Data Protection and Management

Evolution of Data Protection

Learning Outcome

At the end of this lecture you should able to;

- Explain the three big waves of change

- Understand and apply server-centric backup

- Strategize Cloud service-centric data management

Evolution of Data Protection Solutions

The evolution of data protection solutions is caused by three big waves of change:

Server-centric Backup

- Data source – server
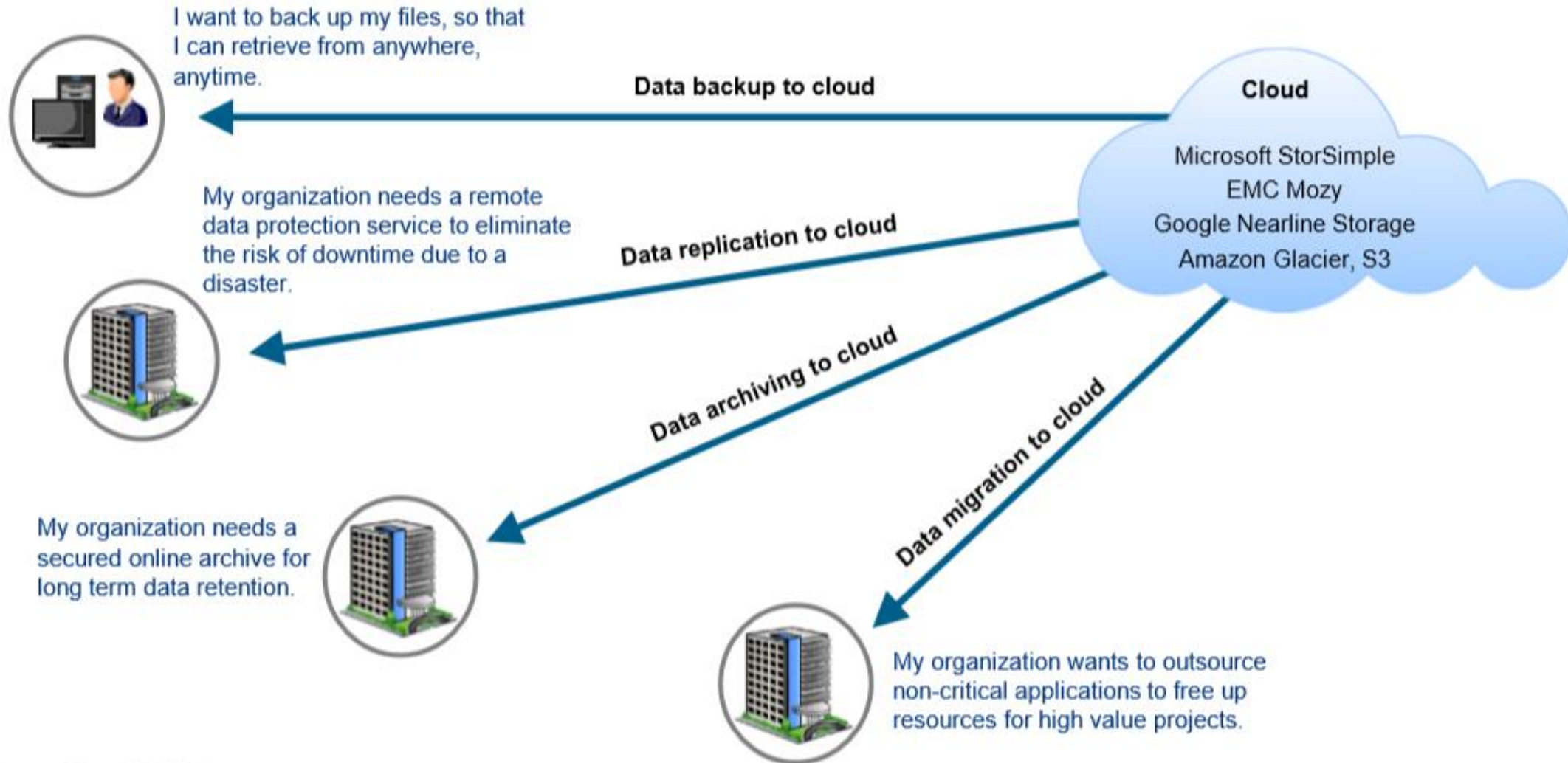- Separate backup infrastructure
- One-size-fits-all

Infrastructure-centric Data Protection

- Data source – infrastructure components
- Leverage embedded backup/replication/archiving features

Cloud Service-centric Data Management

- SLA-driven protection
- Optimized for data management

Data Protection as a Cloud Service

I want to back up my files, so that I can retrieve from anywhere, anytime.

