

**ADDENDUM 2 TO APPENDIX 1 TO SCHEDULE 3.3
TO THE
COMPREHENSIVE INFRASTRUCTURE AGREEMENT
DISASTER RECOVERY SERVICES**

Overview

The Disaster Recovery (DR) Services, a Tier-Level DR Solution, addresses the disaster recovery requirements of the Commonwealth agencies at a Business Impact Analysis (BIA) ranking. The Tier-Level DR Solution approach is an expansion of the Services referenced in Appendix 1 to Schedule 3.3, Cross Functional Services SOW, Section 4.3.2, Table 28.

Service and Operational Components

This section pertains to all Tiered-levels of DR Service.

Service Boundaries: This service is available 24 hours a day, 7 days a week, and 52 weeks a year to support a declared DR event by a VITA official, which is limited the Centralized Management and Operations Center (CMOC) and a VITA Network Operations Center (NOC).

Disaster Recovery Planning: Obtain critical data, processes, service level requirements, and plans to enable those resources at an alternate disaster recovery location. Recommend best practice IT Service Continuity and DR strategies, policies, and procedures. Develop and maintain a detailed IT Service Continuity and DR plan to achieve customer IT Services Continuity and DR requirements. This will include plans for data, back-ups, storage management, and contingency operations that provides for recovering customer's systems within established recovery timeframes after a disaster affects customer's use of the Services, as well as plans for recovery of Vendor-owned and provided Systems and Services that are critical for supporting Customer business operations. Initiate the IT Service Continuity and DR plan in the event of a DR situation and notify customer per DR policies and procedures. Perform scheduled IT Service Continuity and DR tests per agreed policies and procedures.

Supplying the Required Hardware: Hardware specifications identified in the DR plans will be validated to ensure that the equivalent functionality for testing and operations during a disaster event meet the required service levels.

Operating Systems: Operating systems identified in the DR plan will be up-to-date and available during any DR test and during a disaster event in order to meet the required service levels.

Data Protection and Availability: All data identified for receiving DR will be made available at the alternate disaster recovery location for service restoration within the Tier-level service parameters defined in this document.

Pre-Event/Post Disaster Assessment and Recovery Services:

PRE-EVENT READINESS AND RECOVERY SERVICES

As part of pre-event preparedness, a team of subject matter engineers will be in a state of 'readiness' to support all necessary recovery operations. They will work with staff to identify and prioritize the affected systems requiring immediate restoration and develop / implement a recovery plan.

POST-DISASTER ASSESSMENT AND RECOVERY SERVICES

Deploy a team of subject matter engineers to assess and document the post-disaster state of infrastructure, to include systems and servers. Work with staff to identify and prioritize the affected systems requiring immediate restoration and implement the recovery plan.

IT Infrastructure Quality Management: Predict and design for expected levels of availability. Ensure service levels are met by monitoring service availability levels against SLAs.

Availability Reporting: Provide reports on the DR program which will include backup status for data replication, data recoverability, and a comparison of the recovery parameters with the agreed upon Service Level Agreements (SLA) in case of DR tests and disasters, as defined in the SLA Data Collection Documents (DCDs).

Replacement of Recovery System: All recovery equipment that fails and needs to be replaced will be ordered from the hardware and software vendor, received at the recovery facility, and provisioned for operations. The replacement equipment will be Quick Shipped from the vendor. If the equipment fails during a declared disaster recovery, and a comparable spare exists in current inventory, that spare will be provisioned for recovery of operations for the failed system.

Disaster Declaration: Once the disaster notification is validated, the disaster will be officially declared, and the disaster recovery contractual agreement will commence. The activation and escalation procedures will be detailed in all DR Plans addressing the recovery of services and operations at the SWESC facility. The disaster declaration will be conducted in accordance with the DR Plan. In the event of a disaster, fees charged to VITA for the production and DR services will remain unchanged.

Testing Service Level Capabilities and Frequency: All DR testing is conducted in accordance with a written plan that establishes the specific disaster scenario and the specific procedures to be reviewed.

The annual DR test is comprised of a Hot-site failover from the Production site to the DR site with a fail-back test from the DR site to the Production site. Testing a failover of Production to DR site will include production datacenter plus remote operations that fall under a DR-service option.

As part of this service, internal quarterly tests of each type of backup and restore process will be conducted at the Recovery Facility.

Tests, in addition to the annual DR Test can be scheduled at additional cost. This cost is not reflected in the pricing model defined in this document. The types of tests that can be scheduled and executed are:

A.) Structured Walk-through - This is a role-playing exercise in which at a minimum the team leaders walk through their assigned tasks in response to a specified scenario. Plan is checked for errors or omissions.

The disaster recovery “Structured walk-through” test is a cost-effective alternative to hot site testing for many systems. It is a focused brainstorming session in which the business continuity plan is reviewed by key business continuity team members. Participants adopt their roles as team members and verbally go through their assigned recovery steps. The presence of all key team members provides the opportunity for an interchange that will identify weaknesses in the plans, including interdependencies among the various business continuity teams.

B.) Tactical - A tactical exercise is a simulated exercise. This type of simulation is conducted in a war game format in a conference room, video conferencing. All members participate and perform their tasks, actions, and procedures under a speed up clock in response to an announced or unannounced disaster scenario. Any changes to the plan need to be implemented at the end of this exercise. The “tactical exercise” simulation is a more elaborate version of the “walk-through.”

C.) Hot site test - Fully recover the critical system on the targeted recovery system. Any changes to the plan need to be implemented at the end of this exercise.

System Supplies: All system supplies required during a test or actual event will be made available at the recovery facility.

Maintenance: All labor, parts, and travel necessary to maintain the equipment, operating software, and communications at the recovery facility will be provided at a systems availability level in accordance with SLA requirements.

All infrastructure components needed to recover operations for this tier-level will not be inoperable for a period greater than four (4) hours.

Network Services: All required network interfaces meeting defined capacity are in place in CESC and SWESC for site failover. This would include all internet-facing connection technology utilizing dedicated Virtual Private Networks (VPN) as well as Synchronous Optical Network (SONET), Frame Relay or Internet (public) VPN's. Technologies for Wide Area Network (WAN) optimization such as data compression should be evaluated for incorporation into the network to meet any anticipated increase in data bandwidth requirements beyond the current capacity. Firewalls and Virtual Local Area Networks (VLAN) will be defined in the production site as well as in the DR site enabling resource isolation in both environments.

