THE UNIVERSITY OF TEXAS SYSTEM AUDIT OFFICE
Contract Monitoring Audit
Fiscal Year 2024

SUMMARY

BACKGROUND: The University of Texas (UT) System Audit Office had previously conducted an audit of contract monitoring processes in Fiscal Year (FY) 2019, which resulted in six observations. As of December 2023, five of the observations were considered implemented and one observation, which related to tracking contract spend, was closed due to management's acceptance of the risk and other competing priorities. Since the FY 2019 audit, management implemented the Contract Collaboration and Reporting System (CCARS) in September 2022 and has undergone two leadership transitions—once in 2022 and another in 2025. The System Audit Office elected to perform a Contract Monitoring Audit in FY 2024 based on the high risk that an inefficient and decentralized contract monitoring process may lead to overspending above authorized contract limits or exceeding contract terms.

OBJECTIVE: To determine if decentralized contract monitoring processes and controls are adequate and functioning.

CONCLUSION: During contract formation, the Office of Contracts and Procurement (CnP) supports and works closely with the departments by reviewing contract risk assessments and contract monitoring plans; however, contract monitoring is decentralized and the responsibility of the departments, and contract monitoring processes vary widely among departments. In addition, there is no centralized monitoring of high-risk contracts, and neither CCARS nor UT Share (PeopleSoft) has functionality to allow CnP, or the departments, to effectively and efficiently monitor contract spending to ensure contract limits are not exceeded.

For Systemwide contracts that are available to the institutions, there is no process in place to ensure that institutional responsible parties are formally notified of potential requirements for those institutions to complete key compliance contract addendums and to perform information security third-party risk assessments for pending Systemwide contracts that the institutions intend to or may use.

The Departmental Contract Administrators (DCA) and other department staff we interviewed indicated that the contract training provided by CnP was useful but also suggested opportunities for improvement, which included more frequent training, additional monitoring tools, and documented guidance. Additionally, we found that the departments do not have their own documented procedures for contract monitoring processes and several departments do not have a backup for their DCAs.

OBSERVATIONS

1 High	Without centralized monitoring of high-risk contracts, there is a risk that significant contract issues are not anticipated and effectively identified and remedied.
2 High	Without the ability to track contract spending effectively and efficiently, there is a risk that departments may unintentionally exceed contract expenditure limits.
3 High	Without clear guidance and communication regarding Business Associate Agreements, information security assessments, and UT Systemwide agreements, there is an increased risk of noncompliance with key regulations and increased risk that institutions that utilize the contracts do not assess vendors to determine whether they have sufficient information security practices and controls to maintain the confidentiality, security, and integrity of their data that are consistent with the institutions' risk tolerances.
4 Medium	When monitoring plans do not include activities to review a vendor's ongoing information security practices, there is an increased risk of data breaches, unauthorized access, compliance violations, reputational damage, business disruptions, and increased costs.
5 Low	Without initial training and training targeted at addressing department needs, there is a risk that contract monitoring processes are not fully understood and requirements not followed. Without documented procedures or cross training, changes in department staff could become challenging, resulting in time-consuming efforts to reestablish effective and efficient business processes.

Management developed action plans that incorporated System Audit Office recommendations to address these observations and anticipates that all action plans will be implemented by August 31, 2026.

OBSERVATION 1
HIGH

Establish Centralized Monitoring of High-Risk Contracts

Without centralized monitoring of high-risk contracts, there is a risk that significant contract issues are not anticipated and effectively identified and remedied.

For System Administration contracts, the Office of Contracts and Procurement (CnP) reviews contract risk assessments and contract monitoring plans during contract formation and when contract amendments are made. Enhanced monitoring plans are developed for high-risk contracts. While CnP assists in reviewing contract risk assessments and monitoring plans, contract monitoring is decentralized and the responsibility of the departments. There is no centralized, risk-based monitoring in place to monitor and verify that departments are adhering to enhanced monitoring plans. CnP also relies on the departments to monitor contract payments to ensure that contract limits are not exceeded. However, CnP does not have any processes to monitor and verify that departments are effectively monitoring their contract spend.

