Texas Risk and Authorization Management Program Manual

Effective Date

This publication takes effect on 10/28/2021

Table of Contents

I. Purpose ... 3

II. Document Change Management ... 3

A. New or Revised Program Standards ... 3

B. Administrative Changes ... 3

III. Support/Inquiries ... 3

IV. Overview ... 4

V. Compliance Dates for Program Requirements ... 4

VI. TX-RAMP Level Determination ... 5

A. Characteristics and Categories of Cloud Computing Services Not Subject to TX-RAMP ... 5

B. Baseline Levels for Cloud Computing Services within TX-RAMP Scope ... 6

C. Data Classification & Impact Assessment ... 6

VII. Certification ... 9

A. TX-RAMP Certification Levels ... 9

B. TX-RAMP Provisional Certification Status ... 9

C. Required Assessment Documentation for TX-RAMP Certification ... 12

D. Certification Process ... 13

VIII. Continuous Monitoring ... 17

A. Vulnerability Reporting ... 18

B. Ongoing Activities ... 20

IX. Dispute Resolution ... 21

A. Appeals Process ... 21

B. Grievance/Complaint Process ... 21

X. Certification Revocation ... 22

XI. Recertification ... 23

A. Updates to Certification Due to Significant Changes ... 23

B. Recertification after Three Years from Last Certification Date ... 24

XII. Document Version History ... 25

XIII. Appendix A - TX-RAMP Control Baselines ... 26

XIV. Appendix B – Required Documentation ... 27

XV. Appendix C – Supplemental Letter for Authorized IaaS/PaaS Template ... 28

XVI. Appendix D – Glossary of Terms ... 29

XVII. Appendix E – Guidelines for Determining a Cloud Computing Service ... 30

I. 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. DIR has created the Texas Risk and Authorization Management Program (TX-RAMP) in response to this mandate.

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.

II. Document Change Management

A. New or Revised Program Standards

Prior to publishing new or revised program standards, the Texas Department of Information Resources (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 nonsubstantive 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.

III. Support/Inquiries

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

IV. Overview

TX-RAMP is a standardized approach to the assessment and evaluation of cloud computing services. 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 or renewed on or after that date.

Cloud computing service is defined by Texas Government Code § 2157.007. 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.

TX-RAMP has two assessment levels:

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

TX-RAMP has three statuses:

- **Level 1 Certification** is achieved after submitting the assessment responses and meeting the minimum requirements for the Level 1 Assessment Criteria or by submitting evidence of StateRAMP Category 1 authorization or FedRAMP Low authorization.
- **Level 2 Certification** is achieved after submitting the assessment responses and meeting the minimum requirements for the Level 2 Assessment Criteria or by submitting evidence of StateRAMP Category 3 authorization or FedRAMP Moderate authorization.
- **TX-RAMP Provisional Status** provides a provisional product certification permitting a state agency to contract for the use of a product for up to 18 months without receiving full TX-RAMP certification. Upon achieving provisional status, the cloud computing service will need to be certified through a TX-RAMP assessment or equivalent within the provisional status period to maintain compliance with program requirements.

V. Compliance Dates for Program Requirements

- Cloud offerings subject to TX-RAMP Level 1 certification must obtain a TX-RAMP certification to contract with state agencies on or after January 1, 2023.
- Cloud offerings 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 offerings that obtain TX-RAMP Provisional Status must obtain a TX-RAMP certification (or equivalent StateRAMP/FedRAMP authorization) within 18 months from the date that Provisional Status is conferred as reflected in DIR’s files.

VI. TX-RAMP Level Determination

Only cloud computing services, as defined by Texas Government Code § 2054.0593(a), are within scope for TX-RAMP. Products or services that are not cloud computing services are not subject to TX-RAMP. A state agency may use the essential characteristics list found in Appendix E to determine whether their product or service is a cloud computing service subject to TX-RAMP.

Certain specific cloud computing services are outside of the scope of Texas Government Code § 2054.0593 and, as such, are not required to comply with TX-RAMP.

