UTSouthwestern Medical Center™

Office of Institutional Compliance and Audit Services

TX-RAMP Compliance Assessment

Internal Audit Report 24:19

October 31, 2024

Executive Summary

As an entity of the state of Texas, UT Southwestern is required to adhere to the Texas Department of Information Resources (DIR) Texas Risk and Authorization Management Program (TX-RAMP), which was established to provide a standardized approach for security assessment, certification, and continuous monitoring of cloud computing services that process the data of Texas state agencies. State agencies must only enter or renew contracts to receive cloud computing services that comply with TX-RAMP requirements beginning January 1, 2022. TX-RAMP certification requirements apply to all contracts for cloud computing services entered or renewed on or after that date.

This review focused on the processes in place to determine how TX-RAMP requirements are being met by assessing the vendor intake and review process, contracting terms added to sampled agreements, and tracking of compliance activities to demonstrate the program.

Engagement Results

The Office of Institutional Compliance & Audit Services (OICAS) conducted an assessment of the processes used by the Information Security and Contracts Management departments to identify cloud computing service providers and submit and track compliance with TX-RAMP certification levels appropriate for the services provided to UT Southwestern.

Overall, OICAS recognized multiple strengths for the processes including coordination between the Contracts Management and Information Security departments within the Information Systems Acquisition Committee (ISAC), a thorough investigation process with each vendor to determine if TX-RAMP is required, and documentation of the contract language added or refused in vendor contracts.

It is important to note that the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM), managed by Texas DIR, is adding functionality to enable continuous monitoring of TX-RAMP certifications. However, the portal is not currently functioning at its full capacity, which puts additional burden and requirements on UT Southwestern to track these details on their own. While the program appears to be operating despite the lack of supporting resources from the DIR, a number of program improvements were identified that management should consider to strengthen the compliance posture.

A summary of observations is outlined below:

AREA	OPPORTUNITIES	RISK RATING
Information Security TX-RAMP Certification Decision Matrix	• TX-RAMP Certification Decision Matrix • Examples of Completed Decision Matrix	**LOW**

TX-RAMP Compliance Tracking	• Reporting for compliance	**LOW**

Further details are outlined in the Detailed Observations section. Less significant issues were communicated to management.

Management Summary Response

Management agrees with the observations and recommendations and has developed action plans to be implemented on or before February 28, 2025.

Appendix A outlines the objectives, scope, methodology, stakeholder list, and audit team for the engagement.

Appendix B outlines the Risk Rating Classifications and Definitions.

The courtesy and cooperation extended by the personnel in the Information Security and Contracts Management departments are appreciated.

Natalie Ramello

Natalie A. Ramello, JD, CIA, CHC, CHPC, CHRC, CHIAP
Vice President, Chief Institutional Compliance Officer & Interim Chief Audit Executive
Office of Institutional Compliance & Audit Services
October 31, 2024

DETAILED OBSERVATIONS

Information Security TX-RAMP Certification Decision Matrix

The current TX-RAMP Certification Decision Matrix provides limited details and guidance on how to accurately answer whether the solution meets the definition of a cloud computing service. UT Southwestern Business Owners are responsible for coordinating with the vendor to complete the matrix submissions to ISAC for new solutions; however, clear guidance on how to correctly complete the decision matrix and associated workflow is not provided, which may result in confusion on how to respond to the matrix questions and potential noncompliance with TX-RAMP requirements.

LOW

1. TX-RAMP Certification Decision Matrix	Recommendation	Management Action Plan
The current TX-RAMP Certification Decision Matrix provides limited details and guidance for the business to accurately answer whether the solution meets the definition of a cloud computing service as it utilizes a very broad definition outlined in NIST 800-145. Additional clarifying details for what constitutes a cloud computing service are provided by NIST 500-322, which can assist the business and vendor in answering each characteristic question and provides guidance for whether the Cloud Service Provider should answer the question, UT Southwestern, or either party. ***Note:*** Texas DIR made significant changes to the definitions of what constitutes a cloud computing service in the latest 3.0 manual and as a result, the definition is more specific than prior TX-RAMP manuals indicated. The result is likely that less solutions will meet the updated definition than were previously used and those vendors who were tagged as needing TX-RAMP certifications may no longer require it when the contract is up for renewal.	UT Southwestern should enhance the TX-RAMP Certification Decision Matrix with guidance from NIST 500-322 definitions for Cloud Computing, which provides additional definition and detail than NIST 800-145 with more detailed information in the following areas (see Appendix C for full details): • On-Demand Self-Service • Broad Network Access • Resource Pooling • Rapid Elasticity • Measured Service	Action Plan Owner: Sheila Arnold Action Plan Executives: Nathan Routen Tony Lakin Due Date: 02/28/2025 *Management will review and consider enhancing the TX-RAMP Certification Decision Matrix by expanding on the cloud computing definitions provided, aligning them with NIST 500-322.*

