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

Version 3.0

Effective Date

This publication takes effect on 12/1/2023

Table of Contents

1. Purpose

Government Code Section 2054.0593 requires the Texas Department of Information Resources (DIR) 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." In response to this mandate, DIR created the Texas Risk and Authorization Management Program (TX-RAMP).

Per 1 Texas Administrative Code Chapter 202, the Texas Risk and Authorization Management Program Manual (Program Manual) defines the processes, procedures, and compliance requirements relating to the use of cloud computing services by Texas state agencies.

2. Document Change Management

2.1 New or Revised Program Standards

Prior to publishing new or revised program standards, DIR shall comply with the requirements of 1 Texas Administrative Code Sections 202.27(d), 202.77(d) in its review and adoption of the Program Manual.

2.2 Administrative Changes

Administrative changes, such as formatting and grammatical corrections that are non-substantive or additions to out-of-scope cloud computing services, may be implemented without seeking input from external stakeholders or board approval. Administrative changes to the Program Manual are denoted by minor version changes (e.g., "Version 1.0 to 1.1" denotes such administrative changes, whereas "Version 1.0 to 2.0" indicates major changes requiring adherence to the stated requirements listed in *Section 2.1 New or Revised Program Standards*

Document version history may be found in *Section 23 Document Version History*.

2.3 Inquiries

Please direct questions to tx-ramp@dir.texas.gov.

3. Overview

TX-RAMP provides a standardized approach to the security assessment of cloud computing services. Cloud computing service is defined by Government Code Section 2157.007 as having the meaning assigned by the United States Department of Commerce National Institute of Standards and Technology (NIST) Special Publication 800-145. According to the NIST definition, cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

- Government Code Section 2054.0593 mandates that state agencies, as defined by Government Code Section 2054.003(13), 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 into or renewed on or after that date.

Each independent cloud computing service must obtain a distinct certification that reflects the specific characteristics, functions, and security controls of the service. The scope of the TX-RAMP certification for a particular cloud computing service is confined to the system components within the boundaries of the individual solution. This approach ensures that the certification process is both rigorous and relevant, accurately reflecting the security posture of each unique service while avoiding unnecessary duplication of assessments where services are substantively similar.

TX-RAMP has two baseline standards:

- **Level 1** for low impact information resources.
- **Level 2** for moderate or high impact information resources.

TX-RAMP has three certification types:

- **Level 1 Certification** is achieved after submission and DIR approval of the TX-RAMP Acknowledgment and Inventory Questionnaire and the TX-RAMP Level 1 Assessment Questionnaire or by achieving the corresponding accepted StateRAMP or FedRAMP authorization.
- **Level 2 Certification** is achieved after submission and DIR approval of TX-RAMP Acknowledgment and Inventory Questionnaire and the TX-RAMP Level 2 Assessment Questionnaire or by achieving the corresponding accepted StateRAMP or FedRAMP authorization.
- **TX-RAMP Provisional Certification** is achieved after submission and DIR approval of the TX-RAMP Acknowledgment and Inventory Questionnaire and is effective for 18 months from the date that DIR grants the provisional certification. Provisional certification may also be achieved after a cloud computing service receives an accepted status from StateRAMP or FedRAMP (see *Section 10.2 Certification Via External RAMPs* for additional information). A

provisional certification permits a state agency to contract for the use of a provisionally certified product for the length of the active provisional certification. After a cloud computing service achieves provisional certification, the cloud computing service must then achieve TX-RAMP Level 1 or Level 2 Certification through the TX-RAMP assessment process or achieve an accepted StateRAMP or FedRAMP status prior to the expiration of the provisional status period to maintain compliance with program requirements.

A state agency seeking to contract with a provider for cloud computing services is responsible for determining:

1) whether a cloud computing service is in scope for TX-RAMP and
2) the appropriate TX-RAMP level for the service based on the criteria set forth in this document.

A cloud service provider is responsible for submitting all required documentation to DIR. DIR shall confer TX-RAMP certification based on the provider's complete submission of required documentation.

4. Compliance Dates for Program Requirements

4.1 Compliance Date for Level 1 Certification

Cloud computing services subject to TX-RAMP Level 1 certification must obtain a TX-RAMP certification to contract with state agencies on or after January 1, 2024.

4.2 Compliance Date for Level 2 Certification

Cloud computing services subject to TX-RAMP Level 2 certification must obtain a TX-RAMP certification to contract with state agencies on or after January 1, 2022.

4.3 Provisional Certification Period

Cloud computing services that obtain TX-RAMP Provisional Certification must obtain a TX-RAMP Level 1 or Level 2 certification within 18 months from the date that Provisional Status is conferred as reflected in DIR's files, unless the cloud service has achieved an acceptable status within StateRAMP or FedRAMP in which case the provisional certification remains valid for the length of time the cloud service maintains the accepted status.

5. Responsibilities

All responsibilities are set forth in Government Code Section 2054.0593 and 1 Texas Administrative Code Chapter 202.

5.1 Agency Responsibilities

An agency that is contracting with a vendor to receive cloud computing services must comply with statutory requirements[1] and 1 Texas Administrative Code Chapter 202.[2]

These responsibilities include but are not limited to:

- Determining whether a contract with a vendor to provide cloud computing services is subject to TX-RAMP requirements.
- Determining whether a technology that the agency is contracting with a vendor to provide constitutes a cloud computing service.
- Ensuring that the agency's contract terms and conditions require appropriate compliance with TX-RAMP.
- Determining the minimum certification level required for a cloud computing service that the vendor is contracting with the agency to provide.

5.2 DIR Responsibilities

As required by law,[3] DIR must create a risk and authorization management program and is responsible for:

- Administering the TX-RAMP program, including creating and amending TX-RAMP administrative rules and the program manual as appropriate.
- Assessing and certifying cloud computing services.

5.3 Cloud Service Provider Responsibilities

As described by 1 Texas Administrative Code Chapter 202,[4] cloud service providers are responsible for:

- Providing assessment information and responding to TX-RAMP staff inquiries promptly.
- Maintaining compliance with security control requirements and notifying the appropriate parties if the cloud computing service loses its certification.
- Completing the required continuous monitoring reports.
- Notifying DIR and affected customers in the event of a breach of system security.[5]

---

[1] Gov't Code § 2054.0593.

[2] 1 Tex. Admin. Code §§ 202.27, 202.77.

[3] Gov't Code § 2054.0593; *see also* 1 Tex. Admin. Code § 202.5.

[4] 1 Tex. Admin. Code § 202.5.

[5] A cloud service provider must notify DIR and affected customers as required by this program manual in addition to any specific statutory or rule notification requirements that may apply due to the severity or number of impacted customers. Cloud service providers should consult with their legal counsel to determine whether a statute or rule requires specific types of notification in the event of a breach of system security.

6. Scope

6.1 Cloud Computing Services

Only cloud computing services, as defined by Government Code Section 2054.0593(a), are within scope for TX-RAMP.

According to the National Institute of Standards and Technology (NIST) in Special Publication 800-145, a cloud computing service must exhibit five essential characteristics. These characteristics define what makes a computing service a "cloud" service, and a service should meet all of these to be considered a cloud computing service:

1. **On-Demand Self-Service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each service provider.
2. **Broad Network Access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
3. **Resource Pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
4. **Rapid Elasticity**: Capabilities can be provisioned and released rapidly and, in some cases, automatically scale outward or inward commensurate with demand.
5. **Measured Service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Meeting these five essential characteristics is key to qualifying a service as a cloud computing service under the widely accepted NIST definition.

The state agency is ultimately responsible for determining whether a product meets the statutory definition of a cloud computing service and should consult with the agency's own information security personnel and legal counsel.

DIR reserves the right to review and approve or deny any request for TX-RAMP assessment of a given cloud service. DIR oversees the assessment process, which ensures that assessment resources are utilized judiciously and align with the broader cybersecurity objectives and regulations of the state of Texas.

7. Cloud Services Not Subject to TX-RAMP Certification

7.1 Non-substantive Use of Confidential State-controlled Data

Certain cloud computing services are out of scope of TX-RAMP certification due to the unique circumstances of the service.

