UT Southwestern Medical Center
TX-RAMP Vendor Security Assurance Program

Sheila Arnold, MBA, CISA, CCSK, CDPSE
Governance Risk and Compliance Sr. Analyst
Information Security

Gabriel Samuel, CISA, CRISC, CDPSE
Governance Risk and Compliance Sr. Analyst
Information Security
Texas Risk & Authorization Management Program (TX-RAMP)

What is TX-RAMP?
- A standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process UTSW data

Why is TX-RAMP Needed?
- Enhanced risk management of third-party cloud vendors
- Streamline assessment process between third party cloud vendors and ISAC review
- Uniform authorization and assessment of cloud information security and controls
- Increased Visibility into all aspects of cloud security controls

What does TX-RAMP apply to?
- Contracts for cloud services that store, process, or transmit UTSW data entered in, or renewed, on or after Jan 1, 2022

Who does TX-RAMP apply to?
- Organizations subject to information security requirements of Government Code Chapter 2054:
  - State Agencies, Public Institutions of Higher Education, and Public Community Colleges
Certification Levels

TX-RAMP Level 1
- Nonconfidential data OR
- Low-impact information resources
*Must be certified by January 1, 2024, to enter/renew contracts

TX-RAMP Level 2
- Confidential information AND
- Moderate or high-impact information resources
*Must be certified by January 1, 2022, to enter/renew contracts

TX-RAMP Provisional
- Level agnostic
- Agency-sponsored or 3rd party assessment review
  (Only under special circumstances - i.e. the contract is about to expire)
- Valid for 18 months

*Existing contracts for cloud services do not need to be certified until renewed or new contract is executed
<table>
<thead>
<tr>
<th>High Impact Information Resources</th>
<th>Moderate Impact Information Resources</th>
<th>Low Impact Information Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Such an event could:</td>
<td>Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Such an event could:</td>
<td>Resources--Information resources whose loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Such an event could:</td>
</tr>
<tr>
<td><strong>(A)</strong> cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;</td>
<td><strong>(A)</strong> cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;</td>
<td><strong>(A)</strong> cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced</td>
</tr>
<tr>
<td><strong>(B)</strong> result in major damage to organizational assets;</td>
<td><strong>(B)</strong> result in significant damage to organizational assets;</td>
<td><strong>(B)</strong> result in minor damage to organizational assets;</td>
</tr>
<tr>
<td><strong>(C)</strong> result in major financial loss; or</td>
<td><strong>(C)</strong> result in significant financial loss; or</td>
<td><strong>(C)</strong> result in minor financial loss; or</td>
</tr>
<tr>
<td><strong>(D)</strong> result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.</td>
<td><strong>(D)</strong> result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.</td>
<td><strong>(D)</strong> result in minor harm to individuals.</td>
</tr>
</tbody>
</table>
DIR will certify a cloud computing service under the corresponding impact level from accepted statuses of FedRAMP and StateRAMP using the FedRAMP Marketplace & StateRAMP Authorized Vendor List designations.

- StateRAMP Authorized Vendor List: https://stateramp.org/vendor-list/
UT Southwestern Pathways to TX-RAMP Compliance

1. **New Contract**
   - ISAC Request
   - Approved ISAC Request
   - Strategic Sourcing

2. **Approved ISAC Request**
   - Is the third-party cloud vendor on the DIR’s approved vendor list?
     - Yes: Vendor is cleared by InfoSec to enter a contract
     - No: Send the requestor DIR’s TX-RAMP ppt to share with the vendor

3. **Send the requestor DIR’s TX-RAMP ppt to share with the vendor**
   - Assist the vendor with provisional sponsorship – if needed

4. **Assist the vendor with provisional sponsorship – if needed**
   - Enter vendor in SPECTRIM for continuous monitoring

5. **Enter vendor in SPECTRIM for continuous monitoring**
   - Contract Renewal
1. Check the list of cloud computing products that have been certified through the Texas Risk and Authorization Management Program (TX-RAMP):
https://dlr.texas.gov/sites/default/files/2022-03/TX-RAMP%20Certified%20Products.3.22.22.xlsx
If the vendor is on the list, ensure the certification is for the level required for UTSW’s anticipated use and risk factors. If the vendor is not on the list, continue with process below.

Review the questions below to determine if TX-RAMP certification is required.

A. Is the Application or Service hosted by a Cloud Service Provider (accessed through the internet) and requires a new contract or contract renewal?
   *If the answer is NO – TX-RAMP not required
   *If the answer is YES, then proceed to the following three questions – a YES answer to any means TX-RAMP is required.

