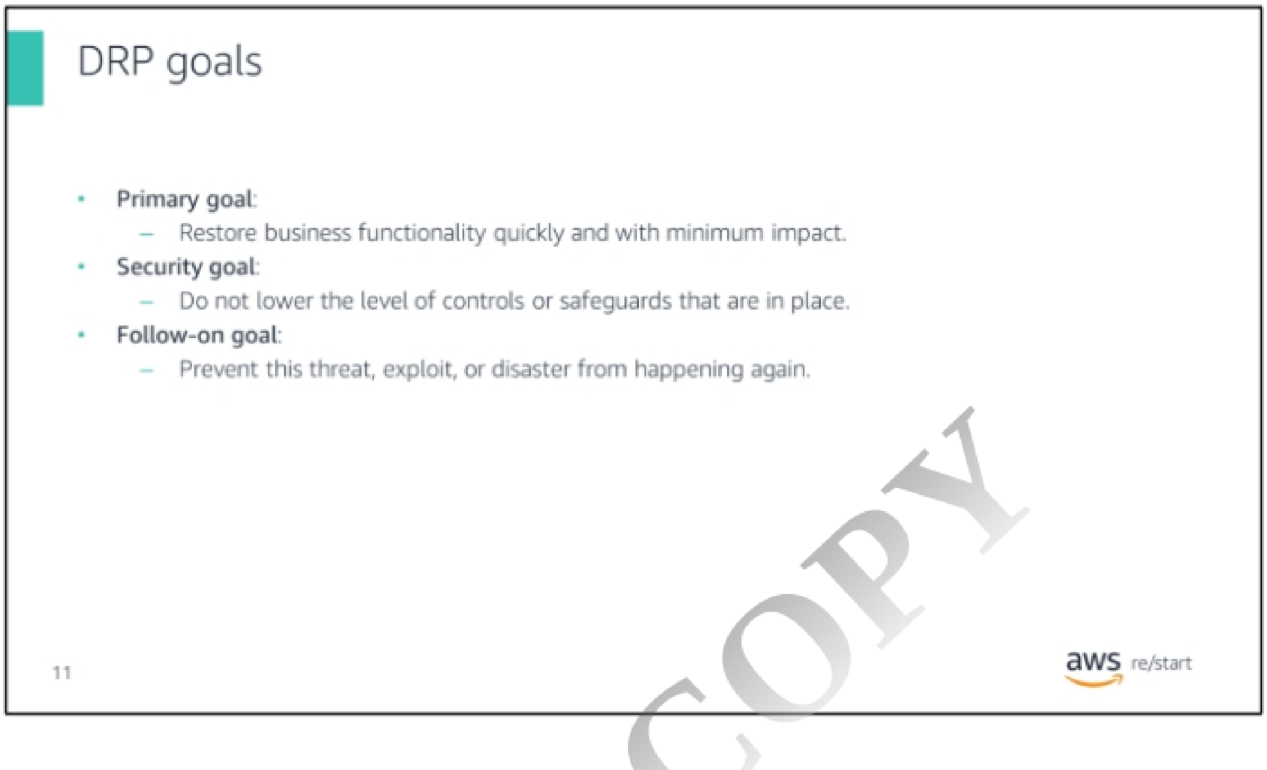


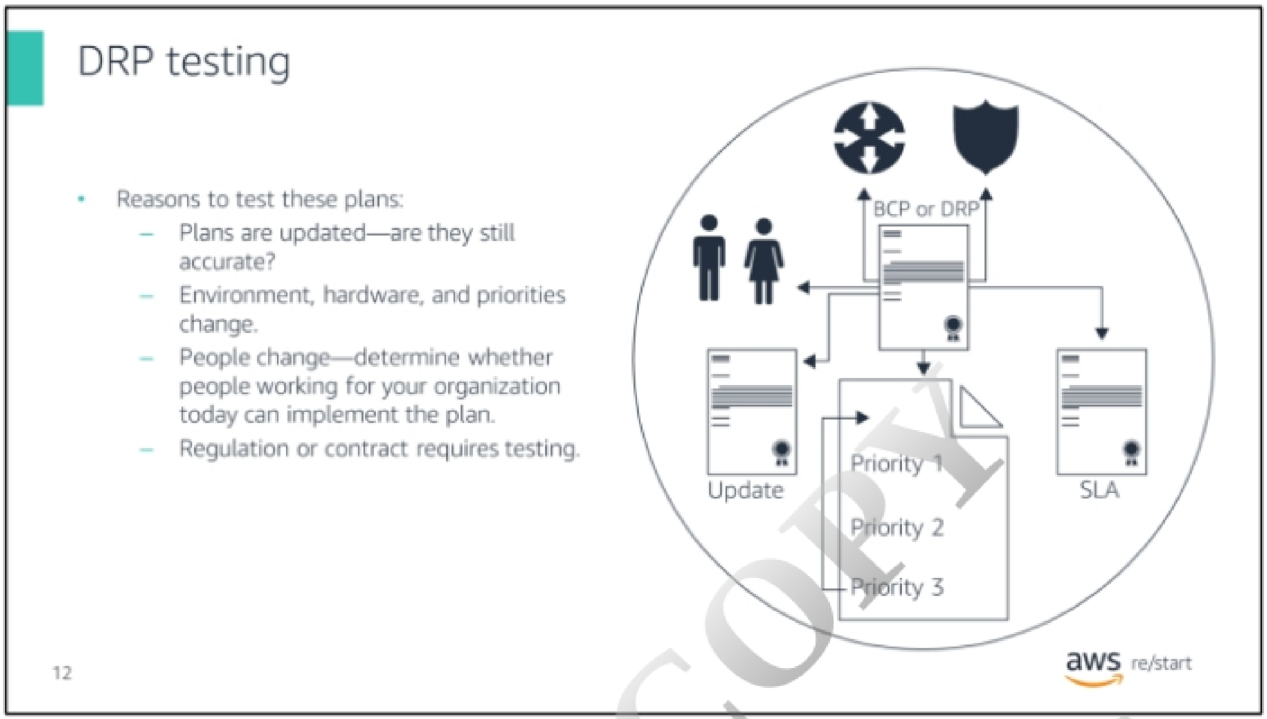
DRP goals

- **Primary goal**:
  - Restore business functionality quickly and with minimum impact.
- **Security goal**:
  - Do not lower the level of controls or safeguards that are in place.
- **Follow-on goal**:
  - Prevent this threat, exploit, or disaster from happening again.

11

Security goal:

- A business might implement different corrective measures for access control based on the impact of the disaster or disruption. However, the business should implement security access controls to the same level of restriction before the disruption.
- If access controls are not implemented to the same level, the business must not permit access or use of resources.



DRP testing

- Reasons to test these plans:
  - Plans are updated—are they still accurate?
  - Environment, hardware, and priorities change.
  - People change—determine whether people working for your organization today can implement the plan.
  - Regulation or contract requires testing.

