Office of Internal Audit

UT Southwestern
Medical Center

Third Party Vendor Relationships Audit

Internal Audit Report 19:16

September 30, 2019

Table of Contents

Executive Summary

Background

The University of Texas Southwestern Medical Center (UT Southwestern) uses third party vendors to perform a variety of services for the institution. A third party vendor relationship is any business arrangement between organizations typically governed by a contract executed with both parties. A third party vendor may provide organizations a variety of services that may be cost beneficial to outsource or the third party may provide specialty services and/or expertise such as an information technology (IT) related service.

For services provided by a third party, it is critical to have careful management of vendor relationships to help ensure the following: vendor services benefit the institution; compliance with the contractual agreement; processes and controls are in place to mitigate reputational, compliance and financial risks; and payments to vendors are accurate and are for services provided. For IT-related services, particularly when the vendor is storing or processing the institution's data, on-going evaluation and monitoring is critical to verify the vendor's access to data is appropriate and verify the vendor maintains adequate controls for protecting the institution's data from possible security breaches and ensuring the confidentiality, integrity and availability of the institution's data.

Currently, third party vendor contract management is decentralized across UT Southwestern. The Contracts Management team ensures executed contracts include key provisions that protect UT Southwestern interests and property. Responsibility for monitoring key contract terms and third party vendor performance and compliance is the responsibility of department leaders who enter into vendor agreements.

Scope and Objectives

The Office of Internal Audit has completed its Third Party Vendor Relationships Audit. This is a recurring, risk-based audit to perform a comprehensive review of third party vendor contracts and was part of the fiscal year 2019 Audit Plan. This year's audit focused on the institution's contractual arrangements and monitoring processes for third party vendors providing IT-related services, specifically for software applications managed by Information Resources. The audit scope was fiscal year 2019 and included interviews with contract owners and their team members; reviews of the contracts, policies and procedures and other pertinent documentation; analysis and testing of invoices and payments to third party vendors; and evaluation of system data.

The primary objectives of the audit were to assess the adequacy and effectiveness of oversight and monitoring processes and controls. Specifically for:

- Appropriate invoice approving and processing based on contract terms
- Appropriate monitoring of contract compliance and payments to contract terms
- Effective and efficient use and resourcing of system tools
- Appropriate system data access and security

We conducted our audit according to guidelines set forth by the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

Executive Summary

Conclusion

Overall, the controls and processes for managing third party vendor relationship are effective. There are opportunities to enhance institutional oversight of IT-related third-party vendor management services that include: (1) re-evaluating and updating procedures for monitoring vendors that store or process the institution's data and (2) implementing ongoing tracking of contract-specific requirements to obtain assurance that vendor systems are adequate and proper measures are in place to protect system data.

Additionally, the Supply Chain team implemented the processing of vendor service contracts as purchase orders within PeopleSoft. This aids in preventing paying invoices with charges higher than purchase order amounts; however, opportunities exist to improve processes that allow departments to confirm purchase order spend ties to the associated contract.

The table below summarizes the observations and the respective disposition of these observations within the UT Southwestern internal audit risk definition and classification process. See Appendix A for Risk Rating Classifications and Definitions.

Priority (0)	High (0)	Medium (3)	Low (0)	Total (3)

Strengths identified during the audit include:

- The Information System Acquisition Committee (ISAC) performs an assessment to review and approve requests for IT-related services prior to contracting with vendors. Additionally, a third-party service provider performs security assessments for the initial vendor risk assessment and provides ongoing monitoring of selected vendors hosting the institution's data.
- Supply Chain Management implemented a new Total Contract Management system (TCM) at the beginning of FY2019 to improve workflow for monitoring contract renewals and key terms including valid certificates of insurance and completion of background checks upon contract execution.
- In conjunction with the TCM implementation was the creation of a contract checklist that provides the Contracts Management team and contract owners clearly defined expectations, roles, and responsibilities.

Executive Summary

Key improvement opportunities are summarized below.

● **1. Enhance Third Party Data Processing Controls Oversight** – Procedures are inconsistent for obtaining or reviewing a System and Organization Controls (SOC) report or other third-party review report for detailing an independent evaluation of controls in place that process and store UT Southwestern data. This increases the risk of non-compliance with Standard 22 of UT System Policy 165 *Information Resources Use and Security (UTS165)*.

● **2. Enhance Third Party Key IT Contract Provisions Monitoring** – Institutional standardized procedures that require adequate monitoring are either not in place or are not performing as intended, which increases the risk of vendor noncompliance with key IT contract terms and the risk of this noncompliance going undetected. In addition, automated flags/reminders are not in place in the Total Contracts Management (TCM) system to ensure departments are aware and can follow up with vendors to verify compliance with key contract provisions.

