Texas Department of Transportation

Information Security Standard

ISS-01-212

Standard Title: TxDOT Information Security Risk and Authorization Management Program (IS-RAMP)

Effective Date: 12/1/2023

Date of Last Revision: 11/15/2023

Division of Primary Responsibility: TxDOT Information Security Office

DocuSigned by:
Steven Pryor
E5B3FA5479BF4DC...

Contents

1. Introduction

1.1 Purpose

The TxDOT Information Security Risk and Authorization Management Program (IS-RAMP) is a component of TxDOT's overarching Information Security Third Party Risk Program and supports the goal of implementing an enterprise-wide security program within TxDOT by providing consistency in procedures and compliance levels for contractors authorized to access, transmit, use, or store TxDOT data.

IS-RAMP and its requirements are designed in accordance with Texas state laws and regulations, particularly the excerpts noted in the table below.

Applicable State Law	State Law Excerpt
Texas Government Code, Section 2054.138 – Security Controls for State Agency Data	Each state agency entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for the agency shall include a provision in the contract requiring the vendor to meet the security controls the agency determines are proportionate with the agency's risk under the contract based on the sensitivity of the agency's data. The vendor must periodically provide to the agency evidence that the vendor meets the security controls required under the contract.
Texas Government Code, Section 2054.0593 – Cloud Computing State Risk and Authorization Management Program	A state agency may not enter or renew a contract with a vendor to purchase cloud computing services for the agency that are subject to the state risk and authorization management program unless the vendor demonstrates compliance with program requirements. A state agency shall require a vendor contracting with the agency to provide cloud computing services for the agency that are subject to the state risk and authorization management program to maintain program compliance and certification throughout the term of the contract.
Title 1, Texas Administrative Code (TAC), Rule §202.24 – Agency Information Security Program	Each agency shall develop, document, and implement an agency-wide information security program, approved by the agency head under §202.20, that includes protections, based on risk, for all information and information resources owned, leased, or under the custodianship of any department, operating unit, or employee of the agency including outsourced resources to another agency, contractor, or other source (e.g., cloud computing).

1.2 Scope

This document outlines steps to implement TxDOT IS-RAMP as required by TxDOT's Information Security and Privacy Controls Standards Catalog:

- CA-02, Control Assessments
- CA-06, Authorization
- SA-04, Acquisition Process
- SR-06, Supplier Assessments and Reviews.

This document applies to all contractors authorized to access, transmit, use, or store TxDOT data.

1.3 Audience and Applicability

This document is intended for contractors and contractor representatives responsible for complying with TxDOT cybersecurity and privacy requirements, as well as TxDOT employees and contractors responsible for coordinating, managing, and monitoring third party risk.

1.4 Organization of this Document

The remainder of this document is organized as follows:

- Section 2 provides guidance and security requirements relating to TxDOT Security Questionnaire (TSQ).
- Section 3 provides guidance and security requirements relating to TxDOT TX-RAMP.
- Section 4 provides guidance for submitting documentation to TxDOT in a secure manner.
- Section 5 provides instruction to immediately notify TxDOT of a potential or confirmed cybersecurity or privacy incident potentially involving TxDOT data.
- Appendix A provides hyperlinks to applicable forms and references for additional guidance.

2. TxDOT Security Questionnaire Guidance and Requirements

Before a contractor is authorized to access, transmit, use, or store TxDOT data within the contractor's environment, the contractor must provide evidence of compliance with TxDOT's cybersecurity and privacy requirements as documented in solicitation requirements or contractual agreements between the contractor and TxDOT. A contractor's cybersecurity and privacy requirements may vary depending on the security baseline and security overlay values noted in the solicitation details or existing contract. Security baselines and security overlays are determined in accordance with the TxDOT Data Classification Policy and regard to the type of TxDOT data to be accessed, transmitted, used, or stored by the contractor.

2.1 Completion Requirements

Contractors that access, transmit, use, or store TxDOT data are in scope to complete and submit the TxDOT Security Questionnaire (TSQ.) For a TSQ to be considered complete, the contractor must complete all required sections. Sections 1 and 2 are required for all contractors. Section 3 is required only if the contractor's security baseline is determined to be Moderate or High. The table below indicates requirements for Sections 1-3 based on the security baseline noted in the solicitation or contract.

Security Baseline	TSQ Requirements Based on Security Baseline		
	Section 1	Section 2	Section 3
Low	X	X	
Moderate	X	X	X
High	X	X	X

Section 4 of the TSQ is required only if the Security Overlays noted in the solicitation or contract include Privacy data. The table below indicates requirements for Section 4 based on the Security Overlays noted in the solicitation or contract.

