TEXAS
The University of Texas at Austin

Cloud Usage and Security

November 2023

Office of Internal Audits

UT Austin's Agents of Change

OFFICE OF INTERNAL AUDITS
THE UNIVERSITY OF TEXAS AT AUSTIN

1616 Guadalupe St. Suite 2.302 · Austin, Texas 78701 · (512) 471-7117
audit.utexas.edu • internal.audits@austin.utexas.edu

Executive Summary

Cloud Usage and Security

Project Number: 23.002

Audit Objective

The objective of this audit was to determine the effectiveness of controls and processes related to cloud usage, security, and third-party risk management.

Conclusion

The University of Texas at Austin (UT Austin) does not have an effective cloud governance model focused on education and enforcement of policies related to the acquisition of cloud-based services. UT Austin also has opportunities to address risks to university data through development of third-party risk management, oversight requirements, and responsibilities.

Audit Observations[1]

Recommendation	Risk Level	Estimated Implementation Date
Cloud Technology Purchasing and Due Diligence	High	July 2024
IT Third-party Management and Oversight	Medium	August 2024
ProCard User Training	Medium	June 2024
TX-RAMP Compliance	Medium	August 2024

Engagement Team[2]

Mr. Jason Boone, CFE, Auditor III
Mr. Paul Douglas, CISA, CCSFP, CDPSE, IT Audit Partner
Ms. Maddy Hall, CISA, IT Audit Manager
Mr. Matthew Stewart, CISA, IT Audit Senior Manager
Ms. Samantha Tatum, CISA, IT Audit Senior Consultant

[1] Each observation has been ranked according to The University of Texas System Administration (UT System) Audit Risk Ranking guidelines. Please see the last page of the report for ranking definitions.
[2] This project was co-sourced with EAG Gulf Coast, LLC.

Detailed Audit Results

Observation #1 Cloud Technology Purchasing and Due Diligence

University employees frequently use procurement cards (ProCards) to purchase high-risk cloud-based technology solutions. Such purchases are not in compliance with the Handbook of Business Procedures (HBP), Part 7.8.1.3, which prohibits purchasing high-risk, cloud-based software with a ProCard. Instead, these purchases should be made through a purchase order or negotiated agreement approved by the Business Contracts Office and should undergo proper vetting and due diligence.

Policy defines high-risk purchases as those meeting certain criteria related to the third-party services being provided and the level of risk to UT Austin. Examples of the criteria include the type of data entered into the application, the application's access to the UT Austin network, and other security and cost considerations. We identified numerous high-risk cloud-based solutions purchased with a ProCard between fiscal years 2021 and 2023. For example, there were approximately 500 unique transactions with Amazon Web Services, totaling nearly $46,000 during this period. Departments do not consult the Business Contracts Office when using a ProCard; therefore, the purchases did not leverage campus-wide negotiated rates. Furthermore, appropriate due diligence, including a security review, does not occur when purchasing directly from a vendor using a ProCard.

Inconsistent enforcement of policy has led to unauthorized cloud technology purchases, thus increasing the University's exposure to third-party risk. Without formal vendor due diligence that includes Information Security Office (ISO) involvement, UT Austin increases the risk of an adverse impact to sensitive data (e.g., data governed by HIPAA or FERPA) stored or processed in an unsecure third-party environment.

Recommendation: Management should evaluate current policies and procedures related to IT software procurement to determine if policy requirements are comprehensive and enforceable. Management should establish an authoritative source to enforce requirements when purchasing software (including cloud technology) using a ProCard. Coordination across campus stakeholders will be essential to ensuring adequate procurement due diligence, supporting the education of ProCard users, and enforcing key requirements documented in policy.

Management's Corrective Action Plan: Procurement and Payment Services (PPS) will conduct a comprehensive review of the relevant policies, procedures, and training applicable to software purchases, including cloud security with a focus on creating clarity and enforceability.

PPS will evaluate the current ProCard Merchant Category Codes, and related object codes, to assess options to provide increased control of ProCard purchases related to software and cloud technology. Additionally, PPS will utilize the HBP and the Use of ProCard for Low Risk Clickwrap Agreements guidance to develop and publish a dedicated Clickwrap Agreements policy webpage specific to ProCards. The webpage will reiterate policies, key requirements, and prohibitions.