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. These are only out-of-scope of TX-RAMP provided that the cloud computing service does not: (1) create, process, or store confidential state-controlled data (except as needed to provide a login capability, e.g. username, password, email) or connect with agency systems or networks that create, process, or store confidential state-controlled data such that any security incident might affect such systems or networks. The below cloud computing services are considered out of scope of TX-RAMP:

- Consumption-focused cloud computing services such as advisory services, market research, or other resources that are used to gather nonconfidential research or advisory information;
- Graphic design or illustration products;
- Geographic Information Systems or mapping products that are not used for confidential purposes or tied to individual identities;
- Email or notification distribution services that do not create, process, or store confidential information;
- Social media platforms and services;
- Survey and scheduling cloud computing services that do not create, process, or store confidential information;
- Cloud computing services used to deliver training that do not create, process, or store confidential information;
- Cloud computing services used to transmit copies of nonconfidential data as required by external governing bodies for purposes of accreditation and compliance; and
- Low Impact Software-as-a-Service cloud computing services as defined by the following criteria:
  - The product meets the definition of a Software as a Service (SaaS), as defined by NIST SP 800-145, The NIST Definition of Cloud Computing;
  - The cloud computing service does not contain personally identifiable information (PII), except as needed to provide a login capability (username, password and email address), or create, process, or store confidential state-controlled data;

- The cloud computing service is a low impact information resource as defined by 1 TAC §202.1; and
- The cloud computing service operates within a TX-RAMP certified Platform as a Service (PaaS) or Infrastructure as a Service (IaaS).

A cloud computing service that is out of scope of TX-RAMP is not subject to the baseline level requirements established herein. However, the cloud computing service must still be compliant with required control baselines established by the Security Controls Catalog and any other federal or statutory requirements that might be applicable to the cloud computing service or the information found therein.

If a cloud computing service does not fall into one of the above categories, then such cloud computing service is considered in scope of TX-RAMP and is required to comply with this Program Manual.

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

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

- 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 nonconfidential data of a state agency or the cloud computing service is determined to be low-impact information resources as defined by 1 Texas Administrative Code § 202.1. The assessment criteria for this baseline are based on NIST-800 53 Low Impact Baseline controls with additional parameters derived from FedRAMP and StateRAMP. Specific technical assessment criteria for this baseline may be found in the spreadsheet provided in Appendix A.

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

TX-RAMP Level 2 is required for cloud computing services that store, process, or transmit confidential data of a state agency and the cloud computing service is determined to be moderate or high impact information resources. The assessment criteria for this baseline are based on NIST 800-53 Moderate Impact Baseline controls with additional parameters derived from FedRAMP/StateRAMP. Specific technical assessment criteria for this are provided in Appendix A – TX-RAMP Control Baselines.

C. Data Classification & Impact Assessment

The contracting state agency is responsible for determining the baseline level a cloud computing services product that it seeks to use is subject to, based upon the below criteria. The state agency shall apply the below questions when analyzing which certification is appropriate for the use of a particular product for a particular purpose. Such analysis shall be the basis for the state agency's determination of which level applies in the state agency's sponsorship of a vendor's request for product assessment through the Statewide Portal for Enterprise

Cybersecurity Threat, Risk, and Incident Management (SPECTRIM).

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 it is at the discretion of a state agency to 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 vendor seeking certification of a cloud computing service without state sponsorship or whose cloud computing service is not subject to a specific state agency procurement must determine which baseline level it is seeking prior to submission of the vendor request for assessment form. After determining whether the cloud computing service is subject to TX-RAMP requirements, the following criteria should be evaluated to determine the TX-RAMP Certification Level Minimum.

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.*
- *Personal Identifiable Information (except as needed to provide a login capability, e.g. username, password, and email address)*
- *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 working papers and draft reports excepted from disclosure under Texas Government Code § 552.116*

If the answer is "no," TX-RAMP Level 1 is required. If the answer is "yes," proceed to the next question.

Does (or will) the cloud offering 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 is required. If the answer is "no," TX-RAMP Level 2 is required.

VII. Certification

Certifications will be determined based upon DIR review of an assessment and related documentation ("assessment"). This assessment entails DIR's review of:

- the assessment form and all answers therein submitted by either the vendor or state agency; and
- all documentation submitted to DIR by the vendor either initially or supplementally.

A. TX-RAMP Certification Levels

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

- Providing assessment responses and documentation to DIR for review; or
- Providing evidence to DIR of an accepted risk authorization and management program status (e.g. FedRAMP, StateRAMP).

