THE UNIVERSITY OF TEXAS SYSTEM AUDIT OFFICE
Third Party Risk Management Audit
Fiscal Year 2025

SUMMARY

BACKGROUND: The University of Texas (UT) System Administration relies on numerous third-party systems and technology services to support key business functions. Inadequately managed third-party relationships can introduce significant legal, regulatory, and data security risks. This engagement was included in the Fiscal Year 2025 annual work plan based on the risk of breach or loss of sensitive/confidential data stored or processed on unapproved or insecure third-party and/or cloud services.

This audit was performed on our behalf by Protiviti. The focus of the audit was on UT System Administration risk management practices for systems and technology services supporting business operations and their compliance with UT System Administration policies and Texas Administrative Code (TAC) §202.76 security control standards as defined in the Texas Department of Information Resources (DIR) Security Control Standards Catalog.

The UT System Audit Office released a separate UT System Administration Contract Monitoring Audit Report on May 1, 2025. The objective of that audit was to determine if decentralized contract monitoring processes and controls are adequate and functioning, with a focus on risks associated with inefficient and decentralized contract monitoring processes leading to overspending against authorized contract limits or exceeding contract terms. The Information Security Office (ISO) and Contracts and Procurement (CnP) created an ad hoc workgroup to address observations communicated in the audit report.

Though this Third Party Risk Management Audit and the prior Contract Monitoring Audit focused on different contract management processes and risks, there were areas of overlap in the audit results. Those areas of overlap are identified in the respective Observations contained in this report.

OBJECTIVE: The objective of this audit was to assess the effectiveness and efficiency of UT System Administration third party risk management practices intended to ensure the security and privacy of data entrusted to third-party systems and service providers. This included the evaluation of processes for vendor selection, risk assessment, contract management, ongoing monitoring, compliance oversight, and vendor termination procedures. The audit aimed to determine whether these processes align with the UT System's policies and standards and comply with relevant laws and regulations.

CONCLUSION: UT System Administration has established foundational Third Party Risk Management practices; however, opportunities remain to enhance their effectiveness. Strengthening the consistency of risk assessment protocols and implementing centralized oversight of vendor monitoring will improve the ability to manage third-party information security risks. Introducing systematic contract tagging and formalized workflows will further support the consistent application of these practices.

OBSERVATIONS

1 **High**	Consistent application of standard risk assessment protocols, including processing timelines, risk rating criteria, documentation of risk rating decisions, vendor attestation requirements, and recurring risk assessment requirements, will help ensure that third-party risks are timely and effectively identified, managed, and monitored.
2 **Medium**	Oversight of vendor performance monitoring will reduce the risk that vendor non-compliance with contractual requirements compromises data security.
3 **Medium**	Implementing a contract tagging process will help ensure contracts are reviewed by the appropriate offices before execution and facilitate ongoing monitoring when required.

Management developed action plans that incorporated recommendations to address these observations and anticipates implementation by August 31, 2027.

OBSERVATION 1

HIGH

Implement Standardized Risk Assessment Protocols

> Consistent application of standard risk assessment protocols, including processing timelines, risk rating criteria, documentation of risk rating decisions, vendor attestation requirements, and recurring risk assessment requirements, will help ensure that third-party risks are timely and effectively identified, managed, and monitored.

UT Systemwide Policy (UTS) 165.1.2 (Cybersecurity Risk Management) requires that security risk assessments be conducted prior to system acquisition. The ISO Vendor Risk Assessment webpage provides instructions to departments on requesting a security risk assessment and specifies that the risk assessment must be performed before use of a third-party system or service begins.[1]

ISO maintains an online request and tracking system to facilitate the risk assessment process, the Information Security Office Third Party Risk Assessment Queue (ISOTRAQ). ISOTRAQ submissions between January and April 2025 were reviewed to determine whether risk assessment requests were submitted and completed as required before use of the third-party system or service began. Out of 55 ISOTRAQ requests submitted during this period, four (7%) were not submitted by the Departmental Contract Administrator (DCA) or other responsible party until on or after the contract start date. One of the four involved the sharing of confidential information with the third party as part of the contract agreement. Although a specific request processing timeline has not been established to indicate how long the DCA should expect the risk assessment to take, nine of the 55 ISOTRAQ requests were submitted within 14 days prior to the estimated contract start date, which may not allow sufficient time to complete the security risk assessment, particularly if the assessment identifies risks requiring follow-up and/or corrective action by the contractor. Establishing and enforcing a risk assessment request and processing timeline will help ensure risk assessments are completed, and risk acceptance decisions, if needed, can be made prior to contract execution and system use.

