UT SOUTHWESTERN
MEDICAL CENTER

Daniel K. Podolsky, M.D.
President
Philip O'Bryan Montgomery, Jr., M.D. Distinguished
Presidential Chair in Academic Administration

Professor of Internal Medicine
Doris and Bryan Wildenthal Distinguished
Chair in Medical Science

December 4, 2013

Raymond S. Greenberg, M.D., Ph.D.
Executive Vice Chancellor for Health Affairs
The University of Texas System
O. Henry Hall, 2nd Floor
601 Colorado Street
Austin, Texas 78701

Dear Dr. Greenberg:

Enclosed for your information is a copy of The University of Texas Southwestern Medical Center Internal Audit Report – 13:22 Texas Administrative Code (TAC) 202 Compliance.

I concur with the auditors' recommendations and support implementation of these recommendations.

Sincerely,

Daniel K. Podolsky, M.D.

Enclosure

cc: Arnim E. Dontes, Executive Vice President, Business Affairs
J. Michael Peppers, System Chief Audit Executive
Valla Wilson, Assistant Vice President, Office of Internal Audit

The University of Texas Southwestern Medical Center

Internal Audit Report 13:22
Texas Administrative Code (TAC) 202 Compliance
FY 2013

December 4, 2013

Office of Internal Audit
5323 Harry Hines Boulevard
Dallas, Texas 75390-9017
(214) 648-6106

University of Texas Southwestern Medical Center
Internal Audit Report 13:22
Texas Administrative Code (TAC) 202 Compliance
FY 2013

AUDIT REPORT
December 4, 2013

Daniel K. Podolsky, M.D., President
University of Texas Southwestern Medical Center
5323 Harry Hines Boulevard, MC 9002
Dallas, Texas 75390-9002

Dear Dr. Podolsky:

We have completed our review of the Texas Administrative Code (TAC) 202 Compliance requirements for institutions of higher education as detailed below. The primary objectives of this assessment were to 1) evaluate the controls and processes in place in support of the University of Texas Southwestern Medical Center's (Medical Center) compliance with Texas Administrative Code Chapter 202 Subchapter C (TAC 202); and 2) assess the associated policy statements and processes.

Executive Summary

Background

Created in 1977 by the Texas Legislature, the Texas Administrative Code (TAC) is a compilation of all state agency rules in Texas. The portion of the code applicable to the Medical Center for purposes of this audit is Title 1 Administration, Part 10 Department of Information Resources, Chapter 202 Information Security Standards, Subchapter C Security Standards for Institutions of Higher Education. The Medical Center's compliance with TAC 202 is required to be audited at least biennially.

The Texas Department of Information Resources provides oversight and guidance to assist state agencies in developing policies and implementing information security programs that comply with the provisions of TAC 202. The Medical Center's Department of Information Resources has developed numerous security policies.

The Medical Center's Information Security (IS) function experienced a key management change in 2011. The current Chief Information Security Officer (CISO) was hired in December 2011. The former CISO left the institution in October 2011, leaving this position vacant for approximately 2 months.

Audit Objectives

The primary objectives of this audit were to evaluate the controls and processes in place in support of the University of Texas Southwestern Medical Center's (Medical Center) compliance with Texas Administrative Code Chapter 202 Subchapter C (TAC 202) and assess the associated policy statements and processes.

Scope and Methodology

The audit covered the period of September 1, 2011 to August 30, 2013. This is a required audit for the fiscal year 2013 Medical Center Audit Plan. Activities included interviewing key personnel regarding processes in place to address TAC 202 requirements and analyzing supporting policies, procedures, and documentation that management referenced in support of their efforts. We performed activities to

evaluate policy statements and processes in the following areas Management/Staff Responsibilities, Managing Security Risks and Physical Security, Information Resources Security Safeguards, Security Incidents, User Security Practices and Removal of Data from Data Processing Equipment.

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

Conclusion

Overall the process, policies, and activities related to the information security program are well-established and address the majority of requirements. Joshua Spencer, Chief Information Security Officer, has an in-depth understanding of the rules and regulations covered in TAC 202 and he is dedicated to ensuring compliance with information security standards. Given the nature of Business Continuity and the collaborative effort required between IS, the Business Continuity team and other business process stakeholders, deliberate integration will be necessary across these stakeholder groups to address the items identified. Continued focus on the remaining two areas will complete compliance expectations. As certain issues are repeat matters from 2011 biennial audit, Mr. Spencer should discuss with management the necessary steps that must be taken to ensure all requirements are addressed in a timely and comprehensive manner.

While no exceptions were noted in seven of the nine policies and processes related to TAC 202, policies and practices related to Security Standards and Business Continuity Planning did not meet expectations. Specific points related to these areas follow:

Segregation of Duties {Rule 202.70 (8)}

The Medical Center does not define security policies regarding adequate controls and segregation of duties for tasks that are susceptible to fraudulent or other unauthorized activity. Maintaining segregation of duties reduces opportunities for unauthorized or unintentional modification or misuse of the Medical Center's assets. Policies should include perspectives related to management roles/responsibilities, access privileges, levels of authority and monitoring expectations.