End-User Support: For an additional cost to be priced through a work request, in the event the agency needs to evacuate the production facility, work space for end users will be provided at the operational backup facility, permitting that space is available.

Infrastructure Recovery – Preventative Controls: All preventative controls (power, cooling and space requirements) are managed and provided at the recovery facility with the service.

Operational Considerations – Scalability, redundancy, reliability, performance, availability, manageability: Dedicated Model – The SWESC will serve as the DR site for CESC with storage access over the SAN. The recovery site will be configured as a replica model of the production site (physical or virtual). This will require the use of server virtualization, concurrent asynchronous data replication and disk cloning technology for data storage. Servers will be dedicated and will be in a cluster for high availability purposes or stand-alone. Array-based asynchronous replication over the WAN including rollback ability is used to provide recovery from data recovery and protection. Security measures are in place to ensure segregation of environments so that user data and applications are completely safe from each other. Measures may include virtualization, firewalls, network virtual segmentation, storage isolation. Additional premium security may be required as specified by the Agency's systems.

DR Site Architecture: The DR Site infrastructure will have available the servers, in either physical or virtual configuration, defined to support agency operations. Those servers can also be allocated from a pool of servers available for repurposing as long as they have similar hardware characteristics

Technical Description

The Tier-Level DR Solution approach provides more granularities on costs of services for the Commonwealth Agencies, and Agencies can choose between larger ranges of services selecting the most applicable solution that will meet their disaster recovery requirements.

IT Service Continuity and Disaster Recovery (DR) Services are the activities required to provide prioritized IT Service Continuity and DR support services for customer's Critical Infrastructure (e.g., CPU, servers, network, data and output devices, End-User Devices) and associated voice and data Networks, customer applications, associated infrastructure and voice communications services. All Tiers supporting the Disaster Recovery Services are defined in section 4.3.2, Table 28 of Appendix 1 to Schedule 3.3 to the Comprehensive Infrastructure Agreement.

There are six Tier-Level DR Solutions:

- Tier 1 which addresses a recovery time objective of not to exceed 4 hours after a declared disaster,
- Tier 2 which addresses a recovery time objective of not to exceed 24 hours after a declared disaster,
- Tier 3 which addresses a recovery time objective of not to exceed 48 hours after a declared disaster,
- Tier 4 which addresses a recovery time objective of not to exceed 72 hours after a declared disaster,
- Tier 5 which addresses a recovery time objective of not to exceed 167 hours after, and

- Tier 6 which addresses a recovery time objective of not to exceed 168 hours after a declared disaster.

Technical Solution

Tier 1 and 2

- **Database Recovery Considerations:** 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. Recovery areas may be configured that can be leveraged for flashing / rolling back database transactions in the event of logical errors. Replication technology utilizing snapshot or rollback features may be used to recover from physical corruption. Consistency groups will be used to maintain consistency between the database files (data, journal, and log) and prevent data corruption. The mirrored or replicated files will be in a consistent and start-able state at the DR site.
- **Server Recovery Considerations:** The environment is comprised of physical and virtual servers and connected to the DR SAN. Servers are racked and ready for booting. Operating system boot images are pre-loaded or readily available. Applications are loaded. If required, physical or virtual servers are configured into clusters with support for active-active or active-passive configurations.

Three failover configurations exist:

- 1.) Physical to Physical – the servers are recovered to a dedicated environment.
- 2.) Physical to Virtual – the servers are recovered to a shared virtual environment.
- 3.) Virtual to Virtual – the servers are recovered to a shared virtual environment.

- **Storage Recovery Considerations:** The storage array will be replicated to the DR site using an array based asynchronous replication. Replication frequency will be configured to enable lower Recovery Point Objectives (RPO). Cloning technology will be used to increase application availability and reduce downtime to perform parallel processing activities, for example, backups if required. Snap technology may be used to create pointer-based, space-saving snapshot copies.

Consistency groups will be used to maintain multiple Logical Unit Number (LUN) replications in a consistent state, enabling fast recovery and avoiding data corruption at the DR site.

Local application data is Redundant Array of Independent Disks (RAID) protected and is mirrored or copied in real-time to the SWESC. Vendor will conduct a wireless survey of the applicable Eligible Customer Locations. The intent of this survey is to assess the impact of the Eligible Customer Location's construction and layout on the theoretical performance of the secure wireless network. Based on the results of this survey, Vendor will recommend the quantity and location of the secure wireless access points to VITA and the customer.

- **Operational Recovery:** Operational recovery for critical applications or clients is achieved through the use of high availability clustered servers when required and the use of asynchronous replication and clone technologies for creating additional data copies.
- **Architectural High-Level Modeling Criteria:** Repurposed server model with optional premium dedicated server model. Production site at CESC and based upon currently

available virtualization and data replication technologies over SAN based storage providing rapid recovery with minimal data loss and enhanced production site operational recovery at SWESC.

- **Data Protection:** Application data available at the Production SAN storage will be replicated to the DR SAN storage using asynchronous remote replication capabilities. Production data will be available on high available/redundant storage in the production site. In some particular situations, there are requirements to have parts of the data recovered through data replication and parts of the data recovered through backup to Virtual Tape Library (VTL) with the backed up files transmitted over the network to the DR site.
- **Server configuration:** For Dedicated Server option, the servers will already be racked and installed with the respective operating system and application, ready to initialize when the data Logical Unit is connected. For Repurposed Server option, the servers will be made available from a pre-defined pool of servers which will need to be connected and re-built to the application requirements prior to connecting the Logical Unit with the application data. A bare metal restoration process can be used to accelerate the recovery time.
- **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. Failover will be done from a virtualized server environment to a virtualized server environment or from a physical server environment to a physical server environment or from a physical server environment to a virtualized server environment. The last option has the potential to increase the application response time once several physical servers will be running simultaneously in the same virtualized server hardware.

The diagrams below describe the proposed solution for both Tier 1 and 2.