TAC §202.76 security control standard RA-2: Security Configuration requires that a security classification be assigned to all information systems, with the supporting rationale documented. Within the ISOTRAQ security risk assessment, vendors are risk-tiered (e.g., 1, 2, 3) and risk rated (e.g., high, medium, low). However, UT System Administration has not established standardized guidance for assigning vendor risk levels. This may result in misclassified or inconsistent ratings of vendor risk levels, which could impact ongoing monitoring of security and technology risks. In addition, two inconsistencies were noted between initial risk ratings provided by ISOTRAQ request submitters and the final risk rating from security reviewers. In these situations, notes were not available to indicate the reason for the change in risk rating, or whether the change was communicated to the DCA so that risk-based monitoring expectations were clear. Establishing standardized risk rating criteria in alignment with existing processes and enhancing documentation of risk assessment rating decisions will further ensure third-party risks are being effectively identified, managed, and monitored.

TAC §202.76 security control standard SA-4: Acquisition Process requires vendors authorized to access, transmit, use, or store data for UT System Administration to periodically provide evidence of compliance with contractually required security controls. In addition, UTS 165 standard requirement 165.1.2.4.3 requires vendor information security and privacy controls to be monitored using a risk-based approach at least once every 12 months. A vendor attestation statement during risk assessment and/or a review of third-party attestation reports (e.g., Service Organization Control 'SOC' 2 Type 2 reports) are methods by which vendors' compliance could be evaluated and monitored, with third-party attestation reports providing greater assurance through independent testing of vendor controls. Clearly defined requirements for obtaining a third-party attestation report during risk assessment, when available and based on risk, will help inform the risk assessment process by providing assurance over vendor controls, supporting efforts to manage identified risks and assess alignment with contractual requirements and applicable policies, standards, and regulatory requirements. See also Observation 2 regarding vendor monitoring.

[1] https://www.utsystem.edu/offices/information-security/system-administration-information-security-program/vendor-risk-assessments

As stated earlier, UTS 165 standard requirement 165.1.2.4.3 requires monitoring of vendor information security and privacy controls at least once every 12 months. Current practices have defined the risk-based approach to require ISOTRAQ security risk assessments determined as Confidential and/or Critical Infrastructure to undergo annual reviews by the ISO, while other vendor types may not be reassessed regularly unless prompted by contract renewals or significant changes in scope. The ISO Vendor Risk Assessment webpage also instructs DCAs to request a new assessment annually for software and services that access, transmit, or create confidential data, or every two years for software and services not involving confidential data. ISO stated their expectation that the DCA initiate reassessments. Based on discussion with DCAs during this audit and the prior Contract Monitoring Audit, responsibility and requirements for performing recurring risk assessments is unclear.

Given the speed at which technology evolves, assumptions and risk mitigations can quickly become dated as vendors change their processes and controls and use of a system or service evolves. By not consistently monitoring and re-evaluating vendor security postures annually as now required by UTS 165, risks to UT System Administration information may not be timely detected and addressed. Establishing standardized, consistent requirements for recurring security risk assessments and ongoing monitoring across all vendor categories will help clarify responsibilities and requirements, enhance the ability to identify and mitigate emerging risks associated with third-party relationships, and ensure ongoing compliance with data protection standards.

ACTION PLAN

ISO will improve transparency and consistency in its vendor assessment process by communicating estimated timelines, standardizing vendor risk rating guidance, documenting rationale for assessment changes, and clarifying third-party attestation requirements by August 31, 2026, depending upon the changes to the contract processes with the addition of the Supply Chain Alliance to UT System Administration.

Anticipated Implementation Date: August 31, 2026

OBSERVATION 2
MEDIUM

Establish Central Oversight for Vendor Monitoring Plans

Oversight of vendor performance monitoring will reduce the risk that vendor non-compliance with contractual requirements compromises data security.

The prior Contract Monitoring Audit noted that sampled monitoring plans did not include details on monitoring activities that the department or DCA should perform to monitor the vendor's information security practices or controls. This audit also determined that individual departments manage their vendor monitoring responsibilities independently, and that this decentralized approach has resulted in varied adherence to established policies for monitoring third-party system and technology contract risk and performance. For example, attestation reports that verify the vendor's adherence to security controls for one sampled contract were not consistently obtained or reviewed. (See also Observation 1.) Additionally, the assigned DCA did not obtain monitoring/status reports from the vendor for this same sampled contract, as marked in their monitoring plan.

In addition, UTS 165 standard 165.1.2 (Cybersecurity Risk Management) subsections 3: Risk Assessments and 4: Vendor Risk Management, and the UT System Administration Contract Management Handbook requirements for vendor monitoring, are not consistent. For example, the UTS 165 standard subsections require monitoring of vendor information security and privacy controls using a risk-based approach at least once every 12 calendar months, while the Contract Management Handbook requires a formal monitoring plan starting with contracts valued at $250,000 or greater and determined to be a high or medium risk. The Contract Monitoring Plan template lacks specific details and requirements for monitoring vendor security compliance with the UTS 165 policy standard stated above.

TAC §202.76 security control standard SA-9: External System Services requires that organizational oversight of external system services be defined and documented, including user roles and responsibilities. In the prior Contract Monitoring Audit report, CnP and ISO indicated that their ad hoc workgroup would develop a process that departments will use to monitor vendors' information security practices and controls. Establishing an oversight function, inclusive of the various groups involved in third party risk management efforts, to standardize monitoring protocols and accountability across departments, evaluate the quality of performed monitoring activities, and train responsible parties to ensure processes are followed will further ensure contracts involving third-party systems and technology services are consistently monitored.

