Texas Risk and Authorization Management Program Manual

Effective Date

This publication takes effect on 12/01/2022

Table of Contents

1. Purpose

Texas Government Code § 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

A. New or Revised Program Standards

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

B. 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 1. A. New or Revised Program Standards).

Document version history may be found here.

3. Inquiries

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

4. Overview

TX-RAMP provides a standardized approach to the security assessment of cloud computing services. Cloud computing service is defined by Texas Government Code § 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."

- Texas Government Code § 2054.0593 mandates that state agencies, as defined by Texas Government Code § 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 products entered into or renewed on or after that date.

TX-RAMP has two baseline standards:

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

TX-RAMP has three statuses:

- **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 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 status based on the provider's complete submission of required documentation.

5. Compliance Dates for Program Requirements

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.

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.

Cloud computing services that obtain TX-RAMP Provisional Certification must obtain a TX-RAMP Level 1 or Level 2 certification (or achieve an accepted StateRAMP or FedRAMP status) within 18 months from the date that Provisional Status is conferred as reflected in DIR's files.

6. TX-RAMP Level Determination

Only cloud computing services, as defined by Texas Government Code § 2054.0593(a), are within scope for TX-RAMP. A state agency may use the essential characteristics list found in *Appendix D – Guidelines for Determining a Cloud Computing Service* to determine whether a product or service is subject to TX-RAMP. 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.

A. Characteristics and Categories of Cloud Computing Services Not Subject to TX-RAMP

Certain cloud computing services are out of scope of TX-RAMP due to the unique characteristics of the cloud computing service. Cloud computing services are out the scope of TX-RAMP provided the service does not[1]:

> (1) process, store, or transmit confidential state-controlled data (except as needed to provide a login capability or as it relates to ecommerce purchasing/reserving/booking for agency functions, e.g. username, password, email, or information required for enabling multifactor authentication); or
>
> (2) have access to read or modify confidential state-controlled data on agency systems such that any security incident might affect such systems.

A cloud computing service that meets the above requirements may be considered out of scope of TX-RAMP if the services falls under one of the following characteristics and categories:

- Consumption-focused cloud computing services such as advisory services, market research, or other resources that are used to gather research or advisory information;
- Graphic design or illustration products;
- Geographic Information Systems (GIS) or mapping products;
- Email or notification distribution products;
- Social media platforms and products;

[1] While these cloud services are out of scope, agencies should still use care when procuring or using such services.

- Survey, scheduling, or general business productivity products;
- Cloud computing services used to deliver training;
- Cloud computing services used to transmit copies of nonconfidential data as required by external governing bodies for purposes of accreditation and compliance; and
- Web applications or 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.
- Low Impact Software-as-a-Service products as defined by the following criteria:
    - The cloud computing service meets the definition of a Software as a Service (SaaS), as defined by the NIST definition of cloud computing in SP 800-145;
    - The cloud computing service does not contain personal identifying information or personally identifiable information, except as needed to provide a login capability (e.g. username, password email address, or information required for enabling multifactor authentication) or for the purpose of purchasing supplies, reserving, and/or booking agency functions through an e-commerce cloud computing service; and
    - The cloud computing service is a low impact information resource as defined by 1 Texas Administrative Code § 202.1.

A cloud computing service that is out of scope of TX-RAMP is not subject to the TX-RAMP certification requirements established herein. 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 out of scope for TX-RAMP and maintaining an inventory of cloud computing services that it has designated as out of scope.

B. Baseline Standards for Cloud Computing Services within TX-RAMP Scope

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

- TX-RAMP Public Controls Baseline (TX-RAMP Level 1); and
- TX-RAMP Confidential Controls Baseline (TX-RAMP Level 2).

TX-RAMP Public Controls Baseline (TX-RAMP Level 1)

TX-RAMP Level 1 is required for cloud computing services that store, process, or transmit the nonconfidential data of a state agency or the cloud computing service is determined to host low-impact information resources as defined by 1 Texas Administrative Code § 202.1. The assessment criteria for this baseline can be found in *Appendix A – TX RAMP Control Baselines*.

TX-RAMP Confidential Controls Baseline (TX-RAMP Level 2)

TX-RAMP Level 2 is required for cloud computing services that store, process, or transmit the confidential data of a state agency and the cloud computing service is determined to host

moderate or high impact information resources. The assessment criteria for this baseline can be found in *Appendix A – TX-RAMP Control Baselines*.

C. State Agency Data Classification and Impact Assessment

A state agency seeking to contract for a cloud computing service is responsible for determining the required TX-RAMP certification level for the 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.

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

If the answer is "no," then TX-RAMP certification is not required.

If the answer is "yes," proceed to the next question.