● **3. Improve Monitoring of Contract Total Spend to Purchase Orders** – Total contract spending limits are unmonitored to ensure contract maximums are not exceeded. This increases the risk payments could be made in excess of contract maximums and not identified prior to payment. Additionally, reported spend amounts within PeopleSoft Accounts Payable (AP) and TCM are not the same and could mislead the department contract owner of the remaining available spend per the contract terms.

Management has implemented or is implementing corrective action plans. Management responses are presented in the Detailed Observations and Action Plans Matrix section of this report.

We would like to thank the Supply Chain, Contracts Management, Accounts Payable and Information Resources departments for their assistance and cooperation during this audit.

Sincerely,

Valla Wilson, Vice President for Internal Audit, Chief Audit Executive

Audit Team:
Melinda Lokey, Director, Internal Audit
Jeffrey Kromer, Director, IT & Specialty Audit Services, Internal Audit
Robin Irvin, Manager, Internal Audit
Angeliki Marko, Supervisor, Internal Audit
Delaunda McCown, Senior Internal Auditor, Internal Audit
Gabriel Samuel, Supervisor, Internal Audit

Executive Summary

cc: Charles Cobb, Associate Vice President, Supply Chain Management
Shawn Cohenour, Director, Contracts Management
Sharon Corcoran, Director, General Accounting
Arnim E. Dontes, Executive Vice President, Business Affairs
Kathryn Flores, Assistant Vice President & Chief Information Officer, University Hospitals
Sharon Leary, Assistant Vice President, Accounting & Fiscal Services
Marc E. Milstein, Vice President & Chief Information Officer, Information Resources
Adolfo Ortuzar, Director, Academic & Administrative IR Operations
Mark Rauschuber, Associate Vice President & Chief Information Officer, Health System, IR Health Systems
Nathan Routen, Information Security Architect & Interim Chief Information Security Officer
Michael Serber, Vice President, Finance & Institutional Chief Financial Officer
Joshua Spencer, Associate Vice President & Chief Technology Officer
Thomas Spencer, Ph.D., Assistant Vice President, IR Operations and Compliance, Academic and Administrative Information Resources
Jarrod Tallman, Director, Purchasing
Elyse Willen, Director, Strategic Sourcing

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium ● **1. Enhance Third Party Data Processing Controls Oversight** Procedures are inconsistent for obtaining or reviewing a System and Organization Controls (SOC) report or other third-party review report for detailing an independent evaluation of controls in place for vendors who process or store UT Southwestern data. This increases the risk of noncompliance with Standard 22 of UT System Policy 165 *Information Resources Use and Security (UTS165)*. The Information System Acquisition Committee (ISAC) performs an assessment to review and approve requests for IT-related services prior to contracting with vendors. Additionally, a third-party service provider is performing security assessments for the initial vendor risk assessment prior to signing a contract and for ongoing monitoring of selected vendors hosting the institution's data. However, unlike a SOC report, this service focuses on security without inclusion of other important controls such as backup, change management, disaster recovery and an independent verification that an assessed vendor's controls are effective. Standard 22 "Vendor and Third-Party Controls and Compliance" of UTS165 requires the institution to obtain copies of any self-assessments or third-party vendor assessments the vendor has access to and also ensure such outsourced services are compliant with the standard at all times.	1. Re-evaluate existing procedures that oversee vendors who process or store UT Southwestern data to identify any necessary enhancements to controls that protect the institution's data. At a minimum, include (1) evaluating vendor risk assessment procedures, (2) implementing a process for periodically obtaining and reviewing SOC reports or other third-party review reports for vendors hosting the institution's data, and (3) use of a risk-based approach to identify the most critical data hosting arrangements to review. 2. Ensure review of SOC or other third-party reports includes (1) verifying the vendor has adequately addressed any deficiencies identified in the report and (2) verifying the institution has procedures in place for any reported controls the institution is responsible (e.g., User Control Considerations). 3. Establish a Contracts Management and Information Resources coordinating effort that ensures contract language is included in all contracts where the vendor is hosting the institution's data to (1) require the vendor to periodically provide SOC reports or other third party review reports, and (2) ensure the institution has a right to audit the vendor's data processing controls.	**Management Action Plans:** 1. a. We will re-evaluate to assess the risks and identify the best options for reviewing third party vendors. b. Once the assessment is completed, we will implement any changes accordingly. Additional resources may be required. 2. We will develop procedures that ensure sufficient review of SOC or other third-party reports when available. When not available, this will be a consideration in the overall risk assessment. 3. We will establish a Contract Management and Information Resources coordinated effort for revising the RFP language and information submission requirements, as well as contract language for IT contracts. **Action Plan Owners:** Director, Contracts Management Director, Strategic Sourcing Information Security Architect & Interim Chief Information Security Officer **Target Completion Dates:** 1. a. November 30, 2019 b. December 31, 2019 2. December 31, 2019 3. December 31, 2019

