TX-RAMP Overview

Matt Kelly
Deputy CISO –
Policy & Governance

Transforming How
Texas Government
Serves Texans

Texas Department of Information Resources

What is a RAMP?

- A Risk and Authorization Management Program focuses on assessing the potential for negative consequences relating to information assets, ensuring that systems are formally approved prior to operationalizing, and monitoring the security posture of those systems on a continuous basis to minimize those potential negative outcomes.

- DIR was charged with building a statewide RAMP (TX-RAMP) by December 1, 2021, via SB 475 of last session.

- Texas is one of the first states to implement a statewide RAMP, taking inspiration from FedRAMP, StateRAMP, and AZRAMP.

Texas Risk & Authorization Management Program

- **Who does this apply to?**
  - State Agencies
  - Public Institutions of Higher Education
  - Public Community Colleges
  - Cloud Service Providers

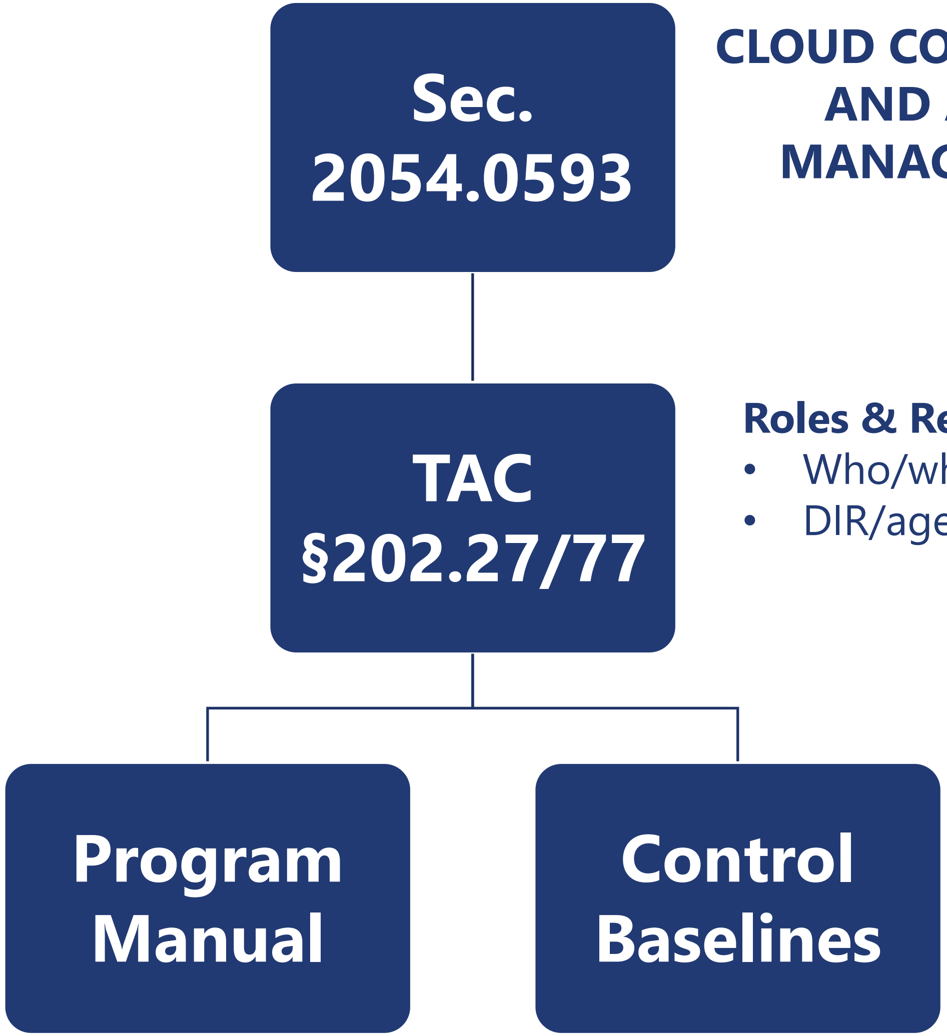
- **What does this apply to?**
  - Contracts to purchase cloud computing services for the state organization.
  - SB 475 also requires agencies to include contract language regarding required security controls expected of third parties (cloud or otherwise).

- **When does this take effect?**
  - The program took effect January 1, 2022
  - Minimum certification level requirements prior to entering or renewing a contract are staggered

TX-RAMP Structure

TX-RAMP

✓ CERTIFIED



Sec. 2054.0593

CLOUD COMPUTING STATE RISK AND AUTHORIZATION MANAGEMENT PROGRAM

TAC §202.27/77

Roles & Responsibilities

- Who/what is subject to the program
- DIR/agency/vendor responsibilities

Program Manual

Details certification process

- How to begin certification
- Decision-tools for baseline selection
- What information is needed

Control Baselines

Specifies applicable controls

- TX-RAMP Level 1
- TX-RAMP Level 2

TX-RAMP 2.0

TX-RAMP Program Manual 2.0

TX-RAMP

✓ CERTIFIED

- **Takes effect 12/1/2022**
- **Control alignment with 800-53r5**
  - Level 1: 122 → 117
  - Level 2: 322 → 223
- **Provisional Certification**
  - Removes 3rd party audit/assessment
  - Removes agency-sponsored (sort of)
  - Granted after completing acknowledgment and inventory of artifacts
  - Incorporates extension
  - Removes January 1, 2023 deadline for provisional
- **Certification Requirements**
  - Consolidates required documentation
  - Reducing number of assessment questions.
  - Moved effective date of level 1 to January 1, 2024

Requests prior to 12/1/2022

- If an assessment was begun or provisional was granted prior to the effective date of the 2.0 version of the program manual, the cloud service provider may
  - submit the existing assessment for review and certification or
  - opt to complete the new assessment.

