The University of Texas Medical Branch
Audit Services

Audit Report

Third Party Risk Management

Engagement Number 2023-009

August 2023

The University of Texas Medical Branch
Audit Services
301 University Boulevard, Suite 4.100
Galveston, Texas 77555-0150

Third Party Risk Management Audit

Engagement Number: 2023-009

Background

Audit Services performed an audit of Third Party Risk Management as part of the fiscal year 2023 (FY23) audit plan. Effective January 2022, due to the passing of Senate Bill 475, the University of Texas Medical Branch (UTMB Health) was required to implement the rules and regulations of the Texas Risk and Authorization Management Program (TX-RAMP) as set forth by the Texas Government Code § 2054.0593 (The Code). The objective of The Code is to establish a state risk and authorization management program to provide a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency. The Code mandates state agencies enter or renew contracts to receive cloud computing services that comply with TX-RAMP requirements.

As part of the requirements, state agencies must take measures to assess vendors for appropriate security protocols to obtain a provisional certificate. Upon review, the vendor is entered into the Statewide Portal for Enterprise Cybersecurity Threat Risk and Incident Management (SPECTRIM) provided by the Texas Department of Information Resources (DIR) and assigned a Level 1 or Level 2 certification based on the confidentiality level of information being stored in the cloud environment. The SPECTRIM portal provides tools for managing and reporting security incidents, conducting risk assessments, storing, and managing organizational policies, performing assessments and authorizations on information systems, templates for agency security planning activities, and more. For UTMB Health, the Office of Information Security is the designated department to authorize access to the SPECTRIM portal.

Objective, Scope, and Methodology

Objective

The primary objective of this engagement was to confirm compliance with TX-RAMP and assess the effectiveness of the vetting and continuous monitoring controls in place for UTMB Health Sponsored TX-RAMP Vendors/Cloud Service Providers.

Scope of Work and Methodology

The scope of the engagement included assessing the internal controls related to TX-RAMP certification and current UTMB Health Sponsored TX-RAMP Vendors/Cloud Service Providers.

Specific methodologies included:

- Conducting interviews and walkthroughs with key personnel and gaining an understanding of processes, associated risks, and controls in place to comply with TX-RAMP.
- Evaluating the TX-RAMP manual to determine proper designation of certifications and verify the appropriateness of vendor security controls.

- Reviewing the DIR and SPECTRIM reports to cross reference information with UTMB Health's information to ensure correct documentation of vendors.
- Observing functionality of the SPECTRIM dashboard provided by DIR to gain an understanding of processes for entering and maintaining TX-RAMP sponsored vendors within the SPECTRIM portal.
- Reviewing evidence of current controls in place regarding expiring certifications and the process for the renewal of certifications.

Executive Summary

Audit Services confirmed UTMB Health's compliance with the TX-RAMP rules and regulations concerning vendor certifications and ongoing monitoring of sponsored TX-RAMP Vendors and Cloud Service Providers. Furthermore, we have identified opportunities to enhance internal controls by establishing comprehensive policies and procedures for vendor tracking, documentation maintenance, vulnerability reporting, recertification, and training.

Detailed Results

Departmental Policies and Procedures for TX-RAMP Vendors

The Texas Government Code 2054.0593 mandates that state agencies perform additional assessments, authorizations, and continuous monitoring for cloud service providers. As a result of this new mandate, the DIR has established the TX-RAMP Manual v2.0 and TX-RAMP Control Baselines 2.0 for state agencies as a guide in complying with this new mandate. Due to this newly established process, UTMB Health has not yet developed formal departmental policies and procedures regarding TX-RAMP vendor certifications to ensure appropriate controls related to certification designation, vulnerability reporting, monitoring and oversight, and renewal of TX-RAMP vendor certifications.

Recommendation 001 - Departmental Policies and Procedures for TX-RAMP Vendors:
The Office of Information Security should establish departmental policies and procedures to include, but not limited to, defining and communicating the following:

- Roles and responsibilities to ensure appropriate segregation of duties regarding certification designations.
- Acceptable security criteria for cloud computing services for maintaining TX-RAMP certification.
- Criteria for vendors who are TX-RAMP certified through another Risk and Authorization Management Program (i.e., FedRAMP or StateRAMP).
- Criteria for the continuous monitoring of TX-RAMP third party vendors.

Management's Response: The Office of Information Security leadership and appropriate staff will formalize the policies and procedures associated with the TX-RAMP process.

Responsible Party: John Flores, Interim Chief Information Security Officer

Implementation Date: March 29, 2024

Cross-Training

The Information Office of Information Security makes the determinations for certification levels regarding TX-RAMP certified vendors working with UTMB Health. There is currently one primary employee involved in reviewing requests, researching the vendor information, reviewing contracts and/or agreements, and determining certification levels. It would be highly beneficial for UTMB Health to consider cross training another employee to ensure the appropriate coverage and decision-making skills are established for determining certification levels in the event of an unexpected absence and/or loss of the employee.

Recommendation 002 – Cross Training:
The Office of Information Security should cross train employees to ensure UTMB Health has the appropriate coverage and decision-making skills needed in determining certification levels in the event of an unexpected absence and/or loss of the employee.

Management's Response: The Office of Information Security leadership and appropriate staff will work to document, formalize procedures, and job duties, responsibilities associated with the TX-RAMP process. The Office of Information Security leadership will identify and train additional staff to complete the documented duties.

