
We have completed our audit of compliance with Texas Administrative Code 202 (TAC 202) requirements for disaster recovery testing. This audit was conducted to fulfill the TAC 202 requirement for a bi-annual audit of compliance with TAC 202 and is part of our fiscal year 2013 audit plan. This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

BACKGROUND

The Texas Administrative Code (TAC) was created in 1977 by the Texas Legislature under the Administrative Code Act and is a compilation of all state agency rules in Texas. There are 16 titles in the TAC. Each title represents a specific category and related agencies are assigned to the appropriate title. Title 1, Part 10, Chapter 202, Subchapter C covers information security standards for institutions of higher education and includes eight sections or rules.

TAC 202.74 Business Continuity Planning includes requirements for annual disaster recovery (DR) testing and was last amended to be effective in September 2009. The goal of DR testing is to document what can be recovered successfully, identify areas that could not be recovered, and communicate the results to the business owners. At the University of Texas Health Science Center at Houston (UTH), it is the responsibility of Information Technology (IT) to conduct the tests. A DR test can range from a desk review to a complete restoration of the system with full-load user testing. While tests can vary in size and scope, a typical DR test will involve several IT areas, including: IT management, application administrators, database administrators, systems administrators, network analysts, datacenter operations personnel, and hardware specialists. A DR test can be conducted over a period of several hours or several days, depending upon the criticality of the application and the complexity of the computing environment. Information Security is also involved in the DR process; they provide oversight for the process and develop formalized reports summarizing the tests results. It is the responsibility of IT to involve the owners of each application to ensure testing methodologies and results meet the owner’s needs.

OBJECTIVE

The objective of this audit was to determine compliance with selected requirements of Texas Administrative Code (TAC) 202 Information Security Standards.
SCOPE AND METHODOLOGY

Auditing and Advisory Services (A&AS) reviewed compliance with DR testing requirements during fiscal year 2012. Where applicable, we reviewed documentation of tests performed in earlier fiscal years. A&AS reviewed backup processes, DR test reports, and the communication of results to system owners and custodians.

AUDIT RESULTS

A&AS selected a judgmental sample of four critical applications, AllScripts EMR, GE Centricity, and PeopleSoft’s Human Capital Management (HCM), and Financial Management System (FMS). We reviewed reports of the DR tests over the past four years. We briefly reviewed plans for testing PeopleSoft Campus Solutions, the recently implemented student information system. Because of the recent implementation, a DR test has not been performed. Plans for testing will be finalized in Spring 2013.

A&AS reviewed system backup schedules and logs for each of the four applications. The schedules were reasonable and controls were in place to notify appropriate individuals of any problems with these jobs.

Each of the four applications had a DR test each year from 2009 through 2012. These tests involved restoring the systems at an offsite location and included varying amounts of functionality and user testing.

HCM and FMS are tested together. HCM and FMS test results are regularly communicated through management of the Disaster Recovery Plan and the Information Services Service Requests (ISSR) process. System owners and representatives from the business areas are included in these communications and processes. Campus Solutions will also follow this process once DR testing has begun.

AllScripts and GE Centricity are tested together, though not all aspects of both systems are fully integrated. This environment is rapidly changing as the integration progresses. DR tests were performed each year from 2009 through 2012. The results of the March 2012 test were communicated during the Information Technology Business Operations Committee meeting on January 23, 2013.

Though the results of testing were communicated to the business owners of the various applications, we noted that the communication process was sometimes ad hoc and may not be well documented. The business owners need to know the type of testing performed, the results of the test, and the nature of any limitations of the recovered environment for business continuity planning. The need for regular, documented communication was discussed with the CIO and CISO during the audit. Both agreed to refine their processes and quickly updated their
processes. Responsibility for communicating the results was reiterated and a formal attestation mechanism was implemented.

CONCLUSION

In our opinion, UTH ealth complies with the TAC 202 requirement for annual disaster recovery testing and communication of the results.

We would like to thank the Department of Information Technology, and the individuals throughout the institution who assisted us during our review.

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

DGS: cs

cc: Audit Committee
    Kevin Dillon
    Richard Miller
    Amar Yousif
    Kevin Granhold
    James Griffiths
    Connie Wooldridge

Audit Manager: Tim Burr MBA, CIA, CISA, CFE
Auditors Assigned: Cara Saldivar

Issue Date: January 30, 2013