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium ● **2. Enhance Third Party Key IT Contract Provisions Monitoring** Compliance with third party key information technology (IT) contract terms is the responsibility of department leaders who enter into vendor agreements. Institutional standardized procedures that require adequate monitoring are either not in place or are not performing as intended, which increases the risk of vendor noncompliance with key IT contract terms and the risk of this noncompliance going undetected. In addition, automated flags/reminders are not in place in the Total Contracts Management (TCM) system to ensure departments are aware and can follow up with vendors to verify compliance with key contract provisions.	1. Develop standardized monitoring procedures for key IT contract provisions and communicate responsibilities to department leaders. 2. Develop automated flags/reminders in the Total Contracts Management system to facilitate reporting to responsible departments of key contract provisions requiring follow up with the vendor to ensure the vendor is in compliance.	**Management Action Plans:** 1. Based on the ISAC approval, a list of key terms will be included in the approval form. The contract will incorporate the list of items needed. 2. We will identify methods to utilize current functionality in TCM or through contract management monitoring procedures to ensure vendor compliance. **Action Plan Owners:** Director, Contracts Management Director, Strategic Sourcing Information Security Architect & Interim Chief Information Security Officer **Target Completion Dates:** 1. December 31, 2019 2. December 31, 2019

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium ● **3. Improve Monitoring of Contract Total Spend to Purchase Orders** Total contract spending limits are unmonitored to ensure contract maximums are not exceeded. Purchase order(s) are created when contracts are executed; however, the purchase orders do not directly reference the applicable contract number in TCM or the total contract maximum spend for tracking. This increases the risk that payments could be made in excess of contract maximums and not identified prior to payment. Additionally, reported spend amounts within PeopleSoft Accounts Payable (AP) and TCM are not the same and could mislead the department contract owner of the remaining available spend per the contract terms. A comparison of TCM spend and the AP spend amounts by vendor during fiscal year 2019 identified multiple contracts in TCM and multiple purchase orders that could not be tied to the appropriate contract for monitoring. Without clear comparison of contracts and spend via purchase orders the risk of overpayments and inaccurate data increases.	1. Develop processes to tie contractual spend to Purchase Orders for each contract to effectively monitor compliance with spending provisions and limits. 2. Implement monitoring processes to notify department leaders when spending provisions and limits are nearing contract maximums.	**Management Action Plans:** 1. We will require PO Requesters to provide contract ID numbers on all purchase requisitions. In addition, Buyers will confirm required information was included. In TCM, Contract Managers will ensure budget limits have been established for the contract. Prior to the latest upgrade, many POs were created in PeopleSoft that did not have the ability to link back to the TCM contract. With the Jaggaer Optimization, this has been remediated. The only POs that can now be created in Peoplesoft are for Inventory and PAR replenishment. 2. Contract Managers will set notifications within TCM for the contract stakeholders when contracts are nearing a specified percentage of the budget or total amount allowed. **Action Plan Owners:** Director, Contracts Management Director, Purchasing **Target Completion Dates:** 1. Completed 2. Completed

Appendix A – Risk Classifications and Definitions

As you review each observation within the Detailed Observations and Action Plans Matrix of this report, please note that we have included a color-coded depiction as to the perceived degree of risk represented by each of the observations identified during our review. The following chart is intended to provide information with respect to the applicable definitions and terms utilized as part of our risk ranking process:

Risk Definition - The degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management.	**Degree of Risk and Priority of Action**	
	🟥 **Priority**	An issue identified by internal audit that, if not addressed immediately, has a high probability to 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 that is considered to have a high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level. As such, immediate action is required by management in order to address the noted concern and reduce risks to the organization.
	🟨 **Medium**	A finding identified by internal audit that is considered to have a medium probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level. As such, action is needed by management in order to address the noted concern and reduce risk to a more desirable level.
	🟩 **Low**	A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level. As such, action should be taken by management to address the noted concern and reduce risks to the organization.

It is important to note that considerable professional judgment is required in determining the overall ratings presented on the preceding pages of this report. Accordingly, others could evaluate the results differently and draw different conclusions. It is also important to note that this report provides management with information about the condition of risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.