Disaster Recovery Services

Expanded Services

Joshua Haravay, VITA Disaster Recovery Specialist
Michael Elkins, NG Director – Data Center Transformation
August 26, 2008

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Agenda

- Objective and Goals
- DR Service Catalog
- Architecture and Proposed Tier Architecture
- Agency Requirements Gathering and DR Tier Mapping
- Other Services
- Questions

Objective and Goals

- Provide an overview of the Services that will be offered under the DR Services Catalog.
- Provide an overview of the solution that falls under a tier level of DR service
- Provide an understanding of the criteria used to help map an agency to a DR Service Tier
- Provide an overview of other available DR Services

Advantages of DR Services Catalog

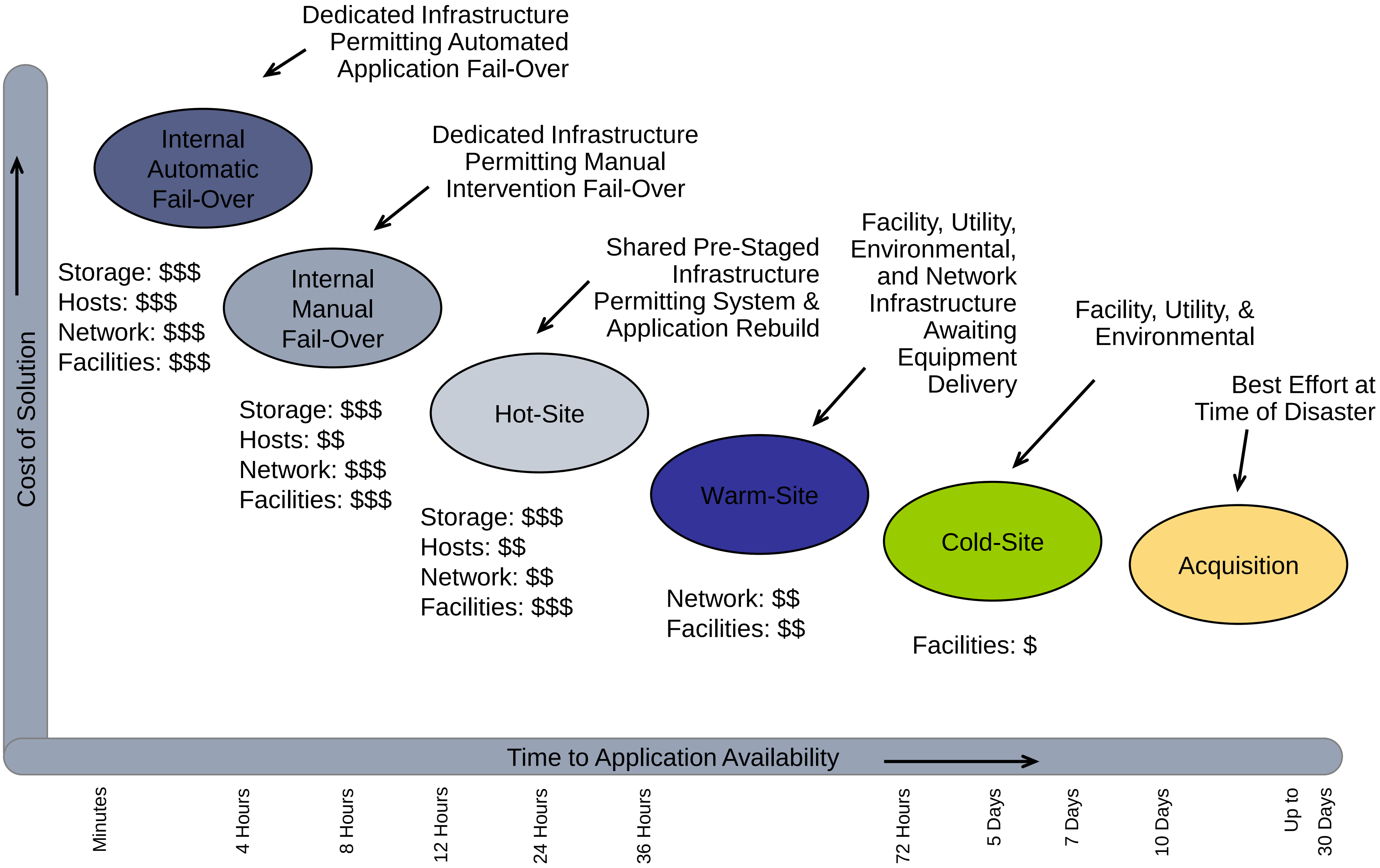
- Provides more granularity on costs of services for the Agencies
    - Agencies can choose between a larger range of services and choose the most applicable for their case
    - Agencies can select lower DR levels with lower costs
    - Agencies can match the solution to their RTO/RPO requirements
- Offers support for immediate needs of the Agencies
    - Agencies desire DR support for their local IT
    - Some Agency ITs cannot have SAN infrastructure
- Provides a logical migration path for the Agencies

