19-202 Texas Administrative Code 202

We have completed our audit of compliance with Texas Administrative Code 202 requirements. This audit is required by Texas Administrative Code 202 and is part of our fiscal year (FY) 2019 audit plan. The audit was performed in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

BACKGROUND

The Texas Administrative Code is a compilation of all Texas state agency rules, with a total of 16 titles. Title 1 Part 10, Chapter 202, Subchapter C (TAC 202) encompasses six sections and includes a Security Control Standards Catalog (Catalog), which was initiated by the Texas Department of Information Resources to assist state agencies and higher education institutions in implementing security controls. The Catalog contains a total of 282 control standards, 155 of which have no required date and are optional. The remaining 127 control standards are required to be implemented.

OBJECTIVES

The objective of this audit was to determine compliance with selected requirements of TAC 202 Information Security Standards.

SCOPE PERIOD

The scope period was February 28, 2017 to November 14, 2018.

METHODOLOGY

Procedures were performed to obtain evidence of compliance with 66 of the 127 (52%) control standards as required by TAC 202, which included the following areas:

- Access
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authorization
- Incident Response
- Maintenance
- Security Assessment and Authorization

The remaining 61 control standards will be audited for compliance in FY 2020, which ensures full TAC 202 coverage on a rolling 2-year timeframe.

713.500.3160 phone
P.O. Box 20036
Houston, Texas 77225
www.uth.edu

AUDIT RESULTS
A&AS identified the following area of improvement:

- There is no guidance document governing administrative/privileged user access currently in place for higher risk applications at UTHealth.

NUMBER OF PRIORITY FINDINGS REPORTED TO UT SYSTEM
None

We would like to thank the staff and management within the IT and IT Security departments who assisted us during our review.

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

MAPPING TO FY 2019 RISK ASSESSMENT

Risk (Rating)	Not applicable.

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Assistant Vice President	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook B. Syers, CPA, CIA, CISA, CFE
Auditor Assigned	Lieu Tran, CISA
End of Fieldwork Date	December 12, 2018
Issue Date	December 20, 2018

Copies to:
Audit Committee
Richard Miller
Kevin Granhold
Amar Yousif
Tammy Gardiner

Issue #1	TAC 202 Control Standard AC-2 requires defined policies and procedures to be in place for creating, modifying, disabling, and removing user accounts in the information system. Information systems include both infrastructure assets (hardware, software, networks, facilities, etc.) and applications. In response to a previous audit finding, an access policy and procedure (for administrative/privileged users) is currently being developed for infrastructure assets; however, A&AS noted no equivalent policy and procedure in place for applications at UTHealth.
Recommendation #1	We recommend a guidance document governing administrative/privileged user access be developed and implemented for higher risk applications at UTHealth.
Rating	Medium
Management Response	We agree with the recommendation and will develop and implement a guidance document governing administrative/privileged user access for higher risk applications at UTHealth.
Responsible Party	Rick Miller, Vice President and Chief Information Officer
Implementation Date	March 1, 2019