BCP or DRP

Update

Priority 1

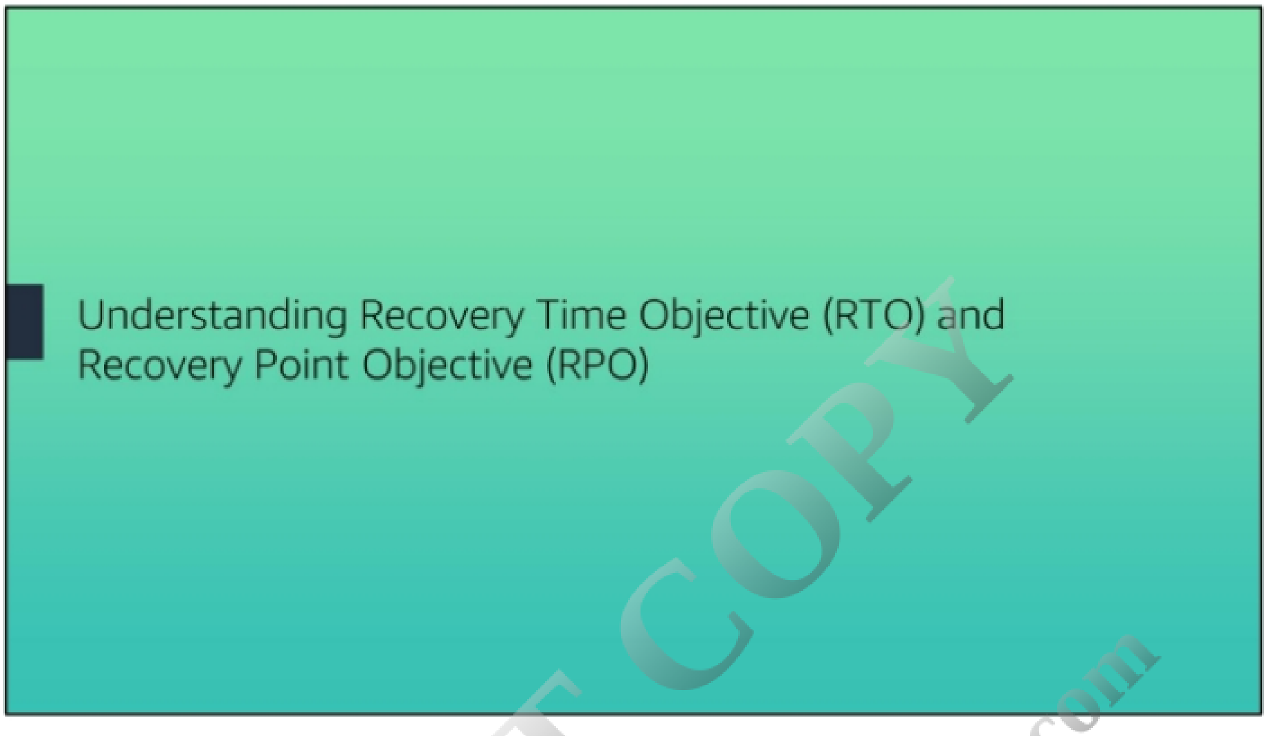
Priority 2

Priority 3

SLA

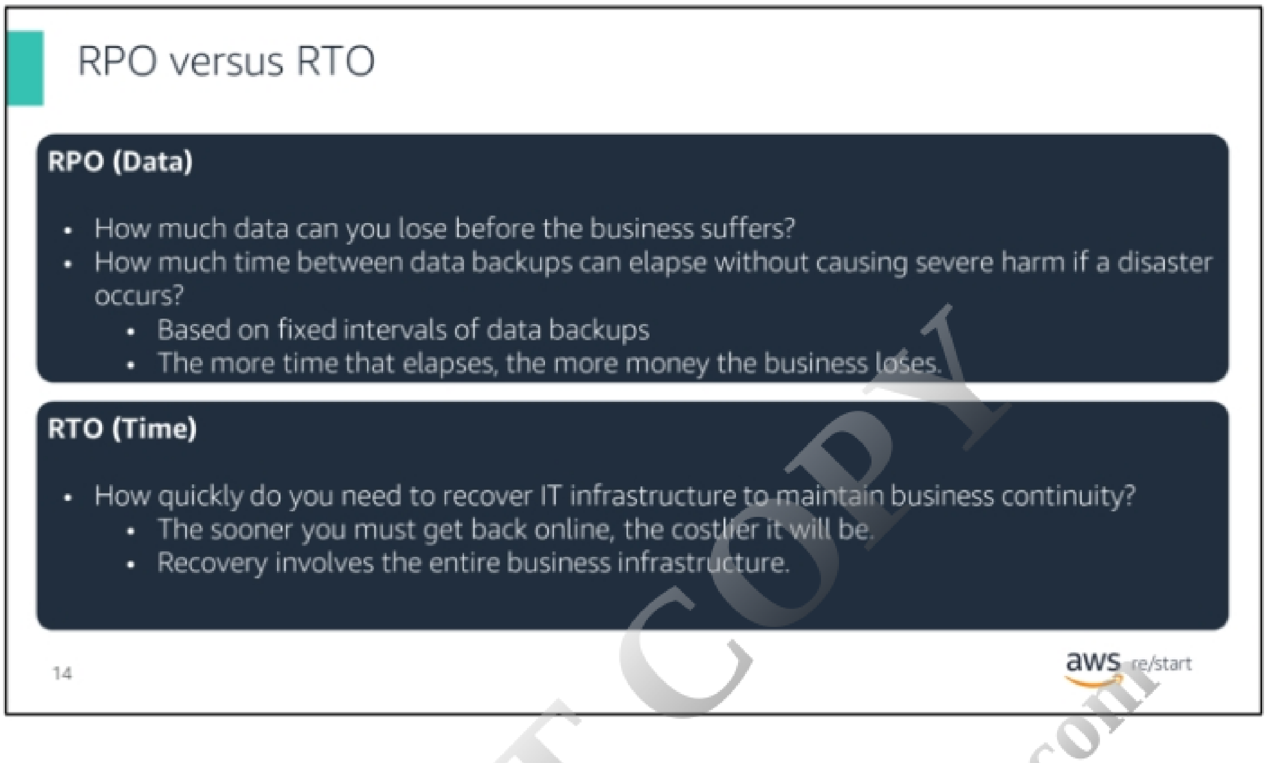
aws re/start

It is important to test the DRP regularly and adjust it as needed because environments, people, and regulations constantly change.



Understanding Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

the next few slides will discuss the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)



RPO versus RTO

RPO (Data)

- How much data can you lose before the business suffers?
- How much time between data backups can elapse without causing severe harm if a disaster occurs?
