State of Texas

Department of Information Resources

Texas.gov Services

Exhibit 2.3

IT Service Continuity Management

DIR-ESS-TGOV-SVCS-254

Table of Contents

1 INTRODUCTION

Upon the occurrence of a disaster, the Successful Respondent shall promptly provide Disaster Recovery (DR) Services, in accordance with the applicable Disaster Recovery Plans (DRPs), including as described in, and in accordance with, the requirements of this Exhibit. In addition, this Exhibit sets forth certain requirements that the Successful Respondent shall comply with in developing, maintaining, and implementing DRPs.

2 DISASTER RECOVERY

2.1 Initial Disaster Recovery

At Commencement, Successful Respondent will take over the current Disaster Recovery plan and testing as is and support that architecture, plan and testing until the Disaster Recovery strategy as defined in **Exhibit 3.1 Service Level Matrix** is implemented.

The Successful Respondent, at a minimum, shall:

2.1.1 Leveraging the existing Disaster Recovery capabilities, work with DIR to establish declaration procedures and document those procedures in the Service Management Manual (SMM). DIR shall have the authority to declare a disaster.

2.1.2 Update the existing Disaster Recovery Plan (DRP), Application Recovery Guide (ARG) and Technology Recovery Guide (TRG) templates as defined in the SMM and referred to in **Sections 5 and 6**.

2.1.3 Support testing of all Third-Party Disaster Recovery contracts in existence, and continue to support such contracts until such time that a successful test has been achieved for alternative Disaster Recovery strategy and DIR requests the cancellation of the Third-Party Disaster Recovery contracts.

2.1.4 Proceed with recovery activities consistent with the Statewide Functional Categories, and RTOs as defined in the SMM.

2.2 Disaster Recovery Strategy

The Successful Respondent, at a minimum, shall:

2.2.1 Working with the MSI and DCS SCP(s), to develop the Disaster Recovery Strategy critical deliverable in **Exhibit 3.3 Critical Deliverables,** design new disaster recovery architectures, DRPs, TRGs, ARGs and update the SMM as required to migrate all Applications to the DIR approved Disaster Recovery model using the DIR-approved disaster recovery levels.

2.2.2 Working with the MSI and DCS SCP(s), in accordance with the Disaster Recovery Strategy critical deliverable in **Exhibit 3.3 Critical Deliverables,** implement new disaster recovery architectures, technology, and Application modifications as required to migrate all Applications to the DIR approved Disaster Recovery Strategy using the DIR-approved disaster recovery levels.

2.2.3 Work with DIR to establish declaration procedures and document those procedures in the Service Management Manual (SMM).

2.2.4 Use the Disaster Recovery Plan (DRP) and Technology Recovery Guide (TRG) templates as defined in the SMM and referred to in **Sections 5 and 6**.

2.2.5 Proceed with recovery activities consistent with the Statewide Functional Categories, and RTOs as defined in the SMM.

2.2.6 Design and implement new disaster recovery strategies as technologies evolve, including, but not limited to, hybrid cloud DR offerings, DR as a Service offering, and so forth, as approved by DIR.

2.3 Disaster Recovery Plan (DRP)

The Successful Respondent, at a minimum, shall:

2.3.1 As applicable, leverage and maintain DRPs where they currently exist in support of Services and in relation to any DIR Customer-specific DRPs, in each case subject to DIR’s and the DIR Customer’s prior review and approval.

2.3.2 Create, define and maintain DRPs where they do not exist in support of DIR Shared Services provided to DIR Customers and in relation to any DIR Customer-specific DRPs, in each case subject to DIR’s and the DIR Customer’s prior review and approval.

2.3.3 Ensure DRPs include the DIR Customer-specific plan and the associated TRGs for each of the DIR Customer’s Applications.

2.3.4 For all Applications, within sixty (60) days after the Commencement Date, update all existing Services DRPs to reflect all changes implemented during the performance of Transition Services.

2.3.5 Update DRPs annually to reflect all changes implemented over the course of Successful Respondent’s performance of the Services. TRGs shall be updated whenever a change is made to the environment or Application.