TX-RAMP Level 1 Certification may be conferred only after a vendor submits any and all assessment responses to DIR documenting that the product meets the minimum requirements for the Level 1 Assessment Criteria or after the vendor submits evidence to DIR of the product's StateRAMP Category 1 Ready/Authorized/Provisional Status or FedRAMP Low Authorized/Ready Status.

TX-RAMP Level 2 Certification may be conferred only after a vendor submits any and all assessment responses to DIR documenting that the product meets the minimum requirements for the Level 2 Assessment Criteria or after the vendor submits evidence to DIR of StateRAMP Category 3 Ready/Authorized/Provisional Status or FedRAMP Moderate Authorized/Ready Status.

B. TX-RAMP Provisional Certification Status

DIR remains cognizant of the urgent need to have cloud offerings certified as of January 01, 2022, for TX-RAMP Level 2 and January 01, 2023, for TX-RAMP Level 1. Due to this statutory deadline, DIR permits certain provisional approvals as described below. TX-RAMP Provisional Status is effective until 18 months from the date the provisional status is granted by DIR. This status shall not be sought for the same cloud offering more than once. TX-RAMP Provisional Status may be achieved in two ways:

- **Third-Party Audit/Attestation Review:** the vendor submits an accepted third-party assessment report to DIR for review to determine if provisional status should be granted.
- **State Agency Sponsored Provisional Status:** A state agency subject to TX-RAMP requirements assesses an accepted self-reported questionnaire and provides DIR with notice of approval of the vendor's self-reported assessment responses.

TX-RAMP Provisional Status may not be requested after January 1, 2023.

Third-Party Audit/Attestation Review

Vendors often: (1) are subject to mandatory contractual reviews or audits of their information security protocol; (2) voluntarily attain accreditation or certification reflecting their information security maturity; or (3) voluntarily request a security audit of their protocols.

A vendor that has received a certification, audit, or report listed below may submit evidence to DIR for review in determining the issuance of TX-RAMP Provisional Status:

- CSA STAR Level 2 Certification
- SSAE 16/18 (SOC 2 Type II)
- ISO 27001/2 Audit
- ISO 27017/18 Audit
- Arizona Risk and Authorization Management Program (AZRAMP) Certification
- Regulatory or Industry Standard Audit Reports

At its discretion, DIR may accept a certification or report not listed above as evidence for review in determining the issuance of TX-RAMP Provisional Status.

A certification, report, or audit creating eligibility under this section must have been received or created within no more than 18 months prior to DIR's receipt of the application for TX-RAMP Provisional Status by a requesting state agency or a requesting vendor.

When seeking provisional status, DIR shall conduct a review of the vendor's provided documentation to ensure sufficiency and authenticity. If there are deficiencies in the provided documentation, then DIR will identify the deficiencies to the vendor and offer the vendor the opportunity to submit additional evidence of compliance or request additional information for review.

State Agency Sponsored Provisional Status

Certain state agencies require that vendors complete a comprehensive self-reported assessment, which provides assertions regarding the vendor's compliance with rigorous protocols regarding a number of issues including information security. This includes the tool known as the Higher Education Community Vendor Assessment Tool (HECVAT).

A state agency may review a vendor's self-reported assessment completed within the previous 18 months and submit notice to DIR asserting that the vendor's self-reported assessment has been deemed satisfactory by the state agency. When submitting its written approval, a state agency will also be asked to provide relevant assessment information, such as:

- The assessment criteria (questionnaires, frameworks) used;
- When was the self-reported assessment evaluated by the state agency;
- Any significant findings or concerns identified in its review of the assessment;
- System security categorizations the state agency has authorized the product for; and
- Other pertinent details as needed**.**

This state agency provisional authorization notification shall be submitted through the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM). DIR will record the state agency's approval of the self-reported assessment in SPECTRIM.

At its discretion, DIR may inquire further regarding a vendor's self-reported assessment.

Any state agency may contract for a product that has a Provisional Status Certification, regardless of whether it was the state agency that supported the vendor's initial submission for Provisional Status assessment.

Provisional Status Risks and Considerations

Attaining provisional status for a vendor providing a cloud computing services product does not indicate full TX-RAMP certification of a cloud computing service product as it is not assessed under the same standards for TX-RAMP certification.