Disaster Recovery Service Measures

Definition	Time to recover the affected Commonwealth Services after a declared DR incident

Disaster Recovery Service Level Requirements			
BIA Application Rankings	**Service Measure**	**Performance Target**	**Minimum Performance % ALL SOWs**
1	Time to recover	< 4 hours	98%
2	Time to recover	5 to 24 hours	98%
3	Time to recover	25 to 48 hours	98%
4	Time to recover	49 to 72	98%
5	Time to recover	>73 hours	98%
6	Time to recover	Within 168 hours	100%

Delivering Degrees of RTO



Dedicated Infrastructure Permitting Automated Application Fail-Over

Internal Automatic Fail-Over

Storage: $$$
Hosts: $$$
Network: $$$
Facilities: $$$

Dedicated Infrastructure Permitting Manual Intervention Fail-Over

Internal Manual Fail-Over

Storage: $$$
Hosts: $$
Network: $$$
Facilities: $$$

Shared Pre-Staged Infrastructure Permitting System & Application Rebuild

Hot-Site

Storage: $$$
Hosts: $$
Network: $$
Facilities: $$$

Facility, Utility, Environmental, and Network Infrastructure Awaiting Equipment Delivery

Warm-Site

Network: $$
Facilities: $$

Facility, Utility, & Environmental

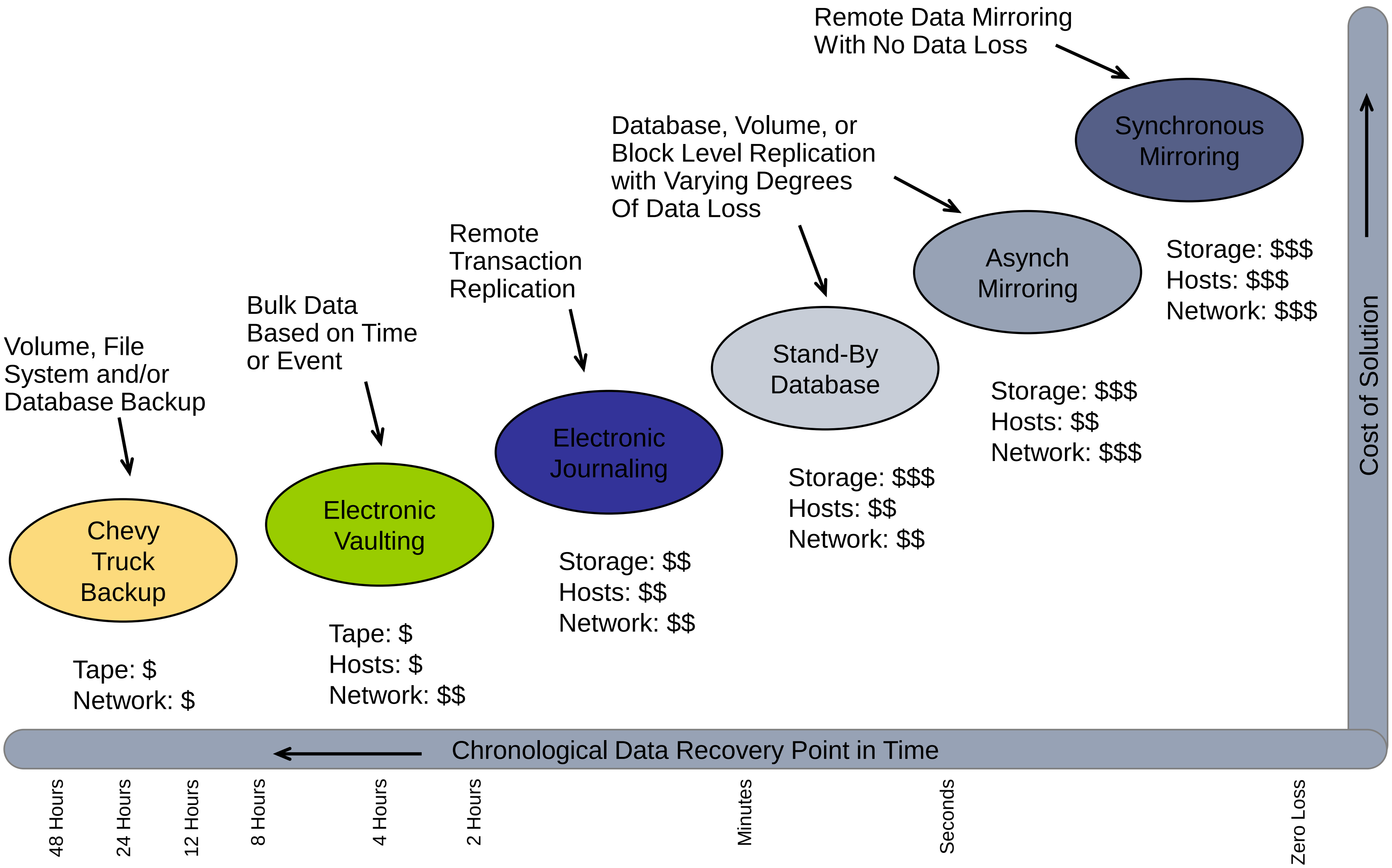
Cold-Site

Facilities: $

Best Effort at Time of Disaster

Acquisition

Delivering Degrees of RPO



Remote Data Mirroring With No Data Loss

Synchronous Mirroring

Database, Volume, or Block Level Replication with Varying Degrees Of Data Loss

Asynch Mirroring

Storage: $$$
Hosts: $$$
Network: $$$

Remote Transaction Replication

Stand-By Database

Storage: $$$
Hosts: $$
Network: $$$

Bulk Data Based on Time or Event

Electronic Journaling

Storage: $$$
Hosts: $$
Network: $$

Volume, File System and/or Database Backup

Electronic Vaulting

Storage: $$
Hosts: $$
Network: $$

Chevy Truck Backup

Tape: $
Hosts: $
Network: $$

Tape: $
Network: $

Cost of Solution

Chronological Data Recovery Point in Time

Gartner

Disaster Recovery Service Reference Architecture		Tier 1 <4 hrs	Tier 2 5 – 24 hrs	Tier 3 25 – 48 hrs	Tier 4,5,6 49 – 72 hrs > 73 hrs Within 168 hrs