Data backup to cloud

Cloud

Microsoft StorSimple
EMC Mozy
Google Nearline Storage
Amazon Glacier, S3

My organization needs a remote data protection service to eliminate the risk of downtime due to a disaster.

Data replication to cloud

Data archiving to cloud

Data migration to cloud

My organization needs a secured online archive for long term data retention.

My organization wants to outsource non-critical applications to free up resources for high value projects.

Cloud Computing

In cloud computing, users rent IT resources such as storage, processing, network bandwidth, applications, or a combination of them as cloud services.

Cloud computing enables on-demand resource provisioning and scalability.

IT resources are provisioned by the users using a self-service portal backed by an automated fulfillment process.
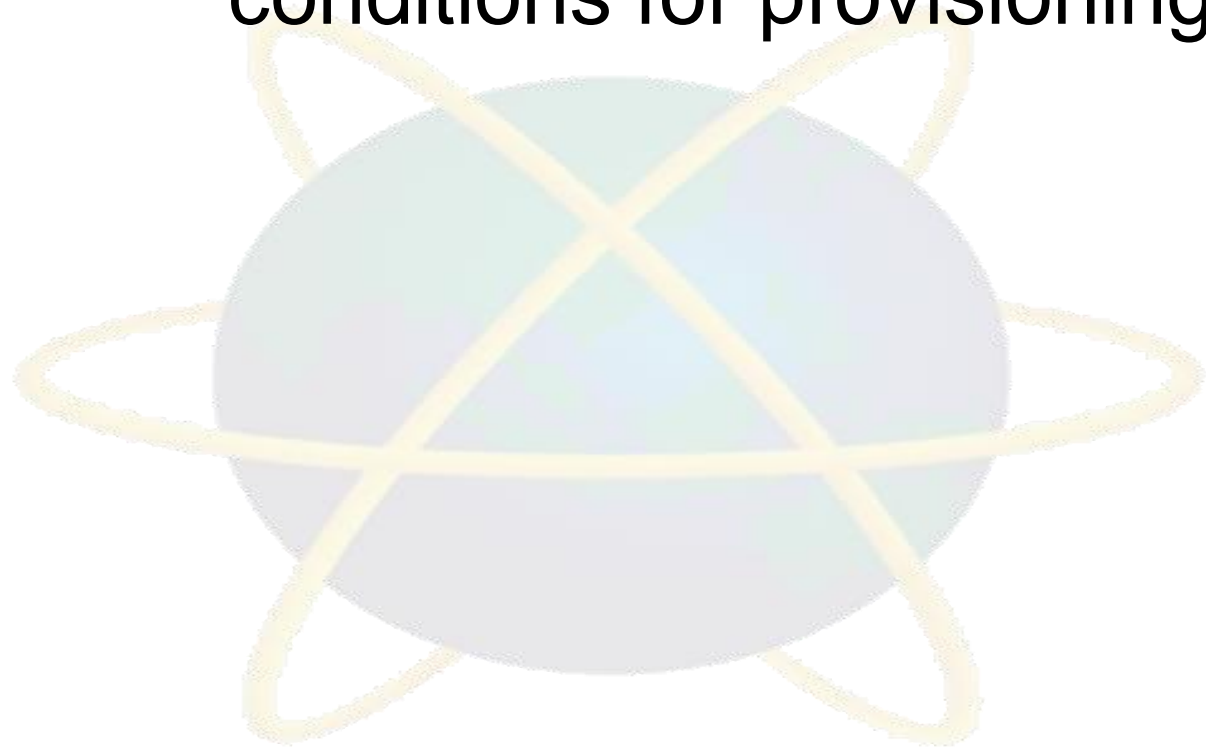
Quick Review