  - Based on fixed intervals of data backups
  - The more time that elapses, the more money the business loses.

RTO (Time)

- How quickly do you need to recover IT infrastructure to maintain business continuity?
  - The sooner you must get back online, the costlier it will be.
  - Recovery involves the entire business infrastructure.

aws re/start

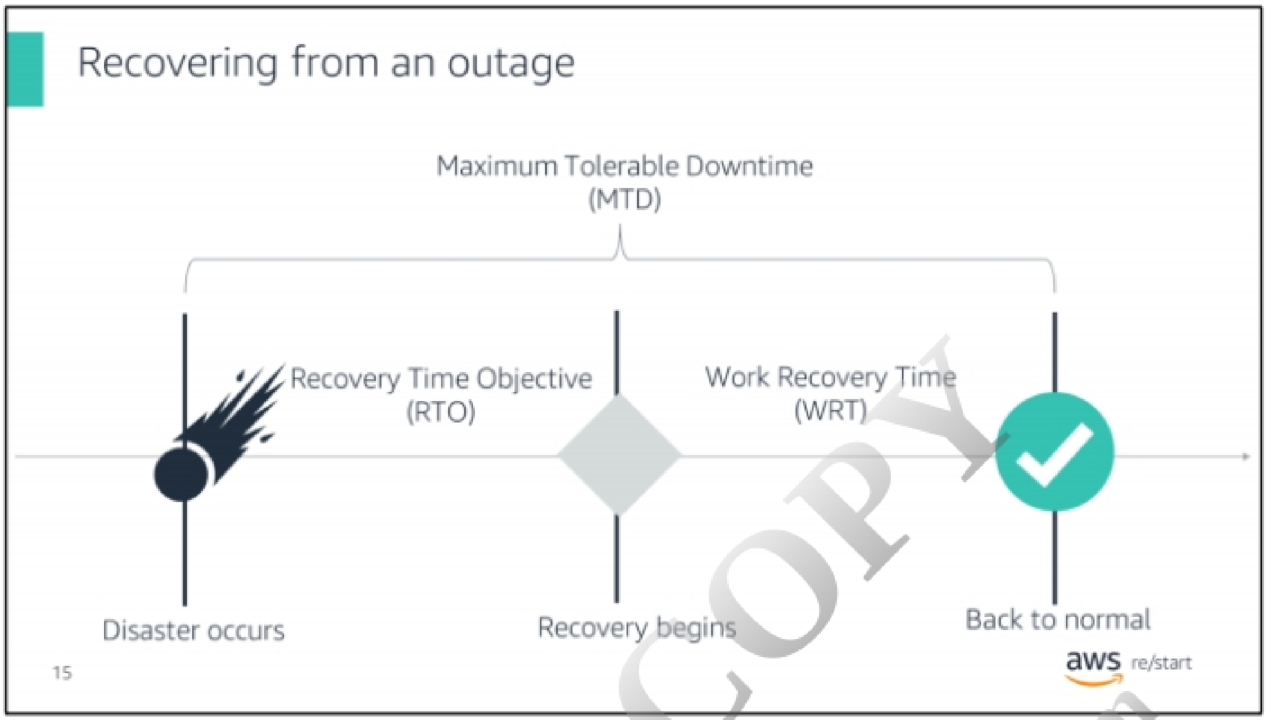
RPO

The main focus of RPO is on data. The RPO represents the point in time, before a disruption, when data can be recovered (given the most recent backup copy of the data) after the disruption. RPO is a factor of how much data loss the business can tolerate during the recovery process.