Cloud computing services are out of scope of TX-RAMP certification provided the service is determined to be a low impact information resource that does not process or store confidential state-controlled data other than as needed for login capability or that processes or stores a negligible quantity and/or quality of confidential data. A state agency is responsible for determining whether the quantity and/or quality of confidential data is negligible.

Additionally, cloud services that process or store personally identifiable information provided for the purposes of purchasing, reserving, or booking for agency functions or solely for the purpose of enabling multifactor authentication do not require TX-RAMP certification.

A cloud computing service that meets the above requirements may be considered out of scope for TX-RAMP certification.

7.2 Common Categories of Cloud Services Not Subject to TX-RAMP Certification

The following types of cloud computing services may be determined to be out of scope for TX-RAMP certification. Contracting agencies may elect to require TX-RAMP certification for any of the following certifications, based on their assessment of risk and potential impact associated with the use of a given cloud computing service.

- **Consumption-Focused Cloud Computing Services**: Advisory services, market research, or other resources that are used to gather research or advisory information.
- **Graphic Design or Illustration Products**: Tools used for design tasks.
- **Geographic Information Systems (GIS) or Mapping Products**: Applications for geographic mapping and spatial analysis.
- **Email or Notification Distribution Services**: Platforms used for generic communication or notifications.
- **Social Media Platforms**: Tools for social interaction and public communication.
- **Survey Tools**: Survey tools not intended to collect confidential or regulated information.
- **Collaboration/Productivity Tools**: Standard collaboration tools for non-sensitive projects, such as shared document editing or project management.
- **Cloud Computing Services for Transmitting Non-Confidential Data**: Cloud computing services used to transmit data as required by external governing bodies for purposes of accreditation and compliance.
- **General Procurement/eCommerce Services**: Services used for purchasing supplies, travel and booking accommodations, reservations, or other general-purpose

procurement applications that only access payment information of the agency or agency personnel.

- **Public-facing Websites**: Hosting static, public-facing websites, or web content that does not process or store confidential state-controlled data.
- **Development and Testing Environments:** Utilizing cloud resources for development and testing activities for non-production, non-critical systems.
- **Educational or Training Platforms**: Cloud platforms that host training materials or educational content, excluding any data regarding sensitive personal information, regulated education records, or proprietary research.
- **Marketing and Social Media Analysis**: Tools used to gather and analyze public social media data, customer feedback, or market trends.

A cloud computing service that is out of scope of TX-RAMP is not subject to the TX-RAMP certification requirements. However, the cloud computing service must still comply with any required control baselines established by the Security Control Standards Catalog, all agency-specific security requirements, and any other applicable federal or statutory requirements.

A state agency is responsible for determining whether a cloud computing service is not subject to TX-RAMP certification, documenting the TX-RAMP scoping determination, and maintaining an internal record of cloud computing services that it has designated as out of scope.

7.3 Managed Services

Contracts for managed cloud services, the primary purpose for which are administration, oversight, deployment, maintenance, and other professional services, are out of scope of TX-RAMP.

7.4 Custom Developed Applications

Cloud services that are specifically designed, developed, and commissioned by an agency for a unique and bespoke solution are not subject to TX-RAMP certification. This does not include commercial off-the-shelf software platforms that are simply configured specifically for agency purposes.

An agency that contracts with a vendor for a bespoke cloud service solution is responsible for dictating the unique specifications and security requirements that must be fulfilled prior to the system becoming operational. Any such system must also comply with any statutory and regulatory requirements, including but not limited to any necessary security control standards required by the agency or DIR. The responsibility for assessing and securing the service in accordance with all applicable laws, regulations, and standards rests solely with the contracting agency. The agency must ensure that proper security controls, assessments, and validations are conducted throughout the development and implementation phases, aligning with the unique nature and specific requirements of the custom-built solution. Agencies are responsible for ensuring that any component cloud services, such as infrastructure as a service or platform as a service, used in the deployment of the custom-developed application comply with TX-RAMP requirements.

8. TX-RAMP Control Baselines

As specified by 1 Texas Administrative Code Sections 202.27, 202.77, there are two baseline standards for cloud computing services subject to TX-RAMP:

- TX-RAMP Low Impact Baseline (TX-RAMP Level 1); and
- TX-RAMP Moderate Impact Baseline (TX-RAMP Level 2).

TX-RAMP Low Impact Baseline (TX-RAMP Level 1)

TX-RAMP Level 1 certification is required for cloud computing services categorized by the agency as low-impact information resources.[6]

TX-RAMP Moderate Impact Baseline (TX-RAMP Level 2)

TX-RAMP Level 2 certification is required for cloud computing services categorized by the agency as moderate or high impact information resources.[7]

The security control criteria for the TX-RAMP impact baselines can be found in *Appendix A – TX-RAMP Control Baselines*.

Agencies are responsible for ensuring that high impact systems also have appropriate control requirements in place.

[6] As defined by 1 Tex. Admin. Code § 202.1.
[7] As defined by 1 Tex. Admin. Code § 202.1.

9. Minimum Baseline Determination

A state agency is responsible for determining the required TX-RAMP certification level for a cloud computing service. The state agency shall apply the criteria in the questions below when analyzing which certification is appropriate for the use of a particular product for a particular purpose. The state agency's analysis shall be the basis for the determination of the minimum TX-RAMP certification level.

It is at a state agency's discretion which agency-created and implemented data classification categories (e.g., public, sensitive, confidential, regulated, etc.) are subject to the below baselines. The broad categories of "nonconfidential" and "confidential" can include regulated, confidential, sensitive, and public data, but a state agency must determine which baseline is most appropriate for a cloud computing service that processes information classified by the state agency subject to the data classification policy implemented by that state agency.

A state agency should evaluate the following criteria to determine the applicable TX-RAMP minimum certification level. Refer to *Figure 1: TX-RAMP Level Determination Process*Figure 1: TX-RAMP Level Determination Process for a graphical representation of the determination process.

Is this a contract to provide cloud computing services for the agency?

- Yes → proceed to next question.
- No → TX-RAMP certification not required.

Does the cloud computing service meet the criteria for out-of-scope cloud computing services outlined in *Section 7 Cloud Services Not Subject to TX-RAMP Certification*Cloud Services Not Subject to TX-RAMP Certification***?***

- Yes → TX-RAMP certification not required.
- No → proceed to next question.

Is the cloud computing service intended to process or store confidential information?

- Yes → proceed to next question.
- No → The cloud computing service is not in scope of TX-RAMP and does not require TX-RAMP certification.[8]

"Confidential Information" has the meaning provided in 1 Texas Administrative Code Section 202.1. Information that is Confidential Information under this definition includes but is not limited to:

- *Dates of birth of living persons*
- *Driver's license numbers*
- *License plate numbers*
- *Credit card numbers*

[8] If the cloud computing service processes or stores confidential information at some time during the contract, then the state agency and cloud service vendor must collaborate to ensure compliance with TX-RAMP requirements.

- *Insurance policy numbers*
- *Attorney-Client communications*
- *Drafts of policymaking documents*
- *Information related to pending litigation*
- *Audit working papers*
- *Competitive bidding information before contract awarded*
- *Sensitive Personal Information*
- *Regulated data*
- *Information excepted from disclosure requirements of Government Code Chapter 552 ("Texas Public Information Act") or other applicable state or federal law*
- *Compliance reports for which the Texas Attorney General has granted permission to withhold*

At which impact level has the agency categorized the cloud computing service?

- Low → TX-RAMP Level 1 Certification required.
- Moderate → TX-RAMP Level 2 Certification required.
- High → TX-RAMP Level 2 Certification required.

