INTERNAL AUDIT
UT HEALTH SCIENCE CENTER®
SAN ANTONIO

AUDIT REPORT

TO: Michael Schnabel, Senior Director, Information Security and Operations and Chief Information Security Officer

FROM: Angela D'Anna, Chief Audit Executive, Internal Audit and Consulting Services

DATE: May 31, 2016

SUBJECT: Texas Administrative Code 202 Security Assessment (16-24)

EXECUTIVE SUMMARY

Internal Audit and Consulting Services has reviewed compliance with Texas Administrative Code 202 (TAC 202) *Information Security Standards* at The University of Texas Health Science Center at San Antonio. TAC 202 Rule §202.76 requires that a review of compliance with specified control standards be performed at least biennially based on business risk management decisions and by individual(s) independent of the information security program. The primary objectives of this review were to: (1) meet the requirements for review by the institution (2) assess the design of the institutional information security program against baseline requirements specified in the TAC 202 *Security Control Standards Catalog* and (3) validate a risk-based sample of control groups. The control groups selected for validation were: (1) Configuration Management (2) System and Services Acquisition and (3) System and Communications Protection.

In general, information security program procedures and processes were implemented and operating as intended to ensure compliance with the TAC 202 *Security Control Standards Catalog* for the three control groups selected for review. However, certain policies related to System and Services Acquisition and to System and Communications Protection were not in writing and included in the Handbook of Operating Procedures.

This audit identified no issues considered priority to the institution. The audit issue was ranked according to the University of Texas System Administration audit issue ranking guidelines. Please see the Appendix for ranking definitions. Attached is the detailed report.

DETAILED AUDIT REPORT

PURPOSE AND SCOPE

Internal Audit and Consulting Services has reviewed compliance with Texas Administrative Code 202 (TAC 202) *Information Security Standards* at The University of Texas Health Science Center at San Antonio (Health Science Center). TAC 202 Rule §202.76 requires that a review of compliance with specified control standards be performed at least biennially based on business risk management decisions and by individual(s) independent of the information security program. This assessment was intended to meet that requirement for the Health Science Center.

We assessed the design of the institutional information security program against baseline requirements specified in the TAC 202 *Security Control Standards Catalog* (Control Catalog). Based on an assessment of risk, we selected the following control groups for validation: Configuration Management, System and Services Acquisition, and System and Communications Protection. For the selected control groups, we reviewed the 24 control standards associated with these control groups. The primary objectives of the review were to:

- Determine whether policies, procedures, and processes were in place for the 24 standards.
- Evaluate supporting documentation of the associated systems and processes.
- Ascertain whether the institution implemented the associated control requirements.

BACKGROUND

In March 2015, the Texas Department of Information Resources (DIR) issued the Control Catalog to comply with the new TAC 202 Rule §202.76 requirements to specify mandatory and minimum requirements for information security controls that State organizations must utilize to provide the appropriate levels of information security based on risk. DIR is authorized by the Information Resources Management Act Chapter 2054 of the Texas Government Code to coordinate and direct the use of information resources technologies by all State agencies.

The new TAC 202 structure facilitated by the Control Catalog utilizes SP 800-53[1] nomenclature, provides specific control practices and streamlines the modification process to more accurately reflect legislative actions. To minimize the impact to State organizations, the DIR phased in security control standard requirements over three years to be effective February 2015, February 2016 and February 2017. Security requirements effective February 2015 included legacy TAC 202 control standards.

RESULTS

In general, information security program procedures and processes were implemented and operating as intended to ensure compliance with the TAC 202 Control Catalog for the three control groups selected for review. However, certain policies related to System and Services Acquisition and to System and Communications Protection were excluded from the Handbook of Operating Procedures.

Attached is the recommendation, management action plan, responsible party, and anticipated completion date. The audit issue was ranked according to the University of Texas System Administration Audit Issue Ranking guidelines. Please see the appendix for ranking definitions. This matter is offered for management's consideration in the spirit of continuously improving processes and reducing risks in the organization.

* * * * * *

[1] The National Institute of Standards and Technology developed Special Publication (SP) 800-53 to further its statutory responsibilities under the Federal Information Security Management Act to develop standards that provide minimum information security requirements and that are otherwise necessary to improve the security of federal information and information systems.

This audit was performed by Esther Villarreal, Intermediate Internal Auditor and assistance was provided by the IT Audit Program Manager at the UT System Audit Office due to the unique complexities of auditing information technology. This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* as promulgated by the Institute of Internal Auditors.

cc: Michael E. Black, Senior Executive Vice President and Chief Operating Officer
Yeman Collier, Vice President and Chief Information Officer
William L. Henrich, M.D., President
Andrea Marks, Vice President and Chief Financial Officer

Information Security Policies and Procedures

Opportunity for Improvement:

Audit Issue Ranking – *Medium*

Our review revealed that information security program policies found in the Handbook of Operating Procedures (HOP) did not include the following:

- **System and Services Acquisition:** A written policy did not exist specifying the security requirements for computing devices (e.g., laptops and desktops) purchased by departments. Security standard SA-1 *System and Services Acquisition Policy and Procedures* states that security requirements shall be identified, documented and addressed in all phases of development or acquisition of information resources.

- **System and Communications Protection:** We noted that use of certain third party cloud services was approved by the Information Security Office; however, a security policy pertaining to the requirements for using cloud services did not exist. Security standard SC-8 *Transmission Confidentiality and Integrity* requires certain controls to be in place when confidential information is transmitted over a public network (e.g., the Internet), which occurs in cloud services.

  Additionally, the process to create and manage digital certificates was not documented in a policy. Security standard SC-12 *Cryptographic Key Establishment and Management* requires that the organization establish and manage cryptographic keys in accordance with the organizationally-defined requirements for key generation, distribution, storage, access and destruction.

  Furthermore, a HOP policy did not exist regarding the use of networked microphones, cameras, whiteboards, etc. Security standard SC-15 *Collaborative Computing Devices* prohibits remote activation of collaborative computing devices, except as permitted by the organization. Moreover, it requires an explicit indication of use to the local users.

Recommendation:

To help ensure compliance with Texas Administrative Code 202, HOP policies should be strengthened to include information security policies and procedures related to:

- Computing devices purchased by departments
- Cloud services
- Digital certificates
- Collaborative computing devices

Management's Action Plan:

Responsible Party:	Michael Schnabel
Estimated Completion Date(s):	July 2016

The Handbook of Operating Procedures will be updated and communicated per the report's recommendations and as outlined in the TAC 202 *Security Control Standards Catalog* by July 31, 2016.

Appendix - Audit Issue Ranking Definitions

The audit issue was ranked according to the following University of Texas System Administration audit issue ranking guidelines:

- ***Priority*** – A Priority Finding is defined as an issue identified by internal audit that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of the Health Science Center or the UT System as a whole.

- ***High*** – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the Health Science Center either as a whole or to a significant college/school/unit level.

- ***Medium*** – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the Health Science Center either as a whole or to a college/ school/unit level.

- ***Low*** – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the Health Science Center either as a whole or to a college/ school/unit level.