RPO is easier to implement than RTO because it affects only the data layer of your infrastructure.

RTO

RTO involves the entire business infrastructure, not only data. RTO establishes the maximum amount of time that a system or resource can remain unavailable before there is an unacceptable impact on other system resources, supported business processes, and the Maximum Tolerable Downtime (MTD).



Recovering from an outage

Maximum Tolerable Downtime (MTD)

Recovery Time Objective (RTO)

Work Recovery Time (WRT)

Disaster occurs

Recovery begins

Back to normal

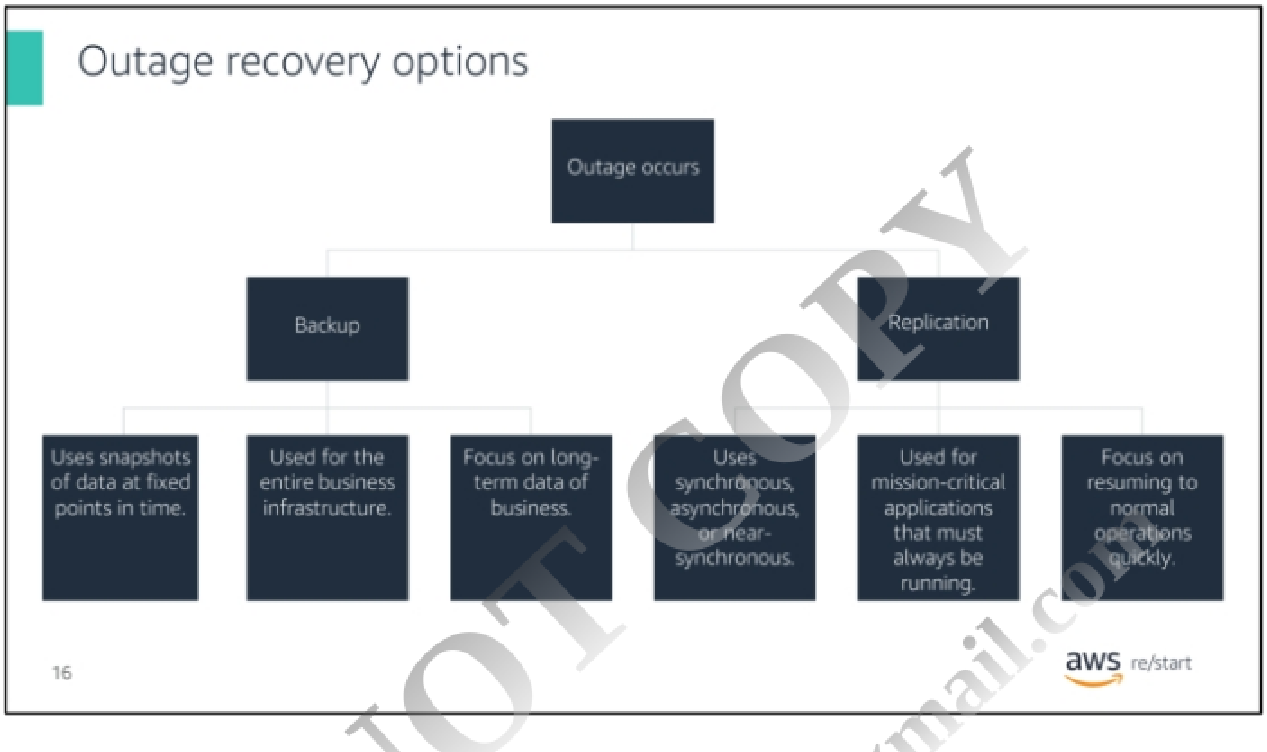
15

aws re/start

Work Recovery Time (WRT) involves recovering or restoring data, testing processes, and then making the system "live" for production. It corresponds to the time between systems and resource recovery and the start of normal processing.

