The University of Texas at Tyler

Audit of Compliance with Texas Administrative Code 202

August 2015

OFFICE OF AUDIT AND CONSULTING SERVICES
3900 UNIVERSITY BOULEVARD
TYLER, TEXAS 75799

The University of Texas at Tyler
Texas Administrative Code 202 Audit
Fiscal Year 2015

BACKGROUND

Texas Administrative Code (TAC) Title 1, Part 10, Chapter 202, outlines mandatory information security controls to be implemented by all State agencies and institutions of higher education. Rule §202.76 further requires that a review for compliance with specified control standards "be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program." This audit is intended to meet that requirement for The University of Texas at Tyler (UT Tyler). Due to the unique complexities of auditing information technology (IT), assistance was provided by the Assistant Director of Specialty Audit Services at University of Texas System (UT System) Audit Office.

AUDIT OBJECTIVE

The objective of this audit was to determine compliance with the Texas Department of Information Resources (DIR) *Security Control Standards Catalog*,[1] as required by TAC 202 rule §202.76(c).

STANDARDS

The audit was conducted in accordance with guidelines set forth in *The Institute of Internal Auditors' Standards for the Professional Practice of Internal Auditing*.

SCOPE AND METHODOLOGY

The scope of the audit included current information security controls in place at UT Tyler. With the assistance of the UT Tyler Chief Information Security Officer, a risk assessment was conducted to identify those security control areas of highest risk for inclusion in audit testing. The specific areas selected included the following:

- Access Controls;
- Configuration Management;
- Contingency Planning;
- System and Communication Protection; and
- System and Information Integrity.

Procedures to determine compliance with control standards included the following:

- Survey and interview of responsible Information Security and IT employees;
- Review of available policy and procedure documentation;
- Walk-through of relevant facilities; and
- Limited testing where appropriate.

[1] http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Security%20Control%20Standards%20Catalog.pdf

AUDIT RESULTS

According to the University of Texas System Audit Office, "*A Priority Finding is defined as an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole. Standard factors for determining a Priority Finding have been established in three categories: namely, Organizational Controls, Quantitative Risks, and Qualitative Risks".* Priority Findings are reported to the UT System Audit, Compliance, and Management Review Committee. This audit resulted in 6 Reportable Findings, but no Priority Findings.

#1 Disaster Recovery Plan Not Tested

DIR Security Control Standard CP-4 requires that the disaster recovery plan be tested and corrective action taken if needed based on the results of the test. In Appendix B of the Disaster Recovery Plan dated March 2015, it indicates that two full-scale tests will be performed before the Plan is considered operational. A full-scale test has not occurred, and limited scale tests were conducted only in response to incidents that required activation of the plan.

> ***Recommendation:*** Limited-scale tests should be performed as required by DIR Security Control Standard CP-4 and UTS 165 Standard 6.2.
>
> ***Chief Information Officer Response and Implementation Date:*** Testing will be completed on a risk basis and the Disaster Recovery Plan will be amended to reflect that adjusted testing scope by March 31, 2016.

#2 Lack of User Account Review

UTS165 Standard 4.2 requires that user accounts be reviewed "at least quarterly," and Security Control Standard AC-2 also requires that accounts be reviewed for continued needs based on the employee's current position. Currently, TexSIS Campus Solutions user access is reviewed three times per year. UT Share user access is not reviewed.

> ***Recommendation:*** UT Share Human Resources (HR) and Finance user authorizations should be reviewed at least quarterly, or more often if warranted by risk, and disabled timely if determined to be unneeded.
>
> ***Chief Information Officer Response and Implementation Date:***
> This requires that management of the HR and the Budget and Financial Reporting departments review employee level access reports and notify IT if changes are needed. The UT System Audit Office has provided new UT Share query reports that UT Tyler did not previously have. UT Tyler IT staff will run the query reports on a quarterly basis. This procedure will be in place no later than December 31, 2015.

