TX-RAMP Vendor Guide:
Completing a TX-RAMP Assessment Questionnaire

April 2023

General Information

Request for TX-RAMP certification can be broken up into various phases, once the cloud service provider has submitted an assessment to DIR, the TX-RAMP assessor will evaluate the completed assessment. Upon evaluation completion, the determination of certification is made.

The information within this document will serve as a guide for submitting the TX-RAMP Assessment Questionnaire, as a part of the Assessment phase.

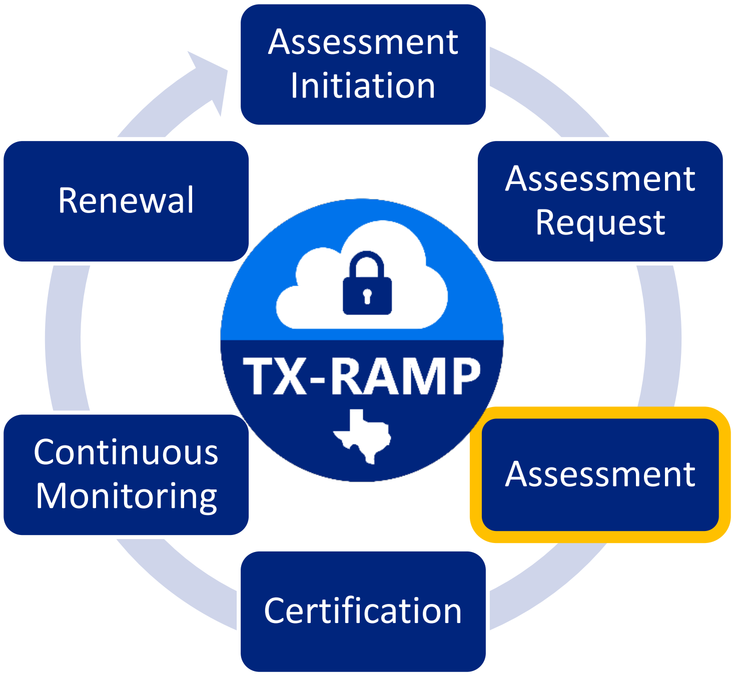


Figure 1. TX-RAMP Certification Lifecycle

Assessment Summary

Upon processing the TX-RAMP request a TX-RAMP Assessment Questionnaire will be sent to the cloud service provider's designated contact to complete. The SPECTRIM Vendor Portal is used to assign and launch assessment questionnaires to vendor contacts to collect assessment responses. TX-RAMP certifications will be determined based upon DIR review of the completed TX-RAMP Assessment Questionnaire. This assessment entails DIR's review of:

- the questionnaire and all responses therein submitted by the vendor; and
- all documentation submitted to DIR by the vendor either initially or supplementally.

The timeline to complete the assessment is dependent upon vendor responsiveness and completeness of the assessment questionnaire. If DIR is required to seek additional documentation or extensive vendor outreach is required, DIR may require more time to certify.

Completing the Assessment Questionnaire Form

The cloud service provider will complete the TX-RAMP Assessment Questionnaire and provide responses to the following sections:

- General
- System Information
- Required Documents

For details, see Appendix A. TX-RAMP Assessment Questionnaire Example.

Providing Responses to the TX-RAMP Assessment Questionnaire

As a submitter, providing relevant responses within the TX-RAMP Assessment Questionnaire will help reduce the challenges an assessor may face when reviewing and processing the completed questionnaire. Guidance for responding to the assessment questionnaire includes:

- Answer questions from the perspective of the Cloud Service Provider and not the Customer.
- Use the free text fields to provide additional context.
- If a security control is not entirely implemented, provide the following information:
- Identify if there are Customer-specific requirements that must be met to address the lack of security control implementation;
- Provide a brief description as to why the control is not met within the comments section;
- Describe how the lack of this control may affect the agency customer;
- Provide compensating controls;
- Provide a remediation plan along with the target date of remediation; and
- If applicable, supply a Plan of Action and Milestones (POAM) or roadmap listing the next steps to illustrate the next steps to achieve implementation. The FedRAMP Documents & Templates contain a Plan of Action and Milestones (POA&M) Template that may be used as a resource.
- If responding with a "N/A", provide the following information:
- Provide a narrative about customer control responsibilities and
- Reference responsible party.