Disaster Recovery Service Reference Architecture		Tier 1 Not to Exceed 4 hrs after a declared disaster	Tier 2 Not to Exceed 24 hrs after a declared disaster
Servers	Server Type	Physical	Physical / Virtual
	Clustering	Optional	Optional
	Continuous Availability	Optional	Optional
	High Availability	Optional	Optional
	Type of Clustering	Active / Active Active / Passive	Active / Active Active / Passive
	Server Status DR Site	Dedicated	Repurposed or Dedicated
	Storage Type	SAN	SAN
	Server Operational Recovery Method	High Availability	High Availability or Rebuild
	Host Bus Adaptors Required (minimum)	1	1
Network Interface Cards Required (minimum)	1	1	

Disaster Recovery Service Reference Architecture		Tier 1 Not to Exceed 4 hrs after a declared disaster	Tier 2 Not to Exceed 24 hrs after a declared disaster
Storage	Storage Frame	Enterprise level High End	Enterprise level High End
	Storage Type	SAN	SAN
	Data Replication	Array-based	Array-based
	Type of Replication	Asynchronous	Asynchronous
	Replication Bandwidth Required	Dependent on Application	Dependent on Application
	Switch Fabric Connections	2	2
	Frequency of Data Replication	<=4 Hours	<=4 Hours
	Data Copies – Production	Variable	Variable
	Data Copies – DR Copy	Variable	Variable
	Data Copies – Backups	Optional	Optional
	Data Protection – Production	RAID 10	RAID 10
	Data Protection – DR Gold Copy	Parity RAID	Parity RAID
	Data Protection – Backup	Optional	Optional
	Continuous Data Protection	N/A	N/A
	Continuous Remote Replication	N/A	N/A
Operational Recovery Method	BCV / Clone / Snap	Mirror / Snap	

Figure 1 - DR Service Catalog Tiers 1 and 2

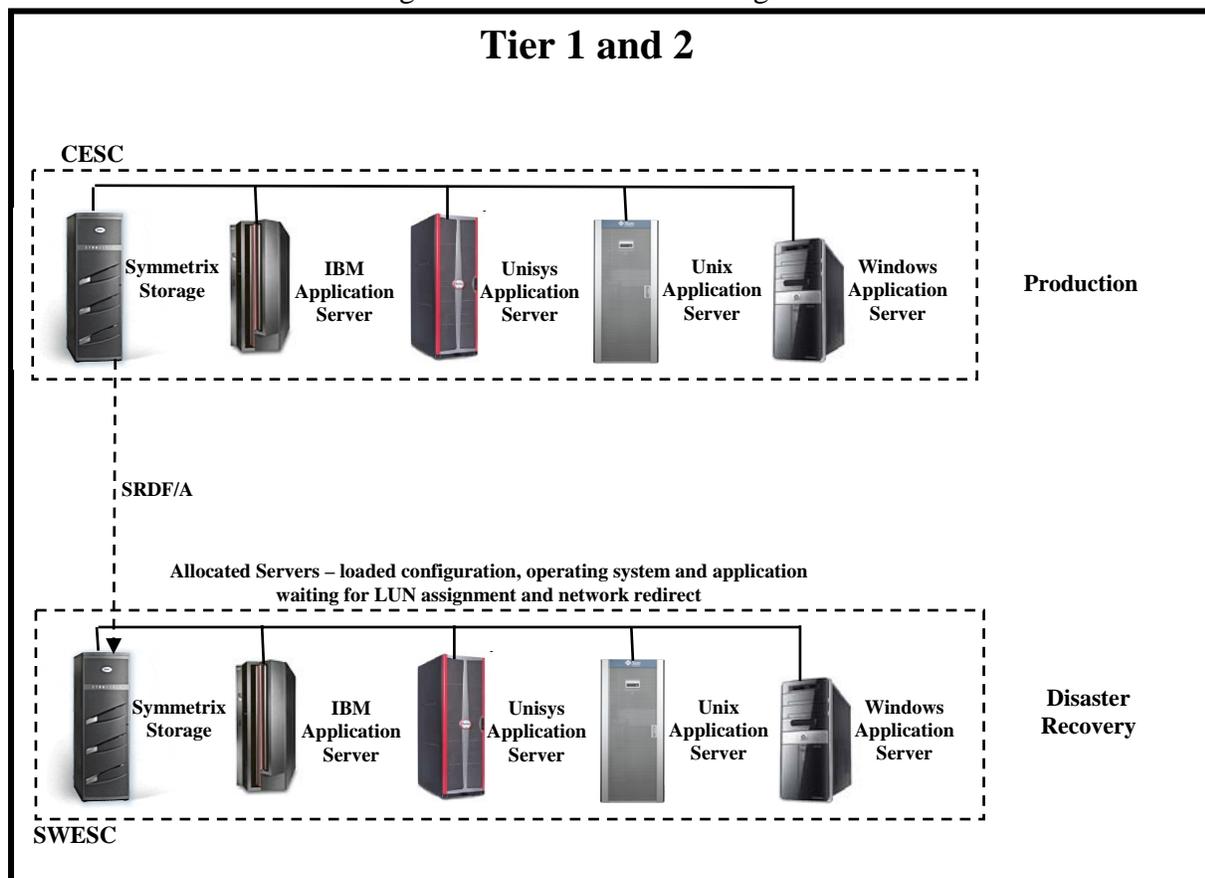


Figure 2 - DR Service Catalog Tiers 1 and 2 Solution

Tier 3

- **Database Recovery Considerations:** 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. The determination of failover to virtual or physical servers will be driven by the level of expected performance for database operations and the type of server resource agreed upon.

Recovery areas may be configured that can be leveraged for flashing / rolling back database transactions in the event of logical errors. 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. This process will provide data to be in a consistent state and usable by the database manager on the DR site.

- **Server Recovery Considerations:** The environment is comprised of physical and virtual servers and connected to the DR SAN. Servers are racked and ready for booting. Operating system boot images are pre-loaded or readily available. Applications are loaded. If required, physical or virtual servers are configured into clusters with support for active-active or active-passive configurations.

Three failover configurations exist:

- 1.) Physical to Physical – the servers are recovered to a dedicated environment.
- 2.) Physical to Virtual – the servers are recovered to a shared virtual environment.
- 3.) Virtual to Virtual – the servers are recovered to a shared virtual environment.