Low impact information resources refer to 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:

- *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;*
- *result in minor damage to organizational assets;*
- *result in minor financial loss; or*
- *result in minor harm to individuals.*

Moderate impact information resources refer to 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:

- *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;*
- *result in significant damage to organizational assets;*
- *result in significant financial loss; or*
- *result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.*

High impact information resources refers to 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:

- *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;*
- *result in major damage to organizational assets;*
- *result in major financial loss; or*
- *result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.*

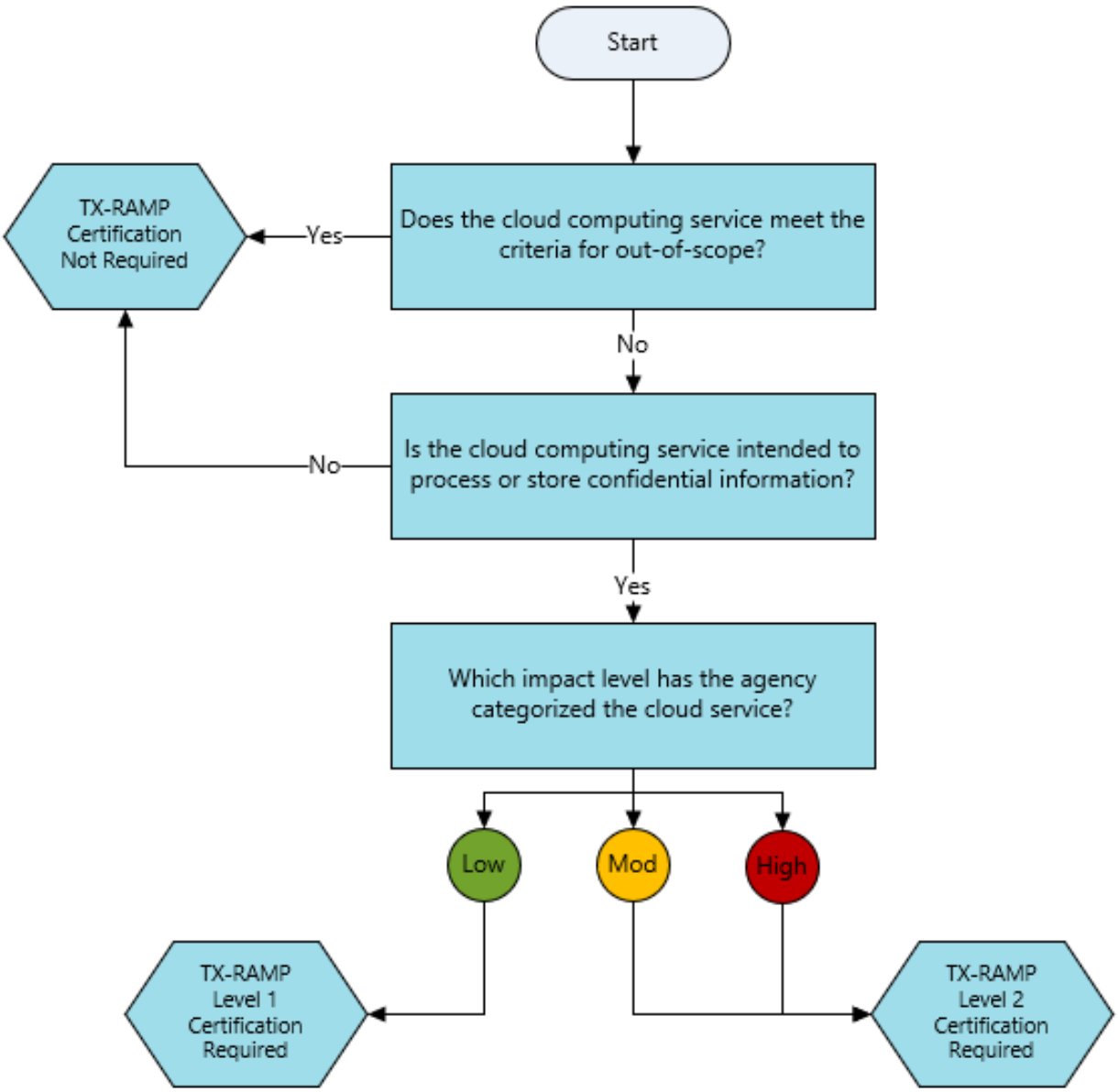

Figure 1: TX-RAMP Level Determination Process

10. TX-RAMP Certification

DIR will determine whether a certification is granted based upon DIR's review of an assessment and related documentation ("assessment"). This assessment entails DIR's review and approval of:

- The TX-RAMP Acknowledgment and Inventory Questionnaire; and
- The TX-RAMP Assessment Questionnaire, including all required documentation submitted to DIR by the cloud service provider.

10.1 TX-RAMP Certification Paths

TX-RAMP certification for any baseline level shall be achieved in one of two ways:

- DIR Conducted Assessment: A cloud service provider submits assessment responses and documentation to DIR for review; or
- Certification via External RAMP: A cloud computing service achieves the corresponding authorization of an approved risk and authorization management program at the appropriate impact level.

TX-RAMP Level 1 Certification may be conferred only after DIR reviews and approves provider assessment responses documenting that the cloud computing service aligns with the security standards for Level 1 as specified in *Appendix A – TX-RAMP Control Baselines* or upon achieving a corresponding equivalency through an external RAMP.

TX-RAMP Level 2 Certification may be conferred only after DIR reviews and approves provider assessment responses documenting that the cloud computing service aligns with the security standards for Level 2 as specified in *Appendix A – TX-RAMP Control Baselines* or upon achieving a corresponding equivalency through an external RAMP.

10.2 Certification Via External RAMPs

Cloud services that receive a designation on the FedRAMP marketplace[9] or StateRAMP authorized products list[10] will inherit a corresponding status within TX-RAMP. The TX-RAMP certification will remain valid as long as the cloud service maintains the appropriate status with the external RAMP (FedRAMP or StateRAMP). If a cloud service loses its external RAMP status, then it must comply with this program manual's requirements to ensure continued certification.

TX-RAMP does not have a Low-impact Software-as-a-Service (LI-SaaS) equivalent. Cloud computing services authorized with LI-SaaS will not inherit a TX-RAMP certification.

Certification via StateRAMP

DIR reconciles its certification records with StateRAMP on a regular basis to ensure that the cloud service status is reflected correctly across both programs.

[9] https://marketplace.fedramp.gov/products
[10] https://stateramp.org/product-list/

StateRAMP Provisional – StateRAMP Provisional status indicates that the cloud service progressing through the StateRAMP authorization process has met the mandatory minimum requirements, submitted a security package for Authorization consideration and is found to meet most but not all security requirements. Providers with a StateRAMP Provisional status comply with continuous monitoring requirements and submit further documentation to obtain authorization. Given the high degree of alignment between TX-RAMP security controls and the StateRAMP Provisional designation, combined with the continuous monitoring requirements, cloud computing services that have StateRAMP Provisional status will be granted the corresponding TX-RAMP Certification Level.

StateRAMP Ready – StateRAMP Ready status indicates that a cloud computing service has been assessed against the mandatory controls, approved by the StateRAMP Program Management Office (PMO), and entered the continuous monitoring phase. Given the independent review and continuous monitoring requirements, cloud computing services that have a StateRAMP Ready status will be granted TX-RAMP Level 1 Certification. StateRAMP Ready status may also be used for TX-RAMP Provisional Certification purposes in the event the cloud service requires a TX-RAMP Level 2 Certification.

StateRAMP Authorized – Cloud computing services that have a StateRAMP Authorization will be granted the corresponding TX-RAMP Certification Level (Low Impact for TX-RAMP Level 1, Moderate or High Impact for TX-RAMP Level 2).

StateRAMP Other Statuses – Other StateRAMP designations not specifically called out above may be eligible for TX-RAMP Provisional Certification; however, DIR will *not consider* StateRAMP Snapshot as a long-term certification solution. A StateRAMP Snapshot is a one-time gap assessment of the cloud service against the StateRAMP standards. A single StateRAMP Snapshot may be used to obtain TX-RAMP Provisional Certification, but the 18-month time restriction will still apply. Cloud services that enroll in the StateRAMP *Progressing* Snapshot program will receive TX-RAMP Provisional Certification for the length of enrollment within the progressing snapshot program.

Certification via FedRAMP

DIR reconciles its certification records with FedRAMP on a regular basis to ensure that the cloud service status is reflected correctly across both programs.

FedRAMP Authorized – Cloud computing services that receive a FedRAMP Authorization will be granted the corresponding TX-RAMP Certification Level (Low Impact for TX-RAMP Level 1, Moderate or High Impact for TX-RAMP Level 2).

FedRAMP In Process – Cloud computing services that receive a FedRAMP *In Process* designation will be granted TX-RAMP Provisional Certification. Once the cloud service receives authorization, then the corresponding TX-RAMP Certification Level will be granted.