General

The assessment questionnaire asks to provide general information about the cloud service for the assessment.

System Information

The assessment questionnaire asks to provide information about the TX-RAMP scoped system including its hardware, software, network components, and external services. This section describes the system's purpose, its configuration, and its architecture, as well as its operational environment, including any other systems it interacts with or relies upon.

Required Documents

The assessment questionnaire asks to provide documentation for the assessment. The required documents include:

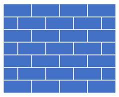
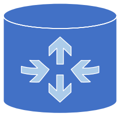
- Authorization Boundary Diagram
- Data Flow Diagram
- TX-RAMP Security Plan
- Additional Documents (Optional)

Do not skip or leave a required document empty. All required documents must be provided to evaluate the TX-RAMP Assessment Questionnaire.

General Diagram Guidance

Diagrams submitted for the TX-RAMP Assessment Questionnaire should be easy-to-read and include a legend or labels on every component. Clear labels and identification will help TX-RAMP assessors review the assessment and reduce the time taken to conduct an evaluation of the completed questionnaire.

Table 1. Example of a legend that provides a description of symbols used within a diagram.

Legend	
Cloud Services for Updates	
Firewall	
Router	
Public User	
Etc.	…

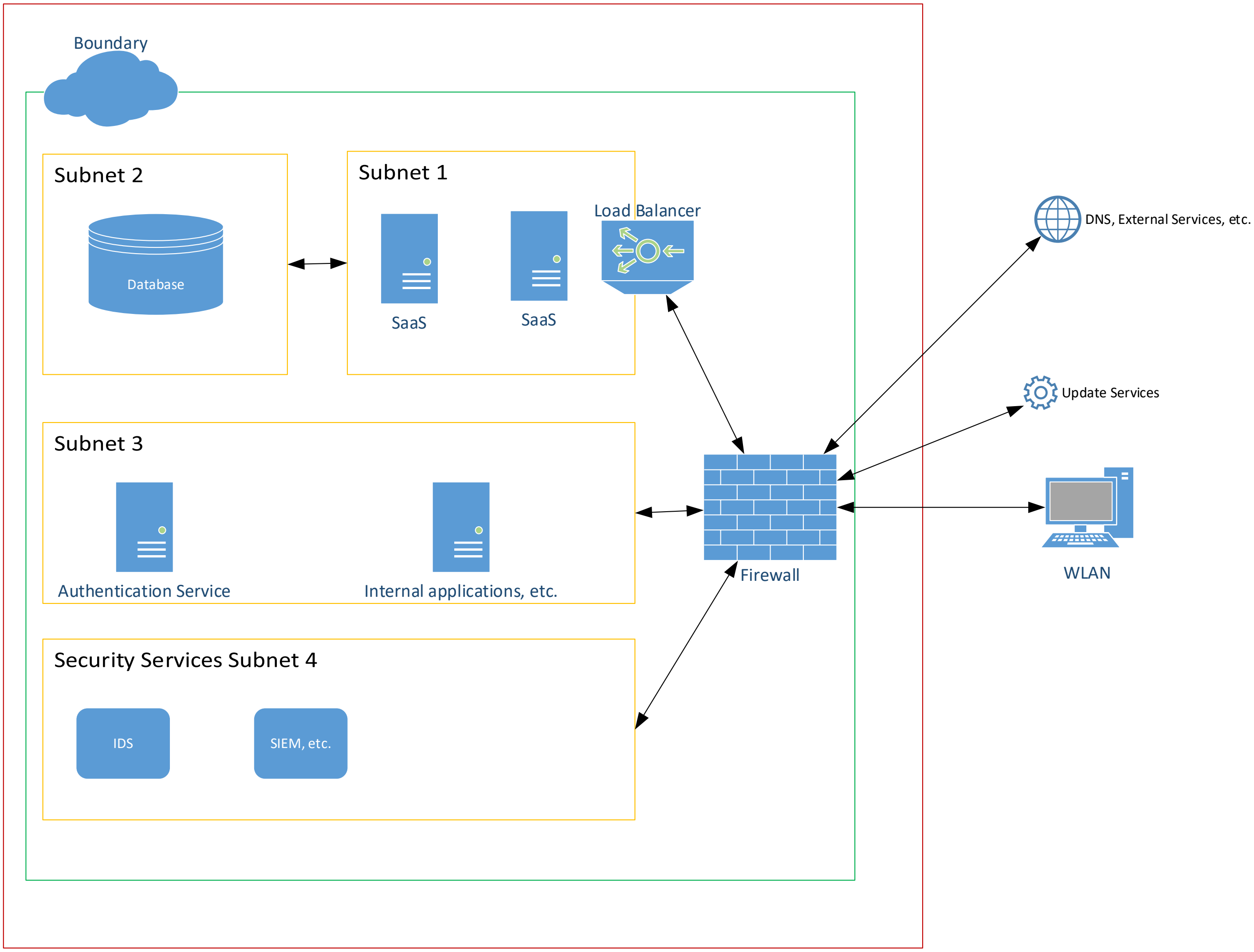
Authorization Boundary Diagram

The Authorization Boundary Diagram (ABD), also referred to as the Boundary Diagram, is attached to the TX-RAMP Assessment Questionnaire. The diagram provides a visual representation of the Information System's Authorization Boundary, including its connections and components. This diagram should include details on how communications are monitored and controlled at the external boundary, as well as at key internal boundaries within the system. It is important to address all components and managed interfaces that are authorized for operation in the information system, such as routers and firewalls. The diagram must be attached and submitted through the TX-RAMP Assessment Questionnaire via the SPECTRIM Vendor Portal.