- Explain the huge shift in data protection trend
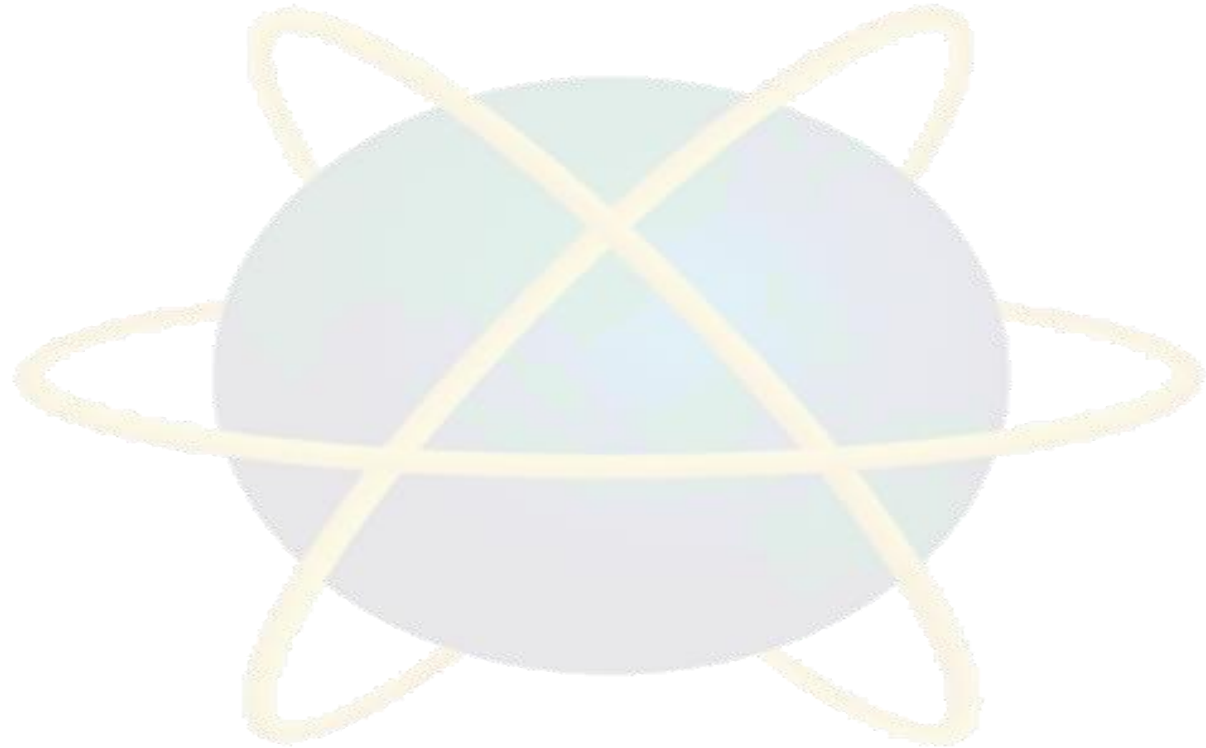
Self-Service Portal

- The self-service portal presents a service catalog that includes the description of services, SLA, terms and conditions for provisioning, and prices.

Measurement of Resource Consumption

- Resource consumption is measured by using a metering service which may help in billing users as per consumption.

- Users can de-provision the rented resources when resources are no longer needed.
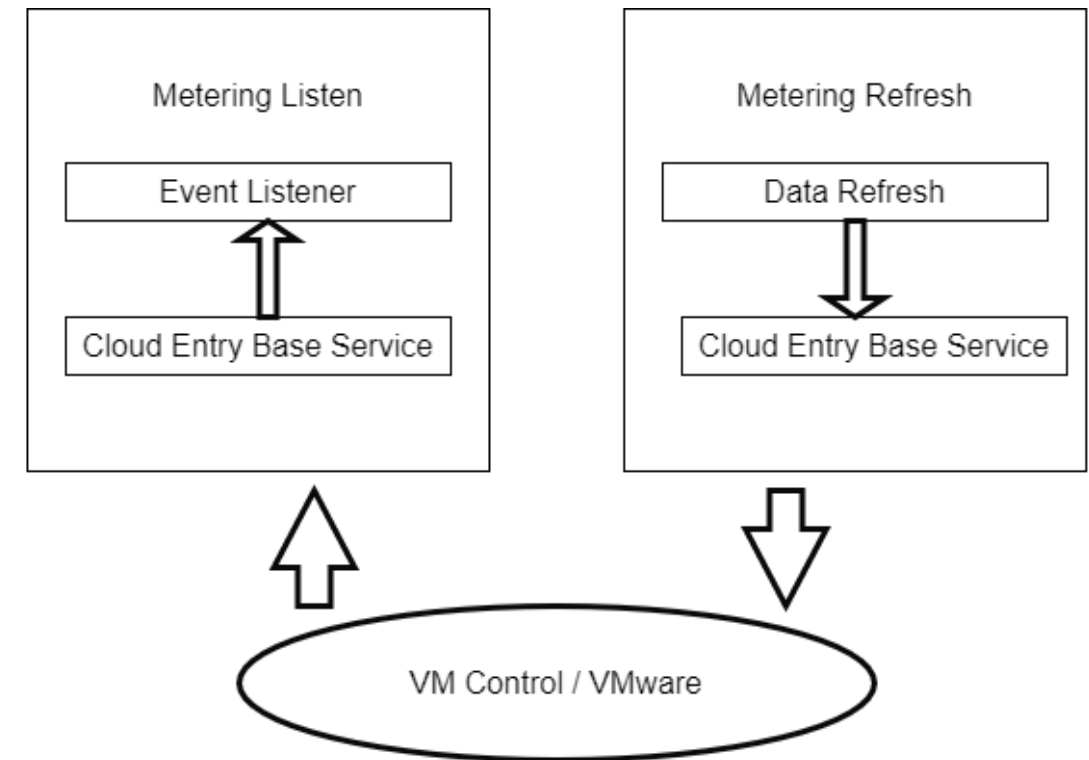
Metering Process Metering to clouds
Source: https://www.researchgate.net/publication/281278299_Measuring_the_usage_of_Cloud