Servers	**Server Type**	Physical	Physical / Virtual	Physical / Virtual	Physical / Virtual
	Clustering	Optional	Optional	Optional	N/A
	Continuous Availability	Optional	Optional	Optional	N/A
	High Availability	Optional	Optional	Optional	N/A
	Type of Clustering	Active / Active Active / Passive	Active / Active Active / Passive	Active / Active Active / Passive	N/A
	Server Status DR Site	Dedicated	Repurposed or Dedicated	Repurposed or Dedicated	Drop Ship or Repurposed or Dedicated
	Storage Type	SAN	SAN	SAN	SAN / DAS / Local
	Server Operational Recovery Method	High Availability	High Availability or Rebuild	Rebuild	Rebuild
	Host Bus Adaptors Required (minimum)	1	1	1	0
	Network Interface Cards Required (minimum)	1	1	1	1
Storage	Storage Frame	Enterprise level High End	Enterprise level High End	Enterprise level High End	Mid-Range
	Storage Type	SAN	SAN	SAN	SAN / DAS / Local
	Data Replication	Array-based	Array-based	Backup	Backup
	Type of Replication	Asynchronous	Asynchronous	Restore from Disk	Restore from Tape
	Replication Bandwidth Required	Dependent on Application	Dependent on Application	Dependent on Application	N/A
	Switch Fabric Connections	2	2	2	1
	Frequency of Data Replication	<=4 Hours	<=4 Hours	<=24 Hours	<=24 Hours
	Data Copies – Production	Variable	Variable	1	N/A
	Data Copies – DR Copy	Variable	Variable	1	N/A
	Data Copies – Backups	Optional	Optional	Weekly full copy and daily incremental	Weekly full copy and daily incremental
	Data Protection – Production	RAID 10	RAID 10	RAID 10	Optional
	Data Protection – DR Gold Copy	Parity RAID	Parity RAID	N/A	N/A
	Data Protection – Backup	Optional	Optional	Disk based	Tape based
	Continuous Data Protection	N/A	N/A	N/A	N/A
	Continuous Remote Replication	N/A	N/A	N/A	N/A
	Operational Recovery Method	BCV / Clone / Snap	Mirror / Snap	Backup to disk	Backup to tape

Tier 1 and 2

RTO - **< 4 hrs (Tier 1) and 5 – 24 hrs (Tier 2)**
RPO – the length of time between the last data update and the disaster declaration is from **several minutes to 4 Hours** for SAN attached storage and **24 hours for direct attached**.

