TEXAS DEPARTMENT OF INFORMATION RESOURCES

DIR

85th Interim – March 27, 2018
HOUSE COMMITTEE ON GOVERNMENT TRANSPARENCY AND OPERATIONS

House Committee on Government Transparency & Operations

Interim Charge #2. Evaluate whether qualifying state agencies are appropriately utilizing available state disaster recovery services, including the statewide technology centers. Consider the costs and benefits of allowing other states to participate in Texas' statewide technology centers under Subchapter L, Chapter 2054, Texas Government Code for disaster recovery purposes.

Disaster Recovery Services

A disaster in information technology (IT) is an unplanned event that interrupts a customer's access to its data and processing capabilities residing at a datacenter or other technical facilities. The interruption must be for a significant amount of time, as determined by the nature of the interruption, to warrant Disaster Recovery (DR) activities to commence. A disaster can be anything that disables an organization's business operations for a prolonged period. If the interruption in service is anticipated to be less than the time it would take to activate the disaster recovery environment, then it would not be considered a disaster and normal remediation activities would occur. The goal of DR is for a business to recover its technical capabilities if lost in the event of a disaster and continue operating as close to normal as possible.

A Disaster Recovery Plan is the combination of policies, procedures, and tools in place that enable technical teams to restore technical capabilities (critical infrastructure, systems, and business applications) following a major disruptive event. The Plan provides information for how service restoration procedures are initiated in the event of a disaster. It lists or references the resources and infrastructure needed to restore vital business processes, and the steps to be executed to implement the recovery of capabilities. The primary purpose of a DR Plan is to document the processes required to recover production systems identified as essential for the functioning of a customer. The plan will be activated when a disaster has been declared.

There can be confusion between high availability systems and disaster recovery services. High Availability (HA) systems are durable and operate continuously without failure for a long time.

The term implies that there are accommodations for failure in the form of redundant components and network connectivity. The same basic approach is used to achieve both high availability (HA) and disaster recovery however, DR fundamentally differs from HA in terms of geographic redundancy, meaning production and recovery sites should be geographically dispersed for DR. HA generally refers to a single site installation that has been thoroughly cleansed of single points of failure, making that single site installation highly resistant to an outage. A DR site is a geographically independent and redundant implementation that may or may not be highly available, depending on customer requirements. High Availability systems still need to be incorporated in a DR plan.

Disaster Recovery Services Available in Data Center Services (DCS) Program

Overview:

In 2005, the 79th Legislature passed HB 1516 directing DIR to consolidate agencies' IT infrastructure to reduce statewide costs for IT services, modernize aging state infrastructure, and increase overall security and disaster recovery capability. Today, the data center services (DCS) program:

- Enables Texas state agencies to share costly data center infrastructure, reduce focus on IT operations and therefore concentrate on enabling their core mission
- Provides mainframe, server, network, data center, application management, cyber security services and print/mail services
- Delivers services in remaining legacy agency data centers while consolidating operations to the two regionally diverse state data centers and eliminating most legacy data centers
- Supports most of the largest state agencies, while providing the flexibility to deliver services to smaller agencies as well.

The diverse requirements of Texas agencies require a program that is collaborative and flexible. The DCS program is purposely built for the government, with government's unique requirements incorporated into the managed service offering.

Additional DCS program benefits include:

- Industry standard service levels
- Disaster recovery in alternate data center, including options for annual full disaster recovery test
- Full compliance with FBI Criminal Justice Information Services (CJIS) requirements, Texas State Auditor requirements, annual SSAE 16 audits and biannual IRS audits
- Architectural design services and reference models to standardize new server builds
- Oversight by customer executives and technical staff through governance committees
- DIR contract management, oversight and budgeting support
- Maintains a refresh schedule so at least 80 percent of hardware is current
- Update program to maintain current and fully vendor supported infrastructure software

A new operating model and multi-vendor contracts were fully implemented July 1, 2012. These contracts offer greater flexibility, increased accountability and monitoring tools, as well as more cost transparency, allowing agencies to better manage their services. The new model allowed DIR to reduce and repurpose staff in this program area by approximately 65% (25FTE's) while increasing contractual oversight.

