last year's documentation"!

Dispelling those Perceptions, Assumptions, and Myths (cont')

- The smaller and more focused the better. Time is critical and personnel only need to have those portions of the plan which pertain to them
  - Who? What? Where? How many? By when?
  - "Cookbook"

- Big differences between "critical" vs. "time sensitive" and "contingency operations" vs. "business as usual"

- Focus on the 3 big areas – loss of personnel, system outage (IT), and denial of access (facility), then implement in degrees

- Analyzing your organization often greatly increases efficiency by reviewing/improving process flows.

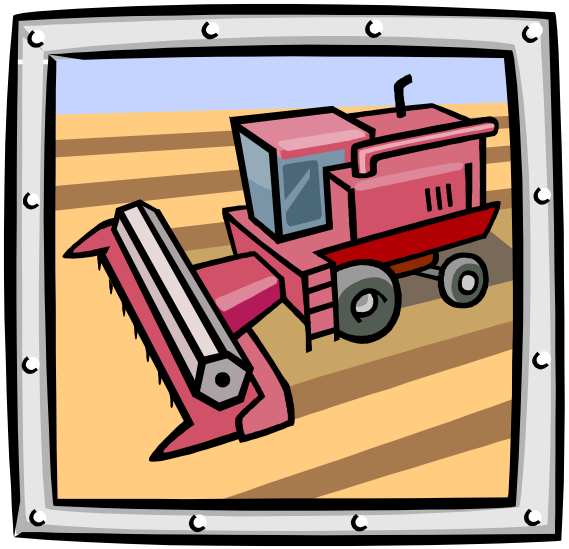
Dispelling those Perceptions, Assumptions, and Myths (cont')

- **Tests are NOT tests (in the traditional sense e.g., pass/fail); they are "exercises". Their goals are NOT to make sure personnel know their jobs, but rather to make sure what's documented is sufficient and accurate and to identify things that can be improved PRIOR to a real disaster. If you're not finding something that can be improved, you're not "testing" strenuously enough!**

Phases

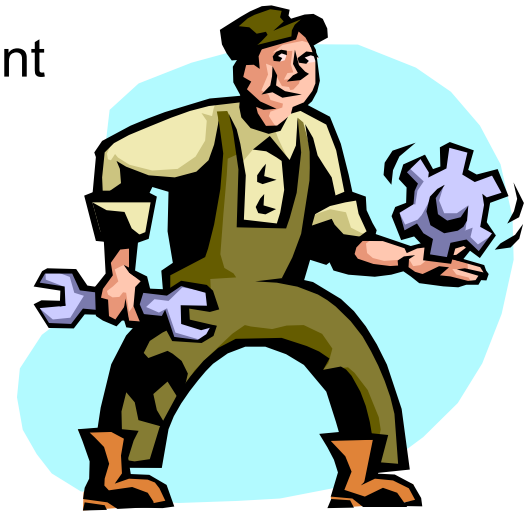
- *Project Initiation Phase*
- *Functional Requirements Phase*
- *Design and Development Phase*
- Implementation Phase
- Testing/Exercise Phase
- Maintenance Phase

Italics indicates completed



Implementation (or Preparation) Phase

- Develop the Preparation Plan
  - Key activities that must be performed “in advance” of an event to ensure a viable recovery posture
  - Assign responsibility for their accomplishment
- Develop BC Plan Maintenance Procedures
  - Type, frequency, responsibility
- Develop BC Team Training and Plan Testing/Exercising Programs
  - Type, frequency, responsibility
  - Scenarios?