FedRAMP Ready – Cloud computing services that receive a FedRAMP *Ready* designation will be granted TX-RAMP Provisional Certification. Once the cloud service receives authorization, then the corresponding TX-RAMP Certification Level will be granted.

11. TX-RAMP Provisional Certification

A valid TX-RAMP Provisional Certification permits agencies to enter or renew a contract for cloud computing services subject to TX-RAMP requirements prior to the services' receipt of a full TX-RAMP certification. TX-RAMP Provisional Certification is effective for 18 months from the date that the provisional certification is granted by DIR.

TX-RAMP Provisional Certification is achieved by completing the TX-RAMP Acknowledgment and Inventory Questionnaire. To initiate the questionnaire, a cloud service provider must complete the TX-RAMP Request Form as described in *Section 12 Assessment Process*.

11.1 Provisional Certification Considerations

TX-RAMP Provisional Certification does not indicate compliance with TX-RAMP security baseline standards of a cloud computing service product. State agencies should carefully evaluate their business needs and organizational risk considerations when selecting a provisionally certified cloud computing service.

State agencies contracting for a cloud computing service that has TX-RAMP Provisional Certification should consider additional rigorous contractual provisions protecting the state agency and its information and data. Such terms may include but are not limited to liquidated damages, termination, and disentanglement provisions and should be discussed with and decided upon by the state agency's general counsel and leadership.

11.2 Failure to Attain Full Certification before Provisional Status Expiration

Failure to attain TX-RAMP Level 1 or Level 2 certification prior to the expiration of the provisional certification will result in a lapse in certification. During this lapse, the cloud computing service will not be TX-RAMP-certified and, as such, will be noncompliant with TX-RAMP requirements unless the obligations stated in *Section 14 14Transitional Grace Period* have been met.

As provided by Government Code Section 2054.0593(f), a state agency shall require a provider contracting with the agency to provide the agency cloud computing services that are subject to TX-RAMP to maintain program compliance and certification throughout the term of the contract.

11.3 TX-RAMP Provisional Certification via FedRAMP or StateRAMP

TX-RAMP Provisional Certification may be granted for a cloud computing service that has achieved a FedRAMP or StateRAMP status other than authorized that indicates progress toward achieving FedRAMP or StateRAMP authorization.

TX-RAMP Provisional Certifications achieved via FedRAMP or StateRAMP are dependent upon the status of the cloud computing service under the respective program rather than the 18-month provisional period.

11.4 Agency-sponsored Interim Provisional Certification

A state agency may submit a request to sponsor a cloud computing service for a temporary pre-provisional interim certification through the Statewide Portal for Enterprise Cybersecurity Threat

Risk and Incident Management (SPECTRIM). Interim certifications are valid for up to 60 days from the date of issuance.

It is the responsibility of the requesting agency to inform the cloud service provider of its intent to sponsor the service for interim certification and communicate the process for attaining provisional certification to the cloud service provider. Once the cloud computing service attains TX-RAMP Provisional Certification, the interim certification is terminated. When possible, a cloud service provider should complete the provisional certification process directly.

12. Assessment Process

The following steps outline the typical workflow of progressing through the TX-RAMP process. DIR's review may differ slightly depending upon variables such as whether the certification process began under a prior version of the TX-RAMP Program Manual. Refer to *Figure 2: TX-RAMP High Level Process* for a graphical representation of the TX-RAMP high level process.

1. Initial Request

- Providers seeking certification of a cloud computing service must first complete the TX-RAMP Assessment Request form (request form) through the TX-RAMP webpage on the DIR website. The request form should be completed by the actual developer of the cloud service. SaaS providers should include their company as the manufacturer/developer, not the underlying IaaS provider.
- DIR staff review and process the form.

2. Engagement Record Creation

- Once the request information is vetted and approved, an engagement record is created.
- The engagement record serves as the central repository for information about the cloud service.

3. Acknowledgement and Inventory Form

- DIR launches the Acknowledgement and Inventory Form to the cloud service provider contact(s) via the Engage platform.
- Cloud service provider contact(s) complete and submit the form back to DIR.
- DIR staff review the submitted form and either approve it or request additional information.

4. Provisional Certification

- Once the Inventory and Acknowledgement Form is approved, DIR may grant provisional certification.

5. TX-RAMP Assessment Questionnaire

- After provisional certification is conferred, DIR launches the TX-RAMP assessment questionnaire to the contact(s) on file.
- The date the assessment questionnaire is launched may vary depending on the requested assessment initiation date.
- Cloud service provider completes the assessment questionnaire, including the TX-RAMP Security Plan (Control Implentation Workbook) and submits it to DIR.

6. Assessment Review

- The assessment goes into a queue. DIR will review assessments in the order that they are received.
- **DIR will not review incomplete submissions, including submissions that do not include all required information or provide incomplete documentation.**
- DIR will review the submitted information to determine whether certification may be granted.

7. Certification Approval

- DIR determines whether the certification is approved.
- Once approved, DIR updates the records and notifies the cloud service provider contact(s) of the decision.

8. Continuous Monitoring

- After certification is conferred, the cloud service enters the continuous monitoring period.
- Cloud service provider is responsible for completing the required continuous monitoring reports.

9. Recertification

- DIR sends recertification notifications to the listed cloud service provider contact(s) prior to the expiration of a certification.
- The cloud service provider may initiate the recertification process up to 12 months prior to the expiration of the certification.

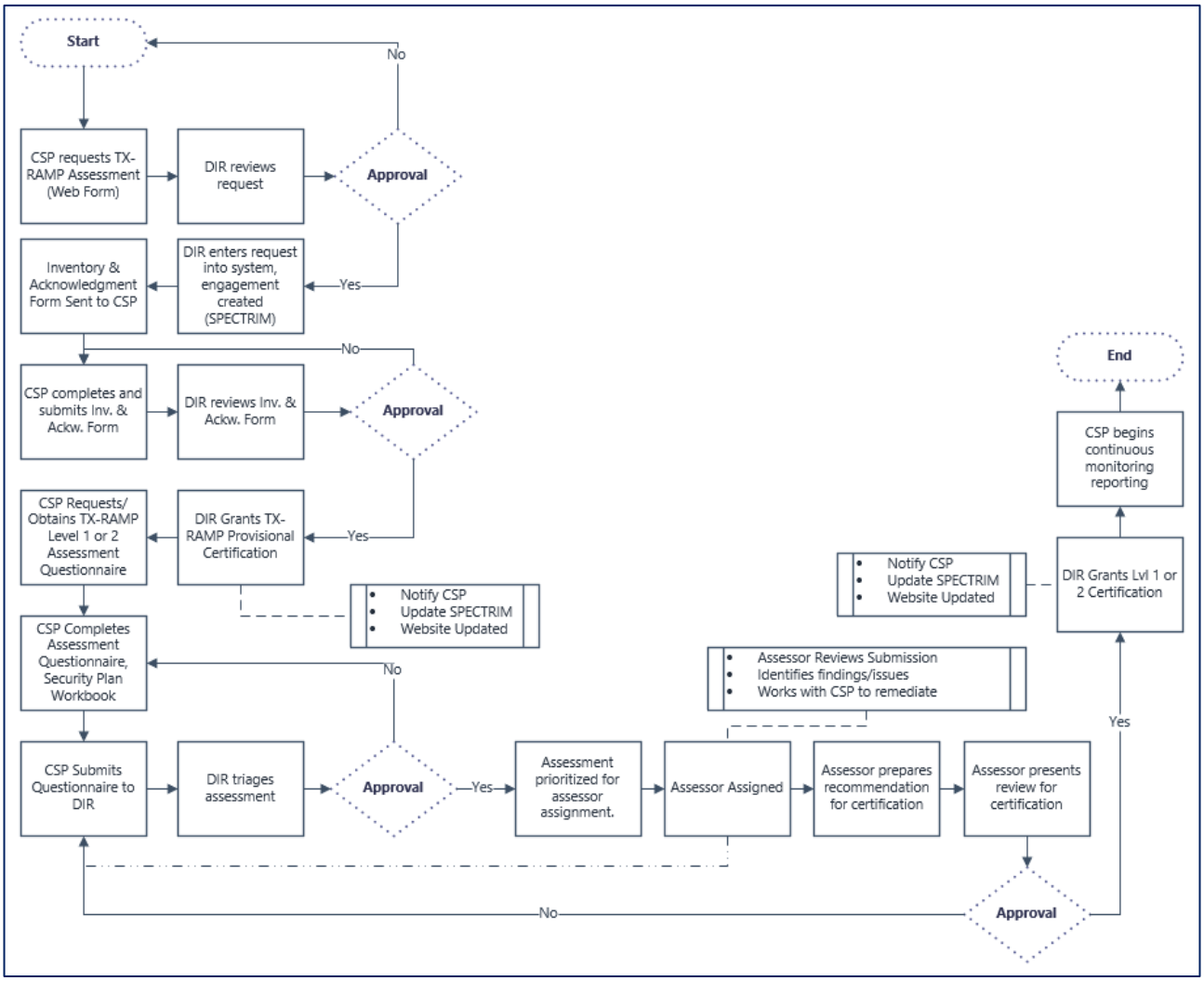

Figure 2: TX-RAMP High Level Process

13. Certification Extensions

13.1 TX-RAMP Provisional Certification Extensions

Cloud service providers may not apply for a new provisional certification for a cloud computing service that was previously granted a provisional certification and failed to achieve a Level 1 or Level 2 certification.

