**Module 5 Risk Management**

**5.6 Disaster Recovery/Business Continuity Plan**

**Planning Documents**

* Business Continuity Plan (BCP) – ensure restoration of organisational functions in shortest possible time, even if services resume at reduced level of effectiveness/availability (Similar to Continuity of Operations Plan COOP)
* Disaster Recovery Plan (DRP) – ensure full recovery of operational capacity following disaster (natural/manmade)
* Should be determined & written prior to incident
* Restoration plan should include contingency planning

**Recovery Sites**

* Backup sites – locations for recovering systems &/or business operations
* Hot site

1. Servers, networks & telecommunications equipment in place & on-line to re-establish service
2. Most expensive

* Warm site

1. Some equipment in place
2. May not be online
3. Requires administrators to install & configure systems to resume operations

* Cold site

1. Facility that isn’t immediately ready to use
2. May need to bring own equipment
3. Least expensive

**Order of Restoration**

* Prioritised restore sequence
* Based on Business Impact Assessment (BIA)
* Most critical systems restored first
* RTO (Recovery Time Objective) – max amount of time process/service allowed to be down & consequences still acceptable
* RPO (Recovery Point Objective) – point last known good data prior to outage that is used to recover systems

**Types of Backups**

* Full

1. Complete backup of data
2. Most time & resource intensive form of backup

* Incremental

1. Need full backup
2. Capture what has changed since last incremental backup
3. Need each incremental backup along with full for complete restoration

* Differential

1. Saves data that has changed since last full backup
2. Needs full backup & most recent differential backup

* Copies & snapshots – like full backup. Stored on system

**Backup Strategy**

* Grandfather-father-son backup – define 3 sets of backups. 1st set, son, represents daily backups. 2nd set, father, used to perform full backups. 3rd set, grandfather, used to perform full backups on last day of each month

1. Over time, son becomes father & father the grandfather
2. Most common strategy

**Geographic Considerations**

* Alternate site planning
* Location for recovery
* Utilities
* Proximity to main site
* Personnel
* Legal implications
* Use of cloud services

**Continuity of Operations Planning (COOP)**

* Policies & procedures – designed to ensure that organisation can recover from potentially destructive incident & resume operations as quickly as possible following event
* Ensures systems, data & personnel availability
* Failover – system redundancy
* Availability of alternate processing, work sites & facilities
* Alternate business practices
* Testing, training & exercises (see 5.4)