Suggested components contained within the diagram include:

- Easy-to-read diagram that includes a legend or labels everything.
- Prominent borders drawn around all components in the authorization boundary.
- Differentiating borders to illustrate different boundaries.
- Illustration of where system components, services, or devices reside within and outside of the boundaries.
- System design components as provided in question SYS-03 of the TX-RAMP Assessment Questionnaire.
- External systems and services as provided in question SYS-05 of the TX-RAMP Assessment Questionnaire.
- List tools, services, or components that are mentioned in the System Security Plan (PL-02 System Security and Privacy Plans of the TX-RAMP Security Controls Baselines (v2.0)). Examples include databases, applications, servers, authentication mechanisms, production systems, jump boxes, connections, Virtual Private Networks (VPN), etc.
- Depict all interconnected systems and external services as mentioned in your System Security Plan.
- Depict all ingress and egress points.
- Depict connections between components within the boundary and to/from external services.
- Depict services leveraged from underlying IaaS, PaaS, and SaaS.
- Depict how cloud service providers, administrators, TX-RAMP scoped customers, and the public access the cloud service.
- If applicable, depict components that require installation on a customer’s device and the connection within the authorization boundary, such as mobile application or client applications.
- Depict security systems in-place between the boundary and external services and access, such as, but not limited to Intrusion Prevention/Detection Systems, System Information and Event Management systems, Web Application Firewalls, etc.
- Depict production, development, and test environments, primary and alternate processing sites, and location of backups including the connections and security mechanisms associated with the connections and services.
- Depict update services (e.g., malware signatures and OS updates) outside the boundary.

Table 2. Example of Boundary Diagram for reference only.