However, at DIR's discretion, a cloud computing service's provisional status may be extended for six months if the service has not received full TX-RAMP certification after the initial 18-month provisional certification.

If, at the expiration of the six-month extension, the provider has not yet received approval of their TX-RAMP certification, then DIR may grant an additional six-month extension if:

- The initial 18-month provisional certification and six-month extension have expired;
- the provider has begun the process to receive full TX-RAMP certification; and
- DIR has not completed the approval process.

It is at DIR's discretion to approve an additional three-month extension. DIR may consider provisional certification extension requests submitted by cloud service providers who do not meet the above criteria on a case-by-case basis.

13.2 TX-RAMP Provisional Certification Extension Request Process

The extension process is designed to provide cloud service providers with the opportunity to maintain their certification status while they complete necessary assessments or while DIR completes its review. It is important for cloud service providers to submit their extension request forms in a timely manner and to provide all necessary information to facilitate the review process.

Extension Request Submission: The cloud service provider submits the extension request form. This form should be filled out with all the necessary details and submitted before the expiration of the current provisional certification.

Form Review and Processing: Upon receiving the extension request form, DIR reviews the form. This involves checking the details provided in the form and assessing the reasons for the extension request.

Provisional Certification Extension: If the review process is successful, DIR may grant a provisional certification extension. The extension period can be up to 6 months, depending on the circumstances.

13.3 Automatic Extension

In certain situations, DIR will apply an automatic extension of a cloud services' provisional certification. This occurs when:

- The cloud service provider has submitted their assessment for review,
- DIR has not completed the review of the submitted assessment, and
- the expiration date of the current provisional certification is at minimum 6 months away.

In such a case, DIR will apply an automatic 6-month extension to the provisional certification. This ensures that the cloud service provider maintains their certification status while DIR completes the review process.

13.4 Level 1 and Level 2 Certification Extensions

Cloud computing services with an active but expiring Level 1 or 2 certification may apply for an extension of their active TX-RAMP certification using the extension request form. Level 1 or 2 certification extensions may be granted after DIR review and approval, not to exceed 6 months. DIR reserves the right to grant additional extensions on a case-by-case basis.

14. Transitional Grace Period

14.1 Purpose

The Transitional Grace Period is established to enable agencies to plan and execute an orderly transition from a non-compliant solution to a compliant solution if a certification lapses or is revoked. This approach recognizes the complexities involved in migrating to a new solution and allows for flexibility to ensure continuity of operations.

14.2 Agency Responsibilities

Agencies are responsible for developing, documenting, and adhering to a transition plan that meets the minimum criteria specified below. The agency must retain this documentation and ensure that all actions are taken in accordance with the plan's timelines.

While agencies are not required to submit the complete transition plan to DIR for review and approval, state agencies must adhere to the below-established criteria to demonstrate compliance with TX-RAMP requirements during the Transitional Grace Period and must submit a report to DIR of their intent to leverage the Transitional Grace Period in compliance with *Section 14.5 Reporting*.

14.3 Minimum Criteria for the Transition Plan

- **Identification of Affected Services**: Clearly list and describe the services affected by the lapse or revocation of certification.
- **Timeline for Transition**: Provide a realistic and achievable timeline for the migration to a compliant solution, including key milestones and deadlines. The timeline for transition may not exceed 24 months from planned inception to execution.
- **Risk Assessment**: Conduct a risk assessment to identify and mitigate potential security and operational risks during the transition.
- **Selection of Compliant Solution**: Detail the process for selecting a TX-RAMP compliant solution that meets the agency's needs.
- **Migration Strategy**: Outline the methods and procedures for migrating data and operations to the new solution, ensuring data integrity and availability.
- **Monitoring and Reporting**: Establish ongoing monitoring and internal reporting mechanisms to track progress and address any challenges or delays promptly.
- **Contingency Planning**: Include contingency measures to address unexpected issues or delays, ensuring uninterrupted service delivery.

14.4 Compliance

Agencies will remain in compliance with TX-RAMP requirements throughout the Transitional Grace Period if the transition plans meet the specified criteria and are executed in accordance with their documented timelines. Any deviations from or exceptions to the stated timeline must be communicated to DIR in compliance with *Section 14.5 Reporting*.

14.5 Reporting

Agencies that leverage the transitional grace period option must report the use of applicable services and their anticipated timeline for transition to DIR on a biennial basis. DIR will collect the usage information via SPECTRIM.

15. TX-RAMP Assessment Components

15.1 TX-RAMP Acknowledgment and Inventory Questionnaire

The TX-RAMP Acknowledgment and Inventory Questionnaire consists of the following components:

- Cloud Service Provider Acknowledgment of Texas Security Requirements; and
- Information Security Documentation Inventory.

Cloud Service Provider Acknowledgment of Texas Security Requirements

The acknowledgment form asks the cloud service provider to acknowledge that:

- Their company is or may be required to comply with certain statutory, rule, or contractual security requirements;
- they must provide an information security point of contact and a process for requesting security documentation or artifacts listed in the TX-RAMP Information Security Documentation Inventory, both of which may be shared with state agencies as authorized by the cloud service provider; and
- they authorize DIR to share the Cloud Service Provider Acknowledgment and TX-RAMP Information Security Documentation Inventory with state agencies.

Information Security Documentation Inventory

The TX-RAMP Information Security Documentation Inventory (ISDI) asks the cloud service provider to confirm the security documentation, questionnaires, certifications, or other designations that are available and relevant to the cloud computing service. The ISDI identifies the security documentation, questionnaires, certifications, or other designations that the cloud service provider will make available to a state agency upon request.

Cloud service providers must identify an information security point of contact and instructions on how a state agency may request documentation. The provider must submit any changes to the inventory or contact information as soon as reasonably possible.

15.2 TX-RAMP Assessment Questionnaire

The TX-RAMP Assessment Questionnaire (questionnaire) is the mechanism by which assessment responses and required documentation are collected from a cloud service provider. The questionnaire contains multiple choice, narrative, and file attachment questions to obtain information about the security posture of the cloud computing service. The questionnaire is a web-based information collection function of the SPECTRIM portal (Archer Engage platform).

The TX-RAMP assessment questionnaire is a critical component of the certification process, demanding careful and comprehensive completion. It consists of several key elements, each of which must be fully addressed for consideration. The assessment questionnaire consists of general questions about the system, company, and functionality as well as file upload attachments for the boundary and data flow diagrams to visually represent the architecture and operation of the service.

The assessment questionnaire also requires the cloud service provider's submission of a

completed TX-RAMP Security Plan Workbook. The TX-RAMP Security Plan Workbook asks the cloud service provider to describe the implementation status, details, and other relevant information related to each baseline control requirement. Cloud service providers should ensure that a sufficient level of detail is provided in the TX-RAMP Security Plan Workbook, fully outlining how each requirement is met. It's important to note that control family policies and procedures are not required to be submitted as part of the assessment questionnaire itself; however, they may be requested as evidentiary artifacts during the assessment process. All components of the assessment must be fully completed, and any omission or inadequacy may result in the application being deemed incomplete, potentially affecting eligibility for certification. This template will be made available on the TX-RAMP webpage of the DIR website.