Does the cloud computing service meet the criteria for out-of-scope cloud computing services outlined in Section 6. A. Characteristics and Categories of Cloud Computing Services Not Subject to TX-RAMP?

If the answer is "yes," TX-RAMP certification is not required, and the agency should internally document the justification.

If the answer is "no," proceed to the next question.

Does (or will) the cloud computing service process, store, or transmit only low impact information resources?

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.*

If the answer is "yes," TX-RAMP Level 1 Certification is required.

If the answer is "no," proceed to the next question.

Does (or will) the cloud computing service process, store, or transmit confidential information?

"Confidential Information" has the meaning provided in 1 Texas Administrative Code § 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*
- *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 Texas 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*
- *Investigative audit working papers and draft reports excepted from disclosure under Texas Government Code § 552.116*

If the answer is "no," TX-RAMP Level 1 Certification is required.

If the answer is "yes," TX-RAMP Level 2 Certification is required.

7. 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 documentation submitted to DIR by the provider either with the initial application or as a supplement to the initial application.

A. TX-RAMP Certification Levels

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

- A cloud service provider submits assessment responses and documentation to DIR for review; or
- 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 a provider completes and submits all assessment responses to DIR 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 the corresponding StateRAMP or FedRAMP authorization.

TX-RAMP Level 2 Certification may be conferred only after a provider submits all assessment responses to DIR 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 the corresponding StateRAMP or FedRAMP authorization.

B. 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 7.C Assessment Process.

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 attained 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.

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.

As provided by Texas Government Code § 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.

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 One or Level Two 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 three-month extension if:

- The provider's 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.

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 current status of the cloud computing service under the respective program, rather than the 18-month provisional period.

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 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.

C. Assessment Process

Assessment Initiation

Cloud service providers seeking certification of a cloud computing service should first complete the TX-RAMP Assessment Request form (request form), accessed through the TX-RAMP webpage on the DIR website. Once the provider submits the request form to DIR, DIR will review the submission to determine whether additional information is needed or if other action is necessary.

Once DIR processes the provider's request form, DIR will send an email to the point of contact

identified by the provider's request form with instructions for completing the TX-RAMP Acknowledgment and Inventory Questionnaire as well as the TX-RAMP Level 1 or Level 2 Questionnaire.

Assessment Prioritization

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.

8. TX-RAMP Assessment Components

A. 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.

B. 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.

The questionnaire includes the TX-RAMP Security Plan Template (Security Plan). A cloud service provider must complete and submit the TX-RAMP Security Plan as a component of its questionnaire. The security plan focuses on capturing general system information, the system boundary, data flows, external systems and services, and control implementation information. This template will be made available on the TX-RAMP webpage of the DIR website.

Documentation Scoring Factors

Category	Description
Compliance	•Documentation provides sufficient and complete evidence of the required control implementation.
Clarity	•Correct and consistent format. •Correct and continuous section numbering. •Logical presentation of material. •Current dates and timely content. •Non-standard terms, phrases, acronyms, and abbreviations defined. •Proper titles and labels on figures. •No ambiguous statements or content. •Minimal and appropriate use of the passive voice. •No awkward phrases, typographical errors, spelling errors, missing words, or incorrect page and section numbers. •Reasonable sentence and paragraph lengths. •Use of generally accepted rules of grammar, capitalization, punctuation, symbols, and notation. •Appropriate and accurate identification of cross-references. •Figure text is readable; figure graphics are sharp.
Completeness	•Responsive to all applicable requirements. •Indicate compliance with applicable requirements. •Includes all appropriate sections of documentation requested. •Includes all attachments and appendices. •Includes table of contents, list of tables, and list of figures if applicable. •Figures include required information, correct labels, and keys to color/line formats.
Conciseness	•Content and complexity are relevant to the audience. •No superfluous words or phrases.
Consistency	•Terms have the same meaning throughout the document. •Items are referred to by the same name or description throughout the document. •The level of detail and presentation style are the same throughout the document. •The material does not contradict predecessor documents. •All material in subsequent documents has a basis in the predecessor document. •Figure content agrees with text.

To the extent that a cloud service provider agrees, DIR may provide assessment documentation to a state agency at the state agency's request.

C. Assessment Considerations

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.

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

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 12. Recertification*, in the infrastructure of the SaaS solution must be reported to DIR.

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 Texas Government Code § 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.

TX-RAMP Certification Level Adjustment

Cloud service providers seeking to modify or change a requested assessment level should email the request to tx-ramp@dir.texas.gov. Cloud service providers with a cloud computing service certified at TX-RAMP Level 2 are not required to seek a TX-RAMP Level 1 certification adjustment if a state agency intends to use their product for a purpose requiring a TX-RAMP Level 1 certification.