State agencies contracting with a vendor who has attained TX-RAMP Provisional Status should consider the addition of rigorous, additional 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 state agency leadership.

A vendor who has received TX-RAMP Provisional Status shall provide regular updates to DIR confirming continued compliance with the report, certification, or self-reported assessment that resulted in the TX-RAMP Provisional Status.

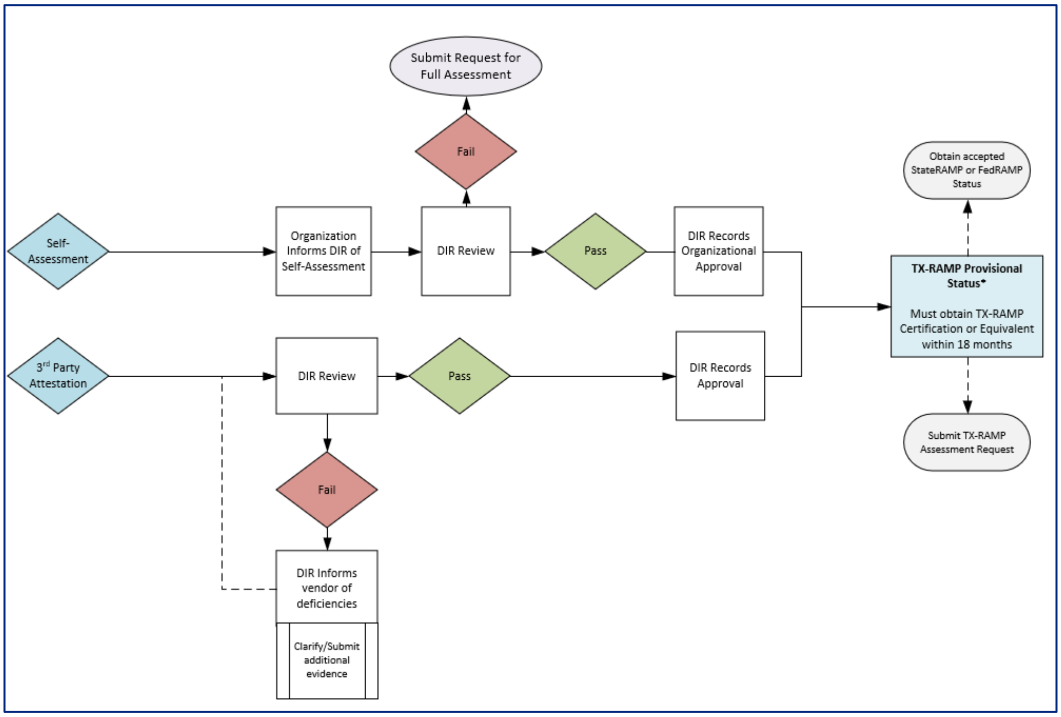
Submit Request for Full Assessment
Fail
Obtain accepted StateRAMP or FedRAMP Status
Self-Assessment
Organization Informs DIR of Self-Assessment
DIR Review
Pass
DIR Records Organizational Approval
TX-RAMP Provisional Status*
Must obtain TX-RAMP Certification or Equivalent within 18 months
3rd Party Attestation
DIR Review
Pass
DIR Records Approval
Submit TX-RAMP Assessment Request
Fail
DIR Informs vendor of deficiencies
Clarify/Submit additional evidence

Figure 1: Paths to Obtain Provisional Status Workflow

Failure to Attain Full Certification before Provisional Status Expiration

A vendor providing a cloud computing service to a state agency is required to receive appropriate TX-RAMP certification prior to the expiration of the cloud computing service's 18-month Provisional Status Certification.

Failure to do so will result in a lapse in certification from the expiration of the Provisional Status certification until such time as the vendor is able to receive full TX-RAMP certification; during this lapse, the vendor's product will not be TX-RAMP-certified and, as such, their product will be noncompliant with TX-RAMP requirements. As provided by Texas Government Code § 2054.0593(f), a state agency shall require a vendor contracting with the agency to provide cloud computing services to the agency that are subject to TX-RAMP to maintain program compliance and certification throughout the term of the contract.