- **Storage Recovery Considerations:** 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. Local application data is RAID protected.
- **Operational Recovery:** Operational recovery for critical applications or clients is achieved through the use of high availability clustered servers when required and the use of asynchronous replication and clone technologies for creating additional data copies.
- **Architectural High-Level Modeling Criteria:** The production site at CESC implements repurposed server model with optional premium dedicated server model and based upon currently available virtualization and data backup technologies providing reasonable recovery time with one day data loss and production site operational recovery at the SWESC.
- **Data Protection:** Application data available at the Production SAN storage will be backed up to Virtual Tape Library (VTL) on a daily basis. The backup data files will be transferred from the Production site to the DR site through the network into another VTL. Data restoration will be done at the DR site using the same backup process that originally created the files.

- **Server configuration:** For Dedicated Server option, the servers will already be racked and installed with the respective operating system and application, ready to initialize when the data Logical Unit is connected. For Repurposed Server option, the servers will be made available from a pre-defined pool of servers which will need to be connected and re-built to the application requirements prior to connecting the Logical Unit with the application data. A bare metal restoration process can be used to accelerate the recovery time.

- **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. Failover will be done from a virtualized server environment to a virtualized server environment or from a physical server environment to a physical server environment or from a physical server environment to a virtualized server environment. The last option has the potential to increase the application response time once several physical servers will be running simultaneously in the same virtualized server hardware.

The diagrams below describe the proposed solution for Tier 3.

Disaster Recovery Service Reference Architecture		Tier 3 Not to Exceed 48 hours after a declared disaster
Servers	Server Type	Physical
	Clustering	Optional
	Continuous Availability	Optional
	High Availability	Optional
	Type of Clustering	Active / Active Active / Passive
	Server Status DR Site	Repurposed or Dedicated
	Storage Type	SAN
	Server Operational Recovery Method	Rebuild
	Host Bus Adaptors Required (minimum)	1
Network Interface Cards Required (minimum)	1	
Storage	Storage Frame	Enterprise level High End
	Storage Type	SAN
	Data Replication	Backup
	Type of Replication	Restore from Disk
	Replication Bandwidth Required	Dependent on Application
	Switch Fabric Connections	2
	Frequency of Data Replication	< = 24 hours
	Data Copies – Production	1
	Data Copies – DR Copy	1
	Data Copies – Backups	Weekly full copy and daily incremental
	Data Protection – Production	RAID 10
	Data Protection – DR Gold Copy	N/A
	Data Protection – Backup	Disk based
	Continuous Data Protection	N/A
Continuous Remote Replication	N/A	
Operational Recovery Method	Backup to disk	

Figure 3 - DR Service Catalog Tier 3

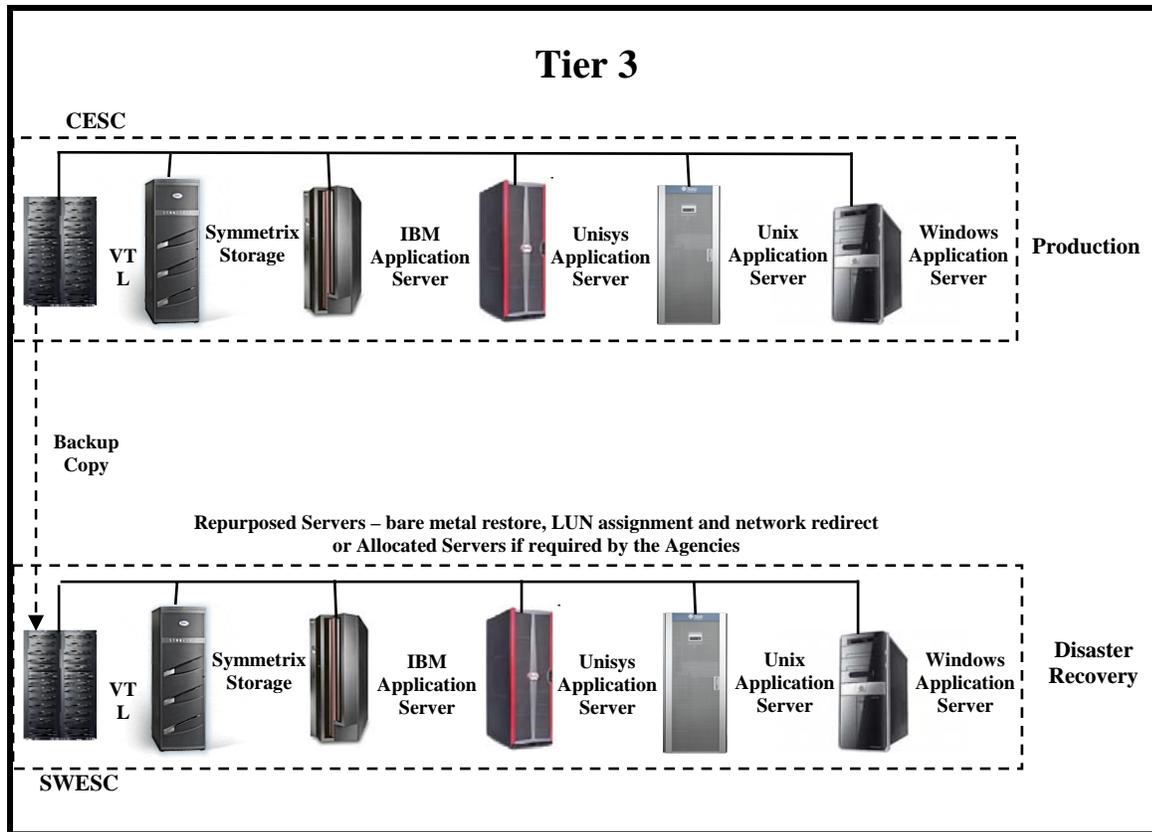


Figure 4 - DR Service Catalog Tier 3 Solution

Tier 4

- **Database Recovery Considerations:** Database servers will be recovered to physical or virtual server in the failover site. The determination of failover to virtual or physical servers will be driven by the level of expected performance for database operations and the type of server resource agreed upon. Recovery areas may be configured that can be leveraged for flashing / rolling back database transactions in the event of logical errors. The backup to magnetic tape 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. This process will provide data to be in a consistent state and usable by the database manager on the DR site.
- **Server Recovery Considerations:** The environment is comprised of physical and virtual servers and connected to the DR SAN or through direct attached storage. Servers are racked and ready for booting or repurposed or in drop-ship model. Operating system boot images are pre-loaded or readily available or it uses resources like bare metal restore. Applications are loaded or it uses resources like bare metal restore.

