UTHealth
The University of Texas
Health Science Center at Houston

16-202 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 part of our fiscal year (FY) 2016 audit plan. This audit was conducted 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, 64 of which have a required implementation by February of 2016.

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 1, 2016 – April 30, 2016.

METHODOLOGY

The following procedures were performed:

- Verified policies and procedures exist and are reviewed on a regular basis for the following: system and communications protection, security assessment and authorization, risk assessments, audit and accountability, system and services acquisition, personnel security, system maintenance, media protection, system and information integrity, baseline configuration settings, remote access authorization, firewall configuration, and cryptographic key management.
- Reviewed server and desktop operating systems for process isolation support. Domain name system (DNS) servers were reviewed for fault tolerance, authentication, and provision of artifacts and authoritative data.
- Obtained the FY2016 IT Risk Assessment and verified that it is developed, maintained, and that corrective actions have been planned and reviewed to mitigate risks. A&AS also verified that vulnerability scans are performed at least annually.
- Verified the information systems inventory and system flaw repository are updated and tracked on a regular basis. A&AS also obtained the 2016 Information Technology Security Annual Report to the President and verified that results of information security performance measures are reported.

713.500.3160 phone 713.500.3170 fax
P.O. Box 20036
Houston, Texas 77225
www.uthouston.edu

- Verified information security resources are allocated in the FY2016 IT Capital Budget.
- Obtained evidence of appropriate employee training and dissemination of security alerts.
- Reviewed documentation and implementation of configuration settings.

AUDIT RESULTS

A&AS identified areas of improvement related to the DNS server requirements:

- The DNS servers are not currently in compliance with the relevant TAC 202 requirements.

NUMBER OF PRIORITY & HIGH 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 2016 RISK ASSESSMENT

Risk (Rating)	R.64 Internal policies are not updated to be in compliance with the new TAC 202 (High)

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Assistant Vice President	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned	Tammy Tran
End of Fieldwork Date	July 27, 2016
Issue Date	August 12, 2016

Copies to:
Audit Committee
Michael Tramonte
Rick Miller
Kevin Granhold
Amar Yousif
Tammy Gardiner

Issue #1	Control Standard SC-20 and SC-21 in the TAC 202 Control Standards Catalog state that the DNS servers must provide "additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries" and perform "data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems." Management informed us the DNS servers do not currently meet Control Standards SC-20 and SC-21; however, a project is currently underway to ensure compliance in the near future.
Recommendation #1	We recommend the progress of the project be assessed and a timeline developed to facilitate tracking and ensure timely completion.
Rating	Medium
Management Response	After assessing the progress of the project, we have concluded that a new set of servers will need to be placed into production along with clean-up, testing, and splitting the DNS zones prior to addressing the Control Standards SC-20 and SC-21. Due to the complexity and time required for these items, we have determined that we will comply with Control Standards SC-20 and SC-21 by February 28, 2017.
Responsible Party	Kevin Granhold
Implementation Date	February 28, 2017