ACTION PLAN

ISO will clarify and refine responsibilities for ongoing vendor monitoring and reassessments, provide training to DCAs, and explore expanding continuous monitoring by August 31, 2026, depending upon the changes to the contract processes with the addition of the Supply Chain Alliance to UT System Administration.

Anticipated Implementation Date: August 31, 2026

OBSERVATION 3

MEDIUM

Implement Contract Tagging and Formal Review Workflows

> Implementing a contract tagging process will help ensure contracts are reviewed by the appropriate offices before execution and facilitate ongoing monitoring when required.

Tagging or categorizing contracts based on risk, type, or compliance requirements helps ensure contract language includes applicable privacy and security provisions, and that contract language is consistent across contracts. A Contract Processing Checklist requires the DCA or person initiating the procurement and contracting process to indicate if the third-party system will have access to confidential data. For contracts in which a third-party system will have access to confidential information, there is an additional requirement to upload the ISOTRAQ security risk assessment to the Contract Collaboration and Reporting System (CCARS) contract management system. As noted in Observation 1, both UTS 165 standard requirement 165.1.2 (Cybersecurity Risk Management) and the ISO Vendor Risk Assessment webpage specify that the risk assessment must be performed before the third-party system or service is acquired and implemented.

Currently, CCARS does not use tagging functionality to clearly identify and route contract requests requiring additional compliance checks and/or security and risk assessments. Implementing formalized workflows for engaging compliance, security, and technology teams will provide added assurance that required reviews and assessments are completed timely for critical contracts involving third-party systems and technology services.

ACTION PLAN

CnP will continue to provide quality reviews when processing a contract (workflow) and ensure that the contract is not executed without the appropriate reviews. CnP is currently updating formal process workflows and is also reviewing solutions-oriented processes to help mitigate risk and is assessing current internal processes specific to contract risk levels. The CCARS tool is not as robust as CnP requires, and CnP is also researching other potential new contract management systems with the ability to identify and route contract requests for compliance checks and security risks prior to the service being acquired and implemented. This transition to a new contract management system will take up to 12-18 months, at minimum. Estimated completion date Aug. 31, 2027.

Anticipated Implementation Date: August 31, 2027

METHODOLOGY

On behalf of the System Audit Office, Protiviti conducted this engagement in accordance with Global Internal Audit Standards and generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the engagement to obtain sufficient, appropriate evidence to provide a reasonable basis for our observations and conclusions based on our objectives. We believe that the evidence obtained provides a reasonable basis for our observations and conclusions based on our objectives. The System Audit Office is independent per GAGAS requirements for internal auditors.

SCOPE AND PROCEDURES

The scope of this engagement included third party risk management practices in place for third-party systems and technology services supporting UT System Administration business operations. Audit procedures were performed in March and April 2025, and included the following:

- Interviewing and collecting documentation from Contracts and Procurement, Information Security Office, and Compliance Office staff responsible for third party risk management.
- Testing a sample of contracts to evaluate operating effectiveness of key controls and processes around contract risk assessments, ongoing monitoring, and vendor termination; and
- Interviewing Department Contract Administrators for three sampled contracts to verify processes around ongoing monitoring and vendor termination.

We will follow up on action plans in this report to determine their implementation status. We validate implementation of action plans for Priority- and High-level observations and review and rely on written affirmation from the responsible department to track completion of action plans for Medium- and Low-level observations. Responsible departments may request an extension to implement their action plans. Extension requests for Priority- and High-level observations require approval by the appropriate executive officer. This process will help enhance accountability and ensure that timely action is taken to address the observations.

OBSERVATION RATINGS

Priority	An issue that, if not addressed timely, has a high probability to directly impact achievement of a strategic or important operational objective of System Administration or the UT System as a whole.
High	An issue considered to have a medium to high probability of adverse effects to a significant office or business process or to System Administration as a whole.
Medium	An issue considered to have a low to medium probability of adverse effects to an office or business process or to System Administration as a whole.
Low	An issue considered to have minimal probability of adverse effects to an office or business process or to System Administration as a whole.

CRITERIA

Texas Administrative Code §202.76 Security Control Standards Catalog
UT Systemwide Policy 165: Information Resources Use and Security Policy
UT System Administration Contract Management Handbook

REPORT DATE

August 5, 2025

REPORT DISTRIBUTION

To: George Finney, Chief Information Security Officer
Derek Horton, Associate Vice Chancellor
Cc: Jonathan Pruitt, Executive Vice Chancellor and Chief Operating Officer
Phil Dendy, Chief Risk Officer
Casilda Clarich, Director, Contracts and Procurement
Lori McElroy, Associate Chief Information Security Officer
UT System Administration Internal Audit Committee
External Agencies (State Auditor, Legislative Budget Board, Governor's Office)