Several failover configurations exist:

- 1.) Physical to Physical – the servers are recovered to a dedicated environment.
- 2.) Virtual to Virtual – the servers are recovered to a shared virtual environment.
- 3.) Physical to Virtual – the servers are recovered to a shared virtual environment.

Servers will require SAN connectivity and may be configured with multiple, redundant

data paths to access the storage network as well as multiple connections to the local IP network.

- **Storage Recovery Considerations:** The storage array will be restored at the DR site using a backup restoration from magnetic tape. Backup tapes will be sent daily from the Production site to a third party tape storage partner and to the DR site in case of a disaster, providing an RPO of 24 hours. Local application data is RAID protected.
- **Operational Recovery:** Operational recovery for applications is achieved through the use of magnetic tape.
- **Architectural High-Level Modeling Criteria:** Drop-ship server model with premium optional repurposed or dedicated server models. Production site at CESC and based upon currently available virtualization and data backup technologies providing reasonable recovery time with one day data loss and production site operational recovery at SWESC.
- **Data Protection:** For dedicated server option, the servers will already be racked and installed with the respective operating system and application, ready to initialize when the data Logical Unit is connected. For repurposed server option, the servers will be made available from a pre-defined pool of servers which will need to be connected and re-built to the application requirements prior to connecting the Logical Unit with the application data. For drop-ship server option, the servers will be made available from a third party pool of servers which will need to be received at SWESC, connected and re-built to the application requirements prior to connecting the Logical Unit with the application data. A bare metal restoration process can be used to accelerate the recovery time.
- **Server configuration:** For dedicated server option, the servers will already be racked and installed with the respective operating system and application, ready to initialize when the data Logical Unit is connected. For repurposed server option, the servers will be made available from a pre-defined pool of servers which will need to be connected and re-built to the application requirements prior to connecting the Logical Unit with the application data. For drop-ship server option, the servers will be made available from a third party pool of servers which will need to be received at SWESC, connected and re-built to the application requirements prior to connecting the Logical Unit with the application data. A bare metal restoration process can be used to accelerate the recovery time.
- **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. Failover will be done from a virtualized server environment to a virtualized server environment or from a physical server environment to a physical server environment or from a physical server environment to a virtualized server environment. The last option has the potential to increase the application response time once several physical servers will be running simultaneously in the same virtualized server hardware.

The diagrams below describe the proposed solution for Tier 4.

Disaster Recovery Service Reference Architecture		Tier 4 Not to Exceed 72 hrs after a declared disaster
Servers	Server Type	Physical / Virtual
	Clustering	N/A
	Continuous Availability	N/A
	High Availability	N/A
	Type of Clustering	N/A
	Server Status DR Site	Drop Ship or Repurposed or Dedicated
	Storage Type	SAN / DAS / Local
	Server Operational Recovery Method	Rebuild
	Host Bus Adaptors Required (minimum)	0
Network Interface Cards Required (minimum)	1	
Storage	Storage Frame	Mid-Range
	Storage Type	SAN / DAS / Local
	Data Replication	Backup
	Type of Replication	Restore from Tape
	Replication Bandwidth Required	N/A
	Switch Fabric Connections	1
	Frequency of Data Replication	<=24 Hours
	Data Copies – Production	N/A
	Data Copies – DR Copy	N/A
	Data Copies – Backups	Weekly full copy and daily incremental
	Data Protection – Production	Optional
	Data Protection – DR Gold Copy	N/A
	Data Protection – Backup	Tape based
	Continuous Data Protection	N/A
Continuous Remote Replication	N/A	
Operational Recovery Method	Backup to tape	