The DCS program uses a shared governance model that engages customer agencies at all levels of decision-making. Customer agencies are divided into five partner groups that choose representatives to serve on governance committees and solution groups. This approach enables complete transparency, standardization and encourages communication across the enterprise.

Data Center Services: Secure Compute/Storage Highlights

DCS supports a fully managed environment designed specifically to protect business critical data, applications and supporting systems. There are four typical types of data storage solutions for large IT enterprises:

- Online Storage - large disk array solutions, minimizing access time to data, and maximizing reliability with geo-redundant data replication
- Backup Storage - offline storage for data protection, with a lesser price per byte than online storage, but at an operational cost of higher average access time

- Archiving - similar to backup, but its purpose is long-term retention, management, and discovery of fixed-content data to meet regulatory compliance, litigation protection and storage cost optimization objectives
- Disaster Recovery Solutions - used to protect the data from localized disasters, usually being a vital part of a broader business continuity plan.

The DCS program supports all four enterprise storage solutions and recently added additional cloud storage options for state agency customers which includes the following:

- Fully managed experience for IT infrastructure storage solutions
- Continuous security operations
- Complies with CJIS, FTI, HIPPA, PCI etc. regulatory policies
- Geo-redundant data centers within the State of Texas for full disaster and data recovery
- Data can be encrypted “at Rest and In-Transit” when under DCS management

All storage solutions comply with FBI Criminal Justice Information Services (CJIS) requirements, Texas State Auditor (SAO) requirements, annual SSAE 16 audits, and bi-annual IRS audits.

Data Center Services (DCS) Disaster Recovery Services

The Data Center Services (DCS) program uses a self-insured disaster recovery model utilizing two geographically dispersed data centers. One in Austin, Texas and one in San Angelo, Texas. The model requires customers to define their level of disaster recovery needs per application (see table 1 below). Utilizing a balanced work load strategy, agency production servers are placed in one data center with test and development servers placed in the other. This ensures that if one data center goes off line during a disaster, there would be equipment already allocated to bring the applications back on-line by repurposing the test and development servers in the alternate data center to become the active production environment.

DCS Disaster Recovery Definition - Declaration

A DCS disaster is:

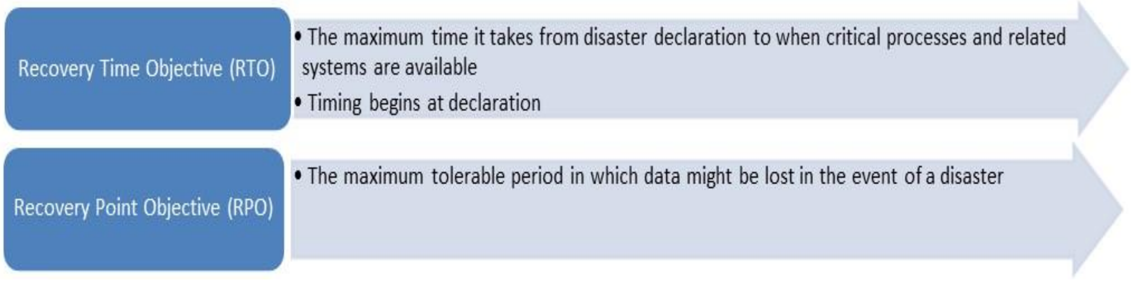
- An unplanned event that interrupts the DCS Customer’s access to its data and processing capabilities residing at a consolidated datacenter or other non-consolidated facilities.

- DIR, in consultation with the DCS Customer (as needed), and the Service Providers must declare that a disaster has occurred before recovery activities commence.
- The interruption must be of sufficient scale and for a significant amount of time, as determined by the nature of the interruption, to warrant data center recovery activities to commence.
    - If the interruption is anticipated to be less in duration than the time it would take to activate the recovery environment, then it would not be considered a disaster.
- Once a disaster is declared, recovery operations will proceed in accordance to the plans and objectives of the DR Class designation.