C. Required Assessment Documentation for TX-RAMP Certification

A vendor seeking certification or for whom a state agency is seeking certification under TX-RAMP is required to provide security documentation so that DIR may assess whether the cloud computing service complies with certification requirements necessary for the baseline level sought. Specific information and documentation requirements may be found in Appendix B.

Vendors may submit policies and other requested documentation in their preferred format provided the documentation demonstrates compliance with control requirements.

Many open-source policy and documentation templates exist that may assist with developing and formatting the required documentation. StateRAMP offers a template library at https://stateramp.org/templates-resources/ that aligns with the documentation requested during a TX-RAMP assessment.

Documents shall be scored in accordance with the following matrix.

Documentation Scoring Factors

Category	Description
Compliance	•Documentation provides sufficient and complete evidence of the control requirements satisfaction.
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 is subsequent documents has a basis in the predecessor document •Figure content agrees with text

To the extent that a cloud computing service vendor agrees, DIR may make a cloud computing service's assessment results available to sponsoring state agencies at the sponsoring state agency's request.

D. Certification Process

Collection Tool - SPECTRIM

The Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) is the vehicle by which TX-RAMP status tracking, agency sponsorship of assessments, and assessments are managed. The SPECTRIM Vendor Portal is used to assign and launch assessment questionnaires to vendor contacts to collect assessment responses.

SPECTRIM is available to state agencies, public institutions of higher education, and public community colleges. Employees of a state agency without an existing SPECTRIM account should contact their state agency's designated Information Security Officer to request access to the portal. Users with an existing account may log into the portal using the following URL: https://dir.archer.rsa.com/Default.aspx

If your account is inactive or locked, the password self-service option will not be functional. Please contact **GRC@dir.texas.gov** to assist with account reactivation.

DIR is responsible for providing and updating guidance for conducting TX-RAMP-related activities in SPECTRIM.

Assessment Initiation

There are two mechanisms by which a request for assessment may be initiated.

First, a state agency may submit a request for assessment of a product directly into SPECTRIM and sponsor the request.

Second, a vendor may initiate a request for assessment. Further, a state agency may request or require a vendor with whom they intend to contract to fill out the vendor request form and identify that the form submitted is for an active procurement. DIR will upload the information into SPECTRIM. A state agency may then sponsor the vendor's request for assessment to prioritize the assessment for DIR's review. See below for further detail.

State agencies should consider leveraging the procurement process to further facilitate vendors' timely compliance. For example, state agencies should consider requiring any vendor that bids on a procurement to initiate the TX-RAMP certification process with DIR and then the state agency can further sponsor vendors that make it further into the procurement process. This allows DIR to start processes and then properly prioritize needed certifications.

Assessment Prioritization

DIR shall review assessments in the order that they are received. Priority will be granted to those assessments sponsored by a state agency, even if the vendor initiates the process. DIR may also consider additional factors in determining the priority of an assessment including, but not limited to:

- The level of certification requested;
- existing authorizations or certifications;
- state agency described priority or justification; and
- existing and planned procurement activities.

As a state agency completes a request for assessment of a cloud computing service, SPECTRIM will review existing vendor cloud computing service requests for assessments to determine whether another state agency or a vendor has already sought an assessment of the cloud computing service. If another state agency has already sponsored a vendor's request for assessment, then other state agencies interested in the same cloud computing service may also sponsor the offering. Cloud computing services with multiple sponsoring state agencies will be prioritized.

A vendor who does not have an existing contract with or is not currently being awarded a contract by a state agency for cloud computing services may initiate a request for certification of its product on its own initiative by submitting a completed TX-RAMP Vendor Contact form. DIR shall review the submitted form and reach out to the vendor at DIR's earliest convenience.

https://survey.alchemer.com/s3/6510630/TX-RAMP-Vendor-Contact

Time Required to Complete Assessment

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

- completeness of vendor-provided documentation and responses;
- TX-RAMP Level assessment required based upon state agency's requirement for the product; and
- vendor responsiveness to DIR outreach.

This timeline is dependent upon vendor responsiveness and completeness of documents. If DIR is required to seek additional documentation or extensive vendor outreach is required, DIR may require more time to certify. DIR is not responsible for delays in a state agency's procurement as a result of vendor failure to timely communicate.