PPS will seek subject matter experts (SMEs) and funding to create a campus level centralized IT procurement review and approval process for the purchase of all software and cloud technology services. PPS will work collaboratively with campus leadership to identify SMEs from key areas and will review software and cloud technology services requests from across campus. SMEs would be responsible for receiving, reviewing, and rendering decisions on the requests while ensuring purchases adhere to all relevant policies, procedures, and requirements of UT Austin, UT System, and the State of Texas.

Responsible Person: Assistant Vice President for Procurement and Payment Services

Planned Implementation Date: July 31, 2024

Observation #2 IT Third-party Management and Oversight

University policy does not define procedures, requirements, or responsible parties necessary for on-going oversight of third-party IT service providers (including cloud service providers). UT Austin lacks defined criteria to determine vendor criticality and necessary oversight procedures, such as obtaining vendor security audit reports, reviewing service level agreements, and verifying compliance with government and state legislation (e.g., Texas Risk and Authorization Management Program (TX-RAMP)).

UT Austin has a responsibility to understand and evaluate risks associated with IT vendors; however, current ad hoc and decentralized oversight processes have limited the ability to monitor risks related to these service providers. Because of the procurement challenges detailed in Observation #1, ISO lacks the visibility needed to maintain a complete and accurate inventory of third-party IT vendors. A complete inventory is essential to supporting the oversight, monitoring, and protection of university data.

The absence of a complete IT vendor inventory and defined oversight procedures can result in both a payment to a cloud services provider that does not meet state (e.g., TX-RAMP) or University requirements to provide cloud services; and inadequate monitoring of cloud services, thus increasing the risk to the security and privacy of sensitive university data.

Recommendation: Management should establish a third-party management and oversight policy that outlines the process for identifying, monitoring, and assessing a third party's service and security environment. Key areas to be addressed within the policy should include:

- Maintaining a comprehensive and risk-categorized inventory of IT third-parties.
- Establishing a process to identify key personnel responsible for third-party oversight.
- Defining criteria to determine the vendor criticality (e.g., data type, user count, cost, criticality of service, etc.).
- Determining oversight requirements based on vendor criticality. Examples of oversight requirements include:
    - Periodic review of security audit and assessment reports (e.g., SOC).
    - Review of service level agreements or contract requirements at defined frequencies or milestones.

- On-going monitoring of vendor compliance requirements (e.g., TX-RAMP, HIPAA, PCI DSS).

Management's Corrective Action Plan: PPS agrees that developing an inventory of software and IT third party suppliers used by UT Austin is critical. A procure-to-pay solution working group began its work in November 2023. This work will lead to the implementation of a solution that addresses the key areas detailed above. Moving towards a modern procure-to-pay system would provide UT Austin with increased visibility, risk management, and accountability for all software and cloud technology purchases made by the University.

PPS, in conjunction with ISO and Information Technology Services (ITS), will create and execute a Cloud Computing policy, to be added to the HBP. This policy will outline requirements, practices, procedures, and standards for management of third-party vendors to ensure compliance with UT Austin policies and other regulations. The proposed Cloud Computing policy will delineate and define the roles and responsibilities of campus personnel responsible for third-party software vendor oversight.

Lastly, PPS will update the Business Contracts Software webpage to include an updated workflow and guidance for procuring software. This updated webpage will also provide guidance and educational information regarding the following: TX-RAMP, HIPAA, FERPA, and other types of university data.

Responsible Person: Assistant Vice President for Procurement and Payment Services

Planned Implementation Date: August 31, 2024

Observation #3 ProCard User Training

Procurement and Payment Services does not consistently provide annual ProCard refresher training, and current training content does not include established policy requirements for the procurement of IT software and services. HBP, Part 7.8.1.B, requires new cardholders to complete training prior to receiving their ProCard and requires existing cardholders to complete refresher training each fiscal year; however, PPS is not enforcing the annual requirement.

Refresher training reinforces cardholders' awareness of ProCard guidelines and restrictions and increases the likelihood of compliance. Additionally, excluding applicable software purchase policy requirements from the training content increases third-party risks and the likelihood of unauthorized purchases. PPS indicated they are developing an on-demand ProCard refresher training for rollout to the campus community in fiscal year 2024.