15.3 TX-RAMP Security Plan Workbook Best Practices

When completing the control implementation descriptions required for assessment submission, there are several best practices that can help cloud service providers ensure accuracy, clarity, and compliance with the requirements.

Understand the Requirements: Thoroughly review the specific control requirements, guidelines, and expectations. Understanding the underlying principles helps in providing precise and relevant information.

Be Detailed and Specific: Offer clear, concise, and specific descriptions of how each control is implemented. Avoid vague or generic statements that could lead to ambiguity.

Use Standardized Terminology: Where possible, use industry-standard terminology and definitions. This ensures consistency and aids those reviewing the document in understanding the implementation.

Provide Evidence and Examples: Where applicable, include evidence or examples that demonstrate the implementation of the control. This could include references to specific policies, procedures, or technical configurations.

Align with Organizational Practices: Ensure that the descriptions accurately reflect the actual practices within the organization. Misalignment between description and practice can lead to non-compliance findings.

Avoid Unnecessary Jargon: While using standardized terminology is encouraged, avoid overly technical jargon that may not be understood by all readers. Keep the language accessible to a broader audience without losing precision.

Maintain Consistency: If there are multiple people working on the description, ensure that there is consistency in style, tone, and content across the document. Consider using templates or guidelines to achieve this.

Review and Validate: Have the description reviewed by subject matter experts within the organization, such as security professionals, legal advisors, or IT operations staff. This helps in identifying any gaps or inaccuracies.

Prepare for Verification: Be ready to provide further evidence or clarification if requested

during an assessment process. This includes having access to supporting documentation, policies, or artifacts.

Document Exceptions and Justifications: If there are deviations or exceptions to standard control implementations, provide a clear justification and explain how the associated risks are mitigated.

By adhering to these best practices, an organization can create a robust and clear control implementation description that not only meets the requirements of a specific framework like TX-RAMP but also provides a valuable internal reference for managing and maintaining the relevant controls.

15.4 Plan of Action and Milestones (POA&M)

Cloud service providers are required to develop a POA&M for each security control identified by either the vendor or DIR as deficient (i.e. not implemented, partially implemented). TX-RAMP requires POA&Ms exclusively for control deficiencies rather than individual vulnerabilities as part of the assessment process.

The POA&M serves to bridge the gap between the services' current state and the TX-RAMP required state, facilitating a better understanding of how these control deficiencies will be addressed. The cloud service provider must generate or otherwise provide a POA&M for each control deficiency and submit these with the TX-RAMP assessment questionnaire. DIR will review POA&Ms during the assessment phase and determine whether the proposed solution sufficiently addresses the failed control.

To ensure consistency, clarity, and completeness, POA&Ms must adhere to the specified format provided by DIR within the TX-RAMP Security Plan Control Workbook.

POA&Ms should be revisited by the cloud service provider on at least a quarterly basis. Once a cloud service provider fully implements a POA&M, the cloud service provider must report the closure of the POA&M to DIR through the next regularly scheduled continuous monitoring report.

16. TX-RAMP Fast Track Assessment

16.1 TX-RAMP Fast Track Assessment Overview

The TX-RAMP Fast Track Assessment is a streamlined process designed to expedite the certification of cloud service providers by allowing providers to leverage existing DIR-approved third-party assessments or audit reports to provide verified evidence of security practices.

As a reminder, DIR cannot enter into any form of nondisclosure agreements with cloud service providers for any components of the TX-RAMP process, including the review of third-party assessment or audit reports required to leverage the Fast Track certification route.

16.2 Third-party Assessment Acceptance Criteria

A cloud service provider may submit third-party assessments or audit documents described by *Section 16.3 Accepted Fast Track Documentation* to DIR for consideration in determining whether the service qualifies for the Fast Track assessment process. This must be done in compliance with the procedures outlined by this section.

DIR reserves the right to accept or reject third-party assessments or audit documents when determining whether a cloud service is eligible for the Fast Track TX-RAMP Assessment process. While these external evaluations can potentially expedite DIR's assessment process, DIR is not obligated to accept these external evaluations. DIR maintains full discretion in its decision-making process, ensuring that all certifications meet the stringent standards set by the TX-RAMP program.

To even be considered for Fast Track assessment, a cloud service provider's documentation must be an assessment or audit listed by *Section 16.3 Accepted Fast Track Documentation* that has been conducted within the previous twenty-four (24) months. This ensures that the evaluation accurately reflects the security posture of the service in question.

16.3 Accepted Fast Track Documentation

DIR accepts the below third-party assessments or audit reports to be considered for Fast Track assessment:

- SOC 2 Type 2;
- HITRUST Authorized External Assessor Validated Assessment;
- PCI DSS Qualified Security Assessor Audit Report on Compliance;
- Any third-party assessment or audit artifacts authorized by DIR and posted as part of the comprehensive list on its website, as described below.

At its discretion, DIR may evaluate and determine that additional third-party assessment or audit artifacts are acceptable for the TX-RAMP Fast Track assessment process. DIR will publish any additional acceptable third-party assessment or audit reports on the TX-RAMP webpage.

A third-party assessment or audit artifact that is not included in the above list or identified by the comprehensive list posted to the DIR website cannot be used for the Fast Track assessment process.

Third-party certification, assessment, or audit reports must be relevant to the cloud service seeking the Fast Track option. Security artifacts related to the underlying IaaS of a SaaS do not qualify for the TX-RAMP Fast Track assessment process.

16.4 TX-RAMP Level 1 Fast Track Assessment

At DIR's discretion, a cloud computing service may qualify for Level 1 Certification based wholly or in part on DIR's review of an accepted third-party certification, assessment, or audit report covered by *Section 16.3 Accepted Fast Track Documentation*.

DIR may require additional information as needed to determine whether certification can be granted.

16.5 TX-RAMP Level 2 Fast Track Assessment

At DIR's discretion, a cloud computing service seeking Level 2 certification may qualify for assessment by the Fast Track process based on the results of an independent third-party certification, assessment, or audit report. A cloud service that qualifies for a Level 2 Fast Track assessment is not guaranteed a TX-RAMP certification; qualifying for the Level 2 Fast Track assessment simply allows the vendor to provide potentially reduced documentation based upon DIR's review and acceptance of the certification, assessment, or audit report.

If a cloud service qualifies for Level 2 Fast Track Assessment, DIR will create a tailored assessment questionnaire for the cloud service provider's completion and submission. This allows DIR to streamline the assessment review and certification process.

16.6 Fast Track Request Process

Cloud service providers seeking the Fast Track process for a cloud service must complete the TX-RAMP Fast Track Request Form. Cloud services currently undergoing a full TX-RAMP assessment may elect to switch to the Fast Track process. Once the initial request is processed and approved, DIR will launch a questionnaire to collect the third-party assessment or audit report. DIR will review the artifacts and determine whether the service qualifies for the Fast Track process. If the service qualifies, then DIR will launch a subsequent Fast Track questionnaire to the cloud service provider.

16.7 Fast Track Continuous Monitoring

Cloud services that receive TX-RAMP certification through the Fast Track process are subject to the same continuous monitoring requirements as the services that obtain certification by the standard assessment process as detailed in *Section 18 Continuous Monitoring*.

17. Assessment Considerations

17.1 Time Required to Complete Assessment Review

The length of DIR's assessment of a certification request depends on several factors including but not limited to:

- Completeness of cloud service provider documentation and responses;
- TX-RAMP assessment level; and
- Cloud service provider responsiveness to DIR outreach.

Cloud service providers are expected to respond to DIR requests for clarification or additional evidence of compliance within 10 business days. Failure to respond to requests for clarification in a timely manner may result in rejection of the assessment and may require resubmission and reprioritization.

DIR is not responsible for delays in a state agency's procurement because of a cloud service provider's lack of responsiveness.

17.2 SaaS and Subservice Cloud Providers

Software as a Service (SaaS) applications operating on a cloud infrastructure/platform (IaaS/PaaS) product do not inherit the underlying TX-RAMP certification from the cloud infrastructure provider. Separate certifications are required for SaaS products that leverage certified cloud infrastructure products. The SaaS product may, however, inherit applicable controls from the certified infrastructure.