Figure 5 - DR Service Catalog Tier4

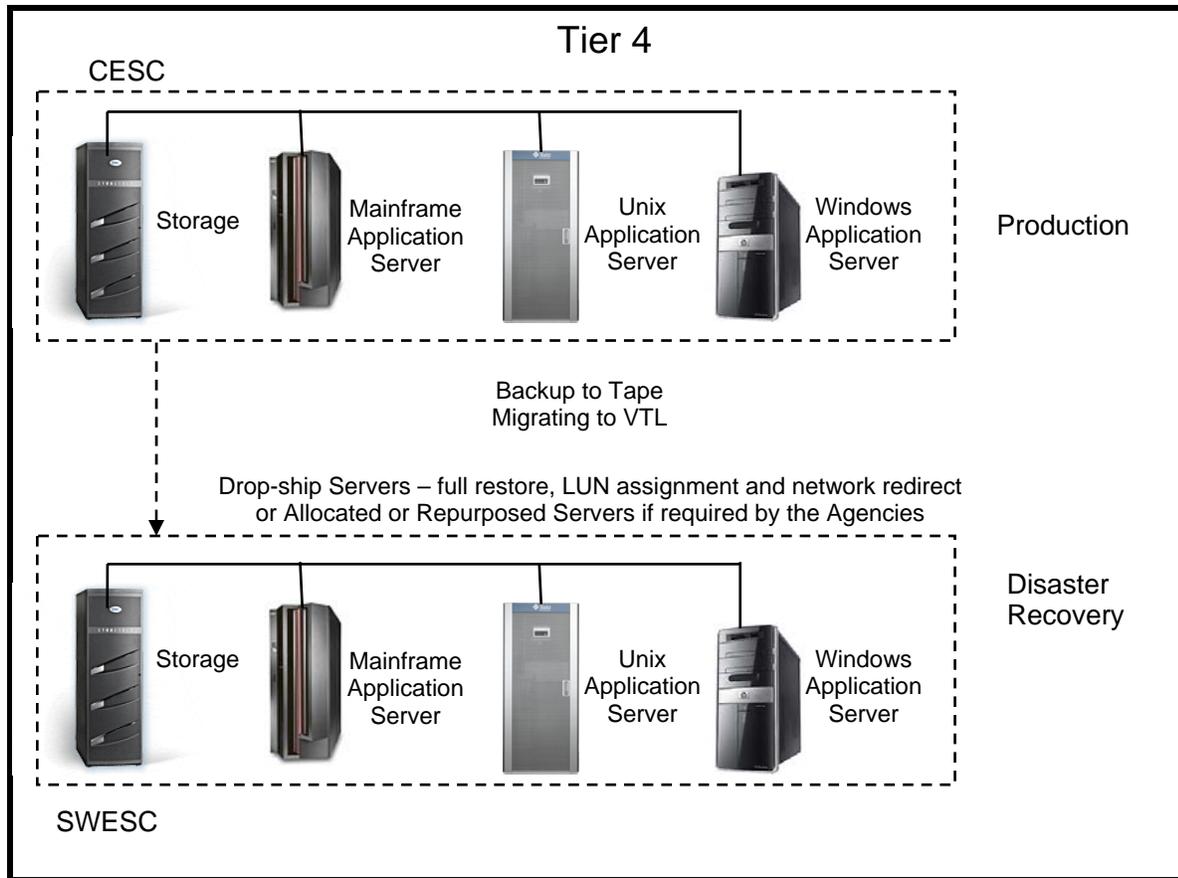


Figure 6 - DR Service Catalog Tier4 Solution

Tier 5

- **Database Recovery Considerations:** Database servers will be recovered to physical or virtual server in the failover site. The determination of failover to virtual or physical servers will be driven by the level of expected performance for database operations and the type of server resource agreed upon.

Recovery areas may be configured that can be leveraged for flashing / rolling back database transactions in the event of logical errors. The backup to magnetic tape 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. This process will provide data to be in a consistent state and usable by the database manager on the DR site.

- **Server Recovery Considerations:** The environment is comprised of physical and virtual servers and connected to the DR SAN or through direct attached storage. Servers are racked and ready for booting or repurposed or in drop-ship model. Operating system boot images are pre-loaded or readily available or it uses resources like bare metal restore. Applications are loaded or it uses resources like bare metal restore.

Three failover configurations exist:

- 1.) Physical to Physical – the servers are recovered to a dedicated environment.
- 2.) Physical to Virtual – the servers are recovered to a shared virtual environment.
- 3.) Virtual to Virtual – the servers are recovered to a shared virtual environment.

- **Storage Recovery Considerations:** The storage array will be restored at the DR site using a backup restoration from magnetic tape. Backup tapes will be sent every day from the Production site to a third party tape storage partner and to the DR site in case of a disaster, providing an RPO of 24 hours.

Local application data is RAID protected

- **Operational Recovery:** Operational recovery for applications is achieved through the use of magnetic tape
- **Architectural High-Level Modeling Criteria:** Drop-ship server model with premium optional repurposed or dedicated server models. Production site at CESC and based upon currently available virtualization and data backup technologies providing reasonable recovery time with one day data loss and production site operational recovery at SWESC.
- **Data Protection:** Application data available at the Production storage will be backed up to magnetic tape on a daily basis. The backup data files will be vaulted from the Production site to a third party tape storage facility and then to the DR site in case of a disaster. Data restoration will be done at the DR site using the same backup process that originally created the tapes.
- **Server configuration:** For dedicated server option, the servers will already be racked and installed with the respective operating system and application, ready to initialize when the data Logical Unit is connected. For repurposed server option, the servers will be made available from a pre-defined pool of servers which will need to be connected and re-built to the application requirements prior to connecting the Logical Unit with the application data. For drop-ship server option, the servers will be made available from a third party pool of servers which will need to be received at SWESC, connected and re-built to the application requirements prior to connecting the Logical Unit with the application data. A bare metal restoration process can be used to accelerate the recovery time.
- **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. Failover will be done from a virtualized server environment to a virtualized server environment or from a physical server environment to a physical server environment or from a physical server environment to a virtualized server environment. The last option

has the potential to increase the application response time once several physical servers will be running simultaneously in the same virtualized server hardware.

The diagrams below describe the proposed solution for Tier 5.

Disaster Recovery Service Reference Architecture		Tier 5 Not to exceed 167 hours after a declared disaster
Servers	Physical / Virtual	Server Type
	N/A	Clustering
	N/A	Continuous Availability
	N/A	High Availability
	N/A	Type of Clustering
	Drop Ship or Repurposed or Dedicated	Server Status DR Site
	SAN / DAS / Local	Storage Type
	Rebuild	Server Operational Recovery Method
	0	Host Bus Adaptors Required (minimum)
	1	Network Interface Cards Required (minimum)
Storage	Mid-Range	Storage Frame
	SAN / DAS / Local	Storage Type
	Backup	Data Replication
	Restore from Tape	Type of Replication
	N/A	Replication Bandwidth Required
	1	Switch Fabric Connections
	<=24 Hours	Frequency of Data Replication
	N/A	Data Copies – Production
	N/A	Data Copies – DR Copy
	Weekly full copy and daily incremental	Data Copies – Backups
	Optional	Data Protection – Production
	N/A	Data Protection – DR Gold Copy
	Tape based	Data Protection – Backup
	N/A	Continuous Data Protection
	N/A	Continuous Remote Replication
	Backup to tape	Operational Recovery Method