#3 Policy Restricting Access Points

DIR Security Control Standard AC-18 requires that State organizations "establish the requirements and security restrictions for installing or providing access to the state organization information resources systems" by establishing a wireless policy, and "prohibit and periodically monitor any unauthorized installation or use of Wireless Personal Area Networks on state organization IT systems by individuals without the approval of the state organization information resources manager." Although wireless routers are not allowed on the campus network according to the Acceptable Use Policy, there is no formal monitoring to detect this activity.

Recommendation: Monitoring should be performed to identify and remediate instances of noncompliance.

Chief Information Officer Response and Implementation Date: Formal monitoring is being developed. This should be completed by December 31, 2015.

#4 Configuration Standards, Change in Management Policies and Procedures

Security Control Standard CM-1 requires documented configuration management policy and procedures to control modifications to hardware and software, and UTS165 Standard 7 also requires a formal change management process and prescribes seven elements the process must include such as a formal request process, testing, assessment of potential impacts, and documentation and tracking of changes. Although a variety of informal documents and practices exist, no documented configuration standards or change management policies/procedures exist, and informal practices do not consistently comply with all required elements.

Recommendation: Configuration and change management policies and procedures should be developed for hardware, software, and network infrastructure, to comply with the elements required by CM-1 and UTS165 Standard 7.

Chief Information Officer Response and Implementation Date: ServiceNow (service management software) is currently being implemented and includes a Change Management module that will be configured to formalize and automate procedures. Policies and procedures will be developed by August 31, 2016.

#5 Network Penetration Testing

Security Control Standard SI-4 requires monitoring information resources (networks and systems) for "attacks and indicators of potential attacks." UTS165 Standard 17 further requires that "an annual, professionally administered and reported external network penetration test" be performed. The most recent external penetration test was performed in July 2011.

Recommendation: An external network penetration test should be conducted as soon as possible, and at least annually thereafter.

Director of Information Security Response and Implementation Date: Network penetration testing has been scheduled with UT System to be conducted on September 28, 2015, and funds will be requested in the budget to have it performed annually.

#6 Timely Notification of Change in Employment Status

UTS165 Standard 4.2 requires that access management procedures include provisions for "reviewing, removing and/or disabling accounts at least quarterly […] to reflect current User needs or changes of User role or employment status." Security Control Standard AC-2 requires that security administrators be notified when users are terminated or transferred. The PeopleSoft (PS) Access Control Analyst does not receive notification of other types of changes, such as interdepartmental transfers or termination of part-time or student employees. When a person is marked as terminated in PeopleSoft, the user domain account is automatically deactivated and UT Share access is disabled. Deactivation of the domain account prevents the ability to connect to TexSIS/Campus Solutions but access is not automatically deactivated. The terminated employees are deactivated in TexSIS by the PS Access Control Analyst when he is notified. Human Resources reportedly sends notices of termination developed from departmental records, but only for full-time benefits eligible employees. There is potential exposure for rehired employees who would automatically regain any PeopleSoft access when their domain account is reactivated. There is also potential exposure for transferred employees whose prior access had not been removed.

Recommendation: Human Resources should identify or develop PeopleSoft reports or queries to provide change in employment status information (new hires, terminations, or departmental transfers); and distribute such information timely to security administrators so access can be appropriately updated or terminated.

Director of Human Resources Response and Implementation Date: Human Resources will use payroll query reports to identify terminated and transferred employees and communicate these changes to NetWork Operations beginning October 31, 2015.

CONCLUSION

UT Tyler generally complies with Texas Administrative Code Section 202, state and federal guidelines, and UT System and UT Tyler policies and procedures related to Information Technology security, except as noted above. We have discussed the audit results with the appropriate personnel, and they have agreed to implement the recommendations. We appreciate the assistance the University of Texas System Audit Office and University of Texas at Tyler personnel provided during this engagement.