UTTyler
THE UNIVERSITY OF TEXAS AT TYLER

Internal Audit Department

August 10, 2022

Dr. Kirk A. Calhoun
President
The University of Texas at Tyler
3900 University Blvd.
Tyler, TX 75799

Dr. Calhoun,

We have completed the Cloud Security Audit that was part of the University of Texas at Tyler's (UTT) Fiscal Year (FY) 2022 Audit Plan. The objective of the audit was to assess the security of cloud services used to process and store University data. This audit meets the biennial Texas Administrative Code (TAC) § 202.76 (c) risk-based review of compliance with Texas Information Security Standards. This audit included testing on the UTT Health Science Center (HSC) campus only. The scope of the audit was for FY 2022.

This audit was conducted in accordance with guidelines set forth in The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and Generally Accepted Government Auditing Standards. We appreciate the assistance provided by management and other personnel and hope the information presented in our report is helpful.

Sincerely,

Stephen Ford
Vice President, Chief Audit Executive

Enclosure
cc:
Dr. Julie Philley, EVP, Health Affairs, Vice Provost
Mr. Daniel Deslatte, Sr. VP, Business Affairs, Chief Operating Officer – Health Affairs
Mr. Carl Baranowski, VP, Chief Legal Officer
Mr. John Yoder, VP, Information Technology, Chief Information Officer – Health Affair
Mr. Bryce Dickey, Information Security Officer – Health Affairs
Mr. Paul Modisette, Information Security Analyst – Health Affairs
Dr. Archie Holmes, UT System Executive Vice Chancellor for Academic Affairs
Dr. John Zerwas, UT System Executive Vice Chancellor for Health Affairs
Mr. Patrick Francis, UT System Associate Vice Chancellor for Health Affairs
Mr. J. Michael Peppers, UT System Chief Audit Executive
Legislative Budget Board audit@lbb.texas.gov
Governor budgetandpolicyreports@gov.texas.gov
State Auditor's Office iacoordinator@sao.state.tx.us

Cloud Security Audit

UTTyler
THE UNIVERSITY OF TEXAS AT TYLER

August 10, 2022

INTERNAL AUDIT DEPARTMENT
3900 UNIVERSITY BOULEVARD
TYLER, TEXAS 75799

AUDIT OBJECTIVE

The objective of the audit was to assess the security of cloud services used to process and store University data. This audit meets the biennial Texas Administrative Code (TAC) § 202.76 (c) risk-based review of compliance with Texas Information Security Standards. This audit included testing on the University of Texas at Tyler (UTT) Health Science Center (HSC) campus only. Texas Administrative Code Chapter 202, Information Security Standards for Institutions of Higher Education, includes requirements related to cloud services, inventory of information systems, data security, and risk assessments.

CONCLUSION

The audit identified five (5) opportunities to strengthen controls associated with cloud services.

OBSERVATIONS

This audit identified the following opportunities for improvement:		
1	High	*Monitor Use of Cloud Services*
2	Medium	*Maintain a Comprehensive Inventory of Cloud Services*
3	Medium	*Ensure Completion and Documentation of Risk Assessments for Cloud Services*
4	Medium	*Update Information Resources Acceptable Use Policy*
5	Medium	*Departmental Procedures should be documented for Security Alerts*

#1: Monitor Use of Cloud Services

High: Data could be at risk if a cloud service is in use but has not been assessed and approved by Information Security (IS).

Use of any cloud service, whether purchased or free, should be monitored to assure only vetted and approved services are in use. Currently, Microsoft Defender for Cloud App Security (MDCA) is in place, but there is no monitoring of the data collected to detect the use of unsanctioned cloud services. Data could be stored or processed on unsanctioned or insecure cloud services without timely detection and mitigation, increasing the risk of loss or unauthorized disclosure of confidential HSC information.

Opportunity for Improvement: IS should develop and implement approaches to efficiently and effectively view the logs and determine high risk cloud services that should be targeted for review.

Management Response: We can utilize Microsoft Defender for Cloud App Security (MDCA) to identify unsanctioned cloud services that use apps to connect to those cloud services. The HSC ISO team will start the process of identifying and tagging cloud services that should be targeted for review.

Anticipated Implementation Date: 12/1/2022

#2: Maintain a Comprehensive Inventory of Cloud Services

Medium: Data could be at risk if stored in or processed by a cloud service not known, vetted, or monitored by IS.

A complete inventory of cloud services should be maintained by IS to support monitoring and protection of confidential HSC information. Policies for Information Technology purchases and monitoring mechanisms are in place.

Audit testing identified 1 of 35 cloud service vendors that had not been risk assessed and approved by IS as required per policy. It was also noted that this vendor was not included on the cloud service inventory list maintained by HSC. This appears to have been caused by the following factors:

1. Acquisition of a new department, and the new department continued use of a cloud service provider, which was not communicated to IS per established processes, and was not risk assessed as required; and
2. Payments for license renewal fees in FY21-22 were issued without a risk assessment performed and without approval from IS.

An incomplete inventory can result in both: (a) payment to a cloud services provider that does not meet state or HSC requirements to provide cloud services; and (b) inadequate monitoring and review of cloud services increasing the risk of confidential HSC information not being properly secured.