Figure 7 - DR Service Catalog Tier 5

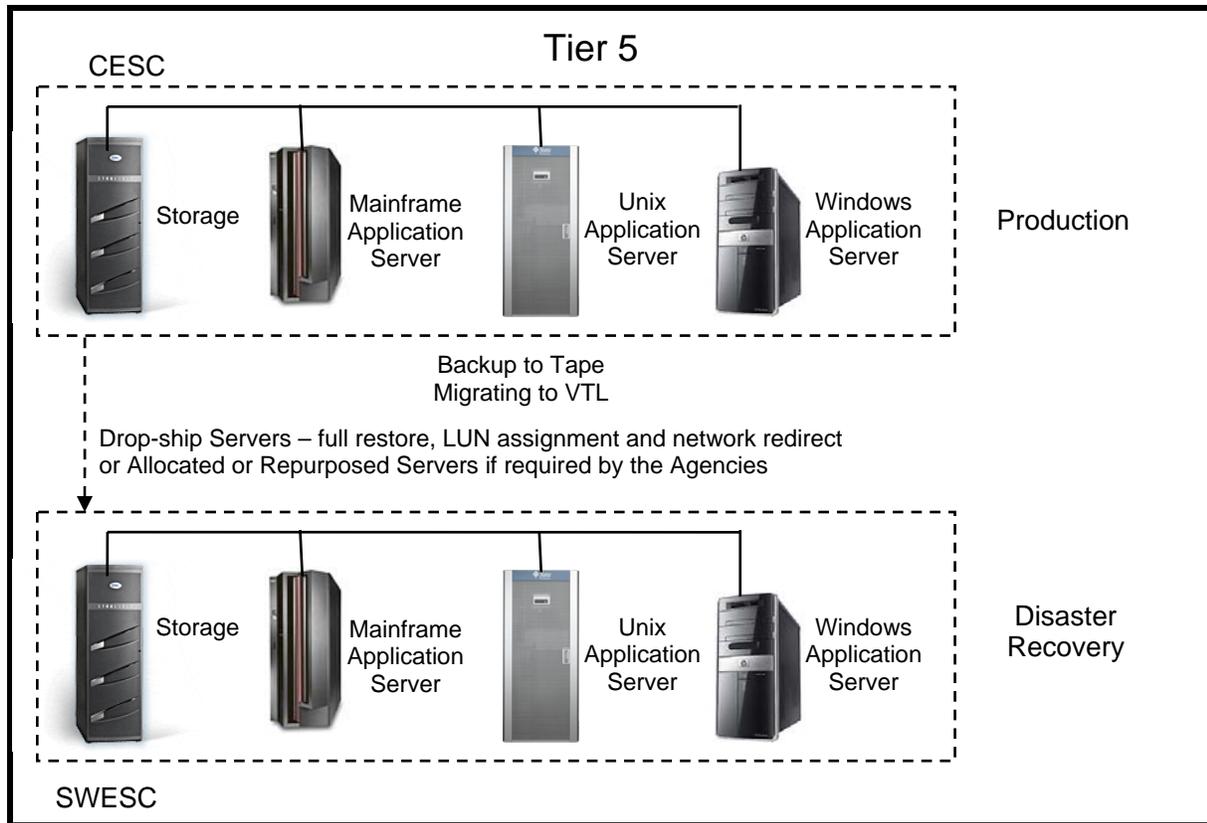


Figure 8 - DR Service Catalog Tier 5 Solution

Tier 6

- **Database Recovery Considerations:** Database servers will be recovered to physical or virtual server in the failover site. The determination of failover to virtual or physical servers will be driven by the level of expected performance for database operations and the type of server resource agreed upon.

Recovery areas may be configured that can be leveraged for flashing / rolling back database transactions in the event of logical errors. The backup to magnetic tape 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. This process will provide data to be in a consistent state and usable by the database manager on the DR site.

- **Server Recovery Considerations:** The environment is comprised of physical and virtual servers and connected to the DR SAN or through direct attached storage. Servers are racked and ready for booting or repurposed or in drop-ship model. Operating system boot images are pre-loaded or readily available or it uses resources like bare metal restore. Applications are loaded or it uses resources like bare metal restore.

Three failover configurations exist:

- 1.) Physical to Physical – the servers are recovered to a dedicated environment.
- 2.) Physical to Virtual – the servers are recovered to a shared virtual environment.
- 3.) Virtual to Virtual – the servers are recovered to a shared virtual environment.

- **Storage Recovery Considerations:** The storage array will be restored at the DR site using a backup restoration from magnetic tape. Backup tapes will be sent every day from the Production site to a third party tape storage partner and to the DR site in case of a disaster, providing an RPO of 24 hours.

Local application data is RAID protected

- **Operational Recovery:** Operational recovery for applications is achieved through the use of magnetic tape
- **Architectural High-Level Modeling Criteria:** Drop-ship server model with premium optional repurposed or dedicated server models. Production site at CESC and based upon currently available virtualization and data backup technologies providing reasonable recovery time with one day data loss and production site operational recovery at SWESC.
- **Data Protection:** Application data available at the Production storage will be backed up to magnetic tape on a daily basis. The backup data files will be vaulted from the Production site to a third party tape storage facility and then to the DR site in case of a disaster. Data restoration will be done at the DR site using the same backup process that originally created the tapes.
- **Server configuration:** For dedicated server option, the servers will already be racked and installed with the respective operating system and application, ready to initialize when the data Logical Unit is connected. For repurposed server option, the servers will be made available from a pre-defined pool of servers which will need to be connected and re-built to the application requirements prior to connecting the Logical Unit with the application data. For drop-ship server option, the servers will be made available from a third party pool of servers which will need to be received at SWESC, connected and re-built to the application requirements prior to connecting the Logical Unit with the application data. A bare metal restoration process can be used to accelerate the recovery time.
- **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. Failover will be done from a virtualized server environment to a virtualized server environment or from a physical server environment to a physical server environment or from a physical server environment to a virtualized server environment. The last option has the potential to increase the application response time once several physical servers will be running simultaneously in the same virtualized server hardware.

The diagrams below describe the proposed solution for Tier 6.

Disaster Recovery Service Reference Architecture		Tier 6 Not to exceed 168 hours after a declared disaster
Servers	Physical / Virtual	Physical / Virtual
	N/A	N/A
	Drop Ship or Repurposed or Dedicated	Drop Ship or Repurposed or Dedicated
	SAN / DAS / Local	SAN / DAS / Local
	Rebuild	Rebuild
	0	0
	1	1
Storage	Mid-Range	Mid-Range
	SAN / DAS / Local	SAN / DAS / Local
	Backup	Backup
	Restore from Tape	Restore from Tape
	N/A	N/A
	1	1
	<=24 Hours	<=24 Hours
	N/A	N/A
	N/A	N/A
	Weekly full copy and daily incremental	Weekly full copy and daily incremental
	Optional	Optional
	N/A	N/A
	Tape based	Tape based
	N/A	N/A
	N/A	N/A
Backup to tape	Backup to tape	