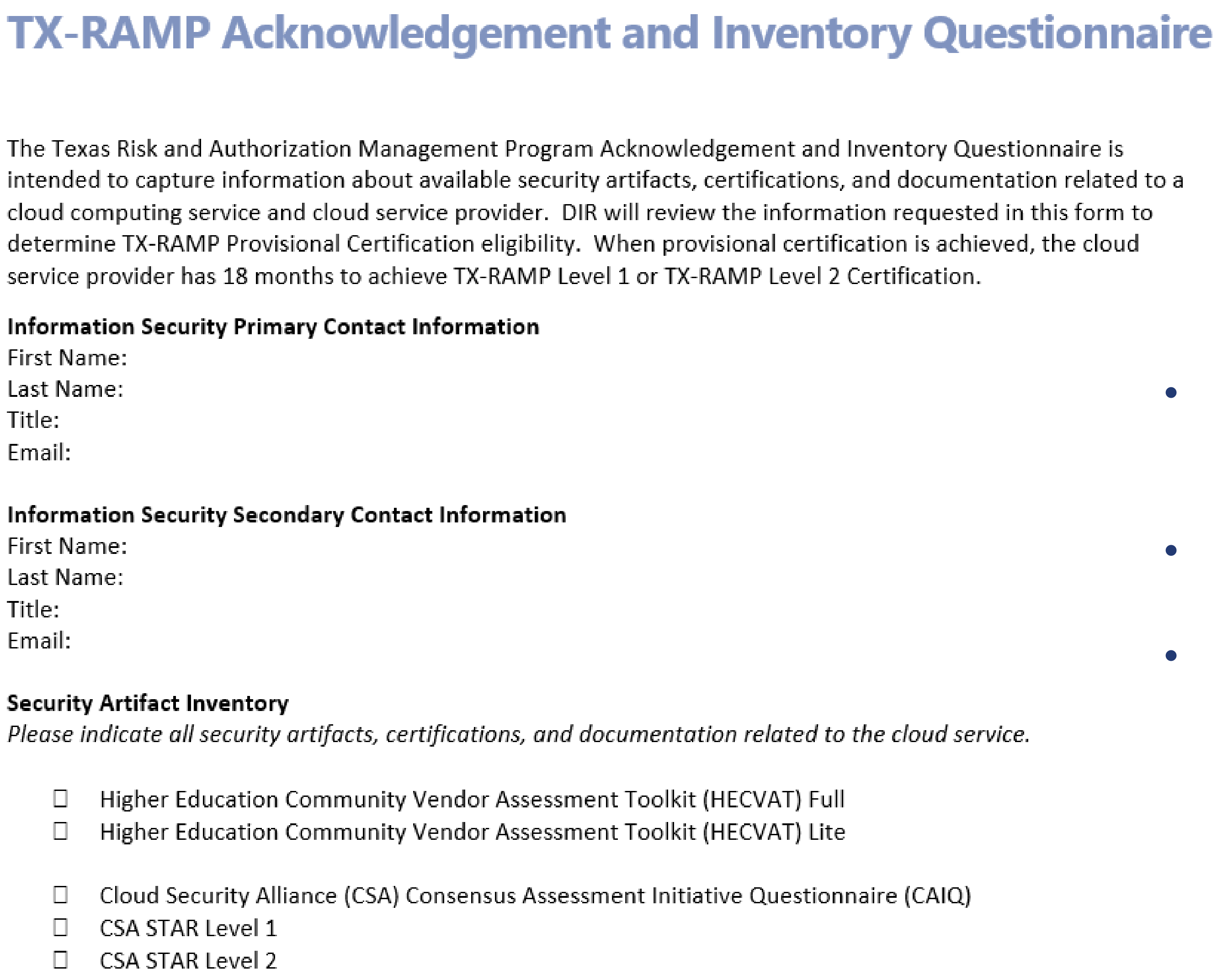
- If a cloud service was granted provisional certification prior to 12/1/2022, the cloud service provider will need to complete the acknowledgement and inventory prior to being granted level 1 or 2 certification.

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**

Level 1: 122 → 117

Level 2: 322 → 223

Acknowledgement and Inventory



TX-RAMP Acknowledgement and Inventory Questionnaire

The Texas Risk and Authorization Management Program Acknowledgement and Inventory Questionnaire is intended to capture information about available security artifacts, certifications, and documentation related to a cloud computing service and cloud service provider. DIR will review the information requested in this form to determine TX-RAMP Provisional Certification eligibility. When provisional certification is achieved, the cloud service provider has 18 months to achieve TX-RAMP Level 1 or TX-RAMP Level 2 Certification.

Information Security Primary Contact Information
First Name:
Last Name:
Title:
Email:

Information Security Secondary Contact Information
First Name:
Last Name:
Title:
Email:

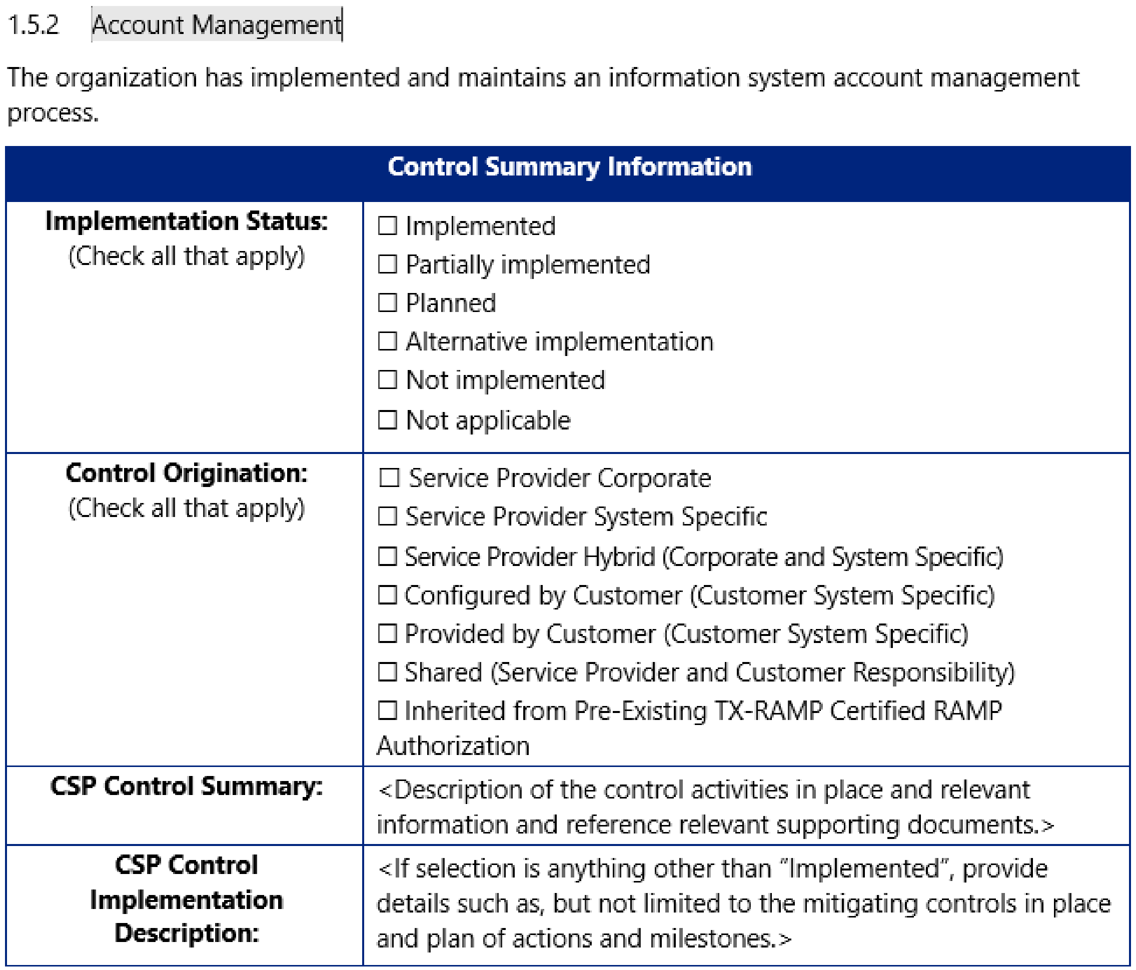
Security Artifact Inventory
Please indicate all security artifacts, certifications, and documentation related to the cloud service.

□ Higher Education Community Vendor Assessment Toolkit (HECVAT) Full
□ Higher Education Community Vendor Assessment Toolkit (HECVAT) Lite

□ Cloud Security Alliance (CSA) Consensus Assessment Initiative Questionnaire (CAIQ)
□ CSA STAR Level 1
□ CSA STAR Level 2

- Will be a SPECTRIM Questionnaire launched to the cloud service provider.
- Information piped back into SPECTRIM.
- Artifact inventory will be listed on the TX-RAMP Engagement record and visible to those with TX-RAMP access.

Assessment and Security Plan



1.5.2 Account Management

The organization has implemented and maintains an information system account management process.

Control Summary Information	
Implementation Status: (Check all that apply)	☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not implemented ☐ Not applicable
Control Origination: (Check all that apply)	☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from Pre-Existing TX-RAMP Certified RAMP Authorization
CSP Control Summary:	<Description of the control activities in place and relevant information and reference relevant supporting documents.>
CSP Control Implementation Description:	<If selection is anything other than "Implemented", provide details such as, but not limited to the mitigating controls in place and plan of actions and milestones.>

- Assessment will be a SPECTRIM Questionnaire launched to the cloud service provider.
- Security Plan will be a word template to be completed and attached as part of the assessment questionnaire.
- Information piped back into SPECTRIM. Information will only be shared if cloud service provider opts in.

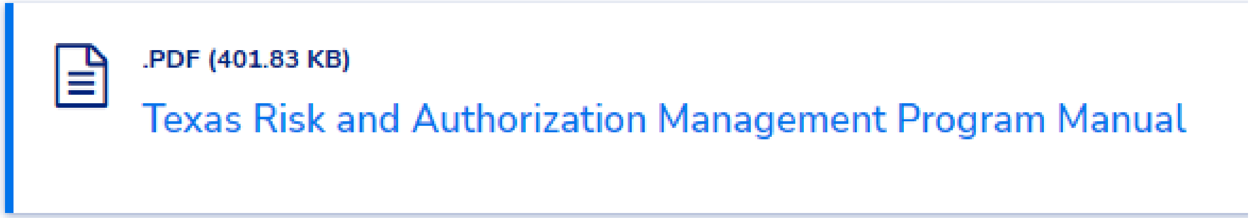
Provisional Certification changes

- 18 months to get level 1 or 2 certification
- 6-month extension if submitted but not granted level 1 or 2
- Additional 3-month extension if DIR has not completed assessment review
- Additional 3-month extension on discretionary basis
- FedRAMP/StateRAMP provisional tied to respective statuses
- Temporary Interim agency-sponsored provisional certification for 60 days.
- Provisional Certification does not imply the product has been vetted.