SaaS Infrastructure - Leveraged Authorizations

Software as a Service (SaaS) applications operating on a currently TX-RAMP Certified cloud offering of infrastructure/platform (IaaS/PaaS) may inherit applicable controls from the certified infrastructure with evidence of operating on the certified cloud computing service provider infrastructure/platform. As such, SaaS products operating on an infrastructure that is already TX-RAMP certified do not have to receive additional TX-RAMP certification for the underlying SaaS infrastructure. A vendor providing a SaaS offering subject to inherited controls shall submit written confirmation as part of the assessment process to DIR attesting that the SaaS product is operating on a certified infrastructure and will maintain compliance with TX-RAMP security control requirements for any IaaS/PaaS configurations that are the responsibility of the SaaS provider.

The SaaS cloud computing service provider will be 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 Recertification, in the infrastructure of the SaaS solution must be reported to DIR.

Cloud Reseller Functions

Primary contracting vendors, including vendors who resell cloud computing service offerings, 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 and require a vendor providing an already certified product to a state agency using the reseller contract to provide documented evidence of the vendor's TX-RAMP certification to them for ready provision to DIR and the state agency.

TX-RAMP Certification Level Adjustment

Vendors with cloud computing services certified at TX-RAMP Level 1 may request an assessment at TX-RAMP Level 2 at any time. Vendors must submit the TX-RAMP Certification Level Adjustment Request form to initiate the process. Upon receipt of this form, DIR will evaluate the request and add it to the queue of prospective assessments. From there, a state agency may sponsor the request within SPECTRIM.

Vendors with a cloud computing service certified at TX-RAMP Level 2 are not required to seek 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.

VIII. Continuous Monitoring

Continuous monitoring is a significant function in managing third-party and vendor risk as it provides assurances to the contracting state agency that the vendor is actively managing and responding to the changing threat landscape and operating with security as a priority.

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. Certified cloud computing services shall be assessed, and security controls analyzed at a frequency sufficient to support risk-based 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 vendors to ensure that cloud computing services certified under TX-RAMP 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 their TX-RAMP certification.

DIR establishes the below continuous monitoring criteria for vendors 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 vendor failing to meet continuous monitoring obligations through the formal Grievance Process described in Section IX. B. Grievance/Complaint 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 vendor'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 vendor will not be required to provide continuous monitoring artifacts because those responsibilities are fulfilled through the respective RAMP processes. State agencies contracting with a vendor 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 vendor contracting with a state agency for that product 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 vendor providing the cloud computing service may request the initiation of a TX-RAMP certification assessment. The processing of this certification by DIR will be conducted in compliance with the requirements of this manual.

Documentation to Be Provided to by a TX-RAMP-Certified Vendor that is Not Certified through Another Risk and Authorization Management Program

The state agency shall require a vendor to provide continuous monitoring artifacts in accordance with this Program Manual beginning on the date that the TX-RAMP certification takes effect to maintain compliance with TX-RAMP. For documents that must be provided to the state agency pursuant to this Program Manual, the state agency may provide for how those documents are submitted to the state agency through its contract or agreement with the vendor or through other agreed upon mechanism.

The following establish the minimum continuous monitoring requirements to ensure vendor compliance with TX-RAMP. Any additional continuous monitoring requirements are at the discretion of the contracting state agency.

A. Vulnerability Reporting

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

State agencies are responsible for the review of the vulnerability reporting items made available to the state agency through SPECTRIM 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.

Vulnerability severity categorization is based on the NIST National Vulnerability Database Common Vulnerability Scoring System.[1]

Vendors must report identified vulnerabilities with vulnerability severity category as part of the vulnerability reporting along with:

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

Vendor vulnerability reporting documentation shall be submitted through the SPECTRIM Vendor Portal. The SPECTRIM Vendor Portal will provide notice to the designated vendor 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

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

computing service in SPECTRIM and make it available to state agencies who have indicated that they are contracted for that cloud computing service.

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 vendor. 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 vendor 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 contract state agency to access and review the information made available regarding a product 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 vulnerabilities to DIR. DIR may require greater frequency of continuous monitoring activities or revoke a vendor'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

B. Ongoing Activities

Critical Security Issues

If a state agency identifies a critical security issue in a TX-RAMP certified cloud computing service that it is using during a required or optional continuous monitoring activity, then the state agency shall notify DIR of the critical security issue immediately but not less than 48 hours after identification of the issue.