The Maximum Tolerable Downtime (MTD) is the sum of the Recovery Time Objective (RTO) and the WRT. In other words, MTD = RTO + WRT.

MTD is the total amount of time that a business can be disrupted after a disaster without causing any unacceptable consequences associated with a break in business continuity. Include the MTD value as part of the BCP and DRP.



Outage recovery options

Outage occurs

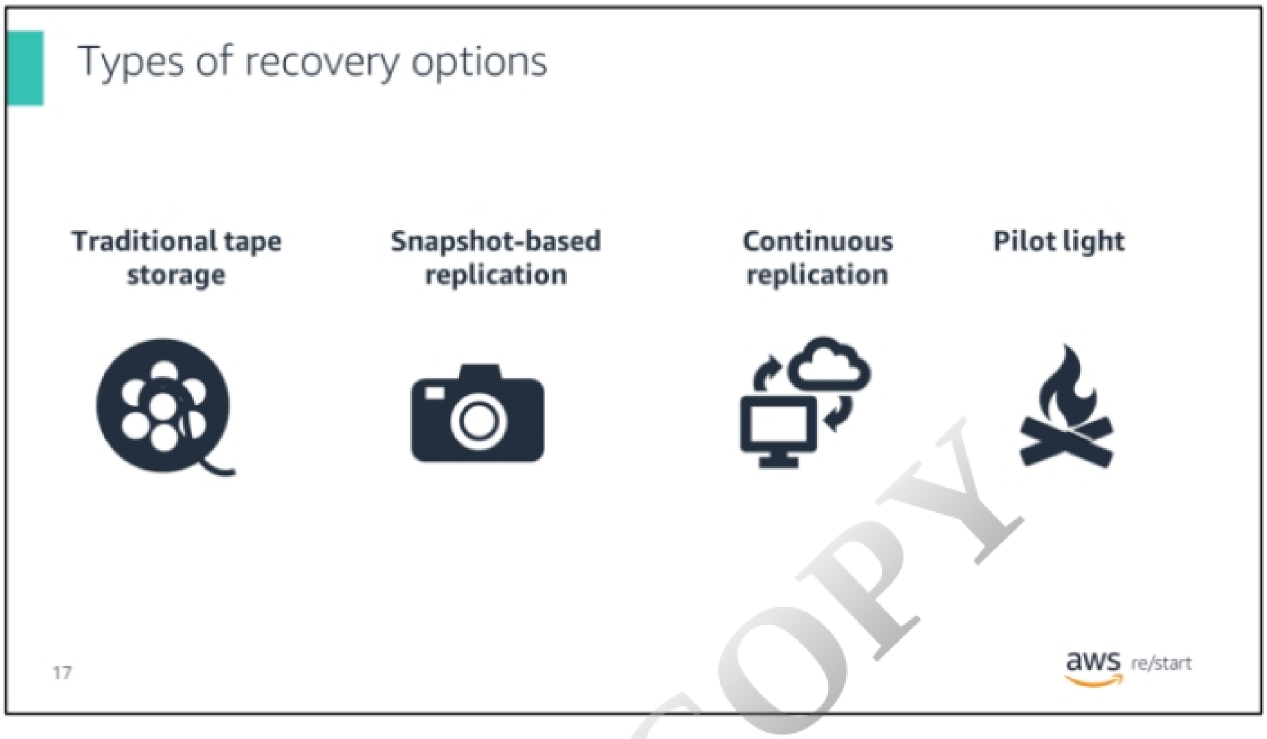
Backup

- Uses snapshots of data at fixed points in time.
- Used for the entire business infrastructure.
- Focus on long-term data of business.

Replication

- Uses synchronous, asynchronous, or near-synchronous.
- Used for mission-critical applications that must always be running.
- Focus on resuming to normal operations quickly.

Recovery from an outage typically relies on the availability of a backup or replication solution that you previously implemented.



