UTHealth
The University of Texas
Health Science Center at Houston

Office of Auditing & Advisory Services

20-202 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) 2020 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 November 14, 2018 to January 15, 2020.

METHODOLOGY

A total of 66 control standards were included in the scope of the FY19 audit. The remaining 61 controls are included in scope of this audit and procedures were performed to obtain evidence of compliance in the following areas:

- Information security program management
- Media protection
- Personnel security
- Physical and environmental protection
- Planning
- Risk assessment
- System and communication protection
- System and information integrity
- Systems and services acquisition

AUDIT RESULTS

A&AS identified the following area of improvement:

- Data center policies and procedures do not address certain physical and environmental protection standards.
- IT and IT Security have not documented and disseminated a formal risk assessment procedure.

- A number of IT policies have not been reviewed and updated since 2017.

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
Associate Vice President & Chief Audit Officer

MAPPING TO FY 2020 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	January 29, 2020
Issue Date	February 4, 2020

Copies to:
Audit Committee
Amar Yousif
Derek Drawhorn
Beverly Moore
Tammy Gardiner

Issue #1	Physical and Environmental Protection Policies & Procedures Control Standard PE-1 (PE-1) under TAC 202 states: “The organization: a. Develops, documents, and disseminates: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.” Currently, data center policies and procedures do not address emergency lighting and exits, evacuation routes, fire detection and prevention, water leaks, training, and other related security controls.
Recommendation #1	We recommend data center policies and procedures be updated to address emergency lighting and exits, evacuation routes, fire detection and prevention, water leaks, training, and other related security controls.
Rating	Medium
Management Response	We will modify data center policies and procedures to address emergency lighting and exits, evacuation routes, fire detection and prevention, water leaks, training, and other related security controls.
Responsible Party	Derek Drawhorn, Associate Vice President of IT Infrastructure
Implementation Date	May 29, 2020

Issue #2	Risk Assessment Controls Standard RA-1 (RA-1) under TAC-202 states: "The organization must develop, document, and disseminate: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls." HOOP 175 *Roles and Responsibilities for University Information Resources and University Data* requires the Chief Information Officer to "perform an annual risk assessment for University Information Resources." While yearly risk assessments are conducted by IT and IT Security, no formal risk assessment procedure has been documented and disseminated per RA-1.
Recommendation #2	We recommend a formal risk assessment procedure (or relevant guidance) be documented and disseminated.
Rating	Medium
Management Response	We will document and disseminate a formal risk assessment guidance document.
Responsible Party	Amar Yousif, Vice President and Chief Information Officer Beverly Moore, Chief Information Security Office, *ad interim*
Implementation Date	May 31, 2020

Issue #3	Various control standards under TAC-202 require the periodic review and updating of IT policies and procedures. Section 5.2.1 of *IT Policy and Standard Operating Procedures (SOP) Approval Process* (ITSOP-001) states: "IT Risk Management & Compliance Manager reviews policies/SOPs biennially, subsets are reviewed annually, or otherwise as changes occur, and sends an email to appropriate Review Groups to notify them the policies/SOPs are ready for review and the date of the meeting in which the policies/SOPs will be discussed (or the due date for submission of comments if no meeting)." A&AS noted the following policies have not been reviewed/updated since 2017: • *Host Configuration Policy* (ITPOL-006) • *Disk Encryption Policy* (ITPOL-032) • *Domain Name System* (DNS) Policy (ITPOL-042) • *Data Backup Policy* (ITPOL-043)
Recommendation #3	We recommend the referenced policies be reviewed and updated.
Rating	Low
Management Response	We have reviewed and updated the referenced policies. (Verified by A&AS)
Responsible Party	Amar Yousif, Vice President and Chief Information Officer
Implementation Date	January 30, 2020