The University of Texas at Tyler

Audit of Compliance with Texas Administrative Code 202

August 2017

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 2017

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) as well as verify compliance with University of Texas System Policy 165, (UTS 165) Information Resource Use and Security Policy.

In 2015, the State of Texas' Department of Information Resources (DIR) started a three-year transition to align TAC 202 controls with the Federal Information Security Management Act (FISMA) and National Institute of Standards of Technology (NIST) 800-53 standards. The required TAC 202 controls are found in the DIR Security Control Standards Catalog. Each of the controls in the catalog is categorized by both the level of impact to information technology (IT) systems and implementation priority.

Due to the unique complexities of auditing IT controls, assistance was provided by the IT Audit Program Manager for Specialty Audit Services at the University of Texas System (UT System) Audit Office.

AUDIT OBJECTIVE

The objective of this audit was to determine UT Tyler's compliance with the DIR *Security Control Standards Catalog Version 1.3*,[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' *International 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. A risk assessment was conducted to identify security control areas of highest risk for inclusion in audit testing. The specific areas selected included the following:

- Assessment and Authorization Controls;
- Identification and Authentication;
- Planning; and
- System and Service Acquisition.

Procedures to determine compliance with control standards included the following:

- Review of available policy and procedure documentation;
- Completion of a control questionnaire by relevant IT staff;
- Interviews with responsible Information Security and IT employees; and
- Limited testing where appropriate.

1 TAC 202 Security Catalog: http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Security%20Control%20Standards%20Catalog.pdf

AUDIT RESULTS

According to the UT 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."* Non-Priority Findings are ranked as High, Medium, or Low, with the level of significance based on an assessment of applicable qualitative, operational control, and quantitative risk factors and probability of a negative outcome occurring if the risk is not adequately mitigated.

Priority Findings are reported to the UT System Audit, Compliance, and Risk Management Committee. This audit resulted in two High and five Medium-level findings, but no Priority Findings.

Finding Level Legend	
Priority	*A finding is defined as an issue that if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Tyler.*
High	*A finding that is considered to have a medium to high probability of adverse effects to UT Tyler as a whole or to a significant college or department.*
Medium	*A finding that is considered to have a low to medium probability of adverse effects to UT Tyler as a whole or to a college or department.*
Low	*A finding that is considered to have a minimal probability of adverse effects to UT Tyler as a whole or to a college or department.*

Audit Findings		
	Level	**Description of Finding**
1	High	*External service providers are not monitored for adequate internal controls.*
2	High	*Inadequate policies for secure management of university-wide authenticators for critical information systems.*
3	Medium	*No comprehensive IT equipment life cycle policy that considers security risks.*
4	Medium	*The Information Security Plan does not address specialized security requirements for critical systems.*
5	Medium	*Purchasing policy does not require approval of external services prior to storage and processing of university data.*
6	Medium	*Information Security Policy does not include procedures for addressing necessary security assessments of university owned information systems.*
7	Medium	*Acceptable Use Policy re-acknowledgement not adequate.*

#1 External Service Provider Security Compliance Review (High)

DIR Security Control Standard SA-9 and UTS 165, Section 22.7, requires organizations to employ processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis. UT Tyler relies on a third party service approved by UT System to deliver continuous monitoring of external providers; however, the reporting provided by the vendor is based primarily on publicly available technical risk data rather than evaluation of internal controls. As a result, there is an increased risk that external service providers do not have adequate controls to ensure unauthorized access, modification, or disclosure of university data by the external service provider.

Recommendation: The Information Security Office should obtain and review internal control compliance reports from external service providers at least annually, or more often, if warranted by risk.

Director of Information Security Response: Challenges in addressing this finding include:
o Obtaining a complete list of external service providers;
o Obtaining the correct contact information for the service providers; and
o Service providers who want an NDA signed in order to complete the risk assessment.

The Information Security Department will run annual risk assessments for external service providers using questionnaires generated in Archer in order to evaluate internal controls. By the implementation date, the Information Security Office will have a list of external providers, contact information for those providers, and documented occurrences when a service provider has requested an NDA be signed. It should be noted that not all will be completed by this date, but should be completed by the end of the 17/18 fiscal year.

Implementation Date: July 31, 2018

#2 Information System Authenticator Management (High)

An authenticator is an electronic password, digital certificate, or cryptographic keys or tokens used by a system in its process to grant access. Examples of authenticators include default administrative passwords, web server encryption keys, and digital certificates for signing electronic documents. Security Control Standard IA-5 requires establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, for revoking authenticators, and for protecting authenticator content from unauthorized disclosure and modification. Although informal practices exist, no formal policies or procedures are in place for the secure management of authenticators used in production information systems. Without secure management of university-wide authenticators, there is an increased risk of unauthorized access to information systems used in the processing, storage, or transmission of critical data.

Recommendation: Cross-organizational policies and procedures should be developed for the secure management of university-wide authenticators for critical information systems. The policies should include procedures for shared management of authenticators.

