UTHealth®
The University of Texas
Health Science Center at Houston

Office of Auditing & Advisory Services

June 17, 2015

To: Giuseppe N. Colasurdo, M.D.
President

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

Report on Compliance with Texas Administrative Code 202 Audit #15-202

We have completed our audit of compliance with Texas Administrative Code 202 requirements. This bi-annual audit is required by Texas Administrative Code 202 and part of our fiscal year (FY) 2015 audit plan. This audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

BACKGROUND

In 1977, the Texas Administrative Code was created by the Texas Legislature under the Administrative Code Act and is a compilation of all Texas state agency rules, with a total of 16 titles. Each title represents a subject category and related agencies are assigned to an appropriate title. Title 1, Part 10, Chapter 202, Subchapter C (TAC 202) encompasses six sections and includes a baseline of information security standards for institutions of higher education.

Recently, a committee of state Information Security Officers and others revised TAC 202 to align it more closely to the standards held by the Federal nformation Security Management Act (FISMA) and the National Institute of Standards and Technology (NIST). The current TAC 202 became effective March 17, 2015 and introduced several changes, including more detailed standards, the re-categorization of rules, and a new Security Control Standards Catalog (Catalog), which was initiated by the Texas Department of nformation Resources to assist state agencies and higher education institutions in implementing security controls.

TAC 202.70-202.75 documents the responsibilities of information security staff members, the institution's information security program, risk management standards, and incident reporting structures. Applicable sections of TAC 202.76 allow for more stringent standards to be established if deemed necessary.

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 assigned the following priorities and required implementation dates:

Count	Legacy or New Control Standard	Priority (P1=highest)	Required Implementation Date
39	Control standards included in legacy TAC 202	P1	February 2015
64	New control standards	P1	February 2016
24	New control standards	P2/P3	February 2017

OBJECTIVES

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

SCOPE AND METHODOLOGY

Through a review of policies and procedures, interviews with IT and IT Security personnel, and testing of supporting documentation, Auditing and Advisory Services (A&AS) audited compliance with TAC 202 requirements, including the 39 control standards required to be implemented by February 2015.

AUDIT RESULTS

A&AS noted that UTHealth is currently in the process of updating HOOP policies and procedures to comply with certain requirements within TAC 202.70-202.75. Depending on the extent of the updates, this initiative could take months to complete. A&AS will verify that the necessary updates to HOOP policies and procedures were adequately addressed during the FY 2016 audit, which will also include the 64 new control standards required to be implemented in February 2016.

Information Security Roles and Responsibilities

TAC 202 contains various requirements around information security roles and responsibilities, including:

- Reporting structure and duties of the Chief Information Security Officer (CISO)
- Exceptions to the information security requirements
- Distinctions between owners, custodians, and users

A&AS reviewed UTS 165, *Information Resources Use and Security Policy* (UTS 165), and HOOP 175, *Roles and Responsibilities for University Information Resources and University Data* (HOOP 175), and verified that all requirements were appropriately documented in the respective policies. No exceptions were noted.

Information Security Standards

TAC 202 contains numerous requirements around information security standards, including:

- Developing, creating awareness of, and assigning responsibility around an information security program
- Exceptions to the information security program
- Authentication policies and procedures

- Reporting the adequacy and effectiveness of security controls
- Capital budget plans
- Addressing the risk of denial of service attacks
- Firewall and intrusion-prevention systems

A&AS obtained HOOP 175, UTS 165, and ITPOL-004, *Access Control Policy* (ITPOL-004), and verified that the respective TAC 202 requirements were addressed. We also obtained the information security annual report, security awareness documents, and the FY 2015 budget plan to verify compliance with the associated TAC 202 requirements. An interview was conducted with the CISO to review and assess the effectiveness of the process to reduce the risk of denial of service attacks. Additionally, we obtained evidence of security awareness techniques and the use of firewall/intrusion-prevention systems to verify compliance with the corresponding TAC 202 requirements. No exceptions were noted.

Information Security Incidents Standards

TAC 202 contains several requirements around information security incidents (a phishing email, for example), including:

- Quick and effective incident response
- Incident reporting hierarchy
- Incident monitoring techniques

A&AS obtained HOOP 175 and ITPOL-017, *Computer Security Incident Response Policy*, and verified that all requirements were documented and addressed. We also obtained a sample of security incident reports and verified that there was a sufficient resolution. No exceptions were noted.

Logical Access Standards

TAC 202 contains two requirements around logical access standards:

- The installation of software is either not allowed, or limited based on access privileges
- Organized information systems should display an accepted system use notification message or banner before granting access to the information system

A&AS obtained UTS 165 and ITPOL-004 and verified that all requirements were appropriately documented in the policies. A&AS also obtained screenshots of log on banners and verified that an acceptable use notification is displayed before granting the user access. No exceptions were noted.

Media Protection Standards

TAC 202 requires the implementation of procedures to dispose of media containing departmental data in a manner that adequately protects confidentiality and renders it unrecoverable.

A&AS obtained ITSOP-015, *Medical and Scientific Device Standard Operating Procedure*, and verified that the requirement was appropriately documented in the procedure. A&AS will review and assess the effectiveness of the medical device disposal process during another audit in FY 2016. No exceptions were noted.

Risk Management Standards

TAC 202 includes several requirements around risk management, specifically:

- A documented data classification policy
- Policies supporting information security related risk assessments
- Approval of security risk acceptance, transference, or mitigation decisions

A&AS obtained HOOP 175, UTS 165, and ITPOL-029, *Data Classification Policy*, and verified that the associated requirements were documented. We also interviewed the IT Risk and Compliance Manager on the risk assessment process, obtained the FY 2014 risk assessment (most recent), and verified that the process is compliant with TAC 202. No exceptions were noted.

Systems Development Lifecycle Standards

TAC 202 requires that the existing systems development lifecycle includes the consideration of information security.

A&AS obtained ITSOP-004, *Software Development Lifecycle Procedure*, and ITGD-004, *System Development Methodology*, and verified that the requirement was appropriately documented in the policies and procedures. No exceptions were noted.

CONCLUSION

In our opinion, UTHealth complies with the selected requirements of TAC 202 Information Security Standards.

We would like to thank the IT and IT Security departments, and the individuals throughout the institution who assisted us during our review.

DGS:tt

cc: Audit Committee
Michael Tramonte
Rick Miller
Amar Yousif

Audit Manager:	Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned:	Tammy Tran

Issue Date: June 29, 2015