TX-RAMP Overview

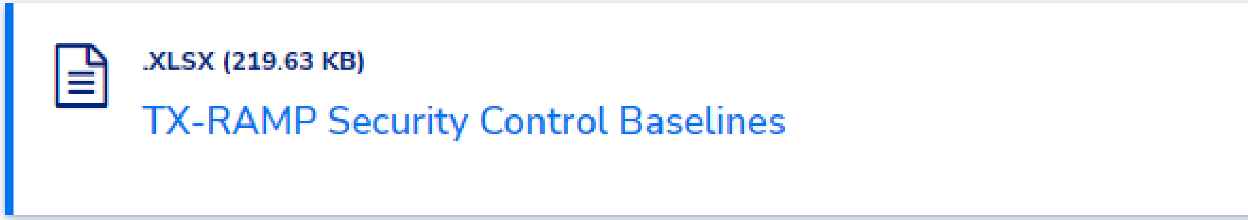
TX-RAMP Webpage

https://dir.texas.gov/tx-ramp



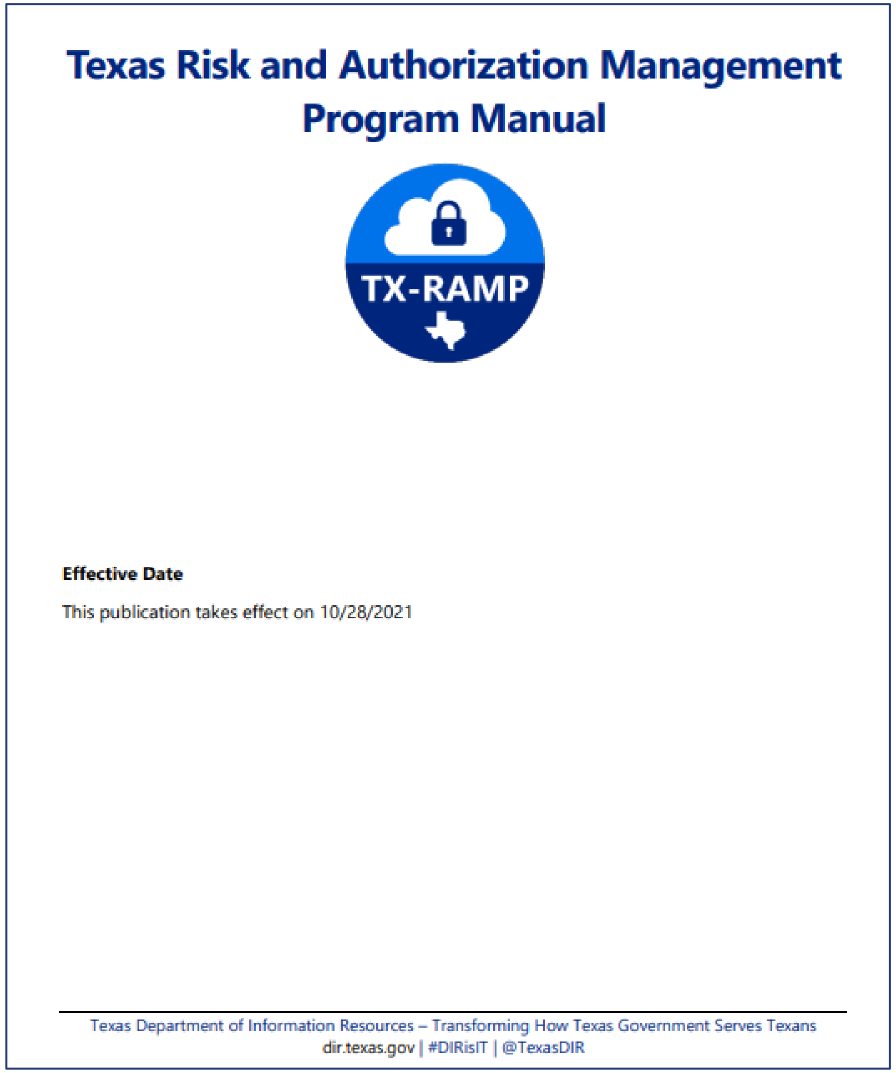
.PDF (401.83 KB)

Texas Risk and Authorization Management Program Manual



.XLSX (219.63 KB)

TX-RAMP Security Control Baselines



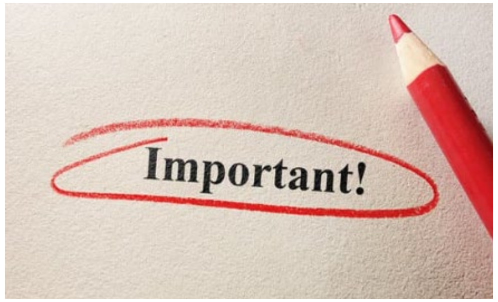
Texas Risk and Authorization Management Program Manual

Effective Date

This publication takes effect on 10/28/2021

Texas Department of Information Resources – Transforming How Texas Government Serves Texans
dir.texas.gov | #DIRisIT | @TexasDIR

Important Points



- Certifications are on a product (system) basis (not vendor).
- The developer/manufacturer of the cloud service seeks certification.
- Resellers of cloud services do not need a separate certification.
- Agencies are responsible for determining whether a product is in scope.
- Agencies are responsible for determining the minimum certification level.
- Time to obtain certification varies and depends on vendor capability.
- Requests are best submitted by the CSP directly.
- You’ll need the right points of contact to get certified – IT/Security/Mgmt.
- Proper documentation is vital.
- FedRAMP/StateRAMP equivalents are certified by proxy, list reconciled ~weekly.
    - No action required, but let us know if something needs to be updated.

Important Points

- Not intended for third party internal cloud services (e.g. vendor email systems).
- Not intended for custom development/builds.
- Look at where your data are when scoping.
- SaaS products are not automatically covered by a certified IaaS.
- Provisional certification does not imply a secure product.
- TX-RAMP does not cover specific regulatory requirements.
- Agencies should communicate requirements to their vendors.
- Vendors should request the assessment.
- Agency-sponsored interim certification should be used sparingly.