Business Continuity Planning {Rule 202.74}

TAC 202 includes a requirement around Business Continuity planning which "covers all business functions of an institution of higher education" and that Business Continuity planning is "a business management responsibility". With respect to Rule 202.74, we identified two issues:

- A formal Business Impact Analysis (BIA) and formal Risk Assessment (RA) have not been completed by the Medical Center. A completed BIA and RA is necessary to determine the criticality of the various business processes by the various business owners and establish clear priorities for IS and IR Senior Management for recovery. Due to the lack of formal business input defining priorities, Disaster Recovery planning may not have covered all critical business systems and processes. This issue was previously noted in audit 11:21 - TAC 202 Compliance issued March 11, 2011.

- The development and testing of the Disaster Recovery Plan for the Medical Center was in the process of being developed during the time of our audit. Despite the lack of formal inputs on determination of critical business processes by the process owners (i.e., BIA), IR has started to test recovery of all 62 systems deemed critical by IR (and has completed tests of all 18 critical infrastructure systems). However, due to the lack of formal business input defining priorities, tests performed may not have covered all critical business systems and processes. This issue regarding testing was previously noted in audit 11:21 - TAC 202 Compliance issued March 11, 2011.

Several recommendations are proposed to strengthen the Medical Center's compliance around Business Continuity Planning. First, a business-validated RA and BIA which identify critical applications and service level requirements such as recovery time objectives should be completed. Once the BIA has been completed, Disaster Recovery plans should be refreshed to outline all the recovery procedures, the required interdependencies, resources, contact information, and considerations required to resume business functions and/or processes based upon business requirements. IS should then reconcile the BIA Analysis with the existing Disaster Recovery plan to ensure IS capabilities during a time of disaster are appropriate. As this program matures, recovery testing of critical business processes should incorporate success criteria form the business owners and validate the mapping of business processes to IT dependencies.

(Note: While this project focuses on current TAC 202 standards related exclusively to Information Resources, Internal Audit has learned that the future revision of TAC 202 is scheduled to include Institution-wide Business Continuity Planning.)

Management has agreed to implement the recommendations made.

We thank Joshua Spencer, Chief Information Security Officer, Sylvia Revell, Business Affairs/Associate Director Business Continuity and the entire Information Security staff involved in this project for their professional courtesy and assistance as we completed our activities.

Detailed Results

Individual results and recommendations are discussed below:

1. Segregation of Duties

In accordance with TAC 202 Rule 202.70, the State of Texas outlines specific security policies which apply to all state institutions of higher education. The following state policy should be addressed, "*Institutions of higher education shall ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.*" Information Security (IS) does not define relevant controls and segregation of duties over information resources vulnerable to unauthorized and fraudulent activities within the Medical Center's security policies.

Recommendations

As IS migrates its policies to the Institutional Policy Handbook, IS should include directives that require the appropriate segregation of duties. These directives should include the management of roles, responsibilities, access privileges and level of authority to include control activities such as 1) allocating access rights and privileges based on only what is required to perform job activities; 2) periodic reviews of access rights to ensure that access is appropriate for the current threats, risks, technology; and 3) business need and allocating roles for sensitive activities so that there is a clear segregation of duties.

Management Action Plan

Management has agreed to implement the recommendations made.

Responsible Personnel: Joshua Spencer, Chief Information Security Officer

Due Date: March 31, 2014

2. Business Continuity Planning

TAC 202 includes a requirement around Business Continuity planning which "covers all business functions of an institution of higher education" and that Business Continuity planning is "a business management responsibility". Within the Medical Center, Business Continuity has responsibility for identifying and prioritizing critical business processes and systems, while IS has been tasked with mapping criticality to operational requirements and ensuring such requirements are implemented and tested in accordance with TAC 202.74. Two key matters exist:

- A Risk Assessment (RA) and Business Impact Analysis (BIA) that identifies critical applications and business processes has not been completed and validated by the business. Without a business-validated list of critical applications, business processes and allowable down-times, business functions may not be able to plan for and recover timely during an outage involving a loss of technology. IS does have listings of departments and critical information systems that are being monitored for progress of completing Disaster Recovery plans and testing. However, there has been no formal determination of critical business processes by the Business Process owners via a BIA. In addition, because a BIA has not been completed, recovery time objectives (RTOs) and recovery point objectives (RPOs) for critical systems may not fully reflect business risks and needs. This issue was previously noted in audit 11:21 - TAC 202 Compliance issued March 11, 2011. Policies and standards governing these interrelationships with Business Continuity and business process owners should be updated accordingly.