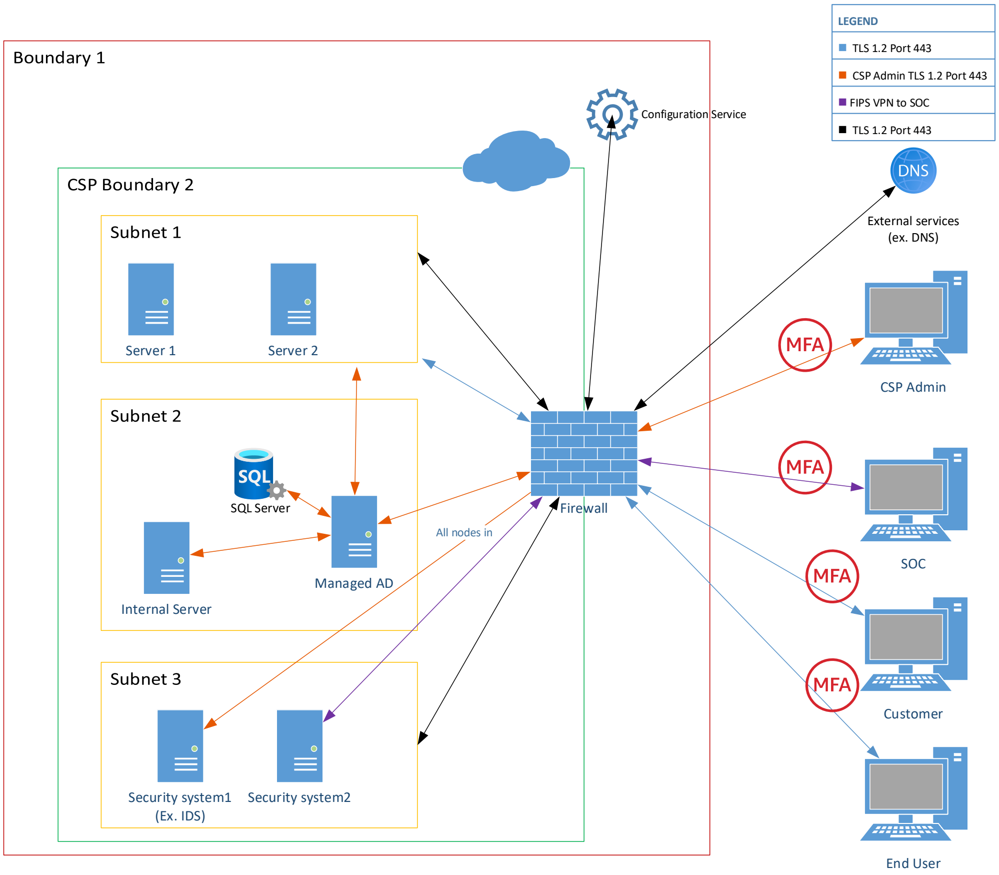
Data Flow Diagram

A Data Flow Diagram is attached to the TX-RAMP Assessment Questionnaire. The diagram provides a visual representation of the flow of data in and out of the cloud service, including the sources and destinations of each data type, as described in the Data Flow Description. The diagram depicts how data is processed, stored, and transmitted within the system, and the protection mechanisms used to secure the data in process, at rest, and during transmission, including cryptographic standards such as TLS v1.2, AES 256, etc. Access controls should also be labeled to provide an understanding of who has access to the data and how it is controlled. The diagram should include labels for user roles, such as administrators, staff, customers, and the public, and indicate data flows between different environments, such as Development, Test, and Production. A legend should be included to label the symbols used within the diagram, and interconnections should be labeled with port numbers and/or protocols, sites and alternate sites should be labeled, and each data type should be clearly labeled. The diagram must be attached and submitted through the TX-RAMP Assessment Questionnaire via the SPECTRIM Vendor Portal.

