Virginia Information Technologies Agency

Enterprise Architecture
RTO-RPO Fit for Purpose Model

RPO – Recovery Point Objective

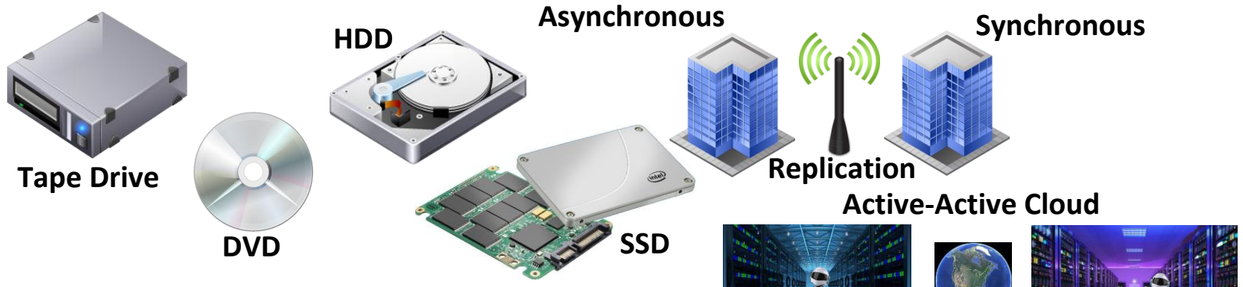
- How much data loss can we tolerate?
- What past point-in-time do we need to recover our data to?
- How frequently should we backup our data?
- How much data are we willing to give up should backups be required to get things operational?
- What is the maximum acceptable time between backups?

- Focused on just data – data risk.
- Data loss potential before significant harm to the organization.
- Considers how often your data changes.
- Lower value means more frequent backups / replication.
- Listed in time from seconds to days.
- Lower RPO means higher costs to implement.
- Measure back in time from a potential event.
- A 4-hour RPO does not necessarily mean you lose 4-hours of data.
  A 1:00am event may mean 1-hr effort in 4-hrs of data lost.
  A 1:00pm event may mean 16-hrs effort in 4-hrs of data lost.
- Typically range from 24-hrs, to 12-hrs, to 8-hrs, to 4-hrs, to seconds.

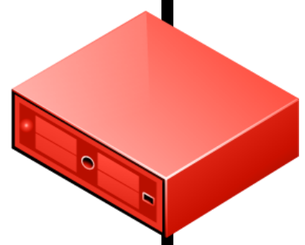
Time BEFORE event

Acceptable amount of lost data.

Month	Week	Day	Hour	Minute	Second



Critical Event
Disaster Strikes



RTO – Recovery Time Objective

- How fast do we need to recover after a failure?
- How long can we go without service after a failure?
- How much disruption can we have after a failure?
- How long until a service should be restored?
- What is our target time to recovery post failure?
- How long can you afford to be in-the-dark?

- Focused on the organization as a whole.
- Represents downtime until fully resume service operations.
- Clock starts at time of the event/disaster.
- The recovery window measured forward in time from the incident.
- Agency's mission essential functions (MEF) drive this value.
- Should be specific (72-hrs) – <u>not</u> a range of time (24-hrs to 48-hrs).
- Is large scale and concerned with applications and systems.
- MEF's should be prioritized by RTOs.
- Goal is to calculate how quickly you need to recover.
- Helps inform development of a DR strategy.
- May be more important than RPO in certain situations.

Time AFTER event

Acceptable amount of downtime.

Second	Minute	Hour	Day	Week	Month

VITA Draft Discussion Document // Jun-6-2019

PURPOSE: To depict the differences between RTO and RPO in support of disaster recovery planning.

This view is intended for a minimum 11x17 printer paper.

