UT Health
San Antonio
Internal Audit &
Consulting Services

Internal Audit & Consulting Services
7703 Floyd Curl Dr. MC#7974
San Antonio, Texas 78229-3900
210-567-2370 Fax: 210-567-2373
www.uthscsa.edu

Date: June 27, 2024

To: Yeman Collier, VP & Chief Information Officer
Todd Holling, Deputy Chief Information Officer
Michael Schnabel, Assistant VP, Info Sec & Ops

From: John Lazarine, Chief Audit Executive
Internal Audit & Consulting

Subject: Audit Report – *Audit of Third-party Security Governance and Access Management*

As part of our FY 2024 Audit Plan, we completed an audit of *Third-party Security Governance and Access Management*. The report detailing the results of this review is attached. Management's Action Plans are included in the section "Detailed Audit Findings" of the report.

We appreciate the cooperation and assistance we received from Governance, Risk, and Compliance and its staff throughout the review.

Respectfully,

John Lazarine, CIA, CISA, CRISC
Chief Audit Executive
Internal Audit & Consulting Services

Distribution:

cc: Dr. Robert Hromas, Acting President and Dean of Medical School
Andrea Marks, Senior Executive Vice President and Chief Operating Officer
Stephen Hargrove, Info Sec & Assurance Manager
Becki Gerwitz, Info Sec & Assurance Manager
J. Michael Peppers, Chief Audit Executive, UT System

External Audit Committee Members:
Randy Cain
Carol Severyn
Ed Garza

INTERNAL AUDIT REPORT

THIRD-PARTY SECURITY GOVERNANCE & ACCESS MANAGEMENT

June 27, 2024| Report No. 24-08

UT Health
San Antonio
Internal Audit &
Consulting Services

Executive Summary

Background Information

UT Health San Antonio (UTHSA) Internal Audit and Consulting Services conducted a Third-Party Security Governance and Access Management audit as part of their Fiscal Year 2024 plan. UTHSA relies on third-party vendors and service providers for various functions to increase efficiency, productivity, and resource flexibility. However, these relationships pose risks that must be monitored and managed to achieve desired outcomes. The audit aimed to ensure that third-party risk exposures are managed according to the organization's risk management framework. These risks include financial, compliance, reputational, and cyber risks.

Objective & Scope

The purpose of this audit was to evaluate the effectiveness of UTHSA's controls and processes for managing third-party access to its systems and data. It ensured that third parties had suitable access levels based on their roles and that access was granted and revoked on time.

The audit period covered July 2023 through February 2024. The scope included an assessment of these control domains: governance, acquisition, access management, monitoring, data security, integrity, and compliance.

Summary of Results

This audit evaluated the effectiveness of third-party security governance and access management within our institution. The assessment focused on security controls, access management practices, risk management frameworks, and compliance measures employed by third-party vendors and service providers.
Below is a summary of the strengths and opportunities identified during the assessment completed.

Key Findings:

Strengths:

- When third-party vendors and service providers are onboarded, the Governance Risk and Compliance (GRC) team conducts regular risk assessments to identify and mitigate potential security threats.
- High levels of compliance with key regulations such as TX-RAMP were observed among the vendors.
- Third-party vendors and service providers undergo electronic information resources (EIR) checks for accessibility requirements and health IT checks for HIPAA-related rules, when applicable.

- The purchasing department notifies third-party vendors and service providers of their agreement ending and inquiries about renewal options.

Opportunities:

- There is no process for periodic re-assessment of risks associated with the third-party vendor and ensuring compliance with security requirements, which could lead to non-compliance with legal and regulatory requirements. This includes evaluating the SOC 2 Type 2 report based on the period covered from when the initial risk assessment was completed.
- There is no system-generated report to validate the completeness and accuracy of third-party vendors. This can lead to the institution inadvertently omitting third-party vendors/applications, thus exposing the system and data to security threats.
- There is no monitoring control designed to detect changes made to the configured Data Loss Prevention (DLP) policy. Thus, unauthorized changes to the DLP policies could lead to intentional or unintentional download of sensitive data (PII, PHI).
- There are no preventive measures in place to restrict an authorized user from downloading sensitive data via a USB port.
- There is no adequate process to ensure that third-party vendor access is terminated when the contract reaches the end of its life. Also, no dedicated individual is representing each department responsible for the third-party service provided to take responsibility for monitoring the contract's end-of-life to system data access. It is crucial that a more formalized and structured process to address these issues is established.
- Inadequate retention of the third-party risk assessment documents negatively impacts the institution’s ability to determine adequate security and protection for UTHSA’s data.

Summary of Management's Response

Internal Audit made recommendations to address the issues identified during this audit. These recommendations are provided at the end of each section in this report. The process owners agreed with the recommendations and have provided action plans to implement them.

Ratings Definitions

Internal Audit used professional judgment and rated the audit findings identified in this report. The issue ratings identified for each chapter were determined based on the degree of risk or effect of the findings with the audit objectives.

PRIORITY - An issue identified by Internal Audit that, if not addressed immediately, has a high probability of directly impacting the 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 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, management needs to take action to address the noted concern and reduce risks 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.