Suggested components contained within the diagram include:

- Easy-to-read diagram that includes a legend or labels everything.
- Data Flow components as described in question SYS-06 of the TX-RAMP Assessment Questionnaire.
- Depict how administrators, staff, customers, and the public access the data.
- Depict which authentication mechanism and multi-factor authentication (if applicable) are in use by the different user roles.
- Depict the types of data, the flow of the data throughout the diagram, including external services.
- Depict interconnections.
- Depict where data is processed, stored, and transmitted.
- Depict the flow of data between sites and backup sites.
- List data flow between Development, Test, and Production environments.
- Label the port numbers and protocols used between connections.
- Label how the data is protected in process, at rest, and when transmitted including the cryptographic standards, such as TLS v1.2, AES 256, etc.

Table 3. Example of Data Flow Diagram



TX-RAMP Security Plan

The TX-RAMP Security Controls Baseline (v2.0) define the security controls required for TX-RAMP Level 1 and Level 2 certification. Implementation details of these security controls are provided within the TX-RAMP Security Plan section of the TX-RAMP Assessment Questionnaire. Cloud service Providers will update the following document TX-RAMP Security Plan and attach the completed workbook to the TX-RAMP Assessment Questionnaire.

TX-RAMP Security Plan is a workbook template and must be completed, attached, and submitted through the TX-RAMP Assessment Questionnaire via the SPECTRIM Vendor Portal.

Components of the TX-RAMP Security Plan include:

- The Instructions tab
- The Control Implementation tab
- The Summary tab

TX-RAMP Security Plan – Instructions

When completing the TX-RAMP Security Plan, start with the Instructions tab. The instructions will help cloud service providers complete the workbook. Reminder, save your document often.

Table 4. Table within the TX-RAMP Security Plan workbook that demonstrates "Step #" the step order, "Tab Name" the location of where the task can be found, "Description" the description of the task required, and "Example" if applicable, an example of the description.

Step #	Tab Name	Description	Example
0	Instructions	Please rename and save the TX-RAMP Security Plan workbook, with the product name and Assessment ID in the filename. Please see corresponding example.	TX-RAMP Security Plan workbook - ABC Cloud Product Name 123456.xlsx

TX-RAMP Security Plan – Control Implementation

When completing the TX-RAMP Security Plan, many of the responses are required within the Control Implementation tab. The Instructions tab will provide details on how to complete the Control Implementation tab and where the cloud service provider will input their responses. All required fields for associated controls for the target certification level must be completed in their entirety to initiate the review process. If uncertain about the requirements for control implementation, the subject matter can be found within the control's Control Description and Additional Control Information columns. The TX-RAMP Parameters column will also specify if there are minimum requirements for TX-RAMP compliance.

Table 5. Different columns from a table within the TX-RAMP Security Plan workbook that demonstrate information about the security control requirements (SORT ID, ID, Control Family, Control Name, Level 1, Level 2, Control Description, TX-RAMP Parameters, and Additional Control Information).

A	B	C	D	E	F	G	H	I	O
SORT ID	**ID**	**Control Family**	**Control Name**	**Level 1**	**Level 2**	**Control Description**	**TX-RAMP Parameters**	**Policy/Document Guidance Resources**	**Additional Control Information**

Table 6. Different columns from a table within the TX-RAMP Security Plan workbook that the cloud service provider will provide responses to the security controls (Implementation Status, Implementation Responsibility, Implementation Details, and Other Comments).