Scoping Questions

1. **Does it meet the definition of “cloud computing service?”**

2. Does it fall into the out-of-scope categories/characteristics?

3. What is the impact level of the information resources?

4. Does it process/store confidential information?

Is it a bird? Is it a plane? No, it's a cloud service!

- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Is it a bird? Is it a plane? No, it’s a cloud service!

Question (Yes/No)	Conclusion
Does the system use virtual machines?	A no response means that system is most likely not a cloud.
Does the system have the ability to expand its capacity to meet customer demand?	A no response means that the system is most likely not a cloud.
Does the system allow the consumer to build anything other than servers?	A no response means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS.
Does the system offer the ability to create databases?	A yes response means that the system is a PaaS.
Does the system offer various developer toolkits and APIs?	A yes response means that the system is a PaaS.
Does the system offer only applications that are available by obtaining a login?	A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS.

Scoping Questions

1. Does it meet the definition of “cloud computing service?”

2. **Does it fall into the out-of-scope categories/ characteristics?**

3. What is the impact level of the information resources?

4. Does it process/store confidential information?

Out of Scope – Categories & Characteristics

- Consumption-focused (training/advisory/research)
- Design/Illustration
- GIS/Mapping
- Email/Notification Distribution
- Social Media
- Survey/Scheduling
- Accreditation/Compliance Requirements
- Web apps for purchasing supplies/reservations/travel
- Low-Impact SaaS

Provided that the cloud computing service <u>does not:</u> create, process, or store confidential state-controlled data (except as needed to provide a login capability, e.g. username, password, email or payment information or agency functions like booking/reservations)

Agencies should document cloud services designated as out-of-scope in accordance with agency policies.

Scoping Questions

1. Does it meet the definition of “cloud computing service?”

2. Does it fall into the out-of-scope categories/characteristics?

3. **What is the impact level of the information resources?**

4. Does it process/store confidential information?

Impact Determination

Information Resources whose loss of confidentiality, integrity, or availability could be expected to have…

Low Impact	Moderate Impact	High Impact
• a limited adverse effect on operations, assets, or individuals.	• a serious adverse effect on operations, assets, or individuals.	• a severe or catastrophic adverse effect on operations, assets, or individuals.
Such an event could:		
• cause a degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is noticeably reduced, • result in minor damage to assets, • result in minor financial loss, or • result in minor harm to individuals.	• cause a significant degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is significantly reduced, • result in significant damage to assets • result in significant financial loss, or • result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.	• cause a severe degradation in or loss of mission capability to an extent and duration the organization is not able to perform one of more of its primary functions, • result in major damage to assets, • result in major financial loss, or • result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries

Impact Determination – Quantified Examples

These figures are for illustrative purposes only – each entity should define what constitutes low, moderate, and high impact based on their organizational needs.

Low Impact	Moderate Impact	High Impact
• a limited adverse effect on operations, assets, or individuals.	• a serious adverse effect on operations, assets, or individuals.	• a severe or catastrophic adverse effect on operations, assets, or individuals.
Such an event could:		
• Fewer than 1,000 confidential records	• 1,000 - 50,000 confidential records	• Over 50,000 confidential records
• No impact on critical operations	• Critical operations impacted <24 hours	• Critical operations impacted >24 hours
• Less than $10,000 in potential damage	• $10,000 - $99,999 in potential damage	• Over $100,000 in potential damage
• Impact restricted to single business unit	• 2-3 business units impacted	• Impact restricted to single business unit
• Reputational damage < 90% likely	• Reputational damage <40% likely	• Reputational damage <10% likely
• <10% chance of fines/judgements	• <25% chance of fines/judgements	• Over 25% chance of fines/judgements
• No impact to public/physical harm	• No impact to public/physical harm	• Potential impact to public/physical harm