A DCS Datacenter Disaster is not:

- A hardware problem limited to a single device
    - Instances of this are “component recovery” items
    - Handled within the data center
- A communications break outside the data center
    - Equipment / line problems at a facility away from the data center
- Business Continuity
    - Plans / methods / procedures developed by Agencies to relocate people during a disaster event
    - Plans/methods/procedures to restore business operations and capabilities for fulfilling mission objectives
    - Manual processes used by The DCS Customer staff to continue business functions during declared data center disaster
        - Also used short term when a “component recovery” event occurs

Two critical objectives are used to focus IT and business resources on the most critical systems during a disaster situation:



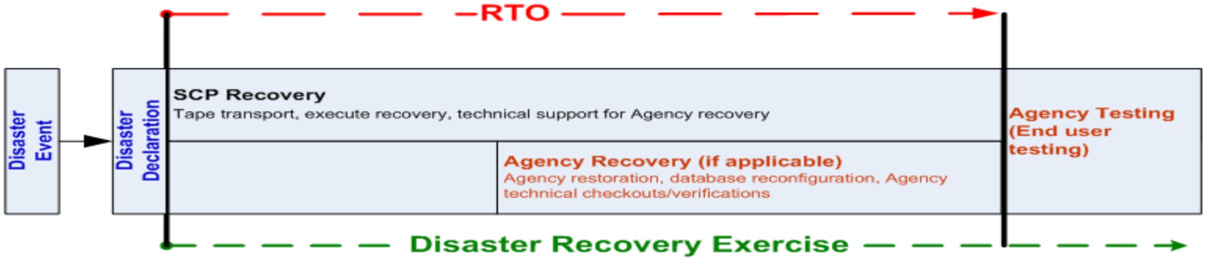
Recovery Time Objective (RTO)

- The maximum time it takes from disaster declaration to when critical processes and related systems are available
- Timing begins at declaration

Recovery Point Objective (RPO)

- The maximum tolerable period in which data might be lost in the event of a disaster

The diagram below illustrates the Recovery Time Objective (RTO) to be used for the State of Texas DCS Disaster Recovery Execution Phase:


RTO
Disaster Event
Disaster Declaration
SCP Recovery
Tape transport, execute recovery, technical support for Agency recovery
Agency Recovery (if applicable)
Agency restoration, database reconfiguration, Agency technical checkouts/verifications
Agency Testing (End user testing)
Disaster Recovery Exercise

DCS Defined Application Functional Categories

Each Application that is incorporated by a DR Plan has a designated RTO. DCS Customers will designate a DR Class and a DR Functional Category Code that is used to establish a priority for the recovery of Applications within the RTO. The RTO and priority information must be maintained in the Configuration Management Database (CMDB) which is the single source of truth for all assets in the DCS program.

The DR Functional Category Codes are described below in order of priority:

1. (SAFE) Physical Security and Safety and Public Health. *Includes all systems that support functions protecting physical security and safety of individuals and the public including but not limited to law enforcement, criminal justice, protective and related services, and homeland security; and systems that protect against imminent threats to public health including but not limited to disease outbreak and sanitation.*

2. (ASST) Essential assistance to vulnerable populations. *Includes all systems that provide financial, medical, or other life-sustaining (e.g., food, shelter) assistance benefits or services to eligible citizens such as aged, persons with disabilities, unemployed persons, and child support recipients. Includes*

both disaster-related support and continuation of ongoing benefits. The focus for this category is support for the individual beneficiary.