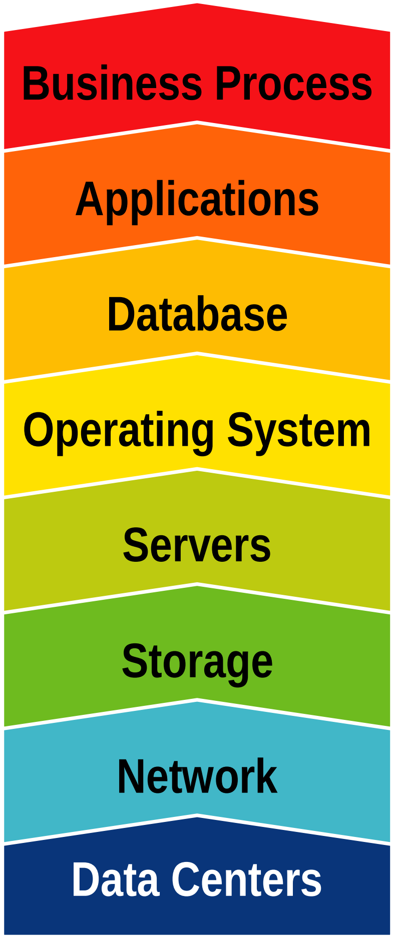
Data Replication <=4hrs

Failover: **Complete failover** from the production site to the DR site

DR Site Architecture: The **DR Site infrastructure will have available** the servers, in either physical or virtual configuration, defined to support agency operations.

Server configuration: **Allocated Servers Physical / Virtual** will already be racked and installed with the respective operating system and application, ready to initialize when the data Logical Unit is connected. **Active/Active – Active/Passive Clustering / SAN storage**

Network Recovery: All required network interfaces meeting defined capacity are in place in each data center for site failover



Business Process

Applications

Database

Operating System

Servers

Storage

Network

Data Centers

Data Protection: Application data available at the Production SAN storage will be replicated to the DR SAN storage using **asynchronous remote replication capabilities (Raid 10 / Parity Raid)**

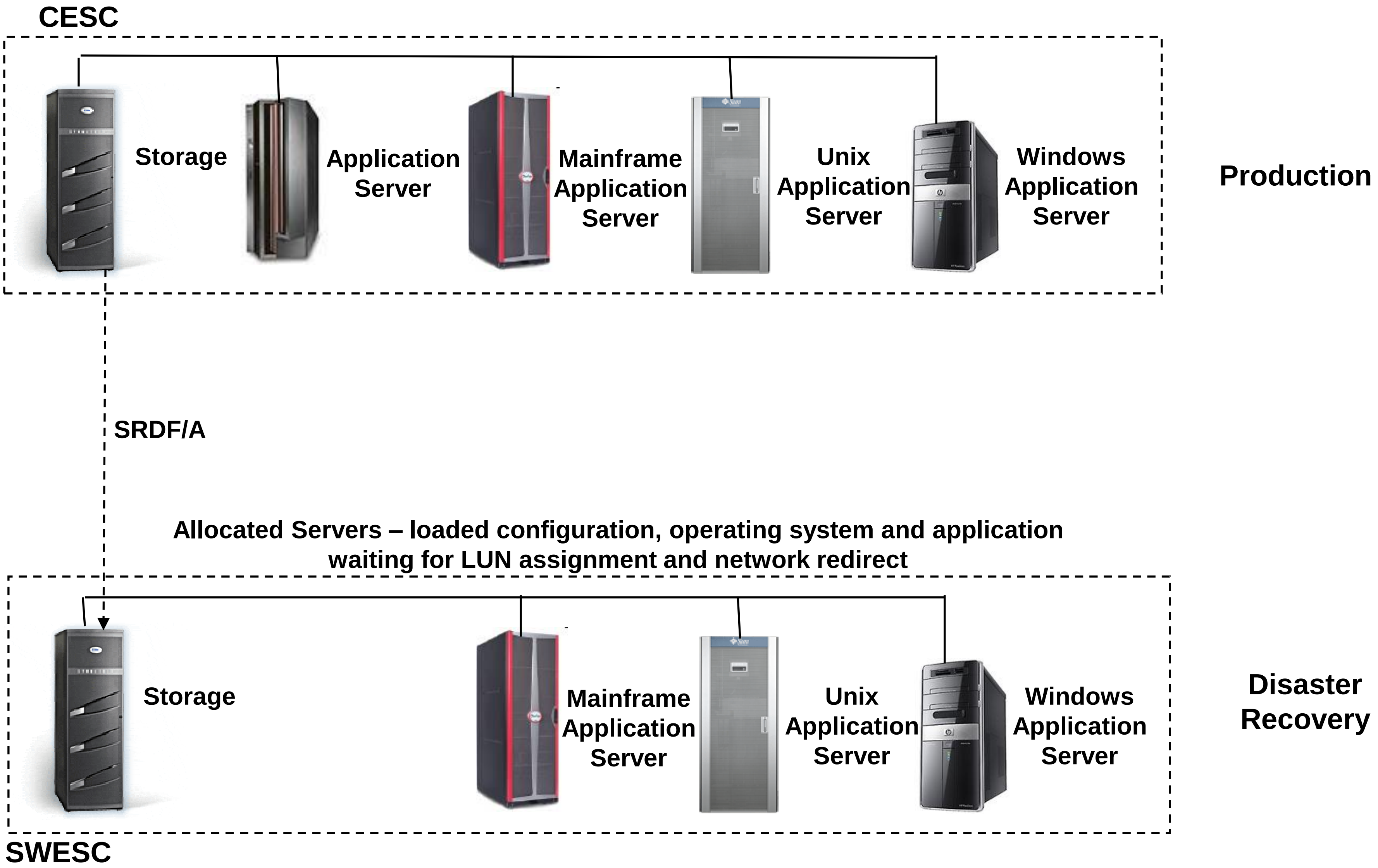
Database Recovery: Database servers will be recovered to physical or virtual server in the failover site; servers may be on a high availability cluster configuration if required