A	D	G	H	J	K	L	M
SORT ID	**Control Name**	**Control Description**	**TX-RAMP Parameters**	**Implementation Status** What is the current state of the control implementation?	**Implementation Responsibility** Who is the responsible party for ensuring that this control is implemented and operating effectively?	**Implementation Details** Provide details on how this security control is implemented and if there are any plans or compensating controls. If applicable, reference the relevant documents that address this control.	**Other Comments** Optional.
AT-04-00	Training Records	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and b. Retain individual training records for [Assignment: organization-defined time period].	AT-4(b) [at least 1 year]	Implemented	Service Provider Responsibility	Our organization documents and monitors information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training (including application developer security training); and we retain individual training records for 2 years.	N/A

TX-RAMP Security Plan – Summary

When completing the TX-RAMP Security Plan, the Summary tab may be used to review your submission before attaching it to the TX-RAMP Assessment Questionnaire. The Instructions tab will provide details on how to complete the Summary tab and where to select the assessment level required for TX-RAMP Certification. TX-RAMP has two assessment and certification levels:

- **Level 1** for public/non-confidential information or low impact systems.
- **Level 2** for confidential/regulated data in moderate or high impact systems.

Additional Documents

Documents such as policies, procedures, and plans are required security controls for the Texas Risk and Authorization Program Manual (v2.0). However, they are optional documents that can be attached to the TX-RAMP Assessment Questionnaire as supportive documentation to illustrate control implementation. Here are some recommendations for document implementation:

- Standard documentation – Standardization across all document types can assist in ensuring compliance, completeness, consistency, clarity, and conciseness.
- Ensure respective documents have the appropriate sections, such as Scope, Purpose, Roles, Responsibilities, etc.
- Security controls, such as those listed in the Control Name column of "Policy and Procedures", provide details on the components required within each policy and procedures type.
- The Resources section of this guide includes additional resources and templates to assist with documentation development.
- A version history table provides confirmation of proper approvals and records when reviews are conducted.

Table 7. Example of a Version History Table. This policy has been reviewed within the TX-RAMP defined parameter of three years.

Date	Version Number	Description	Approving Authority
06/21/2021	1.0	Published Access Control Policy	John Smith Chief Executive Officer
04/15/2023	2.0	Updated Access Control Policy to align with NIST 800-53 rev.5	John Smith Chief Executive Officer

Resources

Texas Risk and Authorization Management Program (TX-RAMP) website

https://dir.texas.gov/resource-library-item/texas-risk-and-authorization-program-manual-20

TX-RAMP Resources Library

https://dir.texas.gov/information-security/texas-risk-and-authorization-management-program-tx-ramp/tx-ramp-resources-0

FedRAMP Resources and Templates

https://www.fedramp.gov/documents-templates/

StateRAMP Resources and Templates

https://stateramp.org/templates-resources/

For TX-RAMP Assistance and Questions

Contact TX-RAMP@dir.texas.gov

Version History

Date	Version Number	Description
06/21/2020	1.0	Published document
04/19/2023	2.0	Updated guide to align with updated TX-RAMP Manual (version 2.0)

Appendix A. TX-RAMP Assessment Questionnaire Example

General

GEN-01: Organization History. Describe how long the organization has conducted business in this product area. Include number of years and in what capacity.

GEN-02: State of Texas Customer Base Extended. Describe the characteristics of the customer base this service is provided to. Of the customer base, include information about Texas state agencies, public institutions of higher education, and public community colleges.

GEN-03: Breach History Past 3 Years. Has the organization had a significant breach of system security in the last 3 years? "Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. [Yes or No]

GEN-03a: Breach History Additional Information. If the organization has had a significant breach of system security in the last 3 years, provide additional information about the circumstances including measures taken to prevent future incidents.

GEN-04: Information Security Personnel. Approximately, how many dedicated information security personnel does the organization employ (including contractors)?

GEN-05: Dedicated Teams. Does the organization have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.) [Yes or No]

GEN-06: Data Export Capabilities. Describe the information system's ability to support data export/portability capabilities (e.g. supported file types, transmission methods, portability requirements, volume, restrictions).