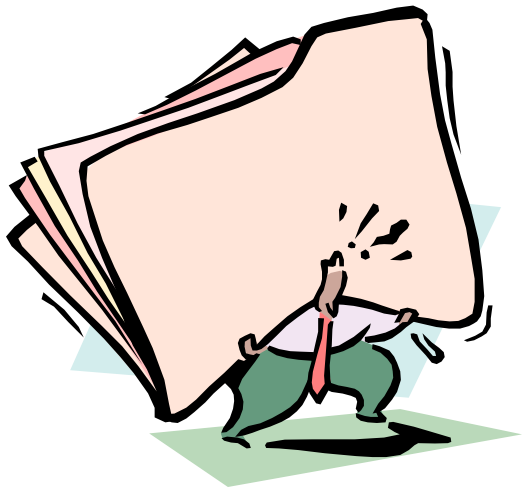


Test/Exercise Phase

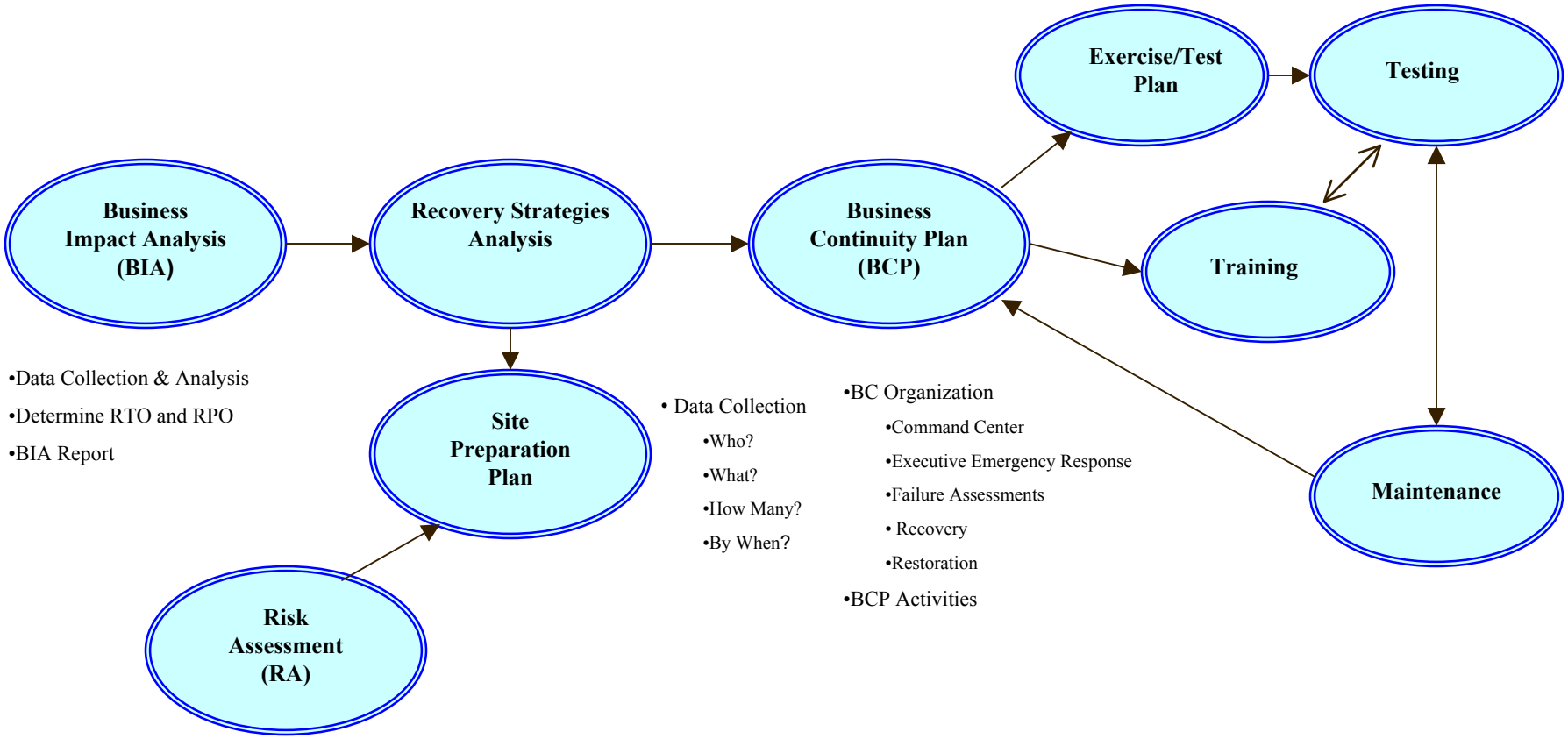
- Implement BC Team Training and Plan Test/Exercise Programs
- Conduct on-going training and testing/exercising
  - Ensure BCP is accurate and up-to-date
  - Provides vehicle for training
  - Ensures continued familiarity with plan contents
  - Activities
    - Preparation
    - Test/Exercise Event
    - After-action (or post-exercise) evaluation
- Test vs. Exercise – What's the difference?
  - Test Objectives
  - Test/Exercise to the point of failure

Maintenance Phase

- Implement BC Plan Maintenance Program
  - Ensure “lessons learned” during test/exercise are incorporated into “master” BCP
  - Ensure BCP remains current
  - Ensure personnel are/remain aware of their respective responsibilities
- Ongoing Process



DR/BCP/COOP Activity Life Cycle



So, What About OSO's Plans?????

- **Yes, Virginia….OSO HAS been developing Business Continuity Plans (BCP) for its Satellite Ground Systems!**
  - **Overarching SOCC Plan**
    - **Establishes command center and executive response teams to manage/coordinate reaction and resolution to an emergency**
    - **Provides guidance for initial notification, failure assessment, recovery, and restoration**
    - **Includes recovery and restoration activities for all three contellations (i.e., it's the master plan for OSO operations in FB4)**
  - **Individual "mini plans" for each respective constellation (i.e., GOES, POES, DMSP) "go team" (deployment team)**
  - **Individual plans for Wallops and Fairbanks CDAs**

So, What About OSO's Plans????? (cont')

- So, are we all done?
  - No!!! It's an ongoing process….we're never really done.
- So, do we have to redo all of our operating procedures to fit them into this new BCP format?
  - No!!! Wouldn't that just be too cumbersome to try to maintain? OSO has excellent operation procedures already documented. These plans supplement documents you already have, and are very familiar with. They are referenced in the BCPs (to include their name and where they are found.)
- I didn't know this was happening and don't know what I'm supposed to do?
  - That's why we're going to be having ongoing training and exercise programs.

So, What About OSO's Plans????? (cont')

- Do I have to follow the plan from start to finish?
  - It would be nice if that were always the case. However, since "disasters" don't necessarily follow a plan, we've built flexibility in to these BCPs. If something doesn't apply (e.g., no equipment has been affected, we just can't access the facility), then those sections can be skipped over.)
- What if I find something in the BCPs that's wrong?
  - Please tell your supervisor. These are YOUR plans. They are living documents and should reflect YOUR contingency operations. If something doesn't work, then it should be changed!!!

Questions?

Thank you for your attention.

For further information:

Deborah A. Dix, CISSP, CBCP
deborah.dix@mitretek.org
(703) 610-2909