Upon receipt of such notification, DIR shall review the identified critical security issue and contact the vendor whose product is identified. DIR shall then work with the vendor to:

- construct a corrective action plan to remedy the issue; or
- revoke the product's certification in compliance with Certification Revocation requirements.

DIR shall determine which of the above steps is appropriate upon notification of a deficiency at its discretion.

DIR reserves the right to revoke the TX-RAMP certification of a vendor who fails to comply with a corrective action plan to remedy an identified deficiency at any time.

Reporting Unauthorized Disclosure of Confidential Information or Personally Identifying Information

A vendor 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 vendor whose TX-RAMP-certified product has a breach of system security shall notify DIR within 48 hours of becoming aware of the breach of system security.

IX. Dispute Resolution

A. Appeals Process

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

Cloud computing service providers or primary contractors/resellers acting on behalf of a cloud computing 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 vendor may not appeal the certification decision of another vendor'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 product'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 vendor disagrees, the vendor 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 vendor 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/Complaint Process

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

Grievances will be evaluated by DIR to determine whether corrective action or revocation of certification status are warranted.

X. Certification Revocation

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

Failure of a vendor 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 offering;
- 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 vendor 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 product's TX-RAMP certification, the loss of such certification will result in the automatic revocation of the product'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.

XI. 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.

Vendors 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 offering 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 computing service provider's previously provided 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.

Significant changes to a certified product shall be reported by the vendor to DIR within 30 days of the date that the change is made. A vendor may also report a significant change to a product 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 product 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 product.

DIR will determine whether a change identified by the vendor 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/removing security controls
- Change in cloud computing service ownership that would result in major changes (e.g. change to contingency planning or incident response processes).
- Changed or updated backup mechanisms and processes.
- Changing alternative (or compensating) security controls.
- Movement of 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 replacement of 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 DBMS (data base management system).
- PaaS/SaaS changing IaaS provider.
- Removal of system components or service offering.
- Scanning tool changes.
- System categorization changes (e.g. FIPS 199 Change from Moderate to High).
- Use of new external services (e.g. ticketing system, monitoring system) in support of the cloud computing service.
- Changes to accepted Risk & Authorization Management Program status (i.e. StateRAMP, FedRAMP).

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 (3) years from the date the last certification was conferred upon a cloud computing service, provided that the vendor is compliant with the program requirements enumerated in this Program Manual. Recertification requires the vendor to review and update control implementation details as necessary and provide updated documentation to DIR for review.

The identified points of contact for vendors with TX-RAMP certified cloud computing services will be notified by automated email at least 12 months and 6 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 vendor or by a contracting state agency up to 12 months prior to the certification end date.

XII. Document Version History

Version	Date	Comments
1.0	October 28, 2021	Initial Publication

XIII. Appendix A - TX-RAMP Control Baselines

TX-RAMP Security Control Baselines.xlsx

TX-RAMP Level	Number of Controls/Enhancements Assessed
Level 1	**124**
Level 2	**325**

CONTROL FAMILY	TX-RAMP LEVEL 1	TX-RAMP LEVEL 2
ACCESS CONTROL	11	43
AUDIT AND ACCOUNTABILITY	10	19
AWARENESS AND TRAINING	4	5
CONFIGURATION MANAGEMENT	8	27
CONTINGENCY PLANNING	6	24
IDENTIFICATION AND AUTHENTICATION	15	27
INCIDENT RESPONSE	8	18
MAINTENANCE	4	11
MEDIA PROTECTION	4	10
PERSONNEL SECURITY	8	8
PHYSICAL AND ENVIRONMENTAL PROTECTION	9	20
PLANNING	3	6
RISK ASSESSMENT	4	10
SECURITY ASSESSMENT AND AUTHORIZATION	8	15
SYSTEM AND COMMUNICATIONS PROTECTION	8	32
SYSTEM AND INFORMATION INTEGRITY	7	28
SYSTEM AND SERVICES ACQUISITION	7	22
TOTAL	**124**	**325**

