UTHealth
The University of Texas
Health Science Center at Houston



May 5, 2015

**Report on Disaster Recovery Capabilities #15-204**

We have completed our audit of Disaster Recovery Capabilities. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

## BACKGROUND

UTHealth relies heavily upon the ability to process and analyze information and has become increasingly dependent on computer-supported information processing and telecommunications. The increasing dependency on these technologies for operational support poses the risk that a lengthy loss of these capabilities could seriously affect the overall performance of UTHealth. A disaster recovery plan outlines the strategy for recovering data in order to continue operations.

A disaster can be broadly defined as:

> "An adverse incident that in some ways causes the loss of the ability to perform a specific or group of business functions or activities."

An incident could be the result of a natural event, a human mistake, or willful damage. An effective disaster recovery plan should respond to each of these and is a comprehensive statement of consistent actions taken before, during, and after a disaster. The plan should be documented and tested to ensure the continuity of operations and availability of critical resources in the event of a disaster. It should also identify the critical functions and the resources required to support them, as well as provide guidelines to ensure that needed personnel and resources are available for disaster preparation, assessment, and response to ensure that a timely restoration of services.

The *Texas Administrative Code Security Controls Standard Catalog* (CP-2 Contingency Plan) requires a written disaster recovery plan, testing the plan on an annual basis, and updating the plan based on information learned during the annual testing. Section CP-6 (Alternate Storage Site) requires that mission critical information be backed up on a scheduled basis and stored offsite in a secure, environmentally safe, locked facility accessible only to authorized personnel.

The IT Security department facilitates disaster recovery planning at UTHealth and coordinates the annual testing for all mission critical applications, which are assigned a disaster recovery strategy based on recovery time and point objectives. The disaster recovery strategies for mission critical applications include:

713.500.3160 phone 713.500.3170 fax
P.O. Box 20036
Houston, Texas 77225
www.uthouston.edu

**High Availability** – Data is either incrementally copied on a continous basis or simultaneously replicated to both the central and backup data centers. An automatic and seamless transition to servers in the backup data center allows business to be continuously operational with little to no interruption.

**Backed Up/DR Tested** - Data is periodically copied and archived to servers in the backup data center. Technical recovery procedures have been developed and are tested on an annual basis. Data is not continuously available, but can be restored within a matter of hours.

**Backed Up** – Data is periodically copied and archived to servers in the backup data center so it may be used to restore the original after a data loss event. Data is not continuously available, but can be restored within a matter of hours. Technical recovery procedures have been developed but are not regularly tested based on direction by management.

## OBJECTIVES

The objective of this audit was to determine whether controls around the disaster recovery process are appropriate and functioning as intended.

## SCOPE AND METHODOLOGY

Through a review of technical recovery procedures, testing results, backups, replication documentation, and interviews with recovery team leaders, Auditing and Advisory Services (A&AS) performed an audit of the disaster recovery process.

## AUDIT RESULTS

### Disaster Recovery Plan

A&AS obtained and reviewed the UTHealth Disaster Recovery Plan (DRP), noting the last revision occurred on March 15, 2011. We discussed the DRP with the Manager, IT Security, and noted the following:

- The annual review of the DRP is not formally performed or evidenced.
- The biannual review of functions to ensure their information and medium dependencies have not changed is not formally performed or evidenced.
- The quarterly requirement for the employee phone call list and equipment inventories to be recreated from their master source is only performed on an annual basis.
- The biannual review of the employee awareness program is not performed or evidenced.

### Technical Recovery Procedures & Annual Testing

A&AS obtained a list of mission critical applications and judgmentally selected a sample of five to determine if the technical recovery procedures were documented and properly tested:

- Allscripts (High Availability)
- Documentum (High Availability)
- MiPacs (High Availability)

- Human Capital Management (HCM) (Backed Up/DR Tested)
- Claims Manager (Backed Up)

We interviewed system administrators in the Data Center Operations team to gain an understanding of the technical recovery process and recovery team awareness for each application, as well as reviewed the technical recovery procedures, documented test steps, results from the most recent annual test, and communications to system owners. We noted that the technical recovery procedures for Claims Manager were not formally documented. Additionally, while test scripts exist and there was some evidence that testing did occur for the annual testing of Documentum, the results of the most recent end user testing was not formally documented or recorded.

**Recommendation #1:**
We recommend that IT and IT Security work together to ensure the DRP is updated to reflect the current business practices and requires the formal documentation of technical recovery procedures and end user testing for all mission critical applications.

***Management's Response:*** IT Security will update the DRP to reflect the current business practices. IT (DCOS) will formally document the technical recovery procedures for all mission critical applications. IT Security will ensure that end user testing is formally documented for all mission critical applications.

*Responsible Party:* Amar Yousif and Kevin Granhold
*Implementation Date:* November 30, 2015

**High Availability**
For Allscripts, Documentum , and MiPacs, we interviewed IT personnel to gain an understanding of the process and related technologies for making data highly available. For each application, we reviewed the adequacy of the process, evidence that the data is highly available, monitoring procedures, and the procedures in the event of a continuous backup or replication failure. No issues were noted.

**Backed Up/DR Tested & Backed Up**
For HCM (Backed Up/DR Tested) and Claims Manager (Backed Up), we interviewed IT personnel to gain an understanding of UTHealth's current ability to recover critical information and to assess the adequacy of the backup processes for compliance with the *Texas Administrative Code Security Controls Standard Catalog*. For each application, we reviewed the backup schedules, evidence of backup completion, the location of the backup, and the process of periodically validating that the backup can be recovered. No issues were noted.

**CONCLUSION**

Controls around the disaster recovery process are appropriate and functioning as intended. A recommendation was made to update the DRP to reflect the current business practices and require formal documentation of technical recovery procedures and end user testing.

We would like to thank the IT Security personnel and management, as well as other personnel throughout the IT department who assisted us during our review.

Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

DGS:bbs

cc: Audit Committee
Rick Miller
Amar Yousif
Kevin Granhold
Beverly Moore

Audit Manager: Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned: Brittney Alexander

Issue Date: May 22, 2015