2. Examples of Completed Decision Matrix	Recommendation	Management Action Plan
Examples for business users and vendors leveraging the decision matrix to demonstrate what does and what does not meet each cloud computing characteristic are not currently provided. It is important to note that both the Information Security and Contracts Management teams provide assistance to the business before a contract is completed. However, due to the number of contracts going through UT Southwestern, it creates a significant lift for these teams to challenge each submission that could be better supported by providing the business owner with more guidance on how to correctly complete the decision matrix.	Consider providing examples for each cloud computing characteristic that leads to a decision for both a “meets the definition” and “does not meet the definition” to assist the business in working with the vendor to accurately answer each characteristic criterion with a “Yes” or “No”.	Action Plan Owner: Sheila Arnold Action Plan Executives: Nathan Routen Tony Lakin Due Date: 02/28/2025 *Management will provide examples for each cloud computing characteristic to guide the vendor in making informed decisions when answering the criterion with a "Yes" or "No." This approach will help clarify whether a cloud service "meets" or "does not meet" the required definitions, thus improving the accuracy and consistency of responses across various assessments.*

TX-RAMP Compliance Tracking

Tracking of cloud computing vendors and solutions is not standardized across system repositories and could potentially result in issues with future audits of TX-RAMP compliance. The procurement portal Jaggaer is the primary inventory of vendors requiring TX-RAMP certification; however, there is additional inventory tracking if ISAC reviews the solution, which is captured in ServiceNow.

LOW

1. Reporting for Compliance	Recommendation	Management Action Plan
Cloud computing vendors that UT Southwestern identifies as requiring TX-RAMP certification are currently tracked in Jaggaer with the contract. This setup creates challenges in how UT Southwestern can clearly demonstrate compliance with TX-RAMP requirements. The contract /vendor's name does not typically match the name of the solution that is in TX-RAMP's inventory. Jaggaer is updated when a new contract is completed and is not easily utilized to pull forward what certification requirements are needed and allow for comparison to the DIR's inventory of TX-RAMP's vendor certifications.	UT Southwestern should consider adding standardized fields to the procurement portal Jaggaer to flag cloud computing service providers who require TX-RAMP certification, and the certification level needed for UT Southwestern. Update tool tips in Jaggaer for cloud computing service providers based upon TX-RAMP 3.0 definitions.	Action Plan Owner: Will Ward Action Plan Executives: Sharonda Lawson Charles Cobb Due Date: 02/28/2025 *Management will ensure* Jaggaer *has a standardized flag for TX-RAMP required vendors.* *Management will also revise existing SOPs to reflect TX-RAMP 3.0 and instruct Sourcing Specialists on recording the TX-RAMP level in the record.*
An additional inventory is maintained by Information Security in ServiceNow tickets for any system reviewed through the ISAC process and those details are captured and retained in comments without any specific distinct fields.	Add standardized fields in ServiceNow to flag cloud computing service providers as requiring TX-RAMP along with the certification level, rather than track results in the comments field, which makes queries for TX-	Action Plan Owner: Sheila Arnold Action Plan Executives: Nathan Routen Tony Lakin

	RAMP cloud computing service providers more cumbersome.	Due Date: 02/28/2025 *Management will update ServiceNow to ensure tracking TX-RAMP results during the ISAC review through adding mandatory standardized fields in ServiceNow to flag certification level.*

Appendix A

Objectives, Scope, and Methodology:

The objectives of the review are to assess the program in place for the intake of vendors, determine if these vendors meet the TX-RAMP Cloud Service Provider definition and adhere to the associated TX-RAMP requirements, and review the compliance tracking mechanisms in place to demonstrate compliance.

The audit scope period included activities of the Contracts Management and Information Security Departments from January 1, 2024 to August 1, 2024. The review included UT Southwestern and Identified Cloud Service Providers per TX-RAMP definitions. The review did not include other systems that do not fall under TX-RAMP requirements.

Our procedures included, but were not limited to, the following:

- Interviewed key personnel and reviewed relevant organizational policies.
- Examined Information Security and Contracts Management processes including:
  - Contracting language to enforce appropriate language for cloud computing services following TX-RAMP requirements.
  - Contracting intake processes to identify cloud computing service providers and contract tracking.
  - Information Security processes to investigate and identify cloud computing service providers are in place.
  - Monitoring for Texas DIR requirement changes and processes.
- Reviewed an inventory of vendors to assess how they were reviewed and tracked under Texas DIR TX-RAMP guidelines, and how UT Southwestern is demonstrating compliance as a result.