XIV. Appendix B – Required Documentation

#	TX-RAMP DOCUMENTATION REQUIREMENTS
1	BOUNDARY & DATA FLOW DIAGRAM
2	ROLES & PERMISSIONS MATRIX
3	INCIDENT RESPONSE PLAN
4	SYSTEM SECURITY PLAN
5	INFORMATION SYSTEM CONTINGENCY PLAN
6	CONFIGURATION MANAGEMENT PLAN
7	SECURITY POLICY - ACCESS CONTROL (AC)
8	SECURITY POLICY - AWARENESS AND TRAINING (AT)
9	SECURITY POLICY - AUDIT AND ACCOUNTABILITY (AU)
10	SECURITY POLICY - SECURITY ASSESSMENT AND AUTHORIZATION (CA)
11	SECURITY POLICY - CONFIGURATION MANAGEMENT (CM)
12	SECURITY POLICY - CONTINGENCY PLANNING (CP)
13	SECURITY POLICY - IDENTIFICATION AND AUTHENTICATION (IA)
14	SECURITY POLICY - INCIDENT RESPONSE (IR)
15	SECURITY POLICY - MAINTENANCE (MA)
16	SECURITY POLICY - MEDIA PROTECTION (MP)
17	SECURITY POLICY - PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)
18	SECURITY POLICY - PLANNING (PL)
19	SECURITY POLICY - PERSONNEL SECURITY (PS)
20	SECURITY POLICY - RISK ASSESSMENT (RA)
21	SECURITY POLICY - SYSTEM AND SERVICES ACQUISITION (SA)
22	SECURITY POLICY - SYSTEM AND COMMUNICATIONS PROTECTION (SC)
23	SECURITY POLICY - SYSTEM AND INFORMATION INTEGRITY (SI)

XV. Appendix C – Supplemental Letter for Authorized IaaS/PaaS Template

COMPANY LETTERHEAD

<Date>
Texas Department of Information Resources
Office of the Chief Information Security Officer
300 W. 15th St. Suite 1300
Austin, TX, 78701

Re: **<Cloud Service Company Name>** Use of **<Certified Cloud IaaS/PaaS Product Name>** for State of Texas Data

I am writing to confirm that regarding the **<Contracted Cloud Computing Service Name>, <Cloud Service Company Name>** will use **< Certified Cloud IaaS/PaaS Product Name>** provided services to host, operate, and maintain State of Texas Data. All production data provided by the State of Texas will remain within **<Certified Cloud IaaS/PaaS Product Name>** at all times.

<Cloud Service Company Name> is a current customer of **<Certified Cloud IaaS/PaaS Product Name>** and will maintain a business relationship with **<Certified Cloud IaaS/PaaS Product Name>** over the course of TX-RAMP Certification. **<Cloud Service Company Name>** will follow all National Institute of Standards and Technology ("NIST") best practices to securely instantiate and operate **<Certified Cloud IaaS/PaaS Product Name>** services. **<Cloud Service Company Name>** will also establish and verify any relevant **<Certified Cloud IaaS/PaaS Product Name>** customer responsibility controls as outlined n**<Certified Cloud IaaS/PaaS Product Name>** Customer/Client Package.

Any requested change to the infrastructure and system boundaries of the TX-RAMP Certified cloud computing service, and in turn to the use of **<Certified Cloud IaaS/PaaS Product Name>**, must be agreed upon in advance by **<Cloud Service Company Name>** and the Texas Department of Information Resources inwriting. If at any time during the course of TX-RAMP Certified operations, **<Cloud Service Company Name>** discontinues using **<Certified Cloud IaaS/PaaS Product Name>** provided services to host, operate, or maintain the certified cloud computing service without the Texas Department of Information Resources' advance written approval, **<Cloud Service Company Name>** shall immediately notify in writing the Texas Department of Information Resources and shall meet all Texas Risk and Authorization Management Program requirements & within the Texas Department of Information Resources' requested timeframe.

<Signature of Authorized preparer>
<Printed Name of Authorized preparer>
<Title of Authorized preparer>

XVI. Appendix D – Glossary of Terms

Assessment – DIR review of a vendor 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.

Critical Security Issue – an issue that exposes or threatens to immediately impact the confidentiality, integrity, or availability of an agency's data.

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

XVII. Appendix E – 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 capability1 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.