Server Operational Recovery: **High-Availability / Rebuild**

Storage Recovery: **SAN** The storage array will be replicated to the DR site using an **array based asynchronous replication**. For Tier 2 depending on the application structure, it will be required that data is recovered using a mixed recovery solution.

Infrastructure Recovery: All preventative controls (power, cooling and space requirements) are managed and provided with the service.

Proposed RTO of < 4hrs (Tier 1) / 5-24 hrs (Tier 2)



CESC

Storage

Application Server

Mainframe Application Server

Unix Application Server

Windows Application Server

Production

SRDF/A

Allocated Servers – loaded configuration, operating system and application waiting for LUN assignment and network redirect

Storage

Mainframe Application Server

Unix Application Server

Windows Application Server

Disaster Recovery

SWESC

Tier 3

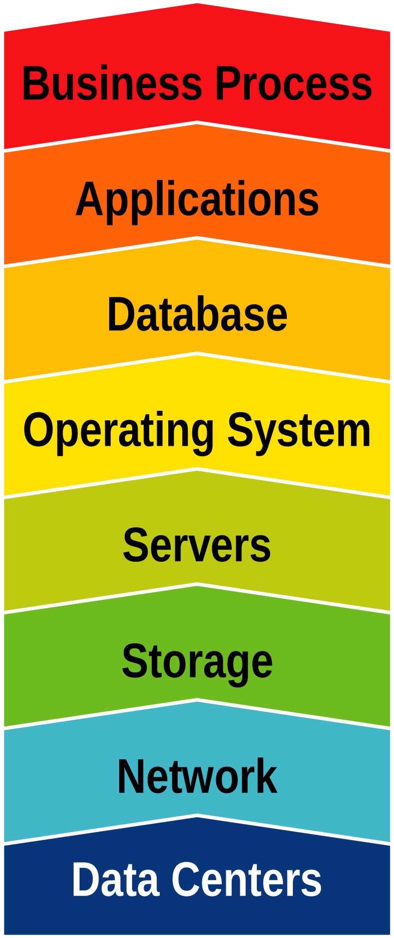
RTO – **25 – 48 hrs**
RPO – the length of time between the last data update and the disaster declaration is from **<=24 hrs.**

Failover: When the operating system and application environments are available and operational and the logical unit with the data is linked to the server a network reconfiguration will enable the complete failover from the production site to the DR site

DR Site Architecture: **Repurposed / Allocated** Servers – connected to SAN Storage.

Server configuration: **Physical / Virtual** will already be racked and **connected to the DR SAN storage**
Active/Active – Active/Passive Clustering

Network Recovery: All required network interfaces meeting defined capacity are in place in each data center for site failover


Business Process
Applications
Database
Operating System
Servers
Storage
Network
Data Centers

Data Protection: **(Raid 10) / Backup is disk based.** The backup to VTL process will need to be done at a synchronized time to avoid data corruption and all files will be backed up including database, journaled transactions and log files.