GEN-07: Data Location Restrictions. Does the information system restrict the location of information processing, information/data, and information system services to only the Contiguous United States? Contiguous United States refers to the 48 states of the U.S. that are connected together, sharing borders with one another, and located within the mainland of North America. The contiguous United States does not include Alaska, which is part of the North American mainland but separated from the other states by Canada, nor does it include Hawaii, which is an island state located in the Pacific Ocean. Washington, D.C., the U.S. capital, is also considered part of the contiguous United States. [Yes, No, or Optionally Upon Customer Request]

GEN-08: Host Structure and Provider. Describe the hosting structure/provider(s) for this cloud computing service. Specifically note where customer data may reside.

GEN-08a: Data Location Restrictions. Describe the data location(s) restriction capabilities (i.e. can a customer request a specific hosting region/location)?

GEN-09: Customer Data. Will customer data be shared with or hosted by any third parties to the cloud service manufacturer (e.g. any entity not wholly owned by your company)? [Yes, No, or Customer Specific]

GEN-09a: Customer Data Sharing Explanation. If yes, please describe the nature of the data sharing, purpose, sensitivity, and mechanisms by which information is shared.

GEN-10: SSO Functionality. Describe the information system's ability to provide customer/end-user single sign-on (SSO) functionality.

GEN-11: MFA Functionality. Describe the customer agency's multifactor authentication capabilities (e.g. native MFA capability, third-party MFA integration, configurable by customer organization, etc.).

GEN-12: Third Party Security Assessments. Please describe the organization's process for evaluating and approving third-party companies, such as hosting providers, cloud services, and other third-party services, that process or store the state of Texas customer data, and how it ensures that security requirements are met.

GEN-12a: Third Party Data Explanation. Provide a description of why each third-party has access to customer data.

GEN-13: Customer Data Breach Liability. What safeguards and legal agreements, including contractual requirements, are in place to address liability in the event of a breach of customer data, and what protections, if any, are extended to the agency customers?

GEN-14: Separate Government and Commercial Offerings. Does this cloud service have separate government and commercial offerings? [Yes or No]

GEN-14a: Offering Differences. If yes, please describe the primary differences between the government and commercial offerings, specifically related to data protection, access controls, SLAs, data sovereignty, auditability, network security, incident response, and pricing and support.

GEN-15: Subservice Cloud Services. Does the cloud service leverage any subservice cloud services? A subservice organization can include Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) providers that are a component in the delivery of higher-order cloud services. For example, many Software as a Service (SaaS) providers leverage cloud services hosted in a public cloud, such as Microsoft's Azure or Amazon's AWS. [Yes or No]

GEN-15a: Subservices Additional Information. If yes, please list the product and provider names of subservices involved in the delivery of the cloud service.

GEN-16: Screening/Background Check Approach. Describe the organization's approach to personnel screening and background checks, including the criteria used to determine their necessity, relevant policies, timelines for conducting checks, the frequency of these checks, and any other relevant considerations.

GEN-17: Outsourced Functions. Does the organization outsource any functions relating to the delivery of the cloud service outside the United States? (e.g. support, administration, development)

GEN-17a: Outsourced Functions Additional Information. If yes, Describe the extent and function of access and information provided to non-US entities or personnel.

GEN-18: Vulnerability Scanning and Penetration Testing. Describe the frequency, breadth, and depth of vulnerability scanning and penetration testing related to the cloud service.

GEN-19: Payment Processing Services. Does the cloud service provide payment processing services? [Yes, No, or Customer Specific]

GEN-20: Annual Cloud Service Security Checks. Are independent assessments of security conducted on the cloud service at least annually? [Yes or No]

GEN-21: User Account and Activity Data. Provide details on the types of user account and activity data that are collected and stored within the cloud environment, such as login times, IP addresses, device information, user actions, and any other relevant data.

GEN-22: Prohibited Technology Relationship. Does your organization have any controlling relationship with any of the entities or technologies included in the Texas Prohibited Technologies (https://dir.texas.gov/information-security/prohibited-technologies) list? Controlling relationship means majority ownership or control by or of a company included in the prohibited technologies list. [Yes or No]

GEN-22a: Prohibited Technology Relationship Additional Information. If yes, please list the name of the entities or technologies.