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

Executive Sponsors:

Tony Lakin, Vice President & Chief Information Security Officer
Charles Cobb, Associate Vice President, Supply Chain Management

Key Stakeholders:

Sheila Arnold, Governance Risk Compliance, Senior Analyst, Information Security
Brian Evans, Associate Vice President, Chief Enterprise Architect, Information Resources
Sharonda Lawson, Director, Sourcing & Contracts Management, Supply Chain Management
Russ Poole, Vice President & Institutional Chief Information Officer
Nathan Routen, Director, Information Security
Gabriel Samuel, Governance Risk Compliance, Senior Analyst, Information Security
William Ward, Senior Manager, Legal Contracting Services, Contracts Management, Supply Chain Management

Audit Team:

Kevin Dunnahoo, Director, Technology & Cybersecurity, Protiviti
Sean Fields, Compliance Auditor, Audit
Monica Frazer, Director, Audit
Matt Jackson, Managing Director, Protiviti
Phillippa Krauss, Senior Project Manager, Audit
Natalie Ramello, J.D., Vice President, Chief Institutional Compliance Officer & Interim Chief Audit Executive
Kevin Watkins, Senior Manager, Technology Privacy & Security, Protiviti
Leslie Wilson, Senior Consultant, Protiviti

Appendix B

Risk Classifications & Definitions

Each observation has been assigned a risk rating according to the perceived degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management. The following chart is intended to provide information with respect to the applicable definitions, color-coded depictions, and terms utilized as part of our risk ranking process:

Degree of Risk & 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 UT Southwestern 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 UT Southwestern 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 UT Southwestern either as a whole or to a college / school / unit level. As such, action is needed by management to address the noted concern and reduce the risk to a more desirable level.
Low	A finding identified by Internal Audit that is considered to have minimal probability of adverse effects to UT Southwestern 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. 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.

Appendix C

Guidance from NIST 500-322: "The NIST Definition of Cloud Computing"

On-Demand Self-Service

Consumers can independently access and allocate computing resources without human interaction with service providers.
(Note: "Consumer" refers to UT Southwestern [per Texas DIR])

"Without human interaction with the service provider" means:

- Option A: Fully automated service provisioning.
- Option B: An automated interface is used to request and track the service.
  (Note: The provider can use manual labor to provision the service on their end.)
  - Examples of computing capabilities include server time and network storage.
  - "Unilaterally" means the customer initiates the service and there may be a process involving humans, such as those for oversight, and approval of expenditures is still valid.
  - "Automatically" refers to automated provisioning but can also include a ticketing process for provisioning if the process is fast enough to support the Service Level Agreement (SLA).
    (Note: The Cloud Service Provider must confirm Option A or Option B.)

Broad Network Access

Capabilities are accessible over the network through standard mechanisms, facilitating use on diverse client platforms.
(Note: This refers to "anytime anyplace access" to computing resources from any machine within UT Southwestern policy and security constraints [definitions].)

- "Over the network" means:
  - Option A: Available over the Internet.
  - Option B: Available over a network that is available from all access points that UT Southwestern requires, such as the UT Southwestern network or Wi-Fi network.
- "Diverse Client Platforms" can include mobile phones, laptops, workstations, and tablets.
- "Standard mechanisms" implies computing communicates over industry standard protocols available on the Internet or most networks.

Resource Pooling

Providers pool computing resources in a multi-tenant model, dynamically assigning physical and virtual resources based on consumer demand.

- The computing infrastructure is shared among more than one customer (Cloud Service Provider must confirm).
- Physical resource location independence is generally not controlled by UT Southwestern over the exact location but may be able to be specified at a higher level (Ex., within the United States or North America).
- Resources include storage, processing, memory, and network bandwidth.
- "Multiple tenants" refers to the ability to serve more than one regardless of how many tenants are actually served.
- Resource Pooling is an inherent benefit of any service model (I.e., Software as a Service, Platform as a Service, Infrastructure as a Service).

Rapid Elasticity

Capabilities can be swiftly provisioned or released, automatically scaling to meet demand fluctuations.

- "Rapidly" is defined as: (*Either the Service Provider or UT Southwestern may confirm*)
  - Option A - Automated and near-real-time.
  - Option B - Not fully automated, but fast enough to support the requirements of UT Southwestern.
- "Scaling to meet demand" means growing or shrinking computing capability dynamically according to need.

Measured Service

Cloud systems optimize resource usage through automatic monitoring, control, and reporting, ensuring transparency for both providers and consumers.

- Resource usage is measured in well enough detail to support the requirements of UT Southwestern (UT Southwestern can confirm).
- If the term "metering" is used, this is defined as being done on a pay-per-use or charge-per-use basis and can mean both showback and chargeback.