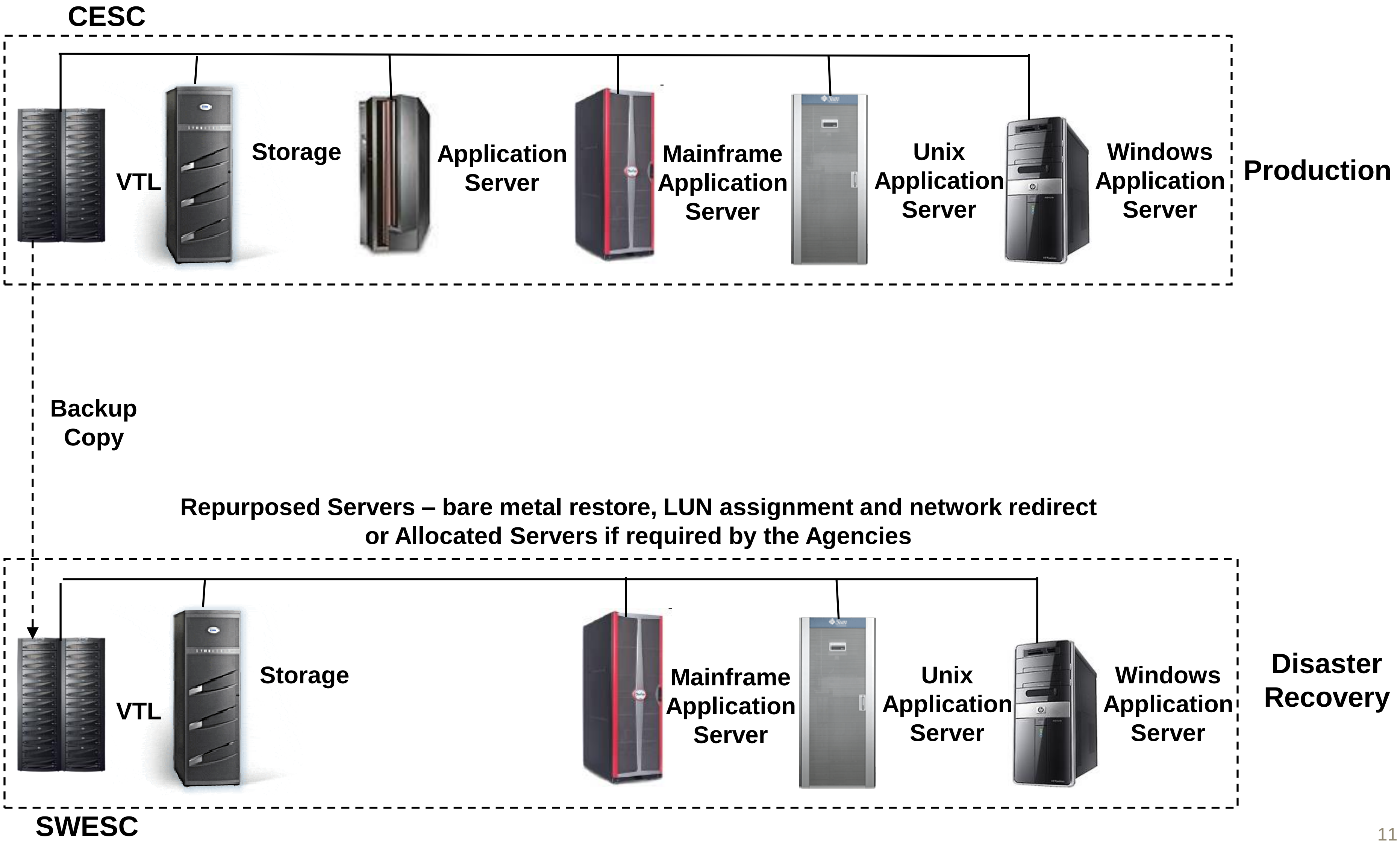
Database Recovery: Database servers will be recovered to physical or virtual server in the failover site

Server Operational Recovery: **Rebuild** The environment is comprised of physical and virtual servers and connected to the DR SAN

Storage Recovery: SAN The storage array will be restored at the DR site using a backup restoration from Virtual Tape Library (VTL). Backup files will be sent from the Production site to the DR site daily through the network, providing an RPO of 24 hours

Infrastructure Recovery: All preventative controls (power, cooling and space requirements) are managed and provided with the service.

Proposed Tier 3



CESC

VTL

Storage

Application Server

Mainframe Application Server

Unix Application Server

Windows Application Server

Production

Backup Copy

Repurposed Servers – bare metal restore, LUN assignment and network redirect or Allocated Servers if required by the Agencies