GEN-23: Information Security Policy Review Interval. Describe the organization's approach to reviewing and maintaining its information security policies, including details on the frequency of reviews, the process used to conduct reviews, the approvals required for policy changes, and any other relevant information regarding policy management.

GEN-24: Information Security Procedure Review Interval. Describe the organization's approach to reviewing, updating, and maintaining its procedures, including details on the frequency of reviews, the process used to conduct reviews, the approvals required for procedure changes, and any other relevant information regarding procedure management.

GEN-25: Cybersecurity Insurance Policy. Does the organization have a current cybersecurity insurance policy? [Yes or No]

GEN-26: Cybersecurity Insurance Policy Additional Information. If yes, describe the cybersecurity insurance policy coverage and any customer-inherited coverage.

General Comments. Optional. Provide any other pertinent details that would be useful for the TX-RAMP evaluation.

System Information

SYS-01. Provide an overview of the information system's purpose, what the system does, its main functions, and the components that make it up. Examples of the types of information that could be included in the response include what type of data the system handles, what business processes it supports, and what technologies or tools are used to build and maintain it.

SYS-02. Information System Operational Status. [Operational, Under Development, Major Modification, or Other]

SYS-03. System Design Components. Provide a description of the design and components of the cloud service. In the case of a SaaS platform, provide a comprehensive list of all the modules and component applications that are included in the scope of the control implementations mentioned in this assessment. Please note that external systems and services will be described in greater detail in a subsequent section.

SYS-04. System Sensitivity Level. [Low, Moderate, or High]

SYS-05. External Systems and Services Details. Describe any external systems and services that relate to the TX-RAMP scoped platform or infrastructure, such as connections between components within the boundary to and from external services, and access external services may have to information systems, tools, services, or components which should appear on the Boundary Diagram. Examples may include databases, applications, servers, authentication systems, production systems, jump boxes, connections, VPNs, firewalls, load balancers, routers, switches, gateways, proxies, and other network infrastructure. It could also include third-party services, APIs, and integrations with other cloud services or platforms.

SYS-06. Data Flow Description. Describe how data flows in and out of the system, encompassing the various user groups involved (internal, external, and customers), system locations (Development, Test, Production, and backup sites), and the types of data handled. Elaborate on the data flows used to process, store, and transmit data within the system, including the security measures implemented to safeguard it. These security measures should conform to industry standards, such as the use of cryptographic protocols like TLS v1.2 and AES 256. The access controls used by the system should be discussed, focusing on identifying who has access to the data and the user roles involved. Additionally, the means by which these users' access and interact with the system's data should be detailed.

Required Documentation

Diagram - Authorization Boundary. Attach an Authorization Boundary Diagram (ABD). The Vendor Guide (https://dir.texas.gov/information-security/texas-risk-and-authorization-management-program-tx-ramp/tx-ramp-resources-0) provides information on what is entailed within an Authorization Boundary Diagram (ABD), also referred to as the Boundary Diagram.

Diagram - Data Flow. Attach a Data Flow Diagram. The Vendor Guide (https://dir.texas.gov/information-security/texas-risk-and-authorization-management-program-tx-ramp/tx-ramp-resources-0) provides information on what is entailed within a Data Flow Diagram.

TX-RAMP Security Plan. Attach the completed TX-RAMP Security Plan workbook (https://dir.texas.gov/resource-library-item/tx-ramp-security-plan-workbook) . All required fields for associated controls for the target certification level must be completed in their entirety to initiate the review process.

TX-RAMP Security Plan Comments. Optional. Provide any relevant additional information concerning the required documentation.

Additional Documents. Optional. Provide any additional relevant security artifacts, policies, procedures, documentation to assist with the assessment.

Documentation Comments. Optional. Provide any relevant additional information concerning the attached documentation.