B. Does the Cloud Application or Service include storing or processing UTSW data at an offsite location?

C. Does the Cloud Application or Service store or process any sensitive information such as SSN, Credit Card information, PHI, PII, etc.?

D. Does the Cloud Application or Service interface with a UTSW application that stores any sensitive information? Ex: The data is managed by a third-party and will interface with Epic or Active Directory.

2. If the vendor has not been certified – is not on the list, they must apply for certification.
Please share the links below:
TX-RAMP Overview for Vendors
TX-RAMP Assessment Request for Vendors
https://survey.alchemer.com/s3/6510630/TX-RAMP-Vendor-Contact

If assistance is needed for determination requirements contact sheila.arnold@utsouthwestern.edu.
## TX-RAMP Criteria included in Contract Risk Assessment Form

### General Contract Factors

<table>
<thead>
<tr>
<th>#</th>
<th>Risk factor</th>
<th>Low Score</th>
<th>Medium Score</th>
<th>High Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Vendor Size</td>
<td>Large National</td>
<td>Medium Regional</td>
<td>Individual Entrepreneur or International</td>
</tr>
<tr>
<td>5</td>
<td>Contract Terms</td>
<td>UT standard terms</td>
<td>GPO Master Agreement</td>
<td>Vendor Paper</td>
</tr>
<tr>
<td>6</td>
<td>Impact on mission of institution</td>
<td>Failure impacts 1 organization</td>
<td>Failure impacts multi orgs</td>
<td>Failure impacts entire org</td>
</tr>
</tbody>
</table>

### Software & Data Specific Factors - If NOT software AND no data access, leave blank

- **TX-RAMP Level 1**
  - The Cloud Application or Service will process, transmit, and/or store non-sensitive data, metadata, and/or data that may be released to the public that requires no additional levels of protection.
  - Failure impacts 1 organization.

- **TX-RAMP Level 2**
  - The Cloud Application or Service will process, transmit, and/or store data as defined by (PCI SSC).
  - Failure impacts multi orgs but does not involve loss of life or serious life-threatening injuries.

- **TX-RAMP Level 2 with contract monitoring**
  - The Cloud Application or Service will interface with a UTSW application that stores any sensitive information.
  - Failure impacts entire org but does not involve loss of life or serious life-threatening injuries.

### Note

*Note if any PHI is exchanged with the Vendor, a BAA is required regardless of other risk factor scorings.*
Overview

- Information Sharing and Project Discussion Kickoff Meeting
- Core team identified and bi-weekly cadence with break-out working groups

Criteria

- Defined Cloud Computing
- TX-RAMP Questionnaire developed
- Developed Use Cases for core team

Level Determination

- Information Security outlined and defined the scope
- Established certification levels based on DIR directives

Certification

- Certification levels and impact criteria added to Risk Assessments and ISACs
- Provisional Sponsorship process documented

Communication Campaign

- Presentation to InfoSec
- Update Information Security Standard
- Update Security website & ISAC form
- Presentation to ISAC Committee

Metrics & Reporting

- Determine Exception Criteria
- Identify reportable fields for ServiceNow & Jagger
- Number of active cloud vendors

Continuous Monitoring

- Register vendors in SPECTRIM
- Work with Procurement to develop vendor monitoring

Measures for ongoing Compliance

- Updates in SPECTRIM
- Changes to TX-RAMP
- Communication to stakeholders

TX-RAMP Vendor Security Assurance Program Roadmap

- Completed Jan. 22
- Completed Mar. 22
- Completed Apr. 22
- Completed May 22
- Completed July 22
UTSW Responsibilities
• Determining applicability and ensuring that cloud services contracted for are TX-RAMP certified
• Ensuring their specific control requirements are met (e.g., HIPPA, PCI, etc.)
• Reviewing vendor alignment to UTSW security requirements and vendor TX-RAMP certification status

DIR Responsibilities
• Maintaining a list of certified cloud services/providers
• Launching vendor assessments and collecting responses/documentation
• Reviewing assessment information and determining certification eligibility
• Providing notifications relating to TX-RAMP changes (certification, reminders, etc.)
• Determining TX-RAMP administrative actions

Shared Responsibilities
• Holding vendors accountable
• Communicating processes/requirements
• Ensuring accuracy
• Communicating identified risks
• Maintaining compliance
Thank you