Recommendation: PPS should continue development of its on-demand refresher training and implement procedures to monitor completion and enforce the annual requirement. Additionally, PPS should consider incorporating content that outlines policy requirements and restrictions for IT software and service purchases and other high-risk transactions.

Management's Corrective Action Plan: PPS has created a pilot annual training program that was rolled out in July 2023. The training is connected to the University's Learning Management System (LMS), UT Learn, and allows users to register online for training. Delivering the training within the LMS will allow ProCard users to complete their required training on a self-service model. Using the LMS will allow PPS to effectively track and manage user training to ensure campus remains current with the required training in accordance with the policy.

PPS will update the training to include more specific requirements regarding the purchase of IT software and cloud technology services. It is anticipated that with the implementation of Card Integrity, PPS will be able to expand the training and audit functions of features to provide greater support to campus in ensuring alignment with the policy and best practices.

The HBP, Part 7.8.1, will be updated to include a specific requirement that users who do not complete the annual training within 30 days of expiration shall have their card access turned off until they successfully complete the training and pass the required assessment.

Responsible Person: Assistant Vice President for Procurement and Payment Services

Planned Implementation Date: June 30, 2024

Observation #4 TX-RAMP Compliance

UT Austin is unable to demonstrate that cloud-based technologies in use across campus comply with TX-RAMP legislation. State legislation requires cloud computing services to maintain TX-RAMP certification, with certification levels, and associated requirements, based on the type of data being processed. However, there is not a due diligence process to verify TX-RAMP certification when these services/technologies are purchased with a ProCard.

While the Business Contracts Office verifies TX-RAMP compliance when cloud-based solutions are acquired through the authorized procurement process, they do not verify continued compliance if the contract exceeds two years. Purchasing cloud computing services without appropriate due diligence and TX-RAMP verification can place university data at risk of residing in an unsecure/untrusted environment.

Recommendation:
Management should identify personnel responsible for managing TX-RAMP compliance verifications throughout the lifecycle of an agreement with a cloud service provider. Essential considerations for the management of TX-RAMP compliance include:

- Reviewing the Department of Information Resources' inventory of TX-RAMP certified cloud computing services for information such as the following:
  - Certification level to ensure it meets minimum requirements for the type of data that will interact with the cloud computing service.
  - Certification expiration dates to ensure the required level of certification is current for the cloud computing services that UT Austin has contracted.
- An inventory of the cloud computing services that do not require TX-RAMP certification should be maintained to provide evidence of a complete and accurate inventory.

Management's Corrective Action Plan: The Business Contracts Office is working to create a Contracts+ report that will allow PPS to identify contracts that require TX-RAMP compliance verification and follow up with contract managers to ensure completion. PPS will work with ISO and ITS to develop webpages that provide clear information and guidance for managing contracts of cloud computing services. These webpages will include TX-RAMP compliance and cloud service providers monitoring requirements.

PPS, in collaboration with ISO, will create and provide resources to departments for securing TX-RAMP certified providers. PPS will also seek to enter into more enterprise agreements for software complying with all UT Austin policies. This will further ensure that future contracting with firms conforms to all requirements.

Responsible Person: Assistant Vice President for Procurement and Payment Services

Planned Implementation Date: August 31, 2024

Conclusion

UT Austin does not have an effective cloud governance model focused on education and enforcement of policies related to the acquisition of cloud-based services. UT Austin also has opportunities to address risks to university data through development of third-party risk management, oversight requirements, and responsibilities.

The following table provides a summary of the audit results.

Table: Controls Assessment

Audit Objective	Controls Assessment
Determine the effectiveness of controls and processes related to cloud usage, security, and third-party risk management.	Ineffective with High/Medium Risk Opportunities.
Breakdown by area:	
Governance	Ineffective
Due Diligence	Ineffective
TX-RAMP Compliance	Ineffective
Ongoing Third-Party Management	Ineffective

Background

As cloud-based solutions have become more affordable and accessible, they have become more prevalent across campus. UT Austin's decentralized operations and purchasing processes challenge the University's ability to manage associated vendor relationships and risks. Increased usage of cloud-based technologies has the potential to increase efficiencies and reduce costs; however, it also reinforces the need for effective security and vendor management controls to address the evolving risks on campus.

