Third-Party Risk Management

Audit Report # 25-AS0007
August 6, 2025

The University of Texas at El Paso

Office of Auditing and Consulting Services

"Committed to Service, Independence and Quality"

The University of Texas at El Paso
Office of Auditing and Consulting Services

500 West University Ave
El Paso, Texas 79968
915-747-5191
www.utep.edu

August 6, 2025

Dr. Heather Wilson
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Wilson:

The Office of Auditing and Consulting Services (OACS) in conjunction with service provider EisnerAmper, has completed a limited-scope audit of Third-Party Risk Management. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the department in strengthening controls and help ensure that the University's mission, goals, and objectives are achieved.

We appreciate the cooperation and assistance provided by the Information Security Office, Disbursement Services, Purchasing and General Services, and Information Resources staff during our audit.

Sincerely,

Courtney H. Rios

Courtney H. Rios
Chief Audit Executive

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

As UTEP continues to grow and engage with third-party vendors, effective oversight and risk management has become increasingly vital to safeguard institutional operations and data.

Audit Objectives

The objective of this audit is to evaluate the effectiveness of the University's Third-Party Risk Management program and evaluate compliance with any applicable Federal and State regulations and UT System Administration policies.

Scope

The scope of the audit includes third-party systems and technology services across the academic, administrative and research functions supporting UTEP operations.

Strengths

The University has established a well-coordinated third-party onboarding process with strong collaboration among key departments, including Purchasing and General Services, Disbursement Services, and Information Resources. Compliance risks are proactively addressed through vendor reviews, conflict-of-interest screenings, and real-time sanctions monitoring via PaymentWorks.

Security controls are in place for sensitive data handling. Sponsored contractor accounts are reviewed annually for appropriateness. Department representatives demonstrated a clear understanding of procurement and purchasing requirements.

Summary of Audit Results

Issue	Risk Ranking
1. Security alerts involving third-party vendors are not formally documented or tracked to resolution.	High
2. Vendor due diligence procedures do not address security risks.	Medium
3. A centralized inventory of third-party vendors is not maintained and reviewed.	Medium
4. The TX-RAMP review process is not standardized or formally documented.	Medium

Conclusion

Based on the results of audit procedures performed, we conclude the following regarding governance, risk, and control: departments have a strong foundation in third-party risk management, but there are valuable opportunities to enhance consistency, formalize processes and documentation, and strengthen oversight.

BACKGROUND

UTEP increasingly relies on third-party vendors and service providers to deliver technology and operational support across the Institution. While this approach offers benefits such as faster implementation and reduced demand for internal resources, it also introduces significant risks that must be identified, assessed, and managed through appropriate governance, risk management, and control processes. A robust Third-Party Risk Management (TPRM) program is essential to ensure that vendors follow sound security practices and comply with applicable federal and state regulations, including the Texas Administrative Code §202 (TAC 202) Security Control Standards (see Appendices).

This audit was conducted to evaluate and enhance the University's processes for managing risks associated with third-party vendors and service providers, and to assess whether practices align with a consistent, comprehensive approach to assessing the design and implementation of third-party governance, risk management, and control processes as outlined in emerging professional standards.

Please refer to Appendix A for additional details regarding the UTS 165 Information Resources Use and Security Policy, the Texas Risk and Authorization Management Program (TX-RAMP), and the Texas Administrative Code §202 (TAC 202).

The audit was conducted in accordance with the Institute of Internal Auditors' *Global Internal Audit Standards* and *Generally Accepted Government Auditing Standards*.

AUDIT RESULTS

1. Security alerts involving third-party vendors are not formally documented or tracked to resolution.	High Risk

TAC 202 Security Control Standards requires the implementation of appropriate controls to manage risk to systems and data (§202.76), a risk-based approach to identifying and responding to threats (§202.71) and outlines the required baseline security controls such as audit logging, access management and continuous monitoring (§202.72). Refer to Appendix B for the specific controls tested.

The Information Security Office (ISO) monitors security alerts using a variety of tools including Security Information and Event Monitoring (SIEM) tools. The tools in place are designed to protect systems from cyber threats in a variety of ways, including but not limited to securing user logins by requiring additional verification, detecting unusual activity, and alerting IT staff.