2.3.6 Updated DRPs and TRGs shall be sent for the applicable DIR and DIR Customer’s review, and must document and demonstrate Successful Respondent’s plan and capability to restore Applications within their applicable RTOs.

2.3.7 Adjust the applicable DRPs and TRGs whenever DIR or a DIR Customer needs and use of the Services change.

2.3.8 Ensure DR Recovery and Test environments in the hybrid cloud align to DIR Customer DR class requirements based on solutions available in the DCS program.

2.3.9 Ensure all DRPs that are developed by Successful Respondent comply with all DIR Standards, including the National Institute of Standards and Technology Special Publication 800-34 and 800-66 Section 4.7, and shall be tested in accordance with applicable Laws and this **Exhibit 2.3 IT Service Continuity Management**.

2.4 Disaster Recovery Testing

The Successful Respondent, at a minimum, shall:

2.4.1 Assume the DR test schedules in existence at the Commencement Date, and work with DIR and DIR Customers to ensure that the annual test schedules continue without disruption.

2.4.2 In cooperation with DIR, DIR Customers, SCPs, and MSI, establish and schedule reasonable windows to accomplish all DR testing for Applications as documented in the Successful Respondent's annual DR test plan and schedule, in accordance with the Disaster Recovery Test Schedule critical deliverable in **Exhibit 3.3 Critical Deliverables**.

2.4.3 Assist DIR and the appropriate governance committee in prioritizing the test schedule of DIR Customer Applications, as specified in **Exhibit 1.2 Governance**.

2.4.4 Propose test objectives for DIR's approval and coordinate with related SCP test objectives.

2.4.5 Support the MSI in planning and preparation for annual test activities, including setting the objectives of the test. Each such test shall address the specific needs of each Application. The Successful Respondent's test execution must demonstrate, at a minimum, the Successful Respondent's and SCP(s)' ability to meet or exceed the designated RTOs for those Applications in the event of a disaster.

2.4.6 Conduct all testing activities in a manner designed to minimize impacts to active production, test, and development environments. If an active environment is required to execute the test, the Successful Respondent will, prior to the test, communicate the use of the environment to and obtain approval from DIR or the DIR Customer.

2.4.7 Notify DIR and DIR Customers of any anticipated DR risks, in accordance with the IT Service Continuity Management processes in the SMM, where DIR or a DIR Customer may choose not to participate in testing.

2.4.8 Evaluate the results of the test and identify potential corrective actions.

2.4.9 Provide initial test results to DIR and the DIR Customer, as applicable, and incorporate their feedback into the final test results report.

2.4.10 Facilitate test result review sessions with the DIR or DIR Customer to gain consensus on the success level of the test (e.g., successful, successful with issues, unsuccessful, etc.) and to identify corrective actions.

2.4.11 Resolve corrective actions and report status to the MSI as defined in the SMM.

3 RECOVERY TIME OBJECTIVE (RTO)

Each Application that is addressed by a DR Plan has a designated RTO. DIR and DIR 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 Category Code must be maintained in the Configuration Management Database (CMDB).

3.1 Disaster Recovery Level Categories

The codes are provided in **Table 1: DR Functional Category Codes**.

Table 1: DR Functional Category Codes

Code	Summary	Description
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.
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.
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.
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.
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.

3.1.1 The Successful Respondent shall perform DR Services to meet or exceed the applicable RTO for each Application, as indicated in the relevant DIR or DIR Customer DRP and tracked in the CMDB.

3.1.2 DIR or DIR Customers may change an Application's DR Class Level, using the appropriate process as defined in the SMM. Successful Respondent will perform a technical assessment of the Application's capability to meet the minimum requirements of the requested RTO, identifying any changes needed to meet the minimum requirements, and propose a solution, as needed, which implements those changes.

3.2 Disaster Recovery Level Application Requirements

3.2.1 To meet RTOs, each Application requires an appropriate supporting infrastructure, tools, and management; as described in the following table. Eligibility for DR testing for each DR class also is noted.