Scope, Objectives, and Methodology

This audit was conducted in conformance with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. Additionally, we conducted the audit in accordance with Generally Accepted Government Auditing Standards and meet the independence requirements for internal auditors. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions on our audit objectives.

The scope of this review included current cloud service providers and processes in place to establish and monitor associated vendor risks. Key areas evaluated as part of this audit included:

- Governance
- Due Diligence
- TX-RAMP Compliance
- Ongoing Third-Party Management

Specific audit objectives and the methodology to achieve the objectives are outlined in the table below.

Table: Objectives and Methodology

Audit Objective	Methodology
Determine the effectiveness of controls and processes related to cloud usage, security, and third-party risk management.	• Reviewed the campus-wide risk assessment, applicable IT policies and procedures, and previous audit-related documents • Assessed design and implementation of key controls • Identified key areas of risk related to cloud usage/security and third-party risk management • Gained an understanding of the division of contract management responsibilities and ownership among Business Contracts, ISO, Colleges, Schools, and Units, and applicable vendors • Conducted interviews with key personnel responsible for procurement and contracting and with IT stakeholders • Obtained and reviewed evidence for limited testing of the key audit objective areas outlined above

Criteria

Texas Government Code §2054.0593 mandates that state agencies must only enter or renew contracts to receive cloud computing services that comply with TX-RAMP requirements beginning January 1, 2022. TX-RAMP certification requirements apply to all contracts for cloud computing services products entered into or renewed on or after that date.

UT Austin HBP, Part 7.8.1, Procedures for ProCard Holders

The table below summarizes the TAC 202 requirements that were reviewed during this audit.

Control Family	Control #	Control Name
Access Control	AC-20	Use of External Systems
Security Assessment and Authorization	CA-1	Policies and Procedures
	CA-2	Control Assessments
	CA-3	Information Exchange
	CA-6	Authorization
	CA-7	Continuous Monitoring
	CA-7(4)	Risk Monitoring
Configuration Management	CM-10	Software Usage Restrictions
	CM-11	User-Installed Software
System and Service Acquisition	SA-1	Policy and Procedures
	SA-4	Acquisition Process
	SA-9	External System Services
System and Information Integrity	SI-1	Policy and Procedures
	SI-4	System Monitoring
	SI-12	Information Management and Retention
Supply Chain Risk Management	SR-1	Policy and Procedures
	SR-2	Risk Management Plan
	SR-5	Acquisition Strategies, Tools, and Methods

Observation Risk Ranking

Audit observations are ranked according to the following definitions, consistent with UT System Audit Office guidance.

Risk Level	Definition
Priority	If not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of The University of Texas at Austin (UT Austin) or the UT System as a whole.
High	Considered to have a medium to high probability of adverse effects to UT Austin either as a whole or to a significant college/school/unit level.
Medium	Considered to have a low to medium probability of adverse effects to UT Austin either as a whole or to a college/school/unit level.
Low	Considered to have minimal probability of adverse effects to UT Austin either as a whole or to a college/school/unit level.

In accordance with directives from UT System Board of Regents, the Office of Internal Audits will perform follow-up procedures to confirm that audit recommendations have been implemented.

Report Submission

We appreciate the courtesies and cooperation extended throughout the audit.

Respectfully Submitted,

Sandy Jansen, CIA, CCSA, CRMA, Chief Audit Executive

Distribution

Dr. Jay C. Hartzell, President
Mr. Rogelio Anasagasti, Assistant Vice President, Procurement and Payment Services
Mr. Cameron Beasley, Chief Information Security Officer
Mr. Jeffrey Graves, Chief Compliance Officer, University Risk and Compliance Services
Ms. Ashley Nemec, Deputy to the Interim Vice President and Chief Financial Officer
Ms. Linda Shaunessy, Business Contracts Administrator
Dr. Daniel Slesnick, Interim Vice President and Chief Financial Officer
Ms. Christy Sobey, Director of President's Office Operations
Dr. Catherine Stacy, Chief of Staff, office of the Executive Vice President and Provost
Dr. Sharon Wood, Executive Vice President and Provost

The University of Texas at Austin Institutional Audit Committee
The University of Texas System Audit Office
Legislative Budget Board
Governor's Office
State Auditor's Office