Scoping Questions

1. Does it meet the definition of “cloud computing service?”

2. Does it fall into the out-of-scope categories/characteristics?

3. What is the impact level of the information resources?

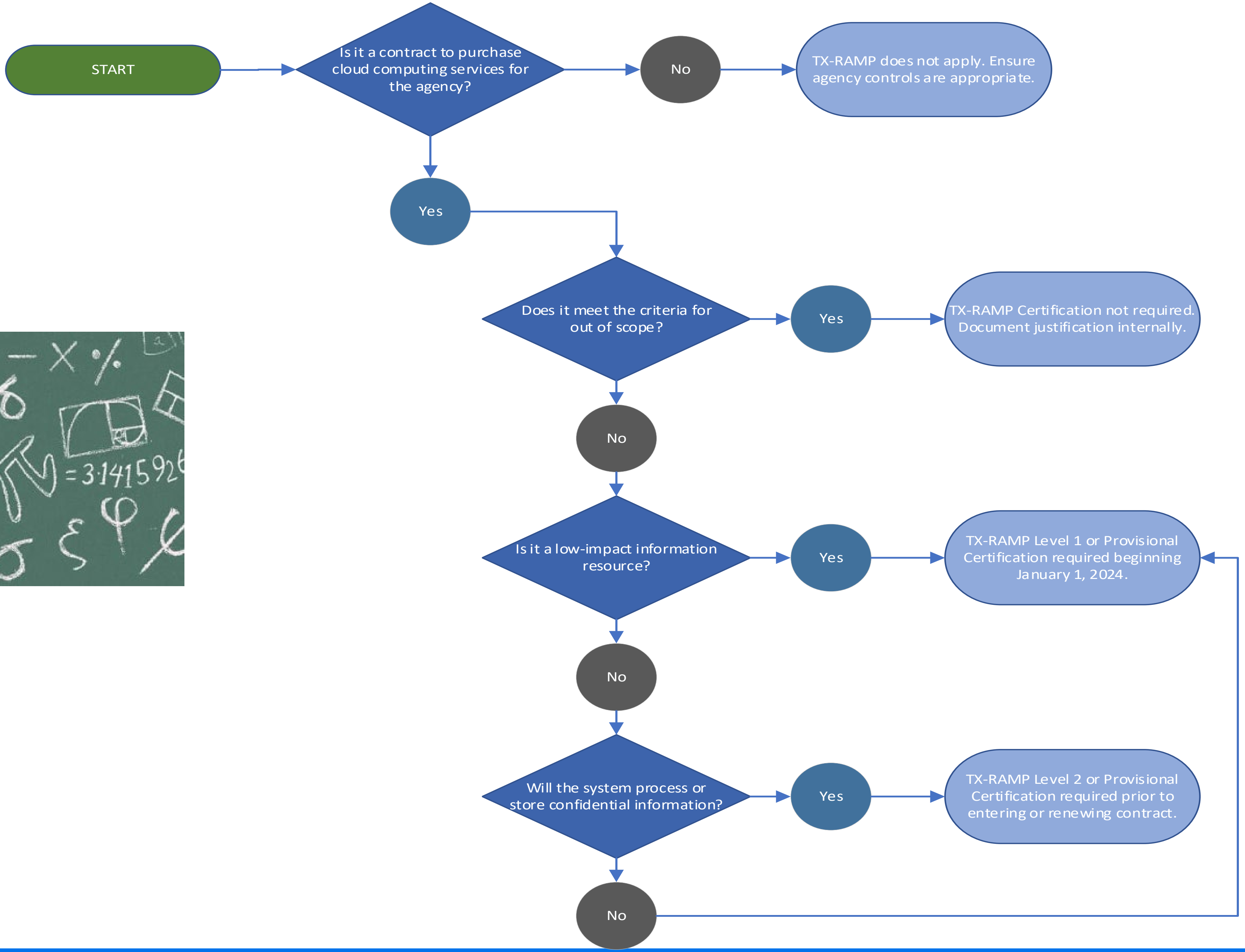
4. **Does it process/store confidential information?**

Confidential Information

- Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement. Common types:
  - Dates of birth of living persons
  - Driver's license numbers
  - License plate numbers
  - Credit card numbers
  - Insurance policy numbers
  - Juvenile offender records
  - Child abuse investigations
  - Peace officer's home address
  - Peace officer's family member information

https://www.texasattorneygeneral.gov/sites/default/files/files/divisions/open-government/publicinfo_hb.pdf

Recap



START

Is it a contract to purchase cloud computing services for the agency?

No

TX-RAMP does not apply. Ensure agency controls are appropriate.

Yes

Does it meet the criteria for out of scope?

Yes

TX-RAMP Certification not required. Document justification internally.

No

Is it a low-impact information resource?

Yes

TX-RAMP Level 1 or Provisional Certification required beginning January 1, 2024.

No

Will the system process or store confidential information?

Yes

TX-RAMP Level 2 or Provisional Certification required prior to entering or renewing contract.

No

Certification Levels

TX-RAMP Provisional Certification

- Not level-specific
- Valid for 18 months
- No Continuous Monitoring Reporting Requirements

TX-RAMP Level 1

- Nonconfidential information **OR**
- Low-impact information resources
- Valid for 3 years
- Required on or after January 1, 2024
- Annual Continuous Monitoring Reporting

TX-RAMP Level 2

- Confidential information **AND**
- Moderate or high-impact information resources
- Valid for 3 years
- Required on or after January 1, 2022
- Quarterly Continuous Monitoring Reporting

