RPO & RTP – Concept & Implications

(Module - 3 : DISSA Course)

Arijit Chakraborty

Feb 06, 2022

STEPS OF BCP & DRP:

- **1. Define Key Assets & Operations**
  (BC/DR) efforts start with identification of key assets of infrastructure & processes - important to keeping business operational.
- **2. Determine Downtime, Availability, & Recovery Window**
  Time is money.
- Determine value of investment used to strengthen BC/DR Plan.
- **3. Define Recovery Solutions**
  Define appropriate approach & solutions based on defined assets & recovery window.

4. Draft a Plan

BC/DR plan : Key processes, communication SOP & assigned responsibilities

5. Establish a Communications Plan & Assign Roles

Establish communication plan & assign roles to key members of BC/DR team.

6. Disaster Recovery Site Planning

decide on systems or capabilities required to deliver BC/DR plan.

7. Accessing Data & Applications

Define communications & security protocols for accessing data & apps.

8. Update the BC/DR Plan, In Detail

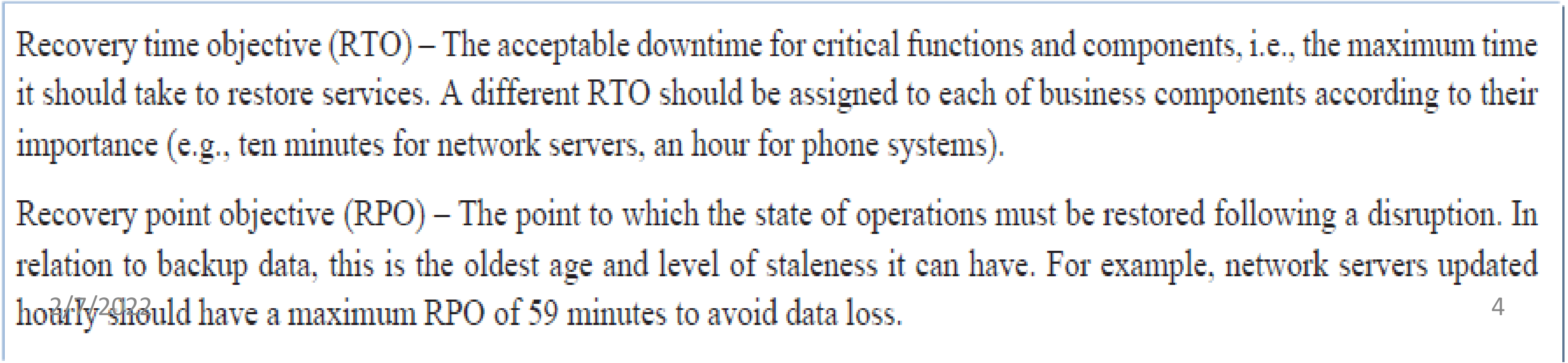
Develop detailed plan for each system & review what needs to be in place **to implement failover to secondary/redundant connections & offsite storage.**

9. Test , Refine & Audit BC/DR Plan

Organize & execute according to each system's plan.

Step D : Develop Key Recovery Targets

- **Recovery time objective (RTO)**
  - Period of time from disaster onset to resumption of business process
  - Based on acceptable downtime
  - Indicates earliest point in time at which the business operations must resume after a disaster
- **Recovery point objective (RPO)**
  - Maximum period of data loss from onset of disaster counting backwards
  - Amount of work that will have to be done over



Recovery time objective (RTO) – The acceptable downtime for critical functions and components, i.e., the maximum time it should take to restore services. A different RTO should be assigned to each of business components according to their importance (e.g., ten minutes for network servers, an hour for phone systems).

Recovery point objective (RPO) – The point to which the state of operations must be restored following a disruption. In relation to backup data, this is the oldest age and level of staleness it can have. For example, network servers updated hourly should have a maximum RPO of 59 minutes to avoid data loss.

RPO – Essence

- **RPO :** time-based **measurement of maximum amount of data loss** that is tolerable to organization.
- **How far back IT must go**, stretching back in time from disaster to the last point where data is in a usable format
- How **frequently entity needs to back up** data,
- **How much data is lost** following a disaster
- RPOs measure back in time to **when data was preserved in usable format**, usually to most recent backup
- If enterprise backs up its data every 24 hours, then only risk of losing data within last 24 hours
- RPO of 60 minutes requires system backup every 60 minutes.
- **Automatic RPO strategies** used

RPO & Industry – Tier 1

- RPO measured in hours.
- **0-1 HOUR**
- If business requires **frequent monitoring & securing** of data---**Tier 1 RPO**
- used in businesses **with high data flow & many variables**.
- Eg : Bank, FI , records in hospitals or universities –

RPO – Tier 2

- **1-4 HOURS**
- available to organizations with sensitivity level **relatively lower** than RPO -1 .
- used for certain sub-sections of an organization’s database

RPO – Tier 3

- **4-12 HOURS**
- used for businesses with a relatively free data set.
- **Example:**

