Business Continuity Plan

* Business Continuity Planning (BCP)
* Disaster Recovery Planning (DRP)

BCP PHASES

* Project Scope and planning
* Business Impact Assessment
* Continuity Planning
* Approval and implementation

Phase 1: Project Scope and planning

1. Identify Stakeholders
   1. Operational departments
   2. Critical support services
   3. Senior Leadership
2. Select Team Members
   1. Representatives of stakeholders
   2. Technical experts in each BCP area
   3. Security professionals
   4. Legal
3. Determine Resource Requirements to:
   1. Develop the plan
   2. Test, train and maintain the plan
   3. Implement in an emergency

Phase 2: Business impact Assessment

* Gap analysis of business processes that identifies:
  + Recovery Time Objective (RTO)
  + Maximum Tolerable Outage (MTO)
  + Recovery Point Objective (RPO)

Phase 3: Continuity Planning

* For each risk, select one of the four risk management strategies
  + Avoid
  + Mitigate
  + Accept
  + Transfer

Phase 4: Approval and Implementation

* Document the plan
  + Written documentation is key
  + Place copies where everyone can locate it
  + Provides an historical record
* Training and Education
  + Everyone needs to know their role
  + Leaders need the big picture
  + Initial and refresher training should be used in combination

DISASTER RECOVERY PLANNING

TYPE OF DISASTERS

* NATURAL DISASTERS
* MAN-MADE DISASTERS

DISASTER RECOVERY PLANNING GOALS

* Rapidly establish an alternate processing facility
* Maintain operations at that facility for extended period of time.
* Efficiently transition back to the primary facility.

Alternate Processing Facilities

* Hot sites: contain all of the hardware, software and data you need to run (recovery time measured in seconds)
* Warm sites: contain hardware and software, but no data (Recovery time measured in hours)
* Cold Sites: contain support systems [HVAC, telecom) but no equipment (Recovery time measured in weeks)

Testing and maintaining the plan

* Checklist reviews
* Tabletop exercises
* Soft parallel tests
* Hard full-interruption Tests

Practice