Notice:

Many organizations use a range of data protection as a service offerings from cloud providers.

As the data protection infrastructure is maintained by the cloud provider, the expenses, tasks, and time associated with data protection management is reduced.

.

Data Protection – Key words

- **Personal data** - any information pertaining or involving to an living person who can be identifiable

- **Processing** - any operation executed on personal data. (e.g. Operations such as storing, collecting, retrieving, using, combining, erasing and destroying personal data)

- **Data Protection Commission** - the Commission is in authority for observing the solicitation of the GDPR in order to protect the rights and freedoms of individuals in relation to processing

- **Data Controller** - a person, company, or other body which decides the purposes and methods of processing personal data

- **Data Processor** - a person, company, or other body which processes personal data on behalf of a data controller.
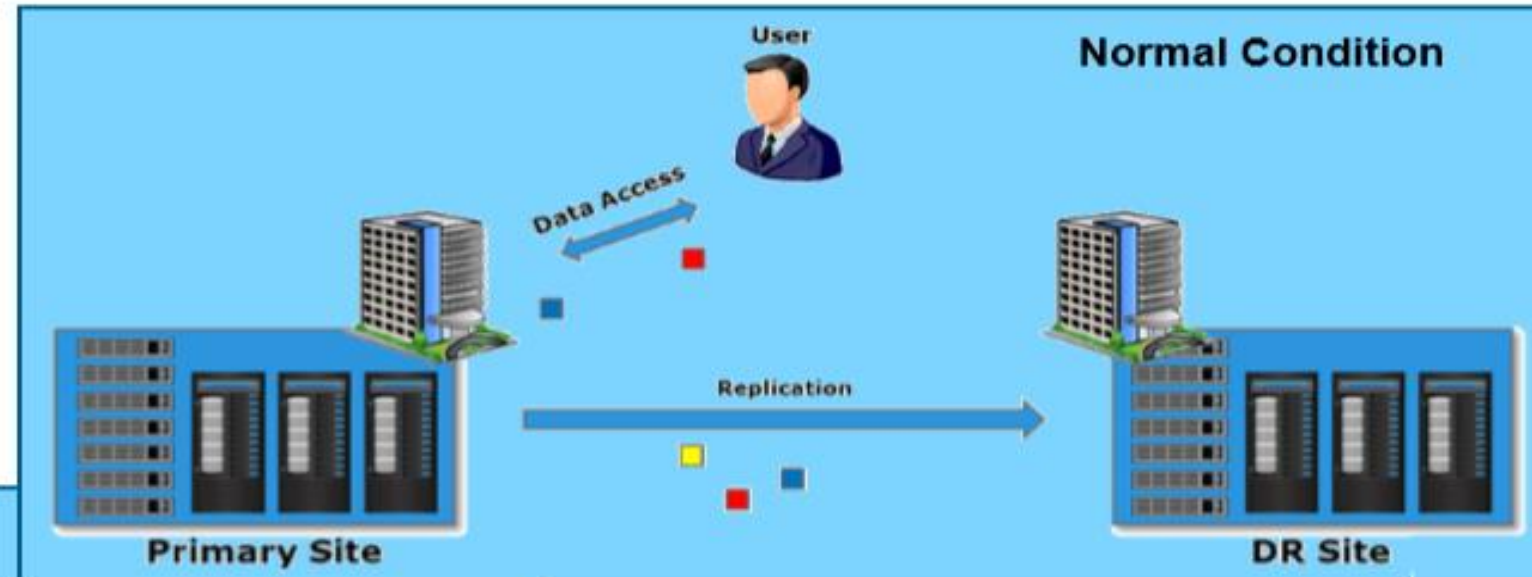
Data Protection – Key words