✓ Email lists,

✓ marketing records,

✓ sales logs

RPO – Tier 4

- **13-24 HOURS**
- ➢ not as sensitive
- ➢ database of these businesses / subsets can tolerate up to 24 hours of an RPO backup.
- ➢ have less data activity when compared to the top-tier RPOs.
- **Examples** include;
- HR department,
- purchase records of a business,

RPO – Analysis

- **RPOs =** measure of disaster range & extent of recovery a database may need to undergo with respect to time frame
- **RPOs =** important in various instances of disaster & system failure.
- Eg : power outages, Ransome wares, data attacks, data corruption, user error problems etc
- RPOs = determine data size, backup frequency
- Both RTOs & RPOs **not fixed values** for all organizations.
- **Factors :**

✓ data nature,

✓ data size,

✓ company budget

RTA & RPA

- Recovery time actual (RTA) & recovery point actual (RPA) = elapsed time & lost data of an **actual recovery process** & often different from RPO & RTO.
- Only ACTUAL business disruption & disaster rehearsals **can expose** these actuals.

Granular Recovery Technology (GRT)

- **Granular data :** detailed data, lowest level data can be in target set
- GRT use : restore certain individual items from backup sets.
- Ex: use Agent for Microsoft Exchange Server to restore **email message** from backup **without restore of entire mailbox.**
- GRT feature must be enabled for backup

NATIONAL STOCK EXCHANGE OF INDIA LIMITED

Continuity Planning(BCP)/Disaster Recovery (DR)

1. *Securities Market heavily dependent on IT infrastructure.*

2. Break down of IT infrastructure could occur from major disasters such as ***Earthquakes, floods, fires, riots or war etc.,*** *which could lead to interruptions to business functions.*

3. In the past, there have been a couple of occurrences of such disasters in India due to which it is very essential that the ***Trading Members should establish a well defined Business Continuity/DR plan.***

- *Given the current technology intensive environment in which Indian Securities market operates, in* ***order to ensure stability in operations of Members*** *so that interest of investors and market at large is not adversely impacted,* ***members are advised to sufficiently review all potential risks along with its impact on the business and put in place BCP/DR plan.***
- *Members who have established BCP/DR plan may please* ***submit the details of their plan to Exchange*** *in the format enclosed at Annexure I.*
- *Members* ***who intend to establish BCP/DR needing any guidance*** *on establishing such BCP/DR plan may please get in touch with* _____

RECOVERY CAPABILITY FOR VARIOUS DISASTER SCENARIOS

- ***Level 1:**.**Minor Outage Scenario***
- *In the event of a **minor outage**, business processes may experience **minor damage / outage and will run at a sub-standard level.** Scenarios include :*
- ✓ *link connectivity being temporarily down,*
- ✓ *switch or router port failures,*
- ✓ *System or network CPU failures, System Fan failures,*
- ✓ *System or Network Power supply failures,*
- ***Level 2: Moderate Outage Scenario***
- *In this scenario, some or all business processes at the location **may experience moderate damage / outage.** Processes may not continue **or may run at a degraded level.** An alternate site **may not be required** for continuing business **but alternate equipment may be required** depending on the criticality of the business process*
- *Some of the examples of such scenarios can be:-*
- ✓ *Equipment is damaged due to Power surge.*
- ✓ *ISDN/VSAT/Circuit router failure*
- ✓ *Core access layer switch failure*
- ✓ *Access/Distribution switch failure.*
- ✓ *LAN switch or router failure. / Temporary outage of power.*

- ***Level 3: Disaster Scenario Risks***

✓ *Member infrastructure* ***may experience a severe disaster resulting in the total shut down of infrastructure of the Member.***

✓ *Full processing capability of all business processes like* ***Trading, Risk Management, settlement systems etc. from that location*** *and related infrastructure may be down.*

✓ *Key personnel* ***may not be able to access*** *the premises.*

✓ *There may also be non-availability of key resources in the building.*

- ***Some of the examples of such scenarios*** *can be*
- *1.* ***Flood / Rain/Fire*** *making office premises like building and Datacenters inaccessible.*
- *2.* ***Riots /war etc., at a location near one of the offices*** *or within the premises of the member may render the office premises inaccessible.*
- *3.* ***Complete power shutdown*** *due to unavailability of generators.*
- ***Members may have to switch their business over to the BCP site****.*
- *Key factors for RTO -* ***key personnel availability, resilient IT infrastructure and robust BCP processes***

- ***Level 4: Catastrophe***
- *In this scenario,* ***major disaster strikes which would result in a major disruption of services****.*
- ***Full processing capability cannot be achieved*** *for a substantial period of time.*
- *Recovery will require use of* ***alternate processing site as well as offsite offices for employees over an extended period of time***

Some of the examples of such scenarios can be

- *1. War*
- *2. Earthquake*
- *3. Extended Communal Riots etc*
- *In such a scenario,* ***capability to achieve their RTO*** *would critically depend upon :*
- ***Key personnel availability, resilient IT infrastructure and robust BCP processes.***