Satisfactory – No reportable findings or observations were identified during the audit.

For more on the methodology for issue ratings, see Report Ratings in Appendix 1.

Detailed Audit Findings

HIGH **Acquisition**

Control: A control process is established to maintain an inventory of all third-party vendors, ensuring that the university knows the location of all its data, systems, and potential exposure points.

Observation #1: Through inquiry with the purchasing department's management, it was noted that not all vendors have contracts signed, as some issue Purchasing Orders that do not require signing a contract. As such, the total contract management tool (TCM) does not include all the third-party vendor listings. This can lead to the institution inadvertently omitting third-party vendors/applications from the security review process, thus exposing the system and data to security threats.

Recommendation #1:
(a) Put in place an inventory listing of all third-party vendors
(b) Ensure there is a process to update the inventory to validate the completeness and accuracy of third-party vendors.
(c) Assign a designated person within each department to oversee the third-party vendor inventory and collaborate with the purchasing department and GRC.
(d) Ensure periodic review of the third-party vendor inventory listing to validate its completeness and accuracy.

Management's Response: The Governance, Risk and Compliance department (GRC) is developing a procurement process that aims to address this issue by including third-party vendors in the TeamDynamix database, allowing for easy querying to obtain an inventory listing. The overall process on updating the database and assigning a designated person will be properly reviewed upon implementation of the new procurement process.

Becki Gerwitz and Stephen Hargrove, Infosec and Assurance Managers, are responsible for implementation with a completion date of 9/1/2024.

Remediation Status: In progress.

HIGH **Monitoring**

Control: The enterprise completely and accurately defines minimum monitoring and management of third-party vendors activities (activities are itemized and ownership documented for proper review and analysis). Monitoring may include certain types of events such as source of event, account-making changes, date/time of events.

Observation #2: There is no monitoring control designed to detect changes made to the enabled Data Loss Prevention (DLP) policy configuration.

Recommendation #2: Implement a monitoring process/procedure to prevent unauthorized changes to the DLP policies in Microsoft Purview. This should include:
(a) A defined frequency for reviewing activities.
(b) Ensuring activities are itemized.
(c) Ownership documented for proper review and analysis. Monitoring may include certain types of events such as the source of the event, account-making changes, and date/time of events.
(d) Tie each change activity to a change document to validate authorization of the change.

Management's Response:
(1) Management will develop a process that includes:
   (a) Create search criteria for the DLP change activities to be captured in the audit log.

   (b) Review the system generated DLP change activities audit log every two months to determine whether an unauthorized change was made.
   (c) Ensure an appropriate authorization of the review is captured.

(2) Management to develop an automation process for the DLP change activity for the future.

Joel Gallegos, IT Systems Architect, is responsible for implementation with an estimated completion date of 8/31/2024.

Remediation Status: (1) Completed (2) In progress.

Observation #3: No preventive measures are in place to restrict an authorized user from downloading sensitive data via a USB port.

Recommendation #3: Establish a monitoring process/procedure to prevent unauthorized access to sensitive data through download to a USB. This should include: (a) A policy/procedure developed to ensure data protection through download(b) Evidence of configuration of data protection through download.

Management's Response: The Office of the Chief Information Security Officer will conduct an assessment to determine the scope of policy and technology procurement to enforce the control and impact of associated configurations. Following this assessment, an implementation plan, including a timeline, policy adoption, and communication plan, will be developed.

Michael Schnabel, Chief Information Security Officer is responsible for implementation with an estimated completion date of 10/31/2024.

Remediation Status: In progress.

HIGH

Access Management

Control: The organization implements a comprehensive offboarding process for third-party vendors, which includes the following steps: notification, data and asset retrieval, contractual obligations, access revocation, transition planning, documentation and audit, feedback, and lessons learned.

Observation #4: When contract end-of-life is reached, there is no periodic monitoring process to ensure the third-party vendor access is revoked to ensure that they do not inappropriately access UTHSA's sensitive data (PHI, PII, HIPPA). This need for a structured process is a significant gap in our data security measures. Although the Contract Specialist performs an informal monthly review of the contract's end of life to determine when a contract renewal is needed, the process is informal as there is no retention of evidence of the review performed for consistency and continuity purposes. The process is not adequate to ensure that third-party vendor access is terminated when the contract reaches the end of its life. Also, no dedicated individual is representing each department responsible for the third-party service provided to take responsibility for monitoring the contract's end-of-life with respect to system data access. It is crucial that we establish a more formalized and structured process to address these issues.

Recommendation #4:
1. Identify the departmental individual responsible for monitoring third-party vendor contracts.
2. Ensure adequate communication and a mechanism are put in place between the contract specialist and the responsible departmental individual to ensure smooth completion of a third-party vendor contract from the beginning to the end of life. The Identified individual responsible for the contract should ensure a periodic review is performed to determine whether access to data is terminated promptly by the end of the contract.
3. Ensure there is a formal periodic review of the contracts.

Management's Response: GRC will modify third-party risk management procedures to include an annual review of the university's contract portfolio. Upon notification of contract termination by Procurement, the university's designated Contract Administrator, the responsible department head, or Office of General Counsel, GRC will assess and validate the termination of the third-party's access to university resources, recovery of any university assets in possession of the third-party, and data repatriation (if in scope of the third-party service).