- **Consent** - Some types of processing are carried out on the basis that you have given your agreement

- **Profiling** - any kind of automated processing of personal data that involves analysing or predicting your behaviour, habits or interests

- **Special categories of personal data** - Certain types of sensitive personal data are subject to additional protection under the GDPR (e.g. Personal data revealing racial or ethnic origin, Religious or philosophical beliefs, genetic data and biometric data, Data concerning health)

Data Protection Terminologies -1

Disaster Recovery (DR)

Policies and procedures for restoring IT infrastructure and data that are required to support IT services after a disaster

Disaster recovery (DR)

The fundamental principle of DR is to maintain a secondary data center or site, called a **DR site**.

The primary data center and the DR data center should be located in different geographical regions to avoid the impact of a regional disaster.

The DR site must house a complete copy of the production data. Commonly, all production data is replicated from the primary site to the DR site either continuously or periodically. Alternatively, a backup copy can be maintained at the DR site.

Data Recovery

When designing a data availability strategy for an application or a service, organizations must consider two important parameters that are closely associated with recovery.
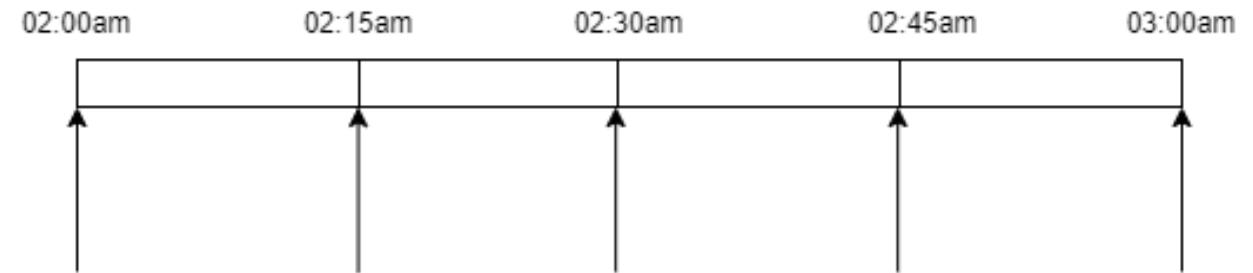
- Recovery Point Objective (RPO)
- Recovery Time Objective (RTO)

Recovery Point Objective (RPO)

This is the total amount of data that a business can afford to loose

How to calculate RPO?

Can be calculated by subtractin the point in time at which the backup or replication is schedule

02:00am　　02:15am　　02:30am　　02:45am　　03:00am
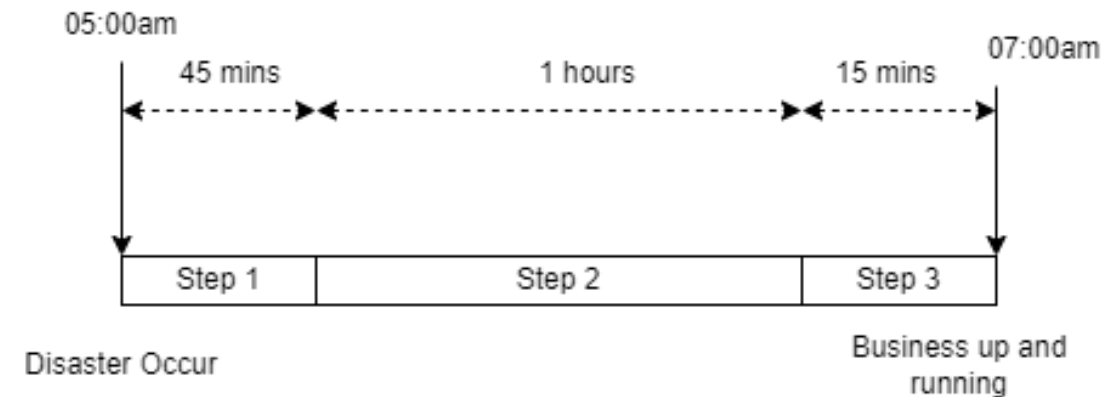
Backup / Replication