Figure 9 - DR Service Catalog Tier 6

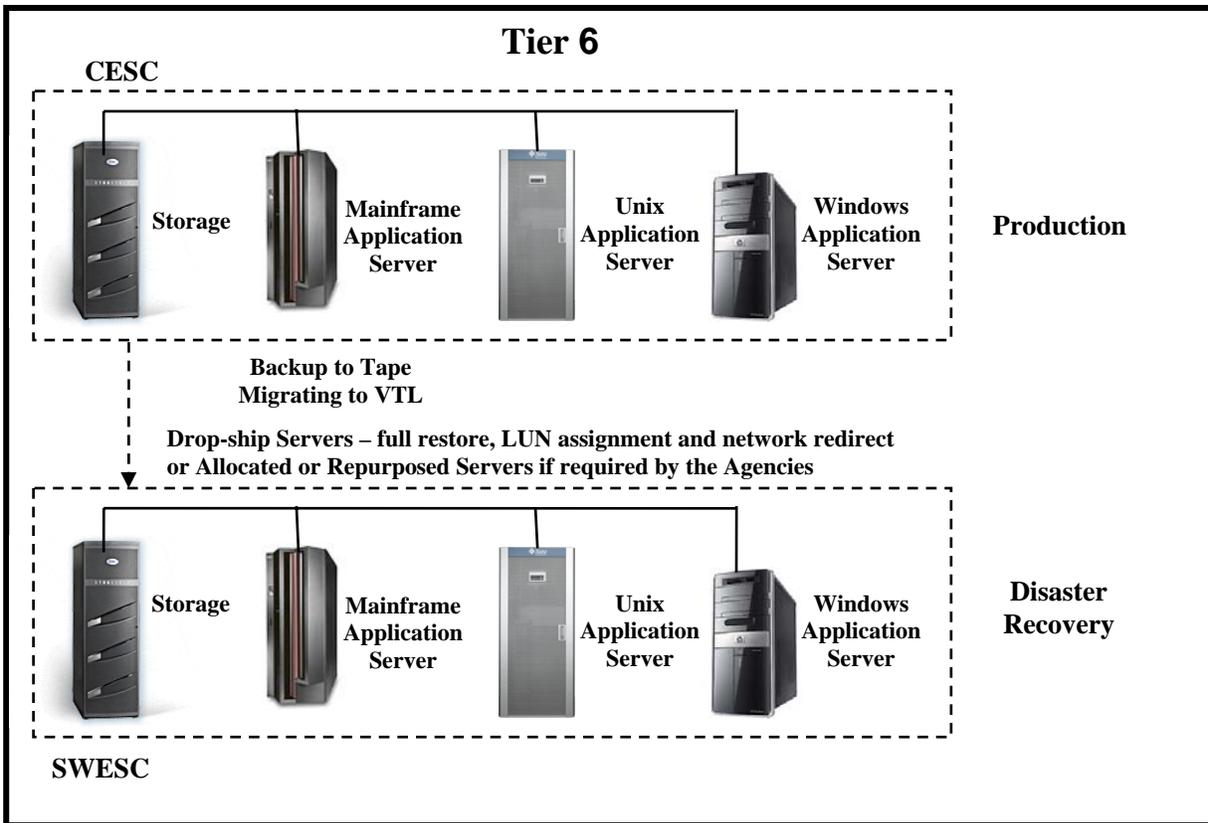


Figure 10 - DR Service Catalog Tier 6 Solution

Components

The solution(s) consists of the following components:

- a. Tier 1 and 2:
 - EMC Symmetrix with SRDF/A replication
 - 600Mbps Network Link between CESC and SWESC; with respective routers, Ethernet Switches, and Fibre-Channel Switches
 - Security Firewall and respective Software
 - PVC for remote access.
- b. Tier 3
 - EMC Avamar Grids and Software.
 - IBM VTL for mainframe
 - Networking and security are the same used for Tier 1 and 2
- c. Tier 4,5, and 6
 - Backup Software.
 - Iron Mountain for off-site storage of tape.
- d. Network, all Tier-levels solutions include:
 - Network links to the MPLS Network
 - Network links to the Internet

- Security Firewall and respective software for agency user access
- e. All Tier-levels solutions include either physical or virtual servers
- f. Storage:
 - EMC Symmetrix that is being used for Tier 2 and 3 servers
 - EMC Celerra for NAS access of some servers
 - EMC CLARiiON for low end storage
 - Server internal or direct attached storage

Architecture

The Architecture for the Tier-Level DR Solutions will reside in the Southwest Enterprise Solutions Center (SWESC) Datacenter in Lebanon, Virginia. This is the 'recovery site'.

Section 1.2 defines the DR Service Tier-Level criteria for each Tier along with a high-level solution diagram.

Security / Authentication

User Interface – 1) User Access, 2) Security and Authentication, 3) Bandwidth and Capability, and 4) Functionality & Performance: All required user interfaces meeting defined capacity are in place in the SWESC for production failover following current network architecture practices. This would include all internet-facing connection technology utilizing dedicated VPN's as well as SONET, Frame Relay, or Internet (public) VPN's. Firewalls and VLANs will enforce security policies. Full application functionality will be available to end users in the event of a failover from the production site.

Technical Assumptions

Vendor's Disaster Recovery Service for Tier-Level DR Solution Approach includes the following technical assumptions:

- Hardware specifications identified in the DR plans will be validated to ensure equivalent functionality for testing and operations during a disaster event to meet the required service levels.
- Operating systems identified in the DR plan will be up to date and available during any DR test and during a disaster event to meet the required service levels.
- All data identified in the DR plan will be made available at the alternate disaster recovery location for service restoration within the Tier-Level service parameters.
- Disaster Assessment and Recovery Services: As part of pre-event preparedness, a team of subject matter engineers will be in a state of 'readiness' to support all necessary recovery operations. They will work with staff to identify and prioritize the affected systems requiring immediate restoration and develop / implement a recovery plan.

A team of subject matter engineers will be deployed to assess and document the post-disaster state of infrastructure, to include systems and servers. Work with staff to identify

and prioritize the affected systems requiring immediate restoration and implement the recovery plan.

- Annual DR testing is conducted in accordance with a written plan that establishes the specific disaster scenario and the specific procedures to be reviewed.

The annual DR test is a Hot-site failover test from the Production site to the DR site, with a fail-back test from the DR site to the Production site. Testing a failover of Production to DR site will include production datacenter plus remote operations that fall under a DR-service option.

- System supplies required during a test or actual event will be made available at the recovery facility.
 - Maintenance: All labor parts and travel necessary to maintain the equipment, operating software, and communications at the recovery facility will be provided at a system availability level in accordance with SLA requirements.
 - Predict and design for expected levels of availability. Ensure service levels are met by monitoring service availability levels against SLAs.
 - Provide reports on the DR program which will include data replication of backup status, data recoverability and comparison of the recovery parameters with the agreed SLA in case of DR tests and disasters.
 - Quick-ship from vendors all equipment that has failed at the recovery facility and provision equipment for a readiness state.
-