3. **(TRAN) Public transportation and movement of goods.** *Includes all systems that enable the use of roads, bridges, ports, airports, and other critical infrastructures and other ancillary support of transportation.*

4. **(GOVT) Essential government administration.** *Includes all systems that enable essential government functions including but not limited to critical vendor payments and financial transactions, especially those activities which if not performed would result in a significant financial loss to the state. The focus of this item is the business of government and may include items that support the functions above.*

5. **(REGU) Education, regulation, taxation, business and economic development and general government administration.** *Includes all systems supporting government functions not listed above, including but not limited to providing for education, regulating industry and business entities, collecting taxes, supporting business and economic development and general government, **which must be restored within the 24 hour or 72 hour disaster recovery window.** (Many systems that support these functions are designated D2 – D4 (medium to very low priority) and will not need to be categorized in the context of this effort.)*

Disaster Recovery Testing

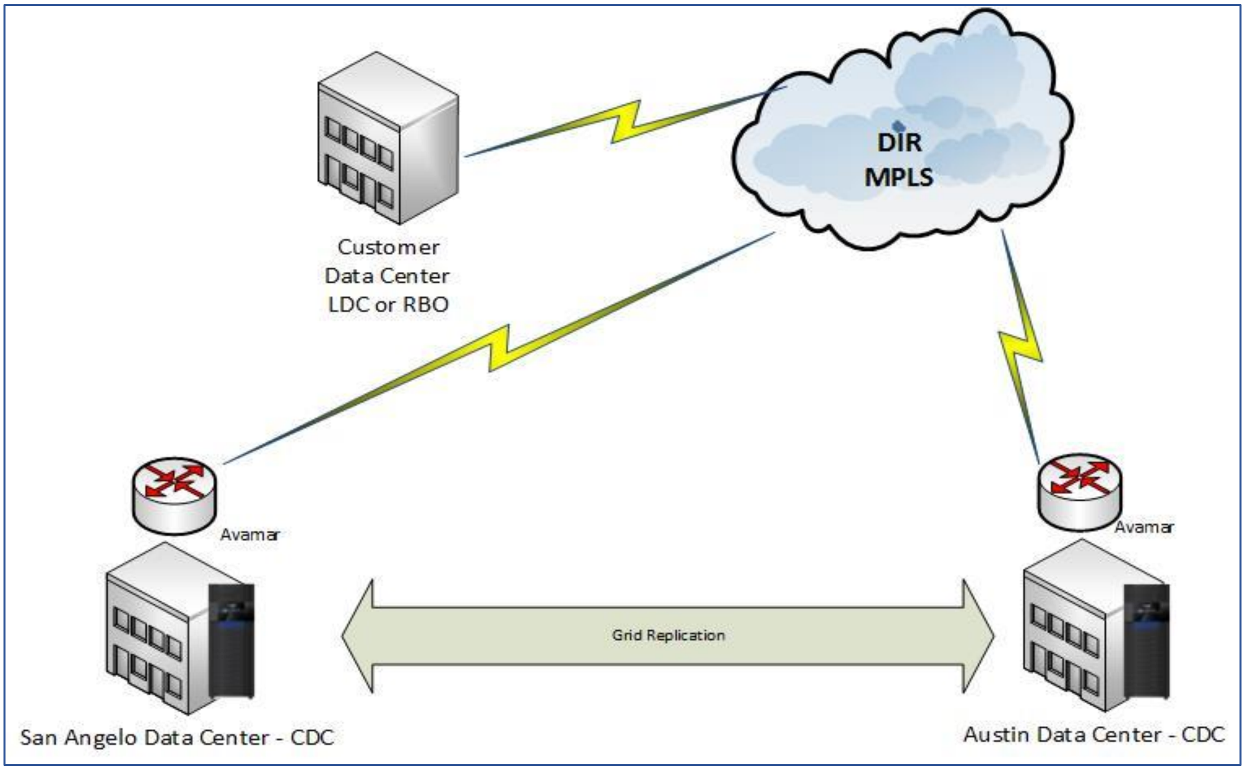
The most important aspect of disaster recovery is to perform annual disaster recovery tests. DCS customers test their disaster recovery plans for their applications annually by either a:

> **Recovery Test (RT):** This Disaster Recovery Exercise (DRE) simulates a real disaster in a controlled environment. During an exercise, the DR Plan can be wholly or partially executed, depending on the scope of the exercise. This option allows participants to evaluate pertinent processes and procedures for completeness and accuracy. The DCS Customer works with the

Primary DCS Disaster Recovery Coordinator (DRC) assigned to the test, to set exercise objectives. The exercise plan includes exercise parameters, scope, objectives, and post exercise activities.