Recovery point objective (RPO) = 02:00am - 02:15am
that is 15 minitues

Recovery Time Objective (RTO)

This is the total amount of needed to make the business up and running since the disaster or outage.
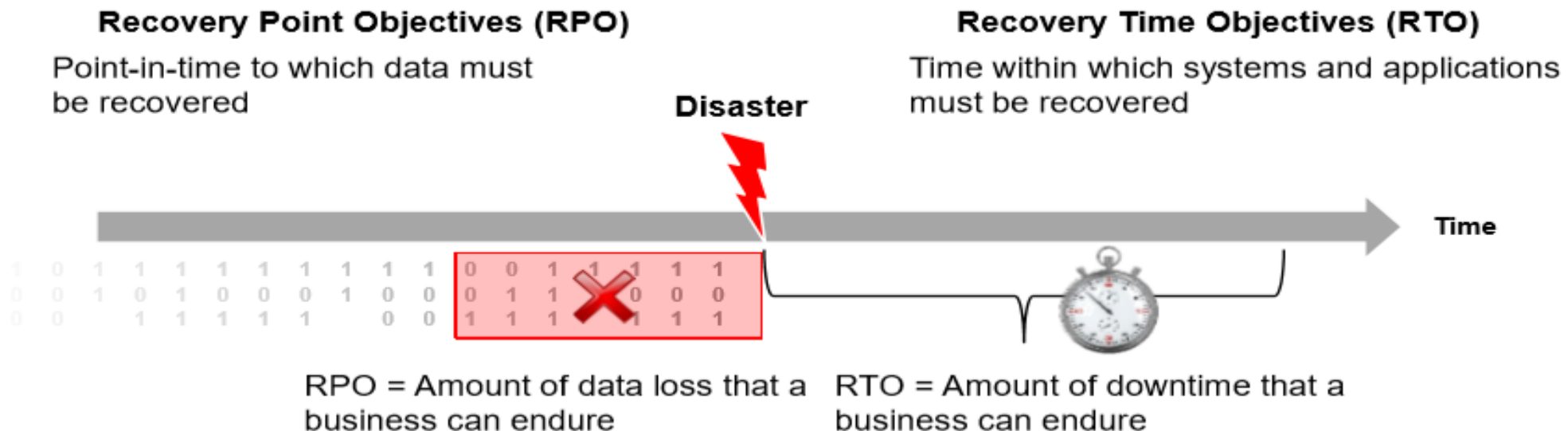
How to calculate RTO?

Adding the total duration of each step performed to bring the business up and running since the disaster or outage
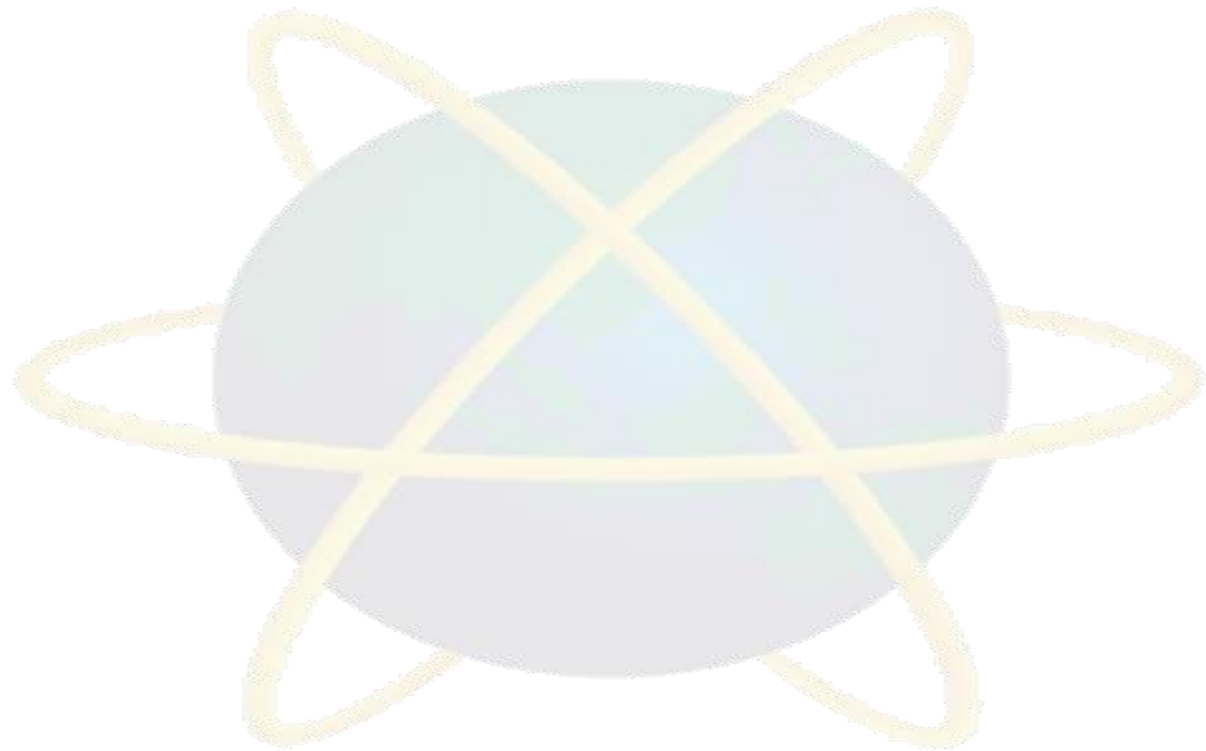
RPO and RTO