Vice President for Technology - Chief Information Officer and Director of Information Security Response: The Information Security Officer (ISO) will work with the Chief Information Officer and Executive Director of Enterprise Technology to craft policies and procedures that will allow for shared management of authenticators between Information Technology and Information Security.

Implementation Date: May 31, 2018

#3 System Life Cycle (Medium)

DIR Security Control Standard SA-4 requires organizations to manage information systems using a system development life cycle that incorporates information security considerations. Currently, a comprehensive life cycle policy does not exist. Without a well-defined system development life cycle, there is an increased risk of ineffective development, implementation, and operation of organizational information systems that considers information security risk and ensures compliance with applicable security policies and standards.

Recommendation: A campus-wide system development life cycle policy should be created and maintained that includes security considerations. The cycle should be dependent on the type and use of the equipment.

Chief Information Officer / Vice President for Technology Response: System refresh guidelines will be developed to ensure compliance with applicable security policies and standards to minimize risk to information security. The process will be amended to state that systems purchased that do not receive IT approval, are beyond economic repair, and/or that are too old to receive security updates, will be prohibited from connecting to the production network and will not receive IT support.

Implementation Date: March 31, 2018

#4 Information Security Plan (Medium)

DIR Security Control Standard PL-2 requires that organizational security plans include descriptions of operational information systems in terms of missions and business processes. Although an inventory of critical information systems exists from a technical standpoint, the Information Security Plan does not address specialized security requirements for critical systems in context of the missions of the university and its operational environment. When Information Security Plans do not contain descriptions of critical systems relating to business processes or mission, it may be difficult for management to determine the level of internal controls needed to mitigate risks to university individuals, operations, or assets.

Recommendation (4a): The information security plan should be updated to include critical information systems and descriptions of those systems within the context of organizational mission and business processes.

Executive Director of Enterprise Technology Response: IT will supply a list of critical systems to the CISO for review.

Implementation Date: July 31, 2018

Recommendation (4b): The Information Security department should review the plan for adequacy.

Director of Information Security Response: The Information Security Department will review the plan for adequacy once it has been submitted by the Executive Director of Enterprise Technology.

Implementation Date: August 31, 2018

#5 External IT Services Purchasing Policies (Medium)

Security Control Standard SA-1 and UTS 165, Section 1.7(d), requires establishing system and services acquisition policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with applicable information security requirements. UT Tyler's purchasing policies cover the acquisition of computer hardware; however, those policies do not include rules covering the acquisition and use of external services such as cloud storage, application, or communication providers. Without policies addressing the purchase of external services, users may store or process critical university data using external providers that do not meet security and policy requirements.

Recommendation: Purchasing polices should be updated to include procedures for approving external services (both paid and "free-to-use") prior to the storage or processing of university data.

Vice President for Technology - Chief Information Officer Response: See response to #3. IT will review current policy to include procedures for approving external services

Implementation Date: March 31, 2018

#6 Information Systems Security Assessments (Medium)

Security Control Standard CA-1 and UTS 165, Section 10.4, requires a security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Although UT Tyler's information security policy covers security assessments of external services, the policy does not include formal procedures addressing the purpose, scope, roles, and responsibilities for security assessments of university owned information systems. Without policies and procedures for security assessments, there is an increased risk that information systems will fail to meet confidentiality, integrity, and availability requirements found in university security policies.

Recommendation: The information security policy should be updated to include the purpose, scope, roles, and responsibilities relating to security assessments of university owned information systems.

Director of Information Security Response: The ISO will develop a policy and procedures relating to risk assessments performed by the Information Security Department.

Implementation Date: February 28, 2018

#7 Acceptable Use Policy Management (Medium)

Security Control Standard PL-4 requires individuals to sign an acknowledgement indicating that they have read, understand, and agree to abide by an Acceptable Use Policy (AUP) before authorizing access to information and the information system. Individuals are also required to re-acknowledge the AUP when changes occur. UT Tyler requires faculty, staff, and student workers to sign the AUP during employee orientation. All other students acknowledge the AUP as they access the system during each use. When updates to the AUP occur, an email is sent to all employees informing them of the changes and requesting their re-acknowledgement; however, there is not an automatic process to verify re-acknowledgement. Allowing users to access information resources without reading and signing an updated AUP may increase operational risk because these users may not know the university's rules of behavior with regard to the secure operation of electronic devices or the safe handling of critical data.

Recommendation: An automated process should be implemented requiring all users to sign the university's AUP annually or when updates are made throughout the year.

Director of Information Security Response: The Information Security Office will send an email to all employees notifying them when a change has been made to the AUP. The email will highlight the changes made in the AUP so that all employees are aware of the changes made. The banners for the domain and wireless logons will be modified to include the date the AUP was last changed.

Implementation Date: This change in procedure will go into effect the next time the AUP is modified.

CONCLUSION

UT Tyler generally complies with the TAC 202 control standards under review except as noted above. The Office of Audit and Consulting Services has discussed the audit results with appropriate personnel, and management has agreed to implement the recommendations. We appreciate the assistance the UT System Audit Office and UT Tyler personnel provided during this engagement.