Table Top (TT) Exercise (Walk through): Table Top tests are conducted using the DR plan and Technical Recovery Guide (TRG) documentation, without interacting with the infrastructure or applications. The same recovery steps are covered, in the form of a logical walk-through of the recovery checklist process, as well as the Technical Recovery Steps in the TRG. Improvements to the DR Plan and TRG documentation will be captured at the end of the test for subsequent updates/additions to the DR documentation.

New Optional Services for Customers:



Backup as a Service (BaaS)

Remote Backup services are now available to DCS customers over existing network connectivity. This same service is scalable and available to any potential customers that may need to backup their data to an off-premise location for data protection.

Service features include:

- Regular (as defined by the user) backup of data to the State's Data Centers via network connections
- Authorized users can request recovery of data or files anytime
- Reporting on backups provided via the State of Texas DCS portal (e.g. success/failure, schedules, retention, targets, and archive)
- Annual backup and recovery reviews with customers

Disaster Recovery as a Service (DRaaS)

- Combines the benefits of Backup as a Service (BaaS) with Disaster Recovery (DR) services
- Provides a Disaster Recovery solution in line with DCS Customer's financial and business continuity planning requirements
- Provides an Enterprise Backup and Recovery solution that addresses business continuity requirements for state agencies
- Provides an annual DR Table Top Exercise to test the recovery capabilities
- Establishes a process to be followed in the event a disaster is declared

Potential customers can take advantage of a proven Enterprise Backup and Recovery solution currently in use in the DCS program and will benefit from using the DCS virtual server platforms within the Consolidated Data Centers (CDCs). This offering has many benefits not generally offered in a typical "Drop Ship" disaster recovery solution. Because data is backed up to a CDC based centralized tapeless environment, DR recovery data is already onsite at the recovery location. This same architecture is used for Backup as a Service (BaaS) offering and allows data to be restored from the CDC to the customers Legacy Data Center (LDC) leveraging de-duplicated cached local system data.

For BaaS, DCS provides a proven architecture and solution that has been successfully deployed within the DCS program. Data backed up from the LDC to the CDC will be replicated to the alternate CDC as an offsite copy within the DCS program and can be used to recover agency applications any time required.