Auditors reviewed the configurations and email alerts for several alerting tools and verified that alerts were configured and sent to the ISO. Auditors inquired of management and noted that alerts are reviewed and addressed by the ISO on a continuous basis; however, investigation of alerts is not formally documented or tracked to resolution in a centralized location. The absence of a centralized tracking mechanism may result in:

- Inconsistent or lack of resolution of security alerts
- Limited visibility into incident trends and response effectiveness
- Gaps in audit trails critical for investigating potential breaches involving third-party systems

Recommendation:

Develop and maintain formal documentation procedures for the investigation and remediation of security alerts. This should include clear guidelines for reviewing, tracking, and resolving identified issues based on risk-ranking to ensure consistency, accountability, and compliance with University policies. Additionally, all alerts should be centrally tracked to support effective oversight and ensure timely resolution of issues.

Management Response:

Management agrees with the recommendation and will work toward documenting the procedures for reviewing and responding to security alerts. While it is not currently feasible to centralize all alert responses due to the distributed nature of our systems and responsibilities, critical alerts impacting the campus will be tracked centrally to ensure appropriate oversight and timely resolution. This approach will support consistent handling of critical issues while aligning with University policies and risk management objectives.

Responsible Party:

Baltazar Santaella, Deputy CISO

Implementation Date:

December 31st, 2025

2. Vendor due diligence procedures do not address security risks.	**Medium Risk**

TAC 202 *Security Control Standards* outlines required baseline security controls such as audit logging, access management and continuous monitoring (§202.72), and requires the implementation of risk management strategies that address the security implications of third-party relationships (§202.75).

Auditors reviewed the University's vendor onboarding and due diligence processes and met with key personnel in Disbursement Services, Purchasing and General Services, Information Resources, and the ISO. Vendor onboarding and due diligence procedures are essential to ensuring the University can proactively manage risk and safeguard the organization's operations, data, reputation, and compliance posture.

Auditors verified the PaymentWorks platform is in place and performs basic verifications on the registered third-party vendors such as address, TIN, and EIN validation, duplicate checks, and nightly screenings against debarment and compliance lists. Additionally, the Purchasing Department assigns risk levels to vendors based on financial risk and the ISO verifies vendors' FedRAMP and TX-RAMP certifications.

However, due diligence procedures including the initial risk categorization do not address security risks that should be evaluated prior to contracting with high-risk vendors (e.g. vendors that store or process sensitive data) and annually thereafter.

Testing of Pro Card, non-PO and Miner Mall vouchers resulted in inconsistent documentation and execution across departments. Due diligence practices varied across purchase types. Notably, the procedures lacked standardization and did not include an evaluation of vendors based on information security risk.

The absence of a formalized and consistently applied vendor due diligence process based on risk ranking increases the University's exposure to third-party risks and may result in:

- Inadequate assessment of high-risk vendors (e.g., vendors that store or process sensitive data)
- Inadequate assessment of vendor security and compliance posture
- Increased exposure to third-party risks over time
- Reduced ability to respond effectively to vendor-related incidents or changes in risk

Recommendation:

Formally define and implement a vendor due diligence process that includes a risk assessment of each vendor's security risk level (i.e. high, medium, low) based on standardized criteria such as data sensitivity, system access, regulatory exposure, historical security posture, etc. For vendors identified as high-risk, due diligence procedures should extend beyond TX-RAMP verification to include the review of additional compliance documentation such as Systems and Organizations Controls (SOC) 2 reports or other relevant security certifications. These reviews should be performed annually or upon significant changes in vendor services. All due diligence activities, including risk assessments, supporting documentation, and approval records should be housed in a centralized location, such as a ticketing system or structured email folder, to ensure consistent documentation and support ongoing monitoring. Consistent, complete records will reduce the risk of data breaches, service disruptions, and policy violations caused by inconsistent oversight.

_____

Management Response:

Management agrees with the recommendation and will work to establish a vendor due diligence process. As part of this effort, a decision matrix will be developed to help identify potential high-risk vendors based on standardized criteria. For those identified, a formal risk assessment process will be created and implemented to evaluate each vendor's risk level.

Responsible Party:

Gerard Cochrane Jr., AVP for Information Security

Implementation Date:

March 31st, 2026

3. A centralized inventory of third-party vendors is not maintained and reviewed.	**Medium Risk**

TAC 202 Security Control Standards, mandates a risk-based approach to identifying and responding to threats(§202.71), baseline security controls such as audit logging, access management and continuous monitoring (§202.72), implementation of risk management strategies that address the security implications of third-party relationships (§202.75), and the implementation of appropriate controls to manage risk to systems and data (§202.76).

