UT HEALTH NORTHEAST

Office of Internal Audit

March 16, 2017

Dr. Kirk Calhoun, President
UT Health Northeast
11937 U. S. Hwy 271
Tyler, TX 75708

Dr. Calhoun:

We have completed the Review for Compliance with Texas Administrative Code (TAC) 202 Security Control Standards as part of our FY 2017 Audit Plan. The objective of the review was to determine the institution's compliance with information security control standards promulgated by the Texas Department of Information Resources in the Security Control Standards Catalog as required by TAC § 202.76 (c). The scope of the review included the time period of September 1, 2015 through January 19, 2017. Based upon results of a risk assessment, the review was focused on access controls and configuration management which were deemed to be higher areas of risk for the institution. Access and configuration management controls reviewed included those with implementation dates effective February 2015 and February 2016.

This review was conducted in accordance with guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing.* We appreciate the assistance provided by management and other personnel and hope the information presented in our report is helpful.

Sincerely,

Gail Lewis

Gail Lewis
Interim Director, Chief Audit Executive

Enclosure
cc:
Mr. Joe Woelkers, Executive Vice President, Chief Operating Officer joe.woelkers@uthct.edu
Ms. Kris Kavasch, Vice President, Chief Financial Officer kris.kavasch@uthct.edu
Mr. John Yoder, Vice President, Chief Information Officer john.yoder@uthct.edu
Ms. Donna Martin, Executive Director of Compliance donna.martin@uthct.edu
Mr. Paul Modisette, Information Security Officer paul.modisette@uthct.edu
Mr. Jeremy Blankenship, IT Infrastructure Manager jeremy.blankenship@uthct.edu
Dr. Raymond S. Greenberg, UT System Executive Vice Chancellor for Health Affairs rgreenberg@utsystem.edu
Mr. J. Michael Peppers, UT System Chief Audit Executive systemauditoffice@utsystem.edu
Mr. Richard St. Onge, UT System Associate Vice Chancellor for Shared Services richardstonge@utsystem.edu
Ms. Dyan Hudson, UT System Director of Specialty Audit Services dhudson@utsystem.edu
Legislative Budget Board – audit@lbb.state.tx.us
Governor – budgetandpolicyreports@gov.texas.gov
State Auditor's Office - iacoordinator@sao.texas.gov
Sunset Advisory Commission - sunset@sunset.texas.gov

Review for Compliance with Texas Administrative Code (TAC) 202 Security Control Standards FY 2017

March 16, 2017

UT HEALTH NORTHEAST
OFFICE OF INTERNAL AUDIT
11937 US HIGHWAY 271
TYLER, TX 75708

TABLE OF CONTENTS

UT Health Northeast
Review for Compliance with Texas Administrative Code (TAC) 202
Security Control Standards
FY 2017

Report

Background

The Texas Administrative Code (TAC) is a compilation of all state agency rules in Texas. The portion of the code that is applicable to UT Health Northeast for the purpose of this review is Title 1, Part 10, Chapter 202, and Subchapter C. The Texas Department of Information Resources (DIR) issued the Security Control Standards Catalog that outlines mandatory and minimum requirements for information security controls to be implemented by all state agencies. To minimize the impact to state agencies, the DIR will phase in security control standard requirements over three (3) years to be effective on February: 2015, 2016 and 2017. TAC 202 requires an independent review at least every two (2) years to ensure that all Texas institutions, including UT Health Northeast, are in compliance. Due to the unique complexities of reviewing information technology (IT), assistance was provided by the UT System Director of Specialty Audit Services.

Objective

The objective of the review was to determine compliance with information security control standards promulgated by the Texas Department of Information Resources in the Security Control Standards Catalog as required by TAC 202 rule § 202.76 (c).

Scope and Methodology

This review covered the period of September 1, 2015 through January 19, 2017. To focus the review on security controls deemed to be higher risk for the institution, Internal Audit collaborated with the Information Security Officer and Information Technology Management to assess the institution's control risks. Based upon the results of this assessment, our work focused on access and configuration management controls that were required by the (DIR) Security Controls Standards Catalog to be in place by February 2015 or February 2016 as follows:

Access Controls	**Configuration Management**
AC-1 Access Control Policy and Procedures	CM-1 CM Policy and Procedures
AC-2 Account Management	CM-2 Baseline Configuration
AC-3 Access Enforcement	CM-4 Security Impact Analysis
AC-5 Separation of Duties	CM-6 Configuration Settings
AC-8 System Use Notification	CM-7 Least Functionality
AC-17 Remote Access	CM-8 IS Component Inventory
AC-18 Wireless Access	CM-11 User-Installed Software
AC-19 Access Control for Mobile Devices	
AC-20 Use of External Information Systems	

The procedures performed to determine compliance with control standards set by the DIR included:

- Survey and interview of responsible Information Security and IT employees;
- Review of applicable policies, procedures and documentation; and
- Limited testing where appropriate.

This review was conducted in accordance with guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing.*

UT Health Northeast
Review for Compliance with Texas Administrative Code (TAC) 202
Security Control Standards
FY 2017

Results/Conclusion

UT Health Northeast generally complies with Texas Administrative Code § 202.76 (c), state and federal guidelines, and UT System and UT Health Northeast policies and procedures relative to Information Technology security. Although the institution generally complies with the guidelines and applicable policies and procedures, the following opportunities for improvement were identified:

Control Standard	Recommendations
AC-2 Account Management CM-11 User-Installed Software	The VP, Chief Information Officer should: • Implement procedures to ensure that IT Security Forms consistently include all required electronic signatures and information before the IT team grants access to systems and information. • Implement procedures for ensuring that IT Security Forms completed for IT employees' access include details of the specific administrative/special access authorized. • Implement procedures to ensure the authorization for administrative rights to workstations is documented according to policy prior to granting this access. In addition, processes must be implemented for periodically monitoring administrative access to workstations and systems. Risk Rating: Low
CM-1 CM Policy and Procedures	The VP, Chief Information Officer should implement procedures for adopting and documenting minimum security configuration standards for all critical systems and infrastructure. Risk Rating: Medium
CM-2 Baseline Configuration	The VP, Chief Information Officer should implement procedures for documenting the baseline security configurations, deviations from the baseline and any subsequent changes made to security configurations for critical systems and infrastructure. Risk Rating: Low
CM-4 Security Impact Analysis	The VP, Chief Information Officer should implement procedures for documenting the results of the security impact analysis and approval of the Information Security Officer for significant changes to critical systems that could affect security. Risk Rating: Low

Management's Response: The Vice President, Chief Information Officer concurs with the recommendations and will begin to implement processes for resolving the six (6) issues identified.

Implementation Dates: Partial implementation by August 31, 2017 and full implementation by December 31, 2017.

According to the University of Texas System Audit Office, "A Priority Finding is defined as an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole. Standard factors for determining a Priority Finding have been established in three categories: namely, Organizational Controls, Quantitative Risks, and Qualitative Risks". Priority Findings are reported to the UT System Audit, Compliance and Management Review Committee. There were no priority findings identified during this review.

Gail Lewis

_____

Gail Lewis
Interim Director, Chief Audit Executive