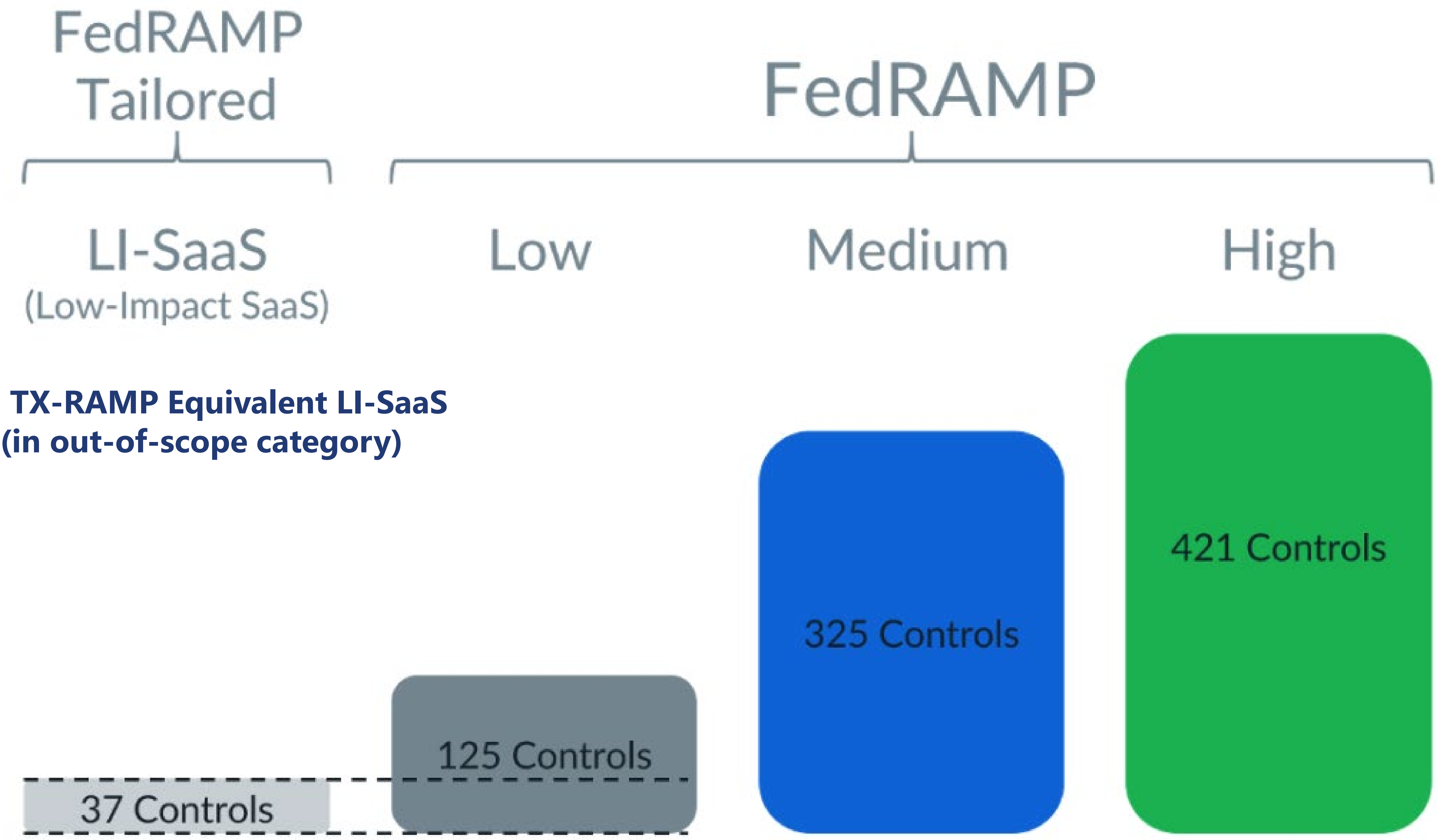
Contract Management Essential Provisions

The recommended TX-RAMP procurement language may be found on page 201 (page 3 of Appendix 23). https://comptroller.texas.gov/purchasing/docs/96-1809.pdf

Clause	Standard Text	Ref	Guidance
Cloud Computing State Risk and Authorization Management Program (TX-RAMP)	Pursuant to Section 2054.0593(d)-(f) of the Texas Government Code, relating to cloud computing state risk and authorization management program, **Respondent** represents and warrants that it complies with the requirements of the state risk and authorization management program and **Respondent** agrees that throughout the term of the contract it shall maintain its certifications and comply with the program requirements in the performance of the contract.	TEX GOV'T CODE § 2054.0593 1 TAC § 202.27	Clause only applies to contractors doing business with an agency for cloud computer services subjected to the state risk and authorization management program. A state agency shall ensure contractor's compliance with the program for contracts it enters or renews after January 1, 2022. The state risk and authorization management program is set out in 1 TAC § 202.27 for state agencies.

TX-RAMP | StateRAMP | FedRAMP

TX-RAMP	StateRAMP	FedRAMP
• Based on NIST 800-53r5	• Based on NIST 800-53r4	• Based on NIST 800-53r4
• Requires DIR Assessment	• Requires 3PAO Audit	• Required 3PAO Audit
• No fees	• Annual/Assessment Fees	• Assessment Fees
• Impact level determined by TAC 202	• Impact determined by classification	• Impact level determined by FIPS 199
• ConMon available to contracting agencies	• ConMon available to public sector members	• ConMon available to federal agencies
• Mandatory for state agencies/IHE	• Not mandatory	• Mandatory for federal executive agencies
• Does not require business w/ state	• 501c(6)	• Must do business with federal gov



No TX-RAMP Equivalent LI-SaaS (in out-of-scope category)

Assessment Information (Process will be updated Nov. 22)

- Agencies can submit a request for a level 1 or 2 assessment in SPECTRIM. **Prefer that vendors make these requests.**

- Agencies can submit a request to sponsor for provisional certification in SPECTRIM. **Prefer that agency coordinates and informs vendor of intention.**