Opportunity for Improvement: IS should collaborate with Information Technology (IT) to strengthen controls for ensuring cloud service providers are risk assessed and approved by IS, and to help maintain a complete inventory of cloud services.

Management Response: Conduct meeting with purchasing to discuss current procedures for making sure all cloud services are approved and added to data owner list before purchase.

Anticipated Implementation Date: 10/1/2022

#3: Ensure Completion and Documentation of Risk Assessments for Cloud Services

Medium: Data can be compromised or lost if a cloud service vendor has inadequate security.

Security risk assessments are required to be completed annually for all cloud services that contain confidential data to help ensure University data remains protected in accordance with University IS policies and minimum standards. Of the five (5) cloud service software tested, two (2) did not have an annual risk assessment re-performed within the required timeline by IS. These two (2) risk assessments were reportedly performed within 18-24 months as noted on the IS cloud service inventory for both vendors. As a result, cloud services currently in use and paid for with University funds may not comply with state or University IS standards, and data could be at risk of loss or unauthorized disclosure.

Opportunity for Improvement: IS should communicate to the Data Owners to re-perform risk assessments annually for cloud services that contain confidential data, as required per policy.

Management Response. Send notification informing data owners that risk assessments are required by policy and should be completed annually. Offer assistance to data owners who are in need of help completing the assessment(s).

Anticipated Implementation Date: 10/1/2022

#4: Update Information Resources Acceptable Use Policy

Medium: Without employee acknowledgement of the Information Resource Acceptable Use Policy, employee discipline for non-compliance may be difficult for the University.

The User Acknowledgement section of the HSC Information Acceptable Use Policy does not include specific language communicating the penalty for non-compliance with requirements for the use of cloud services. The University of Texas System (UTS) Policy #165 Standard 2 template contains the components that should be included in the policy.

Opportunity for Improvement: Management should update the Acceptable Use Policy to include the User Acknowledgement section as specified in the UTS #165 Standard 2 template.

Management Response: Update policy to include specific language communicating the penalty for non-compliance.

Anticipated Implementation Date: Implemented and in the routing process for approval.

#5: Departmental Procedures should be documented for Security Alerts

Medium: Data could be compromised or lost if security alerts are not assessed.

Based upon procedures performed during this audit, IAD notes that the current IS team is knowledgeable and experienced in this area. Informal procedures were provided to IAD demonstrating how IS responds to alerts for malware and occurrences of unusual volumes of file activity/deletion/external sharing. However, these procedures are not documented to ensure the consistent application of the procedures over time or to ensure others not familiar with the informal procedures, such as new staff, would perform procedures correctly.

Opportunity for Improvement: Management should consider documenting departmental procedures for monitoring and responding to security related system alerts.

Management Response: Create procedure document for responding to cloud-based alerts.

Anticipated Implementation Date: 12/1/2022

Other Comments

We will follow up on management action plans to determine their implementation status. This process will help enhance accountability and ensure that timely action is taken to address the observations. Additional opportunities for departmental improvement were discussed with management.

We appreciate the assistance of the Information Security team and the University of Texas System Audit Office during this project.

BACKGROUND

Texas Administrative Code Chapter 202, Information Security Standards for Institutions of Higher Education, includes the following requirements:

- *Rule 202.70: Ensure that senior institution of higher education officials and information-owners, in collaboration with the information resources manager and information security office, support the provision of information security for the information systems that support the operations and assets under the direct or indirect (e.g., cloud computing or outsourced) control.*
- *Rule 202.71: The Information Security Officer shall be responsible for:*
    - *reviewing the institution's inventory of information systems and related ownership and responsibilities;*
    - *coordinating the review of the data security requirements, specifications, and, if applicable, third-party assessment of any new computer applications or service that receive, maintain, and /or share confidential data;*
    - *verifying that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated prior to the purchase of information technology hardware, software, and systems development services for any new high impact computer application or computer applications that receive, maintain, and/or share confidential data.*
- *Rule 202.75: A risk assessment of the institution's information and information systems shall be performed and documented.*
- *Rule 202.76: Mandatory security controls […] shall include […] standards to be used by all institutions of higher education to provide levels of information security according to risk levels.*

This audit was conducted based on the risk assessment included in the Fiscal Year 2022 Annual Audit Plan that was approved by the Institutional Audit Committee (IAC). This audit meets the biennial Texas Administrative Code (TAC) § 202.76 (c) risk-based review of compliance with Texas Information Security Standards.

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* and *Generally Accepted Government Auditing Standards*.

SCOPE AND PROCEDURES

The scope of this audit was control practices currently in place and cloud service purchases made in Fiscal Year 2022 at the UTT Health Science Center (HSC) campus and included the following procedures:

- Governance: reviewed policies and procedures related to cloud services including employee training, contract review, and risk assessments;
- Acquisitions: identified cloud service purchases based on expenditures, and reviewed the inventory of cloud services maintained by IS to determine if it was comprehensive and complete;
- Data Security and Integrity: reviewed policies and documentation for data encryption, backup, and security monitoring tools; and

- Monitoring: reviewed procedures to monitor unapproved cloud services.

OBSERVATION RANKINGS

Internal audit departments across the University of Texas System uses a consistent process to evaluate audit results based on risk factors and the probability of a negative outcome.

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. These findings are communicated separately to management.*