Table 2: DR Exercise Eligibility

DR Level	RTO	RPO	Minimum Requirements	DR Exercise Eligibility
Class P	1 hour	1 hour	1. Application resides on servers within the Consolidated Data Centers 2. Application has automatic failover 3. Application has appropriate data replication	Annual exercise of DR capability with the Successful Respondent, SCPs, and appropriate Third Parties
Class M	24 hours	1 hour	1. Application resides on Mainframes within the Consolidated Data Centers 2. Application has identified target Mainframes installed and managed in appropriate DR location 3. Application has appropriate data replication	Annual exercise of DR capability with Successful Respondent, SCPs, and appropriate Third Parties
Class 1	72 hours	6 hours	1. Application resides on servers within the Consolidated Data Centers 2. Application has identified target systems installed and managed in appropriate DR location 3. Application has appropriate data replication	Annual exercise of DR capability with Successful Respondent, SCPs, and appropriate Third Parties

DR Level	RTO	RPO	Minimum Requirements	DR Exercise Eligibility
Class 2A	7 days	48 hours	1. Application resides on servers within the Consolidated Data Centers 2. Application has identified target systems installed and managed in appropriate DR location with sufficient allocated storage 3. Application has appropriate data backup and restore methods and processes	Annual exercise or table-top exercise of DR capability with the Successful Respondent, SCPs, and appropriate Third Parties.
Class 2B	14 days	48 hours	1. Application has identified target systems installed in appropriate DR location with sufficient allocated storage 2. Application has appropriate data backup and restore methods and processes 3. Application has compatible tape technologies at appropriate DR location	Annual table top exercise of DR capability Successful Respondent, SCPs, and appropriate Third Parties
Class 3	21 days	48 hours	1. Application recovery is supported by “acquired at time of disaster” contracts from the Service Component Provider available to deploy in an appropriate DR location 2. Application has appropriate data backup and restore methods and processes 3. Application has compatible tape technologies at appropriate DR location	Annual enterprise table-top exercise of DR capability with Service Providers and appropriate Third Parties Application recovery is out of scope Upon request during annual planning cycle, annual DCS Customer table-top exercise of DR capability with Service Providers and appropriate Third Parties
Class 4	Low Priority, as part of Service Restore	Low Priority, as part of Service Restore	Application has appropriate data backup and restore methods and processes	No Exercise

DR Level	RTO	RPO	Minimum Requirements	DR Exercise Eligibility
Class 6	14 days	48 hours	1. Application resides on servers within the Consolidated Data Centers 2. Application has identified target systems installed and managed in appropriate DR location with sufficient allocated storage 3. Application has non-Transactional Data only. Agency Assumes the risk that the application will provide acceptable performance on slower disk 4. Application has appropriate data backup and restore methods and processes	Annual table top exercise of DR capability with Service Providers and appropriate Third Parties
Class 8	As per the DR Recovery contract	As per the DR Recovery contract	Application has appropriate data backup and restore methods and processes	Annual exercise of DR capability, as per DR contract, with Service Providers and appropriate Third Parties

3.2.2 On an ongoing basis, Successful Respondent shall report to DIR and DIR Customer where applications do not have appropriate methods to support an Application’s DR Level rating, as part of Successful Respondent’s annual DR Planning update and as part of Successful Respondent’s annual Capacity Planning activities.

3.2.3 When an Application has not been included in DR Testing activities in more than two (2) years, Successful Respondent shall raise risks to DIR and the MSI, in conjunction with Risk Management, where Successful Respondent reasonably may not be able to meet that Application’s RTO.

4 DISASTER RECOVERY CONSIDERATIONS

4.1 Other Considerations

Related considerations for Successful Respondent’s support of DR.

4.1.1 Business continuity planning for DIR Customer business shall remain a function retained by DIR Customers; the Successful Respondent will support the DIR Customer’s business continuity planning through appropriate IT Service continuity planning as described in this **Exhibit 2.3 IT Service Continuity Management**.

4.1.2 DR and business continuity planning in respect of any sites, applications or systems that are managed, controlled, or owned by the Successful Respondent shall be the responsibility of the Successful Respondent. This includes all tools, facilities and technologies the Successful Respondent respectively uses to deliver the Services.