The SaaS cloud service provider is responsible for providing evidence of compliance with required controls and documentation related to the non-inheritable controls to achieve TX-RAMP certification.

Significant changes, as described in *Section 18.4 Significant Change Reporting*, in the infrastructure of the SaaS solution must be reported to DIR.

17.3 Cloud Reseller Functions

Primary contracting cloud service providers, including cloud service providers who resell cloud computing services, shall specifically identify which of the products provided are or include cloud computing services, as defined by Government Code Section 2157.007, and ensure that they have a point of contact for the vendor providing cloud computing services. A reseller shall coordinate assessment responses with cloud computing service vendors. If a cloud computing service is already certified, the reseller shall require the cloud computing service's vendor to provide documented evidence of the service's TX-RAMP certification to them for ready provision to DIR and any state agency contracting with the reseller for the cloud computing service.

18. Continuous Monitoring

18.1 Overview

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. Performing ongoing security assessments determines whether the set of deployed security controls in a cloud computing service remains effective considering new exploits and attacks and planned and unplanned changes that occur in the system and its environment over time.

DIR Support of State Agencies in Continuous Monitoring

State agencies shall require cloud service providers to ensure that TX-RAMP-certified cloud computing services are routinely assessed and monitored for compliance with required security controls and demonstrate that the security posture of the cloud computing services offered is acceptable to maintain TX-RAMP certification.

DIR established the continuous monitoring criteria below for cloud service providers contracting with state agencies for cloud computing services. State agencies may require additional continuous monitoring activities directly through contractual agreements.

Should a state agency identify significant concerns related to the security posture of a certified cloud computing service, the agency shall notify DIR of the identified concern. DIR will provide any assistance to state agencies in resolving the collection of the necessary documentation and, if appropriate, may revoke the cloud computing service's TX-RAMP certification due to the provider's failure to provide accurate or timely documentation as described below.

Continuous Monitoring for Services TX-RAMP Certified via StateRAMP or FedRAMP

If a cloud computing service has been TX-RAMP certified through the FedRAMP or StateRAMP equivalent acceptance process, then the cloud service provider will not be required to provide continuous monitoring artifacts to DIR. State agencies contracting with a cloud service provider who has attained TX-RAMP certification by another risk and authorization management program should consider the addition of rigorous, additional contractual provisions requiring continuous FedRAMP or StateRAMP (as appropriate) acceptable status and notification requirements if such certification is revoked or otherwise removed.

18.2 Vulnerability Reporting

DIR established the following minimum continuous monitoring requirements to ensure that cloud service providers comply with TX-RAMP. Any additional continuous monitoring requirements are at the discretion of the contracting state agency.

For TX-RAMP Level 2 Certified cloud computing services, cloud service providers must provide quarterly vulnerability reports of identified vulnerabilities and mitigation activities to DIR through the SPECTRIM Vendor Portal.

For TX-RAMP Level 1 Certified cloud computing services, cloud service providers must provide annual vulnerability reports of identified vulnerabilities and mitigation activities to DIR through the SPECTRIM Vendor Portal.

Vulnerability reporting for a given cloud service should be related to the assets used in the delivery of the certified service to include application, database, and infrastructure vulnerabilities where applicable.

Vulnerability severity categorization is based on the NIST National Vulnerability Database Common Vulnerability Scoring System (most current version).[11]

As part of the vulnerability reporting, cloud service providers must report identified vulnerabilities with the vulnerability severity category along with:

- a description of remediation plans; or
- mitigation activities associated with high and critical-severity vulnerabilities if the cloud service provider is not remediating the vulnerability.

Cloud service providers shall submit vulnerability reporting documentation through the SPECTRIM Vendor Portal. The SPECTRIM Vendor Portal will provide notice to the designated cloud service provider point of contact to complete the continuous monitoring questionnaires at the required interval. Once submitted, DIR will log the associated vulnerability report information to the TX-RAMP certified cloud computing service in SPECTRIM and make it available to state agencies who have indicated that they are contracting for that cloud computing service.

State agencies are responsible for developing a risk-based approach to the review of relevant TX-RAMP continuous monitoring reports. DIR may require greater frequency of continuous monitoring activities or revoke a cloud service provider's TX-RAMP certification if the cloud service provider does not remediate or adequately address identified vulnerabilities through compensating controls within the prescribed timelines.

DIR reserves the right to intervene and conduct an impromptu request for evidence regarding vulnerability management practices.

Table 1: Vulnerability Severity Reporting Requirements

CVSS Severity	Reporting Components
Low (0.1-3.9)	•Number Identified During Reporting Period •Number Remediated During Reporting Period •Number of Existing Vulnerabilities
Medium (4.0-6.9)	•Number Identified During Reporting Period •Number Remediated During Reporting Period •Number of Existing Vulnerabilities
High (7.0-8.9)	•Number Identified During Reporting Period •Number Remediated During Reporting Period •Number of Existing Vulnerabilities •Planned/Current Remediation •Activities/Mitigating/Compensating Controls

[11] NIST National Vulnerability Database: https://nvd.nist.gov/vuln-metrics/cvss

Critical (9.0-10.0)	•Number Identified During Reporting Period •Number Remediated During Reporting Period •Number of Existing Vulnerabilities •Planned/Current Remediation •Activities/Mitigating/Compensating Controls

18.3 Reporting Breach of System Security

A cloud service provider whose cloud computing service is certified by TX-RAMP shall disclose any breach of system security of the certified cloud offering in compliance with Texas Business & Commerce Code Section 521.053. A cloud service provider whose TX-RAMP-certified service has a breach of system security shall notify DIR within 48 hours of becoming aware of the breach of system security. A breach of system security notifications must be sent by authorized company officials to tx-ramp@dir.texas.gov with a description of the incident, potentially impacted Texas customers, and any additional relevant information.

A cloud service provider must report a suspected or confirmed breach to appropriate parties as required by law. If the suspected or confirmed breach involves the unauthorized disclosure of 250 or more Texans, the cloud service provider must also report the breach to the Office of the Attorney General of Texas as required by law.

18.4 Significant Change Reporting

Significant changes to a cloud computing service, as determined by DIR, may warrant an update to certification upon notification of a change and identification of that change as significant. A significant change is defined as an alteration to a cloud computing service that has a high probability to impact the security posture of the system.

Cloud service providers may occasionally need to make changes (e.g. technical, administrative) to their cloud computing services. As the initial assessment and certification is performed at a certain point in time, it is important to identify any impacts future changes have on the security posture of the cloud computing service. Some changes may have minimal impact on the security of the service while others may warrant additional review to ensure the cloud computing service is maintaining compliance with security requirements.

A significant change is a change that is likely to negatively affect the security state of the information system. Nonsignificant changes would typically be addressed by the cloud service provider's Configuration Management Plan. Significant changes, however, are those outside of typical change management, the scope of which would call the initial assessment judgment into question because of the significance of the change to the product.

A cloud service provider must report significant changes to a certified service to DIR within 30 days of the date that the change is made. A cloud service provider may also report a significant change to a service to the state agencies with whom they contract; this would not, however, meet the requirement to report significant changes to DIR.

DIR is responsible for completing an updated service certification review resulting from a significant change. This review shall be limited to an assessment of any documentation DIR deems necessary to determine the impact of the significant change upon the service.

DIR will determine whether a change identified by the cloud service provider or reported by a contracting state agency qualifies as a significant change and whether the change warrants a review of the certification status.

19. Dispute Resolution

19.1 Appeals Process

Request for Appeal to the State of Texas Chief Information Security Officer

Cloud service providers or primary contractors/resellers acting on behalf of a cloud service provider may appeal a TX-RAMP certification decision directly impacting their cloud computing service by emailing a written request for appeal containing any information pertinent to the issue to TX-RAMP@dir.texas.gov. A cloud service provider may not appeal the certification decision of another service provider's product. The State of Texas Chief Information Security Officer shall review the request for appeal and any necessary documents before issuing a determination either upholding or overturning the initial decision regarding the cloud computing service's certification decision.

Final Request for Appeal to the DIR Executive Director

If the State of Texas Chief Information Security Officer has issued a determination with which a cloud service provider disagrees, the cloud service provider may submit a final request for appeal in writing addressed to DIR's Executive Director at TX-RAMP@dir.texas.gov. This step may only be taken if the cloud service provider has submitted a request for appeal to the State of Texas Chief Information Security Officer and they have already issued a determination regarding the request for appeal. Upon receipt of the final request for appeal, the Executive Director shall review the final request for appeal and any necessary documents before issuing a final determination.