CnP utilizes the Contract Collaboration and Reporting System (CCARS) to manage the contracting process. While CCARS serves as a central repository for contracts, due to data migration issues from IBM Content Navigator and inconsistent procedures at the time of software implementation (for contracts executed prior to 2022), the total value of each contract and increases or decreases with subsequent contract amendments may not be accurately captured in the system. Additionally, departments are required to include the contract risk assessments and contract monitoring plans within CCARS, but the assessed risk level and monitoring type are not captured in a data field within CCARS to indicate whether or not it is a high-risk contract. Consequently, CCARS cannot currently be used to develop a listing of high-risk contracts and those that require enhanced monitoring.

ACTION PLAN

We agree. The University of Texas System Administration continues to focus on process improvement opportunities and to ensure internal controls are in place to mitigate risk. The University of Texas System Administration should have a process in place to monitor high-risk contracts to mitigate the risk of significant contract issues being identified, remedied, and reported. Contracts and Procurement (CnP) does not provide departmental monitoring of high-risk contracts. The department's contract manager and/or Subject Matter Experts (SMEs) are responsible for monitoring their respective contracts with the assistance of their Department Contract Administrators (DCAs).

CnP is currently reviewing solutions-oriented processes to help mitigate this risk and is assessing current internal processes specific to contract risk levels. Specifically, CnP will submit a request to add a field with the contract management software platform, CCARS, to designate high risk contracts, enabling a listing of high-risk contracts which will assist departments with enhanced monitoring.

Anticipated Implementation Date: March 1, 2026

OBSERVATION 2
HIGH

Implement a Centralized Process to Monitor Total Contract Payments

Without the ability to track contract spending effectively and efficiently, there is a risk that departments may unintentionally exceed contract expenditure limits.

Exceeding contract limits could lead to various risks, which can include financial loss, contract disputes, project delays (if additional funding has not been approved), legal consequences, business disruptions, or reputational damage. The ability to effectively and efficiently monitor contract spending can mitigate these risks.

In July 2019, we found that there was no way to effectively track contract spending history without the use of spreadsheets or other tools that are external to UT Share. At that time, we recommended CnP work with the Controller's Office to use an existing field or work with Shared Information Services to incorporate a new field within UT Share to facilitate tracking and summarizing spending by individual contract. Implementing the recommendation required the technical expertise of departments outside of CnP. Ultimately, CnP accepted the risk of not implementing the recommendation due to competing priorities but intended to continue researching the feasibility of the project with the Office of Technology and Information Services (OTIS).

At System Administration, each contract is assigned a unique identification number. However, applicable contract identification numbers are not recorded in UT Share when payments are made and there is no field designated for this information. In addition, vendor invoices would not necessarily include the UT System-assigned contract identification number. Consequently, no user at System Administration can currently utilize UT Share or CCARS to query amounts spent by a specific contract name or contract identification number unless it is a vendor with only one contract (with no amendments) or a dedicated cost center has been set up for one particular contract and subsequent amendments. In addition, CnP would be unable to centrally monitor contract payments, without a significant manual effort, to ensure departments are not exceeding contract expense maximums for high-risk contracts.

Currently, departments cannot track total contract spending by contract identification number using UT Share or CCARs but can manually track contract payments using spreadsheets. While departments can download transactions by vendor, there are some vendors with multiple active contracts. And contracts may have multiple amendments. Sorting out payments for such contracts requires a manual process to reconcile invoices and accurately track contract spending. This process is not efficient and is more at risk of manual errors.

ACTION PLAN

We agree. The University of Texas System Administration relies on the individual departments to monitor contract payments and the subsequent contract expenditures and balances. Without proper and thorough clarification to the departments on ownership of this responsibility for contract spend monitoring, this risk could unintentionally exceed contract expense maximums and not take the required remedial steps.

The University of Texas System Administration currently does not have any processes to monitor and verify that the departments are effectively and accurately managing contract expenditure. To assist the departments, CnP has provided information sessions and business tools (via an excel spreadsheet template) for DCAs to assist with contract spend tracking for their respective departments.

Working with UT System Shared Information Services (SIS) group, the solution is to build out in the PeopleSoft platform a field that will associate each payment invoice with the respective contract number. This will manage contract expenditure and will help mitigate the risk of payments exceeding the contract total value. Additionally, this solution will ensure verification of total payment made against each contract. This will take collaborations between various stakeholders and will require additional time to fully execute.