Auditors reviewed the University's current practices for tracking third-party service providers and met with personnel from the Information Resources Department and the ISO. A centralized inventory of third-party vendors is not maintained and reviewed. Maintaining an inventory of third parties with access to data, systems, or business functions is a foundational control that facilitates the assessment of cybersecurity, operational, financial, and reputational risks.

Auditors received a listing of third-party vendor applications utilizing University Single Sign-On (SSO) integrations to login, as well as a listing of third-party vendors and service providers with access to key systems or information. These lists were created in response to the audit request but were not actively maintained or regularly updated.

Additionally, during testing of Pro Card, non-PO Voucher, and Miner Mall purchases (see Issue 2), it was noted that a centralized inventory of approved vendors is not maintained. Requestors maintain their own records for auditing purposes, and certain approvals are tracked in Miner Mall. This decentralized approach makes it difficult to track when and by whom vendors, including cloud service providers, were evaluated and approved. The absence of a centralized inventory of third parties exposes the University to risks including compliance violations, security breaches, operational inefficiencies, and financial losses. It also limits the ability to manage third-party relationships effectively and respond to emerging threats.

Recommendation:

Establish and maintain a centralized inventory of all third-party systems and applications being used on campus. This inventory should include key attributes such as vendor name, system owner, classification level or type of data processed, integration type (e.g., SSO), purpose (e.g., cloud service provider, hardware, software, etc.), approval status, TX-RAMP status, and whether Information Security and the CISO have formally reviewed the vendor. A centralized inventory of third parties enhances visibility, consistency, and accountability in third-party risk management. Further, it supports compliance, improves operational efficiency, and strengthens the organization's ability to respond to emerging risks.

Management Response:

Management acknowledges the importance of maintaining a central repository for all third-party systems and applications in use across campus. To address this, the Information Resources Department (IRD) will collaborate with the Information Security Office (ISO) and the Purchasing Department to consolidate and review the third-party vendor information maintained by individual departments, creating a centralized repository that identifies vendors with SSO integrations and/or access to sensitive data.

Responsible Party:

Edgar Luna, Assistant Vice President, Enterprise Computing

Implementation Date:

December 31st, 2025

4. The TX-RAMP review process is not standardized or formally documented.	**Medium Risk**

The Texas Government Code §2054.003 (13) requires all state agencies to follow The Texas Risk and Authorization Management Program (TX-RAMP). TX-RAMP provides a standardized approach for security assessment, certification, and continuous monitoring of cloud computing services that process the data of Texas state agencies. The CISO is responsible for reviewing and approving vendors providing cloud services that may require TX-RAMP certification at the University.

The CISO evaluates vendors on a case-by-case basis, reviewing vendor websites, asking clarifying questions, and consulting with departments using purchase orders through Miner Mall, Non-PO vouchers, and Pro Cards.

Inconsistencies in TX-RAMP compliance across purchasing methods were identified:

- **Vendor Claims**: Several cloud vendors asserted that TX-RAMP did not apply; however, no formal exception process or documented approval was in place.
- **Sample Results**:
    - **Non-PO Vouchers**: 3 of 4 cloud vendors were not listed in the TX-RAMP database.
    - **Pro Card**: 3 of 8 cloud vendors were not TX-RAMP certified.
    - **Miner Mall**: 3 of 17 cloud vendors lacked TX-RAMP certification, and 2 additional vendors were not routed to Information Security for evaluation.
- **Approval Gaps**: 5 of 21 TX-RAMP approvals were discussed in internal CISO roundtables but lacked formal documentation.
- **Delayed Assessments**: For one vendor under non-PO Vouchers, a TX-RAMP assessment was performed after two payments, highlighting a compliance lapse.

The lack of a formalized and documented due diligence process for reviewing TX-RAMP exceptions increases the risk of inconsistent application of security standards for cloud service providers. Without clear oversight and transparency, the University may unknowingly engage with vendors that pose heightened risks, potentially resulting in data breaches, operational disruptions, or reputational harm.

Recommendation:

Formalize and document the process for reviewing and approving TX-RAMP certifications for cloud vendors. A standardized procedure will ensure that all exception decisions are based on defined criteria, consistently applied across purchasing methods (e.g., Pro Cards, non-PO vouchers, and Miner Mall), and properly documented. Additionally, conduct a review of existing vendors whose contracts have not been renewed within the past year to determine whether TX-RAMP certification is required.

