Information Technology
Cloud Security Audit

The University of Texas at
TYLER

August 2021

INTERNAL AUDIT
3900 UNIVERSITY BOULEVARD
TYLER, TEXAS 75799

AUDIT OBJECTIVE and CONCLUSION

The objective of the audit was to assess controls in place to protect The University of Texas at Tyler (UT Tyler) Academic campus resources when cloud services, including software and cloud storage, are used to process and store university data. 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.

This audit identified four opportunities to strengthen controls over cloud services.

OBSERVATIONS

This audit identified the following opportunities for improvement:		
1	High	*Maintain Comprehensive Inventory of Cloud Services*
2	High	*Complete and Document Risk Assessments for Cloud Services*
3	High	*Monitor Use of Cloud Services*
4	Medium	*Review Information Technology Contract Verbiage*

#1: Maintain Comprehensive Inventory of Cloud Services

High: Data could be at risk if stored in or processed by a cloud service not known, vetted, and monitored by the Information Security Office.

A complete inventory of cloud services should be maintained by the Information Security Office (InfoSec) so that appropriate security review and monitoring can occur.[1] Although policies are in place for information technology purchases, there are no monitoring mechanisms in place to detect the purchase of cloud services that did not require contract review by the Office of Legal Affairs.

As noted in Observation #2, five cloud service purchases were identified during audit testing that had not been vetted by InfoSec and two were reportedly assessed by InfoSec but not documented on the inventory. Current inventory records maintained by InfoSec did not include these cloud services. This appears to have been caused by the following factors:

1. Departments have purchased cloud services without security assessment and approval by InfoSec;
2. The Information Technology department has not informed InfoSec of all approved items; and/or
3. InfoSec has not consistently updated inventory records as services are vetted and approved.

In addition, the information captured in the inventory does not include key elements that would assist in recording assessment results, categorizing cloud services based on risk, and establishing a regular frequency for re-assessment as suggested in Observation #2. An incomplete inventory can result in an inadequate review of cloud services, which increases the risk of data not being properly secured.

[1] TAC §202.76 Security Control Standard PM-5: Information System Inventory requires that an inventory of information systems be maintained.

Opportunity for Improvement: InfoSec should strengthen controls to maintain a complete inventory of cloud services.

Management Response: *InfoSec will require assistance from the purchasing department moving forward to help identify software purchases made by departments that do not go through the contract routing process. InfoSec may require the assistance of the audit office to help facilitate this new process.*

Information Technology Support has informed InfoSec of some new software purchases in the past, but not all. We will work with management over Technology Support to ensure we are included on all software requests so we can send the departments the new software survey which helps the Information Security Officer (ISO) deduce the risk involved.

The gaps in our inventory were due to solutions purchased and renewed prior to the ISO being involved in the contract routing process. The ISO will review all renewals moving forward to ensure that that have gone through the initial review process.

The UT Tyler Academic ISO will need to confer with the UT Tyler Health Science Center (HSC) ISO to ensure our policies and procedures align with HSC moving forward.

Anticipated Implementation Date: *March 31, 2022*

#2: Complete and Document Risk Assessments for Cloud Services

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

Security risk assessments should be completed for all cloud services to assure university data will be protected in accordance with university information security policies and minimum standards.[2] Of 14 cloud service purchases tested, 5 were made without a risk assessment by or approval from InfoSec. Risk assessments were reportedly performed but not documented on the inventory for 2 others. As a result, cloud services currently in use may not comply with university information security standards, and data could be at risk of loss or unauthorized disclosure.

Opportunity for Improvement: InfoSec should strengthen controls by completing and documenting security risk assessments for every cloud service provider used by the university. Consider the following:

- Develop tiers for risk assessment procedures and frequency based on classification of data and significance of the service to department or university operations;
- Request a Service Organization Control 2 (SOC2) report from vendors for major systems to confirm that security controls reported by the vendor have been validated by a third party;

[2] TAC §202.76 Security Control Standard RA-3: Risk Assessment requires the performance and documentation of risk assessments. Standard CA-3: System Interconnections requires that "risks related to external parties [be] identified and controlled."

- Review the Higher Education Cloud Vendor Assessment Tool (HECVAT) and/or Consensus Assessments Initiative Questionnaire (CAIQ) for all vendors that store or process confidential university data or interface with UT Tyler systems;
- Develop procedures to document the results of the assessment; and
- Re-assess vendor security information at regular intervals or upon renewal, based on classification of data and significance of the service, to confirm that security controls still comply with university minimum standards.

Management Response: *ISO will coordinate with the HSC ISO to develop tiers and frequencies referenced in bullet point 1 of the recommendation.*

InfoSec will request a SOC2 report from vendors who will hold or process confidential data. If a SOC2 is not available, additional risk assessment steps will be conducted.

ISO will coordinate with the HSC ISO and to develop a process on assessing risks for the various tiers of vendors.

InfoSec has updated the inventory records to document additional information suggested during the audit.

ISO will coordinate with the HSC ISO to develop a process on the best way to re-assess vendors security posture and create a timeline for regular intervals of reassessment.

Anticipated Implementation Date: *May 31, 2022*

#3: 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 the Information Security Office.

Use of any cloud service, whether purchased or free, should be monitored to assure only vetted and approved services are in use. There are no monitoring mechanisms in place to detect the use of unsanctioned cloud services. Data could be stored or processed on unsanctioned or insecure cloud services, increasing the risk of loss or unauthorized disclosure.

Opportunity for Improvement: InfoSec should assure monitoring mechanisms are occurring to detect the use of unsanctioned cloud services.

Management Response: *InfoSec will need to research what technologies we can leverage to help us in this area.*

ISO will coordinate with the HSC ISO to see what possible solutions we can both agree on and leverage to help both institutions.

Anticipated Implementation Date: *May 31, 2022*

#4: Review Information Technology Contract Verbiage

Medium: Data could be at risk if contracts do not include appropriate verbiage to establish clear expectations and provide vendor accountability for information security.

Contracts for cloud services should be reviewed to assure they contain verbiage establishing clear expectations and minimum standards to protect university data.[3] Currently, there is no documented review of contract language for information security provisions. Without appropriate contract terms in place, the risk increases that vendors do not adequately protect data, do not comply with university policies and State law, and cannot be held accountable for failures to protect university resources.

Opportunity for Improvement: Contract verbiage for contracts requiring data storage or processing by a third party (including cloud services) should be reviewed to ensure appropriate information security requirements are established. Examples include:

- Commitment to minimum necessary access;
- Expected level of data protection;
- University's right to audit;
- Delineation of responsibilities for security; and
- End-of-contract data ownership and removal.

Management Response: *The ISO will need to work with legal to determine how we can better improve in this area. We will coordinate with the HSC ISO to develop consistent procedures for contract review.*

Anticipated Implementation Date: *March 31, 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.

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

[3] TAC §202.76 Security Control Standard SA-4: Acquisition Process requires certain information security provisions "explicitly or by reference" in contracts for an "information system, system component, or information system service…."

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 2021 Annual Audit Plan and approved by the Institutional Audit Committee. This audit will meet 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 from September 1, 2018, through February 18, 2021, at the UT Tyler Academic 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 InfoSec 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.*