4.1.3 DR planning in respect of out-of-scope equipment shall remain the responsibility of the DIR Customers.

4.2 Texas Emergency Management Council

Any disaster that potentially affects the Consolidated Data Centers and Non-Consolidated Service Locations will require DIR, SCPs, and MSI to interact with the State's Emergency Management Council ("the Council"). The Council, composed of thirty-two (32) agencies, the American Red Cross and The Salvation Army, is established by state law to advise and assist the Governor of the State in all matters relating to disaster mitigation, emergency preparedness, disaster response, and recovery.

During major emergencies, the Council representatives convene at the State Operations Center to provide advice on and assistance with response operations and coordinate the activation and deployment of State resources to respond to the emergency. Generally, State resources are deployed to assist local governments that have requested assistance because their own resources are inadequate to deal with an emergency. The Council is organized by emergency support function, or groupings of agencies, that have legal responsibility, expertise, or resources needed for a specific emergency response function.

5 DISASTER RECOVERY PLAN CONTENTS

DIR expects the DRP and TRGs to provide sufficient level of detail for the Successful Respondent to successfully recover within the RTO.

5.1 Standard Disaster Recovery Plan Contents

5.1.1 All DRPs that are developed by Successful Respondent shall adhere to the Disaster Recovery Plan format and contents as defined in the SMM as approved by the MSI and DIR and address the following topics unless otherwise directed by DIR: Background, Scope, Declaration Criteria, Call-Out Procedure, Contingency Model Resource Plan, Key Documents and Procedures, Notification and Reporting, Technical Recovery Guide Activities for various system types.

6 TECHNICAL RECOVERY GUIDE (TRG) CONTENTS

TRGs shall adhere to the format and contents as defined in the SMM as approved by DIR and address the following items, unless otherwise directed by DIR and the respective DIR Customer.

6.1 Technical Recovery Documentation, Distribution, Review & Approval

6.1.1 Server configurations will be identified, documented, and maintained for each environment ensuring technical recovery to required configurations can be accomplished, such as:

a. Hardware;

b. OS;

c. Storage; and

d. Network.

6.1.2 Server and application environment dependencies will be identified, documented, and maintained ensuring technical recovery steps are known and can be sequenced appropriately to ensure business services operations can be restored including:

a. OS dependencies required to support applications and databases;

b. Directories, File system and other mount points required such as Network File Service (NFS);

c. Inter-server environment relationships and dependencies;

d. Security dependencies;

e. Interface dependencies;

f. Application and/or database specific dependencies; and

g. Operations dependencies associated to the server/application such as required job task procedures (processes and services which will be enabled).

6.1.3 TRGs will be maintained, reviewed and approved. This will include processes of quality control performed by the MSI and review and concurrence with the DIR Customer.

6.1.4 The process of maintaining currency of the TRGs will be fully documented and repeatable.

6.1.5 TRGs will capture operational elements of the environments including:

a. System operational requirements which need to be re-enabled as required to support the business purpose of the environment

b. Post boot instructions required

c. Integration instructions required for cross teams support in restoring the overall business purpose of the environment

6.2 Technical Recovery Procedures

6.2.1 Successful Respondent will utilize technical recovery approaches based on sequenced recovery events and restoration of associated dependencies for each environment. This sequenced order of recovery events will be documented for every environment and be relevant to end-to-end recovery requirements.

6.2.2 Focus of technical recovery will be on restoration of business service, ensuring all related recovery dependencies are addressed.

6.2.3 Backup and recovery technical requirements and related processes in the context of recovering specific environments will be fully described as part of the technical recovery procedures as required to enable end-to-end technical recovery of the business purpose for each environment. This includes specifics associated to each environment including distinction of:

a. Hardware/OS recovery
b. Application software and related OS configuration recovery
c. Non-database data recovery
d. Database recovery

6.3 Recovery Technology Standards

6.3.1 Enterprise recovery technology standards will be fully documented and demonstrate technology standards used to enable technical recovery of all environments supported.

a. Hardware/OS recovery for all platforms supported
b. Application software and related OS configuration recovery
c. Non-database data recovery
d. Database recovery (all DB platforms)