9. Continuous Monitoring

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

A state agency contracting for a TX-RAMP certified cloud computing service shall notify DIR in the event of a cloud service provider failing to meet continuous monitoring obligations through the formal Grievance Process described in *Section 10. B. Grievance Process.* 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 Vendors who are TX-RAMP Certified through Another Risk and Authorization Management Program

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.

If the cloud computing service certified through the FedRAMP or StateRAMP equivalent acceptance process has the status revoked at any time, the cloud service provider contracting with a state agency for that service shall immediately notify DIR (by emailing TX-RAMP@dir.texas.gov) and the contracting state agency of the change in status. At that time, the cloud service provider may request the initiation of a TX-RAMP certification assessment. DIR will process the certification assessment in compliance with the requirements of this manual.

B. 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 severity categorization is based on the NIST National Vulnerability Database Common Vulnerability Scoring System (most current version).[2]

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 vulnerability 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 reviewing the vulnerability reporting items on a quarterly basis for TX-RAMP Level 2-certified cloud computing services and on an annual basis for TX-RAMP Level 1-certified cloud computing services. A state agency must indicate within SPECTRIM that it is contracting for a particular TX-RAMP-certified cloud computing service to be granted access to the product vulnerability reports submitted by the cloud service provider. If a state agency has not indicated this within SPECTRIM, then the state agency is responsible for arranging to receive the quarterly vulnerability reports through another mechanism agreed upon by the cloud service provider and the state agency.

DIR does not review individual product vulnerability reports submitted through the SPECTRIM Vendor Portal. It is the specific responsibility of the contracting state agency to access and review the information made available regarding a service within SPECTRIM or through another mechanism agreed upon by the vendor and the state agency.

If a state agency determines that there are vulnerabilities that have not been resolved or mitigated in accordance with this Program Manual, then the state agency shall report these

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

vulnerabilities to DIR. DIR may require greater frequency of continuous monitoring activities or revoke a cloud service provider's TX-RAMP certification if vulnerabilities identified are not remediated or adequately addressed 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
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

C. Ongoing Activities

Reporting Unauthorized Disclosure of Confidential Information or Personal Identifying Information

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 § 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.

10. Dispute Resolution

A. 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 and addressed to DIR's Executive Director at TX-RAMP@dir.texas.gov. This step may only be taken if the cloud service provider has a 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.

B. 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.

11. 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.

12. Recertification

A. Updates to Certification Due to Significant Changes

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.

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 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.

Changes Likely Considered Significant

The following are examples of what would likely constitute a significant change in a cloud computing service that would warrant notification to DIR and require an update to certification.

- Adding or removing security controls.
- A change in cloud computing service ownership that would result in major changes.
- Changing or updating backup mechanisms and processes.
- Changing alternative (or compensating) security controls.
- Moving information system data to a different system boundary.
- New authentication mechanisms or changes to existing mechanisms.
- New boundary protection mechanisms or changes to existing mechanisms.
- New cloud computing service offering or feature outside of the scope of initial assessment.
- New data center or moving to a new facility.

- New interconnection or changes to existing interconnections.
- New system monitoring capabilities or replacing system monitoring capabilities.
- New technology (New OS variant, including COTS and appliance, none of which currently exist in the cloud computing service environment).
- New/upgrade of the data base management system (DBMS).
- Platform as a Service (PaaS) or SaaS changing Infrastructure as a Service (IaaS) provider.
- Removing system components or service offering.
- Scanning tool changes.
- System categorization changes.
- Using new external services in support of the cloud computing service.
- Changing an accepted risk and authorization management program status.

At the onset of the update to certification process, the target assessment level may be adjusted.

B. Recertification after Three Years from Last Certification Date

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.

13. TX-RAMP Certifications Prior to TX-RAMP Program Manual 2.0

A. 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.

B. 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.

14. 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**

15. Appendices

A. 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**

B. Appendix B – Required Documentation

Cloud service providers are required to complete the TX-RAMP Security Plan Template 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.

C. 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 Texas Business & Commerce Code § 521.053(a).

Cloud Computing Service – As defined by Texas Government Code § 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 § 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 § 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.

D. Appendix D – Guidelines for Determining a Cloud Computing Service

"Cloud computing services" is defined in Texas Government Code § 2054.0593(a); however, a state agency may use the below list to assist it in determining whether the product, application, or service in question is a cloud computing service. A state agency should also consult with its legal counsel to determine whether Texas Government Code § 2054.0593 is applicable to the offering in question. Essential characteristics of a cloud computing service are:

- **On-demand Self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad Network Access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- **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. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid Elasticity.** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **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 (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.