19.2 Grievance Process

A state agency may file a grievance or complaint against a TX-RAMP certified cloud service provider if the state agency obtains credible information that a cloud service provider has deviated from the requirements of TX-RAMP by emailing TX-RAMP@dir.texas.gov.

DIR will evaluate grievances to determine whether corrective action or revocation of certification status are warranted.

20. Certification Revocation

DIR reserves the right to revoke TX-RAMP certification status at its discretion.

Failure of a cloud service provider to maintain baseline compliance with TX-RAMP requirements described by this Program Manual will result in revocation of a product's TX-RAMP certification. Events that will result in a revocation include but are not limited to the following:

- Failure to inform required parties in a timely manner of significant changes to the cloud computing service;
- Failure to inform required parties of the loss of other accepted risk and authorization management program (e.g. FedRAMP, StateRAMP) certification;
- Failure to provide required continuous monitoring documents;
- The report of false or misleading information to DIR or a state agency;
- Referencing non-certified cloud computing services as TX-RAMP certified; and
- Failure to report a breach of system security to DIR within 48 hours of discovery.

If a cloud service provider fails to maintain a cloud computing service offering's FedRAMP, StateRAMP, or other DIR-accepted risk and management authorization program certification and that is the basis for the cloud computing service's TX-RAMP certification, the loss of such certification will result in the automatic revocation of the service's TX-RAMP certification as soon as DIR receives notice or otherwise becomes aware of the lapse. DIR shall review the circumstances of any reported violation of the TX-RAMP program to determine if a product's TX-RAMP certification shall be revoked.

21. Recertification

TX-RAMP Level 1 and Level 2 certifications are valid for three years from the date the last certification was conferred upon a cloud computing service, provided that the cloud service provider is compliant with the program requirements enumerated in this Program Manual. 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. This email will include instructions for completing the recertification process. 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.

22. Program Certification Change Management

22.1 Provisional Certifications Granted Under Program Manual Version 1.0

Provisional certifications granted under the TX-RAMP Program Manual Version 1.0 (via state agency sponsored and third-party audit or assessment) will remain valid for the initial length of the provisional certification and any extensions thereto. A cloud service provider must complete the TX-RAMP Acknowledgment and Inventory Questionnaire prior to being granted TX-RAMP Level 1 or Level 2 Certification for products with TX-RAMP Provisional Certification granted under the TX-RAMP Program Manual Version 1.0.

22.2 Level 1 and 2 Assessments Begun Under Program Manual Version 1.0

If a cloud service provider initiated a TX-RAMP Level 1 or Level 2 Assessment prior to the effective date of this manual, the provider may elect to either complete that assessment for review and certification or request to undergo the new assessment process established by the revised program structure instead. A cloud service provider that elects to pursue its certification through the assessment process established by the TX-RAMP Program Manual Version 1.0 must still complete the TX-RAMP Acknowledgment and Inventory Questionnaire prior to its receipt of TX-RAMP certification.

22.3 Control Changes Compliance Timeline

As the TX-RAMP program evolves, it may adopt or modify security control requirements to stay aligned with prevailing standards and threats. Cloud service providers are expected to remain responsive to these changes and adhere to any updated requirements promptly. For control changes that go beyond administrative or superficial adjustments, cloud service providers must implement the new or revised controls no later than 18 months from the date the changes are formally adopted by the program. It is incumbent upon cloud service providers to develop a systematic and well-articulated plan to meet these new or revised control requirements within the prescribed timeline. This plan should encompass a clear understanding of the changes, an implementation strategy, and necessary resources allocation. If a cloud service provider anticipates any challenges in satisfying the controls within the specified timeframe, it must timely communicate these concerns to DIR.

23. Document Version History

Version	Date	Comments
1.0	October 28, 2021	Initial Publication
2.0	October 20, 2022	1st Major Revision: • Control Alignment with NIST 800-53 Revision 5 • Added TX-RAMP Acknowledgement and Inventory • Extension of provisional certification beyond January 1, 2023 • Modified provisional certification process and criteria • Added provisional certification extension requests • Clarification to out-of-scope services • Modified required documentation • Administrative/clerical revisions • TX-RAMP Level 1 Certification requirements effective date changed from January 1, 2023 to January 1, 2024
3.0	TBD	2nd Major Revision: • Added POA&M requirement • Revised StateRAMP/FedRAMP inheritance language • Added/revised determination process • Added/revised high level process • Added transition plan/period • Clarified services not subject to TX-RAMP Certification • Revised/aligned control impact baselines • Added TX-RAMP Fast Track Assessment process • Added section addressing new or revised controls • Added Transitional Grace Period • Revised Significant Change requirements • Added Responsibilities Section

24. Appendix A – TX-RAMP Control Baselines

TX-RAMP Baseline Controls 2.0.xlsx

TX-RAMP Level	Number of Controls/Enhancements Assessed
Level 1	**117**
Level 2	**223**

CONTROL FAMILY	TX-RAMP LEVEL 1	TX-RAMP LEVEL 2
ACCESS CONTROL	9	33
AUDIT AND ACCOUNTABILITY	10	11
AWARENESS AND TRAINING	4	6
CONFIGURATION MANAGEMENT	9	21
CONTINGENCY PLANNING	6	11
IDENTIFICATION AND AUTHENTICATION	10	16
INCIDENT RESPONSE	7	10
MAINTENANCE	4	9
MEDIA PROTECTION	4	7
PERSONNEL SECURITY	8	8
PHYSICAL AND ENVIRONMENTAL PROTECTION	9	17
PLANNING	3	5
RISK ASSESSMENT	6	8
SECURITY ASSESSMENT AND AUTHORIZATION	8	9
SYSTEM AND COMMUNICATIONS PROTECTION	8	23
SYSTEM AND INFORMATION INTEGRITY	6	13
SYSTEM AND SERVICES ACQUISITION	6	16
TOTAL	**117**	**223**

25. Appendix B – Required Documentation

Cloud service providers are required to complete the TX-RAMP Security Plan Workbook as part of the Level 1 and Level 2 assessment submissions. This document will be made available on the TX-RAMP webpage of the DIR website. Additional documentation or artifacts may be requested by DIR as part of the assessment process to provide evidence of compliance.

26. Appendix C – Glossary of Terms

Assessment – DIR review of a cloud service provider or state agency request for assessment of a product and all related documentation.

Breach of System Security – As defined by Business & Commerce Code Section 521.053(a).

Cloud Computing Service – As defined by Government Code Section 2054.0593(a). A cloud computing service may also be referenced as a cloud offering.

Cloud Service Provider - Vendor of a cloud computing service. A cloud service provider may also be referenced as a cloud computing vendor or a cloud computing services provider or vendor.

FedRAMP – Federal Risk and Authorization Management Program.

Infrastructure as a Service (IaaS) – The meaning assigned by Special Publication 800-145 issued by the United States Department of Commerce National Institute of Standards and Technology, as the definition existed on January 01, 2015.

Low Impact Information Resources – As defined by 1 Texas Administrative Code Section 202.1.

Nonconfidential Data – Information that is not required to be or may not be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement.

Platform as a Service (PaaS) – The meaning assigned by Special Publication 800-145 issued by the United States Department of Commerce National Institute of Standards and Technology, as the definition existed on January 01, 2015.

Private Cloud Deployment – The meaning assigned by NIST SP 800-145 issued by the United States Department of Commerce National Institute of Standards and Technology, as the definition existed on January 01, 2015.

Program Manual – Program manual for the Texas Risk and Authorization Management Program.

State-controlled Data – As defined by 1 Texas Administrative Code Section 202.1.

Software as a Service (SaaS) – The meaning assigned by Special Publication 800-145 issued by the United States Department of Commerce National Institute of Standards and Technology, as the definition existed on January 01, 2015.

StateRAMP – The risk and authorization management program, built upon the National Institute of Standards and Technology Special Publication 800-53 and modeled after the FedRAMP program, that provides state and local governments a common method for verification of cloud security.

TX-RAMP – The Texas Risk and Authorization Management Program.