Michael Schnabel, Chief Information Security Officer is responsible for implementation with an estimated completion date of 10/31/2024.

Remediation Status: In progress.

MEDIUM

Governance

Control: The organization implements mechanisms to identify all third-party vendors and ensures their active participation and adherence to policies and procedures addressing contractual agreements, including the Processing of Software and IT Service Transactions form (PSST), the right to audit, and insurance coverage.

Observation #5: There is no process for periodic re-assessment of risks associated with the third-party vendor during the life of the contract and ensuring compliance with security requirements. This includes evaluating the SOC 2 Type 2 report based on the period covered.

Recommendation #5: Formally implement a re-assessment of risks associated with the third-party vendor. This should include:
(a) To ensure compliance with security requirements, third-party vendor risk assessments need to be retroactively reviewed.
(b) Define the frequency of the periodic re-assessment of risks associated with the third-party vendor.

Management's Response: (1) Third-party risk management procedures will be updated to reflect the procedure for re-assessing the vendor's control responses and validating gaps based on the classification of the vendor's risk to university operations, data sensitivity and/or laws/regulations that may increase the sensitivity of the product or services provided by the third-party. Critical risk classified vendors will be re-assessed on an annual basis; Low to Medium risk classified vendors will be re-assessed upon contract renewal or every 3 years whichever is sooner.

(2) The university's contract portfolio will be assessed to identify third parties who may be classified as critical to university operations, data sensitivity, and/or laws/regulations that may increase the sensitivity of the product/services provided by third-party. "Critical" rated third parties will be re-assessed to validate their control responses and validate its risk profile.

Michael Schnabel, Chief Information Security Officer is responsible for implementation with an estimated completion date of 8/30/2024 for management's response (1) and 12/31/2024 for management's response (2).

Remediation Status: In progress.

MEDIUM

Data Security and Integrity

Control: The organization conducts assessments to determine whether cloud services support data classification and encryption requirements.

Observation #6: As indicated in the PSST form, the risk assessment documentation was not retained for 1 of 25 sampled vendors with access to data related to FERPA, PII, credit card information, and data stored in the vendor server/data center to determine whether the assessment was completed appropriately.

Due to the inability to review the risk assessment document and ensure encryption capabilities were identified, we could not determine whether there is adequate security and protection for UTHSA data. This underscores the need for immediate action to address this gap in our security assessment process.

Recommendation #6: 1. Risk assessment is performed for every third-party vendor and documentation is retained.

Management's Response: The Governance, Risk and Compliance department (GRC) is developing a procurement process that addresses this issue by including each risk assessment portion in separate fields of the TeamDynamix database, allowing for easy querying to obtain the information needed. Although the new process will not include historical information, it will help identify risks from third parties by listing the third parties working with confidential data.

Becki Gerwitz and Stephen Hargrove, Infosec and Assurance Managers, are responsible for implementation with an estimated completion date of 9/1/2024.

Remediation Status: In progress.

The following members of the Internal Audit & Consulting Service's staff performed the audit:

- Sam Babajide, MSEM, CISA, CIPT, CPSP, ITIL (IT Audit Director)
- Wumi Awotoye, MBA, CISA, CPA (IT Audit Senior)

APPROVED FOR RELEASE

John Lazarine

John Lazarine, Chief Audit Executive, Internal Audit & Consulting Services

APPENDICES

Appendix 1

Criteria

The audit was intended to meet the TAC 202[1] biennial review, as the State of Texas and UT System Administration required.

Texas Administrative Code Chapter 202 (TAC §202) outlines the minimum information security and cybersecurity responsibilities and roles at state agencies and institutions of higher education. TAC §202 requires agencies and institutions of higher education to use the TAC §202 Security Controls Standards Catalog (SCSC). The security controls catalog is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, R5. Other frameworks used are the Control Objectives for Information and Related Technologies (COBIT) and the Center of Internet Security (CIS – IT related). Using a centrally managed controls catalog effectively ensures that all agencies and institutions use common language and minimum standards when implementing security measures.

Methodology

We conducted this performance audit from July 2023 through February 2024 in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. 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 based on our audit objectives.

Report Ratings

In determining the ratings of audit findings, auditors considered factors such as financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Internal Audit also identified and considered other factors when appropriate.

[1] *Texas Administrative Code Chapter 202 (TAC §202), RULE §202.76 (c) A review of the institution's information security program for compliance with these standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the institution of higher education head or his or her designated representative(s).*

Distribution List

Copies of this report have been distributed to the following:

- Dr. Robert Hromas, Acting President
- Andrea Marks, Chief Operating Officer
- Yeman Collier, VP & Chief Information Officer
- Todd Holling, Deputy Chief Information Officer
- Michael Schnabel, Assistant VP, Info Sec & Ops
- Stephen Hargrove, Info Sec & Assurance Manager
- Becki Gerwitz, Info Sec & Assurance Manager
- J. Michael Peppers, Chief Audit Executive, UT System