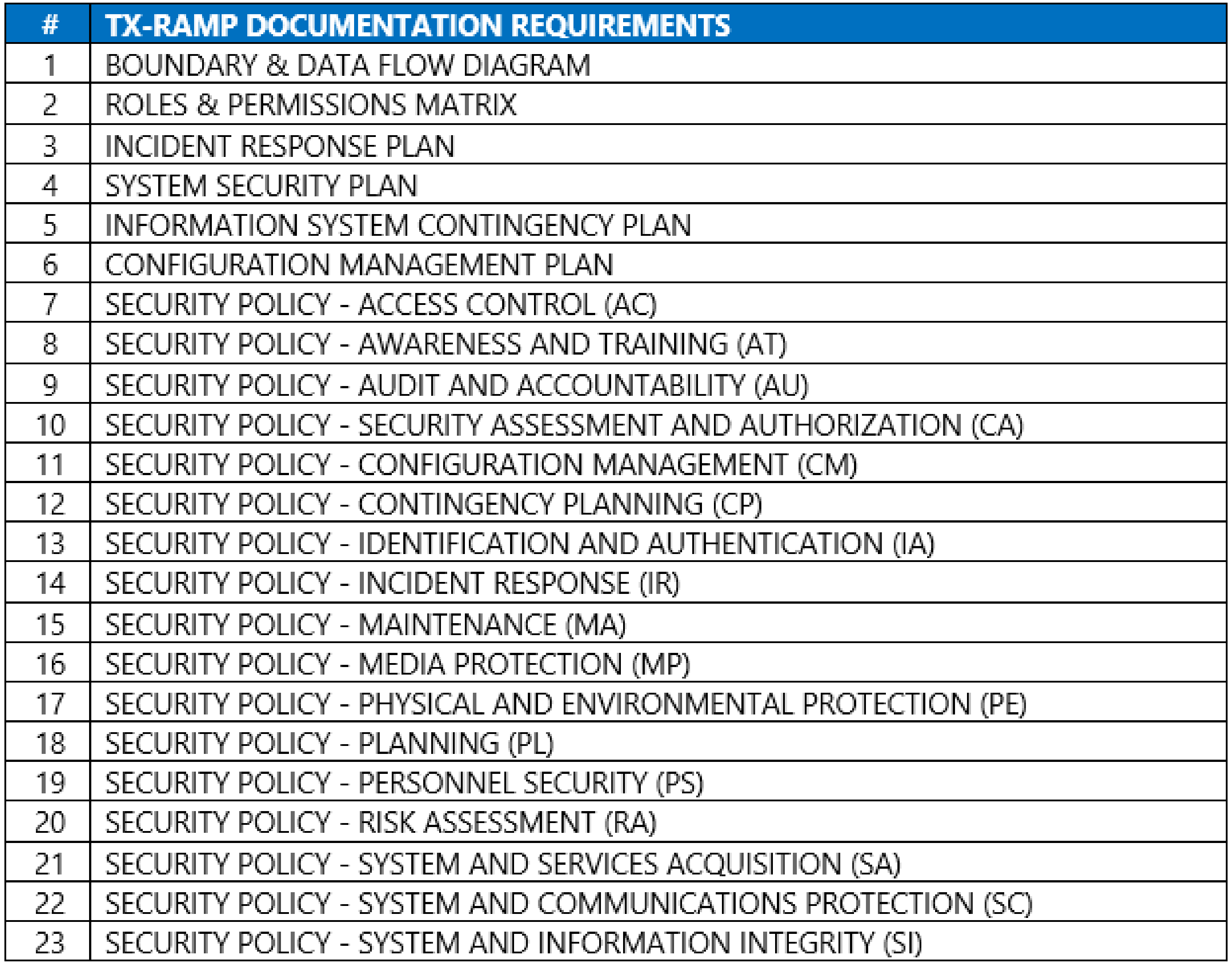
- Vendors can submit this external form to request a level 1 or 2 assessment or request provisional certification review directly:
  - https://survey.alchemer.com/s3/6510630/TX-RAMP-Vendor-Contact

- Assessments consist of control implementation questionnaire & providing required documentation.

Assessment Questionnaire (Process will be updated Nov. 22)

- Some controls may be the responsibility of subservice organizations, or the customer themselves.
- Some other than satisfied controls may require remediation plans, closer monitoring, or full remediation prior to achieve certification.
- Providing context of who’s responsible for what, mitigating/compensating control information, and deeper context helps assessors expedite the process.
- All documentation must be submitted for consideration.

Documentation – Consolidated into template but required to be in place.



#	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)

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

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

TX-RAMP Assessment Requests

- **Assessment requests submitted by agency should include:**
  - Appropriate point(s) of contact for vendor (to notify/begin assessment)
  - Clear description of the product being requested
  - Direct link to vendor product description page
  - Informative and consistent product name
  - Single product to the extent possible (modular software platforms may be considered a single product)
  - Correct/accurate vendor (cloud provider OEM aka Third-Party Profile)
  - More context > less context
- **Assessment requests should NOT include:**
  - Identifying organizational information
  - Descriptions specific to how you are using the product
  - Custom Product URLs or Authentication URLs
  - IaaS provider as the manufacturer of a SaaS product

Assessment Review

- Review of assessments is prioritized according to several factors:
  - Submit date
  - Assessment level
  - Completeness of submission

- Time to review depends heavily on:
  - Vendor responsiveness
  - Completeness of documentation
  - Response accuracy

- General processing times (note: this can vary and is based on a typical example)
  - 3rd Party Provisional Review = 1-7 Days
  - Agency Sponsorship Review = 1-7 Days
  - Level 1/2 Review = 2-4 Weeks

Continuous Monitoring Reporting

- **Vulnerability Reporting**
  - Level 1 – Annual
  - Level 2 – Quarterly
- **Breach of Confidential/PII**
  - As needed
- **Significant Changes**
  - As needed

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/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/Compensating Controls

Resources

- **TX-RAMP Website:** https://www.dir.texas.gov/tx-ramp
- **Certified Cloud Products List:** https://dir.texas.gov/sites/default/files/2022-08/TX-RAMP%20Certified%20Products.8.5.22.xlsx
- **TX-RAMP Program Manual:** https://dir.texas.gov/sites/default/files/2021-11/TX-RAMP%20Manual_0.pdf
- **TAC §202.27:** https://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=27
- **Vendor Assessment Request Form:** https://survey.alchemer.com/s3/6510630/TX-RAMP-Vendor-Contact
- **TX-RAMP Staff Meeting Request:** https://outlook.office365.com/owa/calendar/TXRAMP1@dir.texas.gov/bookings/
- **TX-RAMP FAQ:** https://dir.texas.gov/sites/default/files/2022-01/TX-RAMP%20FAQ.12.30.21.pdf
- **Vendor Assessment Guidance:** https://prod.dir.texas.gov/resource-library-item/tx-ramp-vendor-guide-completing-assessment-questionnaire
- **StateRAMP Templates:** https://stateramp.org/templates-resources/
- **Questions –** tx-ramp@dir.texas.gov
- **SPECTRM Assistance –** GRC@dir.texas.gov

Q & A

Thank You

dir.texas.gov

#DIRisIT

@TexasDIR

Transforming How Texas Government Serves Texans

Texas Department of Information Resources