Responsible Party: John Flores, Interim Chief Information Security Officer

Implementation Date: March 29, 2024

Independent TX-RAMP Vendor Listing to Ensure Accurate Tracking

The SPECTRIM portal currently utilized by UTMB Health's TX-RAMP subject matter expert stated that the tool can be unreliable at times, therefore it is recommended to establish and maintain an accurate inventory listing. UTMB Health currently relies on the SPECTRIM report to obtain UTMB Sponsored TX-RAMP Vendors/Cloud Service Provider information. In addition, UTMB Health relies on the DIR report to obtain out-of-scope Vendors/Cloud Service Provider information. However, The Office of Information Security leadership should maintain an independent consolidated and complete inventory listing of vendors subject to TX-RAMP certification to ensure accurate tracking, monitoring, and oversight.

Recommendation 003 – Independent TX-RAMP Vendor Listing:
The Office of Information Security should maintain an independent consolidated and complete inventory listing of vendors subject to TX-RAMP certification to ensure accurate tracking, monitoring, and oversight.

Management's Response: The Office of Information Security leadership and appropriate staff will maintain a list of all TXRAMP certified technologies and vendors and utilize a Ticketing System, Risk Register, and Inventory to track them.

Responsible Party: John Flores, Interim Chief Information Security Officer

Implementation Date: March 29, 2024

Oversight and Maintenance of TX-RAMP Documentation

Information Security utilizes the SPECTRIM and DIR reports to review cloud service provider information. Audit Services obtained and evaluated these reports to review vendor information and noted that these reports do not reflect vendors with a TX-RAMP interim provisional status. During the course of our fieldwork, we were advised the reports do not currently have the functionality to ensure all interim provisional status cloud service providers' information is reflected within the reports.

In addition, Information Security currently retains all TX-RAMP certification and related communications through email. Due to the incomplete reporting, it is imperative to establish a centralized repository for maintaining related TX-RAMP certification information for accessibility and institutional record keeping.

Recommendation 004 – Oversight and Maintenance of TX-RAMP Documentation:
The Office of Information Security should develop a process for storing and maintaining all TX-RAMP documentation within a centralized repository for accessibility and institutional record keeping.

Management's Response: The Office of Information Security leadership and appropriate staff will work to move the current email-based request process into our Ivanti ticketing system, this will allow for better tracking, service level agreements, documentation, and record keeping.

Responsible Party: John Flores, Interim Chief Information Security Officer

Implementation Date: March 29, 2024

Required TX-RAMP Vulnerability Reporting

The DIR requires that state agencies are responsible for reviewing the vulnerability reporting items on a quarterly basis for TX-RAMP Level Two - certified cloud computing services, and on an annual basis for TX-RAMP Level One - certified cloud computing services. Copies of the reports are uploaded within the SPECTRIM portal by the cloud service provider. However, there are no vulnerability reports that the TX-RAMP subject matter expert can access or review within the SPECTRIM portal. The subject matter expert has contacted DIR for more information; however, additional guidance has not been received. Furthermore, DIR states that it is the specific responsibility of the contracting state agency to access and review the information made available regarding a service within SPECTRIM or through another mechanism agreed upon by the vendor and the state agency.

Recommendation 005 – Required TX-RAMP Vulnerability Reporting:
The Office of Information Security should develop an alternate procedure for contacting the vendor to gain access and review vulnerability reports on their respective basis when they are not accessible within SPECTRIM, as required by TX-RAMP and to ensure UTMB is aware of exposures.

Management's Response: : The Office of Information Security leadership and appropriate staff will work to include additional verbiage in our vendor contracts to request vendors provide a vulnerability report for their supported or hosted systems and applications and provide a point of contact to produce these reports upon request. The frequency and details of the reports will be determined by the Office of Information Security leadership and based off TXRAMP requirements

Responsible Party: John Flores, Interim Chief Information Security Officer

Implementation Date: March 29, 2024

Recertification Responsibilities

TX-RAMP recertification requires the cloud service provider to review and update control implementation details as necessary and provide updated documentation to DIR for review. The identified points of contact for TX-RAMP certified cloud computing services will be notified by automated email at least 12 months and six months prior to the certification end date. The request to initiate the recertification process may be made by the cloud service provider up to 12 months prior to the certification end date.

While the cloud service provider is responsible for the recertification process, Information Security has not established a process regarding certifications that are nearing their expiration

date. Additionally, during the engagement it was communicated by the TX-RAMP subject matter expert that this responsibility is expected to be maintained by the respective department working with the cloud service provider. However, this expectation has not been communicated or formally established with the departments.

Recommendation 006 – Recertification Responsibilities:
The Office of Information Security should develop a process that defines the responsible party for monitoring TX-RAMP vendor renewals to ensure UTMB Health is not collaborating with noncompliant vendors whose certification has expired.

Management's Response: The Office of Information Security leadership and appropriate staff will work to develop communication templates and notifications, alerting the Office of Information Security, and vendors of recertification dates and TXRAMP certification expiry. Additionally, the Office of Information Security will review and amend vendor contract language, requiring that vendors pursue recertification if their certification expires during an active contract.

Responsible Party: John Flores, Interim Chief Information Security Officer

Implementation Date: March 29, 2024

Conclusion

We would like to thank the Office of Information Security staff and management who assisted us during the review.

This audit was conducted in conformance with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. Additionally, we conducted the audit in accordance with Generally Accepted Government Auditing Standards. Those 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 on our audit objectives.

Desolyn Foy, CPA, CIA, MHA, ACDA
Vice President and Chief Audit Executive

W. Nathaniel Gruesen, MBA, CIA, CISA, CFE
Director, Audit Services