VTL

Storage

Mainframe Application Server

Unix Application Server

Windows Application Server

Disaster Recovery

SWESC

Tier 4, 5, 6

RTO – **49-72 hrs (Tier 4) / > 73 hrs (Tier 5) / with 168 hrs (Tier 6)**

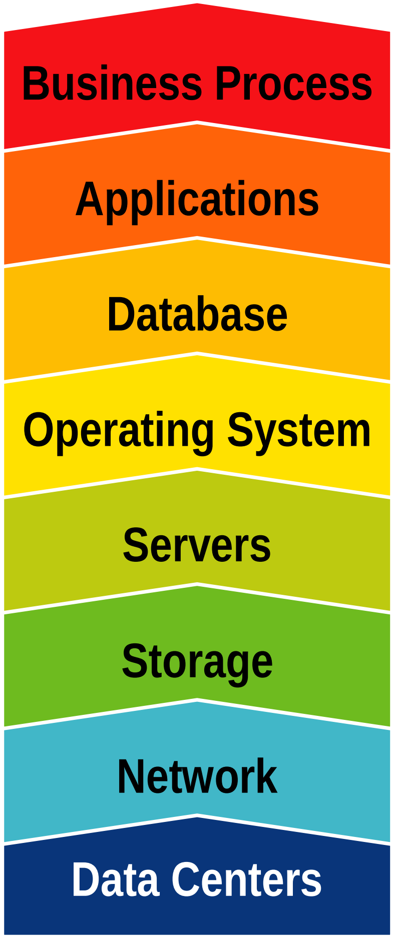
RPO – length of time between the last data update and the disaster declaration is **<=24 Hours**.

Failover: When the operating system and application environments are available and operational and the logical unit with the data is linked to the server a network reconfiguration will enable the complete failover from the production site to the DR site

DR Site Architecture: **Drop Ship / Repurposed / Allocated** connected to SAN / DAS / LOCAL Storage.

Server configuration: Physical/Virtual servers and connected to the DR SAN or through direct attached storage.

Network Recovery: All required network interfaces meeting defined capacity are in place in each data center for site failover



Data Protection: Synchronized-timed backup with restore from Tape. Weekly full copies, daily incremental. **Backup is tape-based** / ***optional RAID 10.***

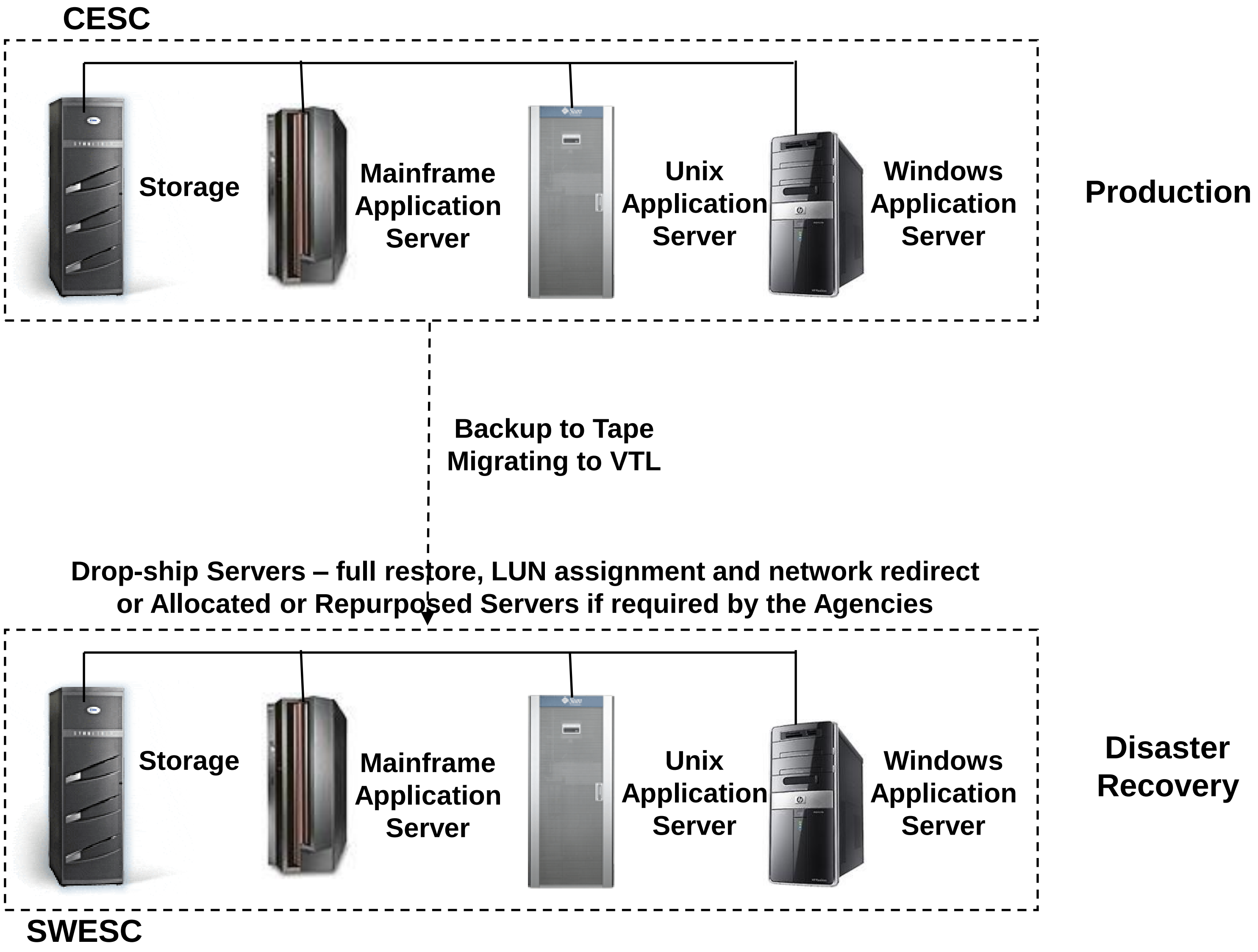
Database Recovery: Database servers will be recovered to physical or virtual server in the failover site.

