CISSP
Business Continuity Planning and Disaster Recovery Planning

Disaster Recovery Planning (DRP)

- **Introduction**
  - A statement of actions to take before, during, and after a disruptive event
  - Procedures for responding to an emergency, providing backup operations during a disaster
  - Goals and objectives
- **Data processing continuity**
  - Mutual aid agreements
    - Providing Backup systems and facilities
    - Reciprocal
  - Subscription services
    - Hot Site
      - Fully configured with HVAC
      - F&P and Workstations
      - Servers with Apps
      - Allows walk in
      - Short time
      - High cost
    - Warm Site
      - In between hot and cold
      - HVAC
      - Simple infrastructure
      - Not all systems
      - Medium time
      - Medium cost
    - Cold Site
      - HVAC
      - No hardware on site but ready for it
      - Long time
      - Low cost
    - Mobile Site
      - Variation of a cold site
      - In a truck or trailer
      - HVAC
  - Multiple centers
    - Processing spread over multiple centres
  - Service bureau
    - Contract with a bureau for alternative backup processing
  - Transaction Redundancy
    - Electronic Vaulting
      - Backup off site
      - Restore from remote
    - Remote Journaling
      - Parallel processing of transactions at remote site
    - Database Shadowing
      - Like journaling but creates more redundancy by duplicating the database sets
- **Testing the Plan**
  - 5 DR Tests
    - Tested on a regular basis
    - No recovery ability exists until the plan is tested
    - Verifies the accuracy of the plan
    - 1 Checklist
      - Distribute plan for review
    - 2 Structured Walk Through
      - BU managers walk through the test plan for review
    - 3 Simulation
      - All people involved go through a practice session
    - 4 Parallel
      - Primary processing does not stop
      - Most common
    - 5 Full Interruption
      - Cease normal operations
      - Best but scary
- **Recovery Procedures**
  - Recovery Team Duties
    - Implement the recovery procedures in a disaster
    - Get critical functions operating at backup site
    - Retrieval of materials from off site storage
    - Installs critical systems and applications
  - Salvage Team Duties
    - Separate from Recovery team
    - Returns primary site to normal operating conditions
    - clear and repair the primary processing facility
  - Normal Operations Team
    - May be a task of the recovery team
    - Returning production from DR to primary
    - Disaster not over until all operations have returned to their normal location and function
  - Other Recovery issues
    - External Groups
    - Employee Relations
    - Fraud and Crime
    - Financial Disbursement

Business Continuity Planning (BCP)

- **Introduction**
  - **BCPs are created to prevent interruptions to normal business**
    - Protect critical business processes from natural or manmade disasters
    - Strategy to allow for the resumption of normal business activity
    - Examine all critical information areas
      - LAN /WAN
      - Telecomms
      - Apps and Data
    - Disruptive Events
      - Staff Duties
      - Manmade events
        - Including strikes
    - The Number One priority is to preserve life
- **Four Prime Elements**
  - **Scope and Plan Initiation**
    - Companies operations
    - Create detailed account of the work
    - List resources
    - Define management practices
    - Roles and responsibilities
      - BCP Committee
        - management
        - IT
      - Deal with scope of plan
      - Senior management
        - Ultimate Responsibility
        - Includes all phases
        - Support is essential
        - Concept of due diligence may hold management responsible if a loss occurs with due care could have prevented it
  - **BIA**
    - A document to understand the impact a disruptive event would have on the business
      - Impact may be financial or operational
    - Vulnerability assessment is normally a part of the BIA
    - 3 primary Goals
      - 1 Criticality Prioritization
      - 2 Downtime estimation
        - maximum Tolerable Downtime (MTD)
      - 3 Resource requirement
    - 4 Steps of the BIA
      - 1 Step 1 – Gather Assessment Materials
      - 2 Step 2 – Vulnerability Assessment
        - Quantitative Loss Criteria
          - Financial Loss
        - Qualitative Loss Criteria
          - Loss of competitive advantage
          - Loss of public confidence
      - 3 Step 3 – Analyze Information
      - 4 Step 4 – Document results and present recommendations
  - **BCP development**
    - Create a recovery plan
    - Two steps
      - 1 Define the continuity Strategy
        - Computing
        - Facilities
        - people
        - Supplies and equipment
      - 2 Document the continuity strategy
  - **Plan Approval and Implementation**
    - Must contain a rapid map for implementation
    - Senior management approval
    - NOTE THIS IS NOT A TEST OF THE PLAN

MindCert.com
Utilize the power of your mind

Motivation and Study Techniques to help you learn, remember, and pass your technical exams!

- Cisco
- CISSP
- CEH
- More coming soon...

Visit us www.mindcert.com