Management Response:

Management agrees with the recommendation and will work to develop a formal review and approval process for TX-RAMP certification of cloud vendors. This process will help ensure consistency across purchasing methods and provide clear documentation for exception decisions. A review of existing vendors will be conducted on an as-needed basis to determine whether TX-RAMP certification is required, based on contract status and service changes. Information Resources will establish a defined partnership with Procurement to take advantage of opportunities to use existing processes/systems to collect data and possible automate some of the decision tasks.

Responsible Party:

Gerard Cochrane Jr., AVP for Information Security

Implementation Date:

December 31st, 2025

RANKING CRITERIA

Priority	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.
High	A finding identified by internal audit considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.
Medium	A finding identified by internal audit considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.
Low	A finding identified by internal audit considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

Report Distribution:

University of Texas at El Paso:

Ms. Andrea Cortinas, Executive Vice President and Chief of Staff

Dr. Catie McCorry-Andalis, Vice President for Student Affairs and Interim Vice President for Business Affairs

Mr. Luis Hernandez, Vice President for Information Resources

Mr. Gerard Cochrane, Associate Vice President, Chief Information Security Officer

Mr. Edgar Luna, Assistant Vice President, Enterprise Computing

Ms. Mary Solis, Director/Chief Compliance and Ethics Officer, Office of Institutional Compliance (OIC)

University of Texas System (UT System):

System Audit Office

External:

Governor's Office of Budget, Planning and Policy

Legislative Budget Board

Internal Audit Coordinator, State Auditor's Office

Audit Committee Members:

Mr. J. Stephen DeGroat, Audit Committee Chair

Mr. Fernando Ortega, External Member

Dr. John Wiebe, Provost, Vice President for Academic Affairs

Mr. Daniel Garcia, Senior Associate Athletic Director, Business, Finance, & Facilities

Ms. Guadalupe Gomez, Assistant Vice President for Research Administration

Auditors Assigned to the Audit:

Ms. Courtney H. Rios, CPA, CIA, CFE, Chief Audit Executive

Ms. Cecilia Estrada Lozoya, CPA, CIA, CISA, Audit Manager

Mr. Paul Douglas, CISA, CCSFP, CDPSE, IT Audit Partner

Ms. Danielle Keller, CISA, CCSFP, CHQP, IT Audit Director

Ms. Anna Fowler, CCSFP, CHQP, IT Audit Senior Manager

Ms. Samantha Tatum, CISA, IT Audit Senior Consultant

Ms. Jessica Howley, IT Audit Consultant

APPENDIX A: CRITERIA

The UTS 165 Information Resources Use and Security Policy objectives and expectations for information security can be found here.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to the security assessment, certification, and continuous monitoring of cloud computing services used by federal agencies. TX-RAMP is a similar program specifically for the state of Texas, administered by the Texas Department of Information Resources (DIR) to ensure that cloud services used by Texas state agencies meet established security requirements. TX-RAMP guidance and requirements for third-party cloud solutions, including security standards and authorization levels, can be found here.

Texas Administrative Code §202 (TAC 202) security standards, roles, and responsibilities that state agencies and higher education institutions must follow can be found here.

APPENDIX B: TAC 202 SECURITY CONTROLS STANDARDS CATALOG

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

Control Family	Control #	Control Name	TAC 202 Reference(s)
Access Control	AC-3	Access Enforcement	§202.76
	AC-20	Use of External Systems	
Awareness and Training	AT-3	Role-Based Training	§202.71, §202.72
Audit and Accountability	AU-2	Event Logging	§202.76
	AU-6	Audit Record Review, Analysis, And Reporting	
Configuration Management	CM-8	System Component Inventory	§202.75
	CM-10	Software Usage Restrictions	
Assessment, Authorization, and Monitoring	CA-1	Policies and Procedures	§202.71, §202.75
	CA-3	Information Exchange	
	CA-6	Authorization	
	CA-7	Continuous Monitoring	
System and Services Acquisition	SA-3	System Development Life Cycle	§202.72, §202.75
	SA-4	Acquisition Process	
	SA-5	System Documentation	
	SA-9	External System Services	
Supply Chain Risk Management	SR-3	Supply Chain Controls and Processes	§202.72, §202.75
	SR-8	Notification Agreements	