- Both RPO and RTO are counted in minutes, hours, or days and are directly related to the criticality of the IT service and data. Usually, the lower the RTO and RPO, the higher is the cost of a data protection solution or technology.

Recovery Point Objectives (RPO)
Point-in-time to which data must be recovered

Disaster

Recovery Time Objectives (RTO)
Time within which systems and applications must be recovered

Time

RPO = Amount of data loss that a business can endure

RTO = Amount of downtime that a business can endure

Expert opinion

https://www.youtube.com/watch?v=eOe1Q7ALcRA

Data Protection Management Program

STEP 1:
GOVERNANCE AND
RISK ASSESSMENT
Establishing a governance structure to define values and identify risks with organisational leadership

STEP 4: MAINTENANCE
Detailing steps to keep data protection policy and processes up to date

STEP 2:
POLICY AND PRACTICES
Developing a data protection policy and data protection practices

STEP 3: PROCESSES
Designing processes to operationalise policy

[1] *Organisations should note that adopting the suggestions in this guide does not mean that it would be in compliance with the PDPA. An organisation should consider whether the suggestions in this guide could be adapted for its specific circumstances.*

Data Protection Management Activities

Monitoring
Gathering information on resources and checking status of protection operations

Reporting
Presenting the details on performance, capacity, configuration, and chargeback

Capacity Planning
Estimating the amount of resources required for data protection and forecasting capacity requirement