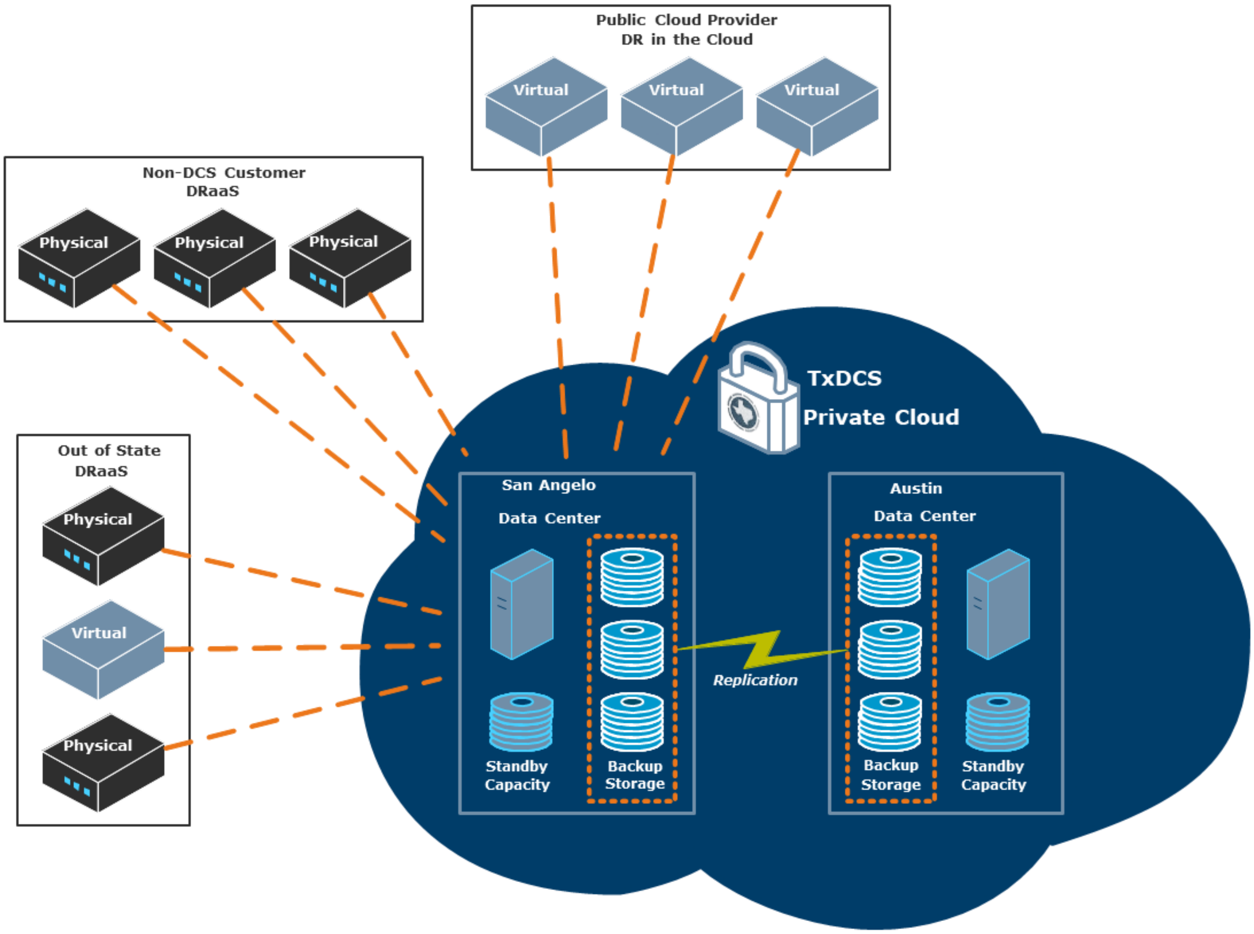
Hybrid Cloud Services (HCS)

HCS was introduced to the DCS program to provide customers with expanded cloud and self-management options, while meeting the business, security, and regulatory requirements of Texas state government. The services include Fully Managed and self-managed options, as well as DCS private community cloud and public government cloud options.

Some of the key features and benefits of this service are:

- Integrated DCS private community cloud with public government cloud options in the consolidated data centers
- Semi-managed and fully-managed service options
- Automated cloud self-provisioning
- Next generation tools & infrastructure automation improving service delivery and infrastructure availability
- Agility, transparency, and control of customer IT infrastructure and financial spend
- TAC 202 security compliance

(DR in the Cloud)



DR in the Cloud in DCS is a backup and restoration strategy that involves storing and maintaining copies of data records in a public cloud environment. The goal of cloud DR is to provide customers with an efficient and rapid way to recover data in the event of a disaster.

The benefits that make cloud disaster recovery appealing include: in-house, partially in-house or purchased as a service. This flexibility allows any type or size of customer to implement robust disaster recovery plans. Typically, cloud providers charge for storage on a pay-per-use model, based on capacity, bandwidth or seat. Because the provider is in charge of purchasing and maintaining its storage infrastructure, the customer doesn't have to spend money on additional hardware, network resources, data center space and the personnel required to support them.

Effective DCS cloud disaster recovery provides continuity for services and the ability to fail over to a second site if there is a hardware or software failure of IT systems for customers outside the DCS program. Workloads are then failed back to their original locations when the crisis is resolved. Failover and failback can be automated. Customers should run tests at regular intervals on isolated network segments that do not impact production data.

Other States use of DCS

Subchapter L, Chapter 2054 Government Code currently does not allow for tax payer funded entities outside the state of Texas to access DCS services. A legislative policy change would be required to allow other states to become customers. To date, several other states have expressed interest in having discussions about using the DCS program in their DR plans, including Kansas, Vermont and Georgia.