- Integrated testing has not been performed on all critical systems to verify that Disaster Recovery plans are adequate to support critical operations or to ensure the successful recovery of significant functional services. IS has identified 62 critical systems (18 infrastructure systems and 44 applications). These have been vetted by IS and IR Senior Management, but have not been confirmed against a completed BIA. While all 18 critical infrastructure systems have been tested, 44 critical applications have not had their recovery documentation validated through IS review and testing. This validation establishes the recovery time capability and provides gap analysis for business driven RTOs and RPOs. Finally, integrated recovery exercises, such as tabletop or walkthrough exercises, at the Arlington Regional Data Center (ARDC) hot site that would address full recovery of all critical systems supported by the Data Hall have not yet been conducted. Without regular testing of Disaster Recovery plans and alignment to a completed BIA, the time and resources required to fully recover from a disaster cannot reliably be determined and the Medical Center is at risk of not being able to resume operations at the ARDC in the event the Data Hall is not functional. This issue was previously noted in audit 11:21 - TAC 202 Compliance issued March 11, 2011.

Recommendations

IS should continue with the efforts that have been established over the last few months and plan to implement the following key activities:

- Continue to work closely with Business Continuity in their update of policies and standards to ensure that they:
    - Guide Business Continuity planning efforts;
    - Establish the process for the escalation of business process impacting events;
    - Define the roles and responsibilities for identifying and recovering business processes;
    - Define communication pathways between Business Continuity, Disaster Recovery, Information Resources (IR) and the effected Business Process owners; and,
    - Ensure Business Continuity plans are developed only after a BIA and recovery strategies (procedures, interdependencies, resources, contact information and considerations to resume business functions) have been respectively performed and identified.

- IS should continue to work closely with Business Continuity to establish a consolidated electronic system (eBRP) to perform the Business Owner survey and utilize this information to map business processes to the required technology components.

- Criticality of systems should be mapped to IT resources to establish institutional criticality and resiliency needs. This should ultimately result in the development of a formalized BIA.

- Once a BIA has been completed, IS should reconcile the already developed Disaster Recovery plans with the BIA to ensure that business requirements during a disaster and/or business disruption and the current institution's IS capability are still appropriate. In addition, a specific disaster recovery plan governing failover processes of critical systems, with appropriate roles and responsibilities, event escalation pathways and communication channels to impacted users should be completed.

- IS should continue to work with critical IT system owners to conform existing disaster recovery plans to the institutional requirements and validate plans through testing. Progressive testing should be done collectively by Business Continuity Plan Owners along with any senior leaders, business unit managers, and/or vendors. Types of exercises include Tabletop, Functional and Full-Scale.

Within these key activities, points of focus around enhancing the maturity of Business Continuity Planning should include:

Disaster Recovery Plan Development

- Outline assumptions or plan limitations, including but not limited to which skill sets are needed to execute specific tasks, or the contingencies for when key individuals or skills are unavailable;
- Criteria for triage considerations and plan activation should be identified;
- Related dependencies (e.g., personnel, technology, business units) and interrelationships required to execute specific tasks should be included within the plans;
- Identification of which skill sets are needed to execute specific tasks and include contingencies for when key individuals or skills are unavailable;
- Validation tasks and criteria for successful activation of technology should be in place to confirm that systems are fully ready to support the business; and,
- Fail-back criteria and procedures for DR testing.

Disaster Recovery Plan Testing

- Detailed guidelines for test facilitators to conduct tests, report observations, and track follow up activities.
- Proof of successful test completion in achieving success criteria provided by business units.
- Identification of key deficiencies.
- After action reports and corrective actions to be taken with due dates.
- Required changes in resources to support plan activation.
- The quality of the performance and support of vendors or technology service providers.
- Participation and support of technology service providers.

Management Response

Management has agreed to implement the recommendations made.

Responsible Personnel: Joshua Spencer, Chief Information Security Officer

Due Date:

- All critical systems will have plans validated and tested by March 1, 2014.
- Integrated testing (tabletop) for the Data Hall Recovery Plan will be performed by June 1, 2014.
- Contingent on completion of Business Continuity department surveys within eBRP by April 2014 and financial resources available, IR will then need to address any gaps identified from the BIA, conduct testing and validate system priorities and interdependences. Due to the limited resources available to support the new Clements University Hospital conversion in November 2014, the action plan will be completed by June 1, 2015.

Sincerely,

Valla Wilson, Assistant Vice President for Internal Audit

Audit Team:
Kamal Patel, PwC Internal Audit Services
George Galindo, PwC IT Internal Audit Services
Debbie McKibben, PwC Internal Audit Services
Jeffrey Kromer, UTSW Internal Audit

cc: Arnim E. Dontes, MBA, Executive Vice President for Business Affairs
Joshua Spencer, CPHIMS, CISSP, Chief Information Security Officer
Sylvia Revell, Associate Director, Environmental Health & Safety