Troubleshooting
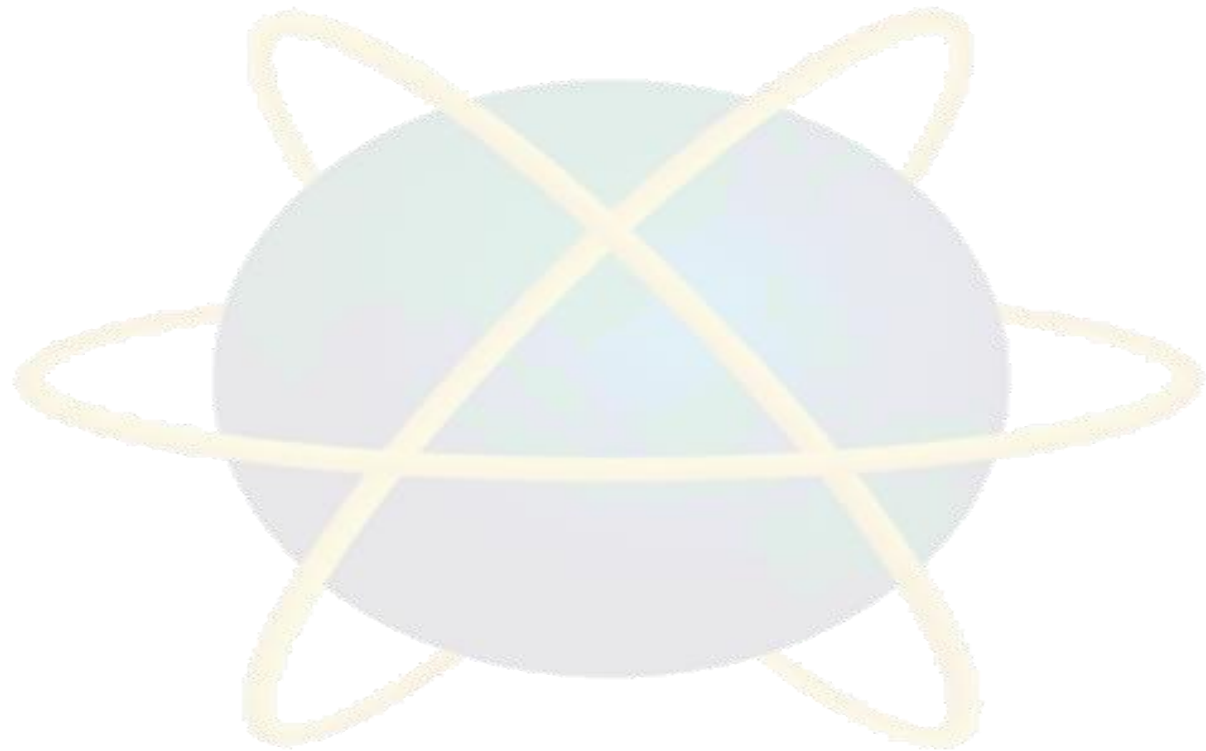Identifying the root cause of issues and resolving the issues
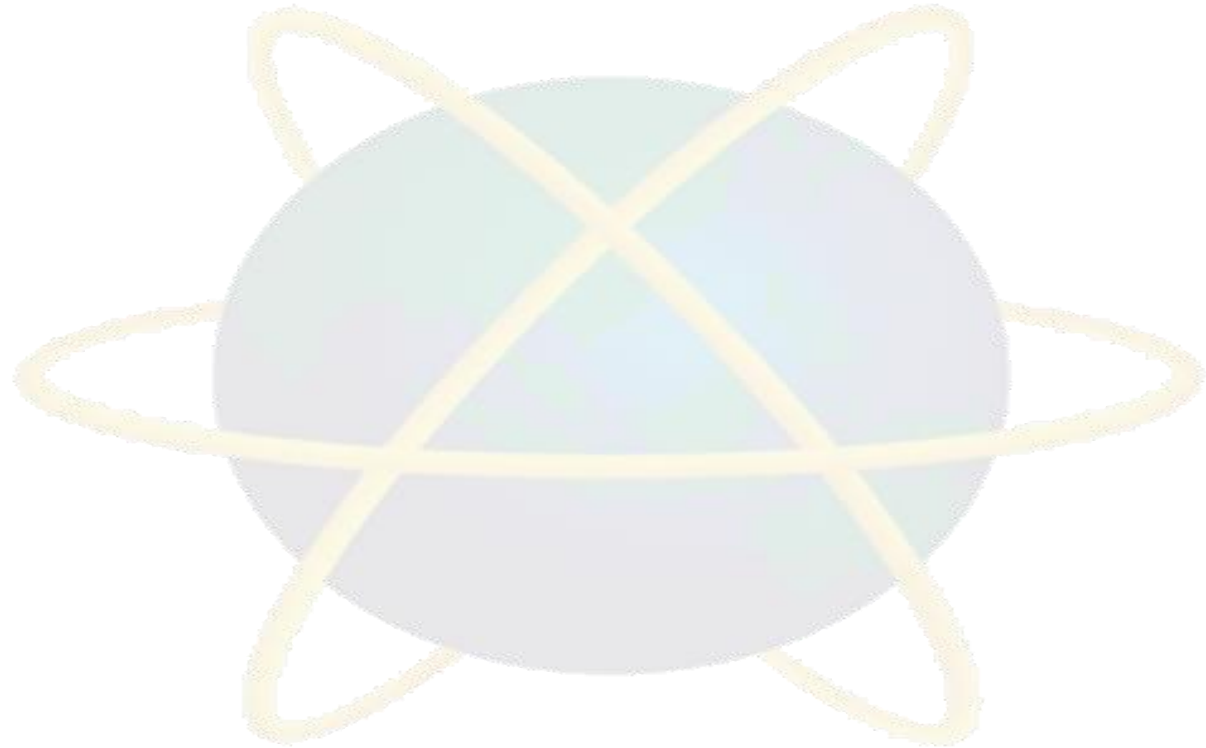
Resource Optimization
Improving the overall utilization and performance of IT resources

Q & A

Next Topic

Availability Solution

• Data can be retrieved from a cloud-based archive within six hours.