Anticipated Implementation Date: August 31, 2026

OBSERVATION 3
HIGH

Implement a Process to Address HIPAA Requirements and Information Security Third Party Risk Assessments

Without clear guidance and communication regarding Business Associate Agreements, information security assessments, and UT Systemwide agreements, there is an increased risk of noncompliance with key regulations and increased risk that institutions that utilize the contracts do not assess vendors to determine whether they have sufficient information security practices and controls to maintain the confidentiality, security, and integrity of their data that are consistent with the institutions' risk tolerances.

For Systemwide contracts that are executed by either System Administration or an institution (and are used by the institutions and not System Administration), there is no process to ensure the UT institutional responsible parties are formally notified of the potential requirements for those institutions to complete key compliance contract addendums or to perform information security risk assessments for pending Systemwide contracts. Specifically, there are no documented procedures with decision trees that provide guidance as to what contracts may be required to include certain key compliance addendums, such as a Health Insurance Portability and Accountability Act of 1996 (HIPAA) Business Associate Agreement (BAA), and would need to be executed by the institutions before a service is started and confidential information is shared or developed with a third party.

In addition, there is currently no process to ensure that CnP, the UT System Information Security Officer (ISO), applicable UT System departments, and institutional ISOs communicate and coordinate regarding who is responsible for performing an Information Security Office Third Party Risk Assessment Queue (ISOTRAQ) before participating in or sharing information with a third party. While communication about UT Systemwide contracts occurs, including informing institutions which may need to perform their own ISOTRAQ assessments, such communications are informal, and the information may not be consistently shared with the appropriate individuals at the institutions.

For Systemwide contracts, a process should be implemented to ensure that responsible parties at the institutions are formally notified of the potential requirements for those institutions to complete key compliance contract addendums and perform information security third party risk assessments for pending Systemwide contracts that the institutions intend to use. The process should also ensure that all applicable UT institutional responsible parties who were formally notified have taken appropriate action before contract execution.

ACTION PLAN

We agree. CnP created an ad hoc working group with the ISO department to develop guidance and communication regarding Business Associate Agreements (BAAs), information security assessments, and UT Systemwide agreements. This will ensure established processes are in place so that institutions utilizing the contracts understand their role in maintaining the confidentiality, security, and integrity of their data. In addition to the working group, CnP will update the launch brief, a document which spells out compliance requirements that the institutions must follow when participating in UT Systemwide contracts.

Anticipated Implementation Date: August 31, 2025

OBSERVATION 4
MEDIUM

Ensure Monitoring Plans for Contracts that Provide Vendors Access to UT System Information Systems or Data and Include Monitoring Activities to be Performed by Responsible Departments

When monitoring plans do not include activities to review a vendor's ongoing information security practices, there is an increased risk of data breaches, unauthorized access, compliance violations, reputational damage, business disruptions, and increased costs.

When a vendor has access to UT System confidential information, it becomes vital to periodically monitor and review the vendor's ongoing information security practices. Such reviews can help ensure, during the contract term, that the vendors have policies, procedures, and practices in place to safeguard sensitive information, to mitigate risks of breaches and potential financial or reputational damage, and to operate in compliance with regulations like HIPAA. They can also demonstrate due diligence and provide information regarding the extent to which the vendor is keeping up with evolving cyber threats. The extent of such reviews should be risk based, consider other information security review activities in place, and when appropriate, be included as part of a contract monitoring plan.

Of the four contracts reviewed, there were two where the third-party vendor would have access to faculty, staff, or student confidential information, including protected health information. For one monitoring plan, the vendor is to immediately notify the department contract manager of any data security issues. However, the monitoring plan does not describe the monitoring activities that the department or the department's contract manager would do with respect to monitoring the vendor's information security practices or controls. For the other vendor, there is no reference to any monitoring of the vendor's information security practices or controls.

When applicable, monitoring a vendor's information security practices or controls can be a helpful part of UT System's overall information security strategy. Such monitoring can help the department ensure that the vendor is taking adequate steps in protecting confidential data, complying with regulations, maintaining trust, and ensuring business continuity in a challenging cyber environment.