Robert Kowalke ~ Enterprise Architecture ~ robert.kowalke@vita.virginia.gov
Commonwealth Security and Risk Management (CSRM) @ Virginia Information Technologies Agency (VITA)
Commonwealth Enterprise Solutions Center (CESC)

Architectural Artifacts/Graphs/Views/Matrices/etc. reference page: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap35.html

Cold site

- Little or no equipment
- No network connectivity
- Not ready for automatic failover
- No data synchronization
- High risk of data loss
- Cheap

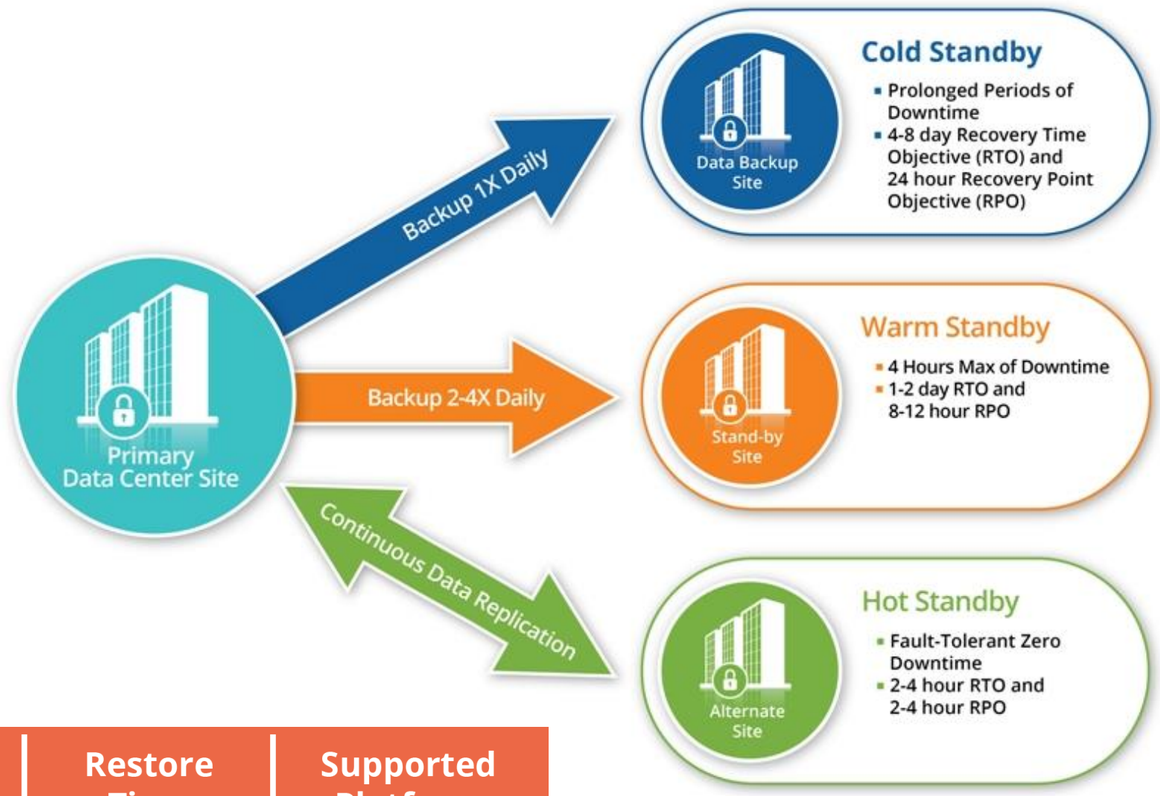
Warm site

- Partially redundant equipment
- Network connectivity is enabled
- Failover occurs within hours or days
- Daily or weekly data synchronization
- Minimum data loss
- Cost-effective

Hot site

- Fully redundant equipment
- Network connectivity is enabled
- Failover occurs within hours or days
- Near real-time data synchronization
- Zero data loss
- Expensive

Disaster Recovery Solutions



	DR Mode	Services Needed	Resources	Failover Scenario	Restore Time	Supported Platform
COLD DR	Back up	BaaS	• Storage • Compute (unreserved)	Restore	Up to one day / instance	• Windows • Linux
WARM DR	Standby (off)	• OS • IaaS • BaaS	• Storage • Compute	Boot on VM	4 - 6 hours / instance	• VMware • Hyper - V
HOT DR	Fully Automated	• OS • Replication • IaaS	Dedicated	Automatically	Less than 10 minutes	• VMware • Hyper-V