Types of recovery options

Traditional tape storage

Snapshot-based replication

Continuous replication

Pilot light

17

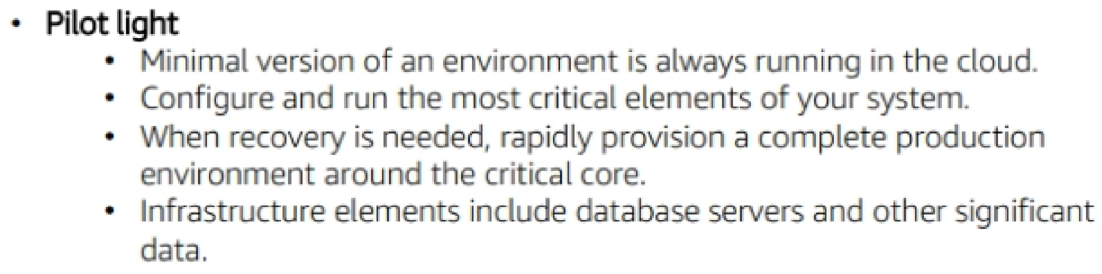
aws re/start

Types of backup and recovery options:

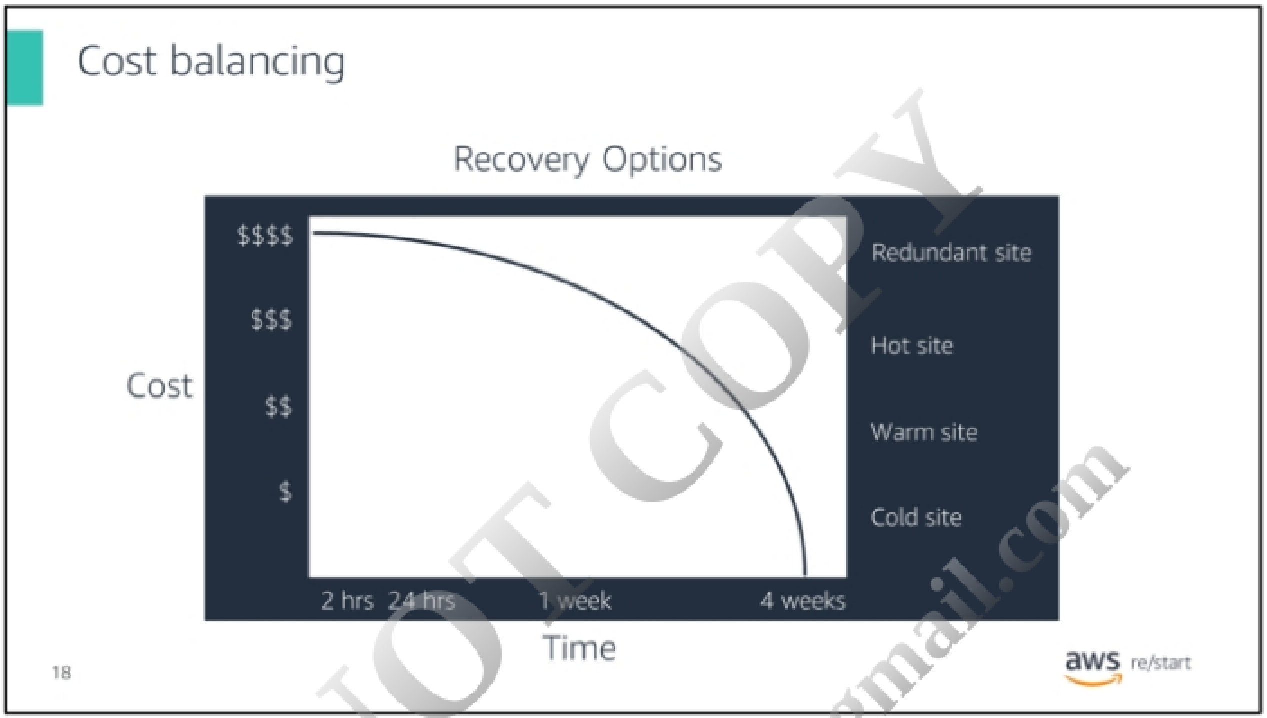
- **Traditional tape storage**
  - Store a large amount of data.
  - Reliable and cost-effective
  - Not time-effective—could lose hours or days of availability

- **Snapshot-based replication**
  - Captures the current condition of an application at a moment in time.
  - Writes only changed data since the last snapshot.
  - Protects data based on how often snapshots are taken.

- **Continuous replication**
  - The newest copy of a disk or application is continuously replicated to the cloud or another location.
  - Reduces downtime.
  - Offers more granular recovery points.