ACTION PLAN

We agree. The same ad hoc working group described above will also analyze current procedures with the ISO group to ensure established processes are in place. These procedures will outline a process the departments will use to monitor a vendor's information security practices and controls. This will help ensure vendors have taken adequate steps to protect confidentiality of our data and to comply with applicable regulations.

Anticipated Implementation Date: August 31, 2025

OBSERVATION 5
Low

Provide Additional Training and Centralized Documented Guidance and Consider Mandatory Training for New DCAs

Without initial training and training targeted at addressing department needs, there is a risk that contract monitoring processes are not fully understood and requirements not followed. Without documented procedures or cross training, changes in department staff could become challenging, resulting in time-consuming efforts to reestablish effective and efficient business processes.

CnP periodically provides training for the Departmental Contract Administrators (DCAs). Within the two-year audit scope, CnP conducted three training sessions. However, CnP did not maintain an up-to-date listing of DCAs or track who attended the training. Consequently, DCAs may not be sufficiently aware of their contract monitoring responsibilities or CnP resources available to them. While training for personnel involved with contract monitoring is not required by the UT System Contract Management Handbook, it is encouraged in Section 1.4, Training for Purchasing Personnel and Contract Managers. It is also considered a best practice in Appendix 1, Contract Management Best Practices Matrix. CnP should consider requiring mandatory training for new DCAs to ensure they have been properly trained.

During the audit, we interviewed a sample of nine departments, including their DCAs. Those interviewed indicated that the training provided by CnP was useful but suggested more frequent training, additional monitoring tools, and centralized documented guidance. Specifically, the DCAs indicated that further training and centralized documented guidance could be helpful in the following areas: (1) information technology purchases requiring OTIS approval, (2) completing the ISOTRAQ assessments, (3) tailored guidance for unique contracts, and (4) tips for new DCAs. Additionally, one DCA expressed that it would be helpful to have a DCA community where questions and ideas could be shared. While CnP created a DCA Teams site in February 2024, the site is not actively being utilized to share information with the DCAs. Currently, training materials, monitoring tools, and applicable contract forms may be found on CnP's website, CnP's SharePoint site, or the DCA Teams site, but there is no central location for all presentations and documentation.

In addition, we found that the departments do not have their own documented procedures for contract monitoring processes and several departments do not have a backup DCA. Documented procedures ensure consistency in tasks, facilitate training for new employees, improve productivity, reduce reliance on a single individual within a department, and preserve knowledge within the department.

ACTION PLAN

We agree. We identified a contract management gap across the University of Texas System Administration's 32 departments two years ago and created the DCA role to assist with each respective department's contract management responsibilities. A DCA training roadmap was developed that identified training opportunities, including an initial 4-hour workshop that established core job expectations of the DCA role. Numerous DCA training sessions have been held since then with a commitment to conduct annual DCA training sessions for all DCAs. However, there is room for improvement in DCA training and robust utilization of the DCA Teams. A commitment to monthly 'office hours' for DCAs will be implemented in the summer of 2025. Providing consistent, quality annual DCA training for all departments will continue to be a focus for CnP. (Upcoming DCA training is in May 2025.) Additionally, CnP is updating the CnP website with Resources and Tools for the DCAs, including workflow processes. Training videos will be available in the future with the new and improved CnP website. Furthermore, CnP will explore development of a policy that will require all DCAs who work on contracts 50% or more as part of their job responsibilities, including managing complex contracts over $5 million, to become Certified Texas Contract Managers (CTCM).

Anticipated Implementation Date: August 31, 2026

METHODOLOGY

The System Audit Office conducted this engagement in accordance with the 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

Active contracts between September 1, 2022, and August 31, 2024, excluding memoranda of understanding (MOUs) with other institutions and construction contracts for major capital construction.

Procedures performed included interviewing nine departments regarding their departmental contract monitoring processes, examining the monitoring efforts for four high-risk contracts, and reviewing centralized training and guidance. Audit procedures were conducted between September 2024 and February 2025.

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

- UT System Contract Management Handbook (August 2022)
- UT System Office of Contracts and Procurement's Contracting Procedures, 3.8 Contract Monitoring
- UT System Contract Management Best Practices Matrix
- UTS 165.1, *Information Security Organization, Personnel & Privacy Policy*
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), *Covered Entities and Business Associates*

REPORT DATE

May 1, 2025

REPORT DISTRIBUTION

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