Server Operational Recovery: **Rebuild** Servers are racked and ready for booting or repurposed or in drop-ship model. Operating system boot images and applications are pre-loaded or readily available or it uses resources like bare metal restore.

Storage Recovery: SAN / DAS / LOCAL The storage array will be restored at the DR site using a backup restoration from magnetic tape.

Infrastructure Recovery: All preventative controls (power, cooling and space requirements) are managed and provided with the service.

Proposed Tier 4, 5, 6



CESC

Storage

Mainframe Application Server

Unix Application Server

Windows Application Server

Production

Backup to Tape
Migrating to VTL

Drop-ship Servers – full restore, LUN assignment and network redirect
or Allocated or Repurposed Servers if required by the Agencies

Storage

Mainframe Application Server

Unix Application Server

Windows Application Server

Disaster Recovery

SWESC

Disaster Recovery Requirement Questionnaire

- **Recovery Time Objective / Recovery Point Objective**
- **Application(s)**
- **Network**
- **Infrastructure Components**
- **Backup**
- **Data Storage**
- **Security**
- **User Testing**
- **Inter-Dependencies to/with other agencies**

Checklist of Results

DISASTER RECOVERY REQUIREMENTS QUESTIONNAIRE

This checklist is for the gathering of Agency DR requirements.

Agency Name:	
Date Checklist Completed:	

		Data Supplied			
Item	**Application**	**Yes**	**No**	**N/A**	**Comments**
1	Application Software Name				
2	Application type (File System, Online Transaction Processing, Data Warehouse, Web Host, etc.				
3	Application Functional Description				
4	Application Inputs and Outputs				
5	Is there an existing DR Plan/COOP for the application?				
6	Is an offsite disaster recovery facility used? If yes, type of site (hot site, warm site, cold site)				
7	Who provides the offsite disaster recovery facility? (In-house, VITA/NG)				
8	Users (who, number of users, location, expected growth, and benefits)				
9	Percentage of successful recoveries in test and real disaster.				
10	When does the application need to be available for use (24x7x365, Mon-Fri @ 9:00 - 5:00, etc)?				
11	When is the application maintenance window?				
12	What is the guaranteed availability rate of the application (99.999%, 99.99%, 99.9%, 98% etc.)				

Determine Final Recommendations

Risk Based **Decision Matrix**	Meets RTO, RPO's	Transactional Consistency	Technology Scalability	Technology Maturity	Customer Install Base	Certified Vendor Interoperability	Logical Corruption Protection	Physical Corruption Protection
Tier 1	✓	✓	✓	✓	✓	✓	✓	X
Tier 2	X	X	✓	✓	✓	✓	✓	✓
Tier 3								

Functionality Based **Decision Matrix**	Enables Offline Backups	Recovery to Granular Point-in-time for App Data	Management & Maintenace Requirements	Granular Recovery from DB Corruption	Protection from Lost Trans in DB Corruption	Easiest to add/modify at later date
Tier 1	✓	X	✓	✓	X	✓
Tier 2	✓	X	X	✓	X	✓
Tier 3	✓	✓	✓	✓	✓	X

Identify Tier-Level Solution

Agency	Application	IPlatform	Status	RTO	RPO	Tier-Level
CWA	EMS	IBM	Non-critical moving to Windows in 2 years	24 hours	72 hours	3
CWA	HTRIS	IBM	Non-critical moving to Windows in 2 years	24 hours	72 hours	3
CWA	File Server	Windows	Business Critical	72 hours	72 hours	3
CWA	Web Server	Windows	Business Critical	24 hours	>4 hours	1

Value Added Services

DR Services

- Assist agencies with IT DR Plan updates or creation
- Assist agencies with identifying business requirements for DR testing
- Assist agencies with identifying business requirements for a DR solution

Testing Services

- Annual test for each agency
- Internal tests performed
  - will uncover and reduce errors
  - speed up recovery process by 'practicing'

Dedicated Services

- Ensure data availability and integrity
- 24/7 availability monitoring
- Real-time performance reporting
- Provides complete activation of processes and procedures at the time of a declared event
- Provides constant monitoring and management of the replication environment
- End-user recovery assistance
- Dedicated team of technical engineers