- **Pilot light**
  - Minimal version of an environment is always running in the cloud.
  - Configure and run the most critical elements of your system.
  - When recovery is needed, rapidly provision a complete production environment around the critical core.
  - Infrastructure elements include database servers and other significant data.

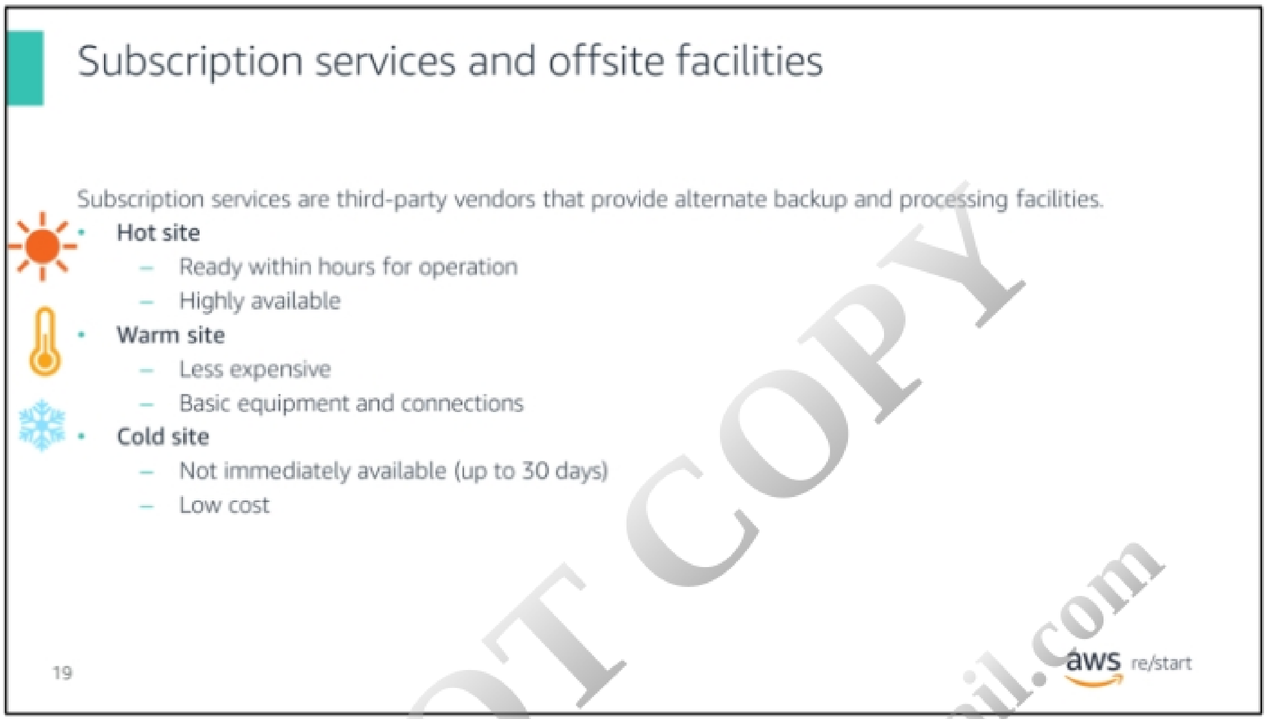


Cost balancing

The longer a disruption is allowed to continue, the more costly it can become to the business and its operations.

When you must decide on a backup solution for a business system that involves a hot, warm, or cold site, ask where on this curve the system needs to be. A tradeoff exists between speed of recovery and cost.

The answer is not the same for all systems. For example, an employee database can probably be down for a couple of days, but the ecommerce site can only be down for minutes.



Subscription services and offsite facilities

Subscription services are third-party vendors that provide alternate backup and processing facilities.

- Hot site
  - Ready within hours for operation
  - Highly available
- Warm site
  - Less expensive
  - Basic equipment and connections
- Cold site
  - Not immediately available (up to 30 days)
  - Low cost

The Amazon Simple Storage Service (Amazon S3) is an example of a cloud storage service that can be used to back up data with different levels of restoration speed and cost.

For more information about Amazon S3, refer to the Amazon S3 product webpage.