Security Overlay	TSQ Requirements Based on Security Overlays
	Section 4
Sensitive	
Privacy	X
PCI	
CJIS	

The contractor may receive data from TxDOT that originates from another regulatory or federal source that has additional assessment requirements beyond what is mentioned above. The contractor must refer to its contractual agreement with TxDOT for any added requirements.

2.2 Submission Frequency

Use the table below to determine how often to complete and submit a TSQ to TxDOT.

Security Baseline	TSQ Submission Frequency	
	Upon Solicitation Response	Upon Renewal
Low	X	X
Moderate	X	X
High	X	X

NOTE: TSQs may not be required for contracts or renewals that meet TSQ exclusion requirements provided in Section 2.4.

NOTE: If not defined by the Division responsible for the procurement and administration of the contract renewal, then for this section renewal is defined as any extension of the contract beyond the initial term of the contract.

Vendors must submit TSQs to TxDOT for each contract being solicited or renewed unless the contract has been approved to be excluded from contract requirements in accordance with Section 2.4.

2.3 Deviation for Non-Compliance

If any TSQ question in sections 2 through 4 has a “No” response the contractor must provide an explanation of the non-compliance as well as actions and get-well dates for the non-compliance. The TSQ must be submitted to the TxDOT Information Security Office and the risk accepted by the TxDOT Chief Information Security Officer, Chief Information Officer, and Information Owner before the award or renewal of the contract. For TSQs with approved non-compliant items, the vendor must submit an updated TSQ before the expiration date set by the TxDOT Information Security Office.

2.4 Exclusion Requirements

Contractors may not be required to submit a TSQ if they meet one or more of the following criteria and the exclusion is approved by the TxDOT Chief Information Security Officer:

For **Public or Sensitive** data, the criteria include**:**

- Cloud Computing Services for Transmitting Non-Confidential Data to External Governing Bodies: Cloud computing services used to transmit data as required by external governing bodies for purposes of accreditation and compliance.
- Consumption-Focused Cloud Computing Services: Advisory services, market research, or other resources that are used to gather research or advisory information.
- Educational or Training Platforms: Cloud platforms that host training materials or educational content, excluding any data regarding sensitive personal information, regulated education records, or proprietary research.
- Encrypted Data: TxDOT data is fully encrypted by TxDOT and TxDOT has ownership of the encryption keys.
- General Procurement or eCommerce Services: Services used for purchasing supplies, travel and booking accommodations, reservations, or other general-purpose procurement applications that only access payment information of the agency or agency personnel.
- Graphic Design or Illustration Products: Tools used for design tasks.
- Marketing and Social Media Analysis: Tools used to gather and analyze public social media data, customer feedback, or market trends.
- Social Media Platforms: Tools for social interaction and public communication.

For **Confidential or Regulated data**, the criterium is Encrypted Data. This means when TxDOT data is fully encrypted by TxDOT and TxDOT has ownership of the encryption keys.

For an **Authority to Operate**, the criterium is when, as part of the TxDOT Security Categorization process, the Chief Information Security Officer and the Information Owner determine the system does not require an Authority to Operate.

2.5 Exceptions

TxDOT may authorize a temporary exception allowing a contract to be awarded without a TSQ if necessary to meet a statutory or regulatory requirement. Exceptions must be approved by TxDOT Chief Information Officer, Chief Information Security Officer, the Information Owner, and the Information Owner's Chief, and must include a remediation plan for when the agency will become compliant.

3. Texas Risk and Authorization Management Program (TX-RAMP) Guidance and Requirements

3.1 Cloud Computing Service Provider Requirements

Contractors providing cloud computing services to TxDOT must be certified via the Department of Information Resources (DIR) Texas Risk and Authorization Management Program (TX-RAMP) prior to contract award or renewal unless TxDOT Information Security has determined the service is not subject to TX-RAMP per section 3.2. See the *TX-RAMP Program Manual* for a further definition of “cloud computing services.”

NOTE: If not defined by the Division responsible for the procurement and administration of the contract renewal, then for this section renewal is defined as any extension of the contract beyond the initial term of the contract.

The required TX-RAMP Certification Level is determined by the security baseline assigned by the TxDOT Information Owner and Information Security Office.

Security Baseline	TX-RAMP Certification Level Requirement	
	Level 1	Level 2
Low	X	
Moderate		X
High		X

Contractors who provide cloud computing services to TxDOT must achieve and maintain TX-RAMP Certification in accordance with the table below before TxDOT can award a new contract or renew an existing contract.

Required TX-RAMP Certification	Effective Date
Level 1	1/1/2024
Level 2	1/1/2022

NOTE: TX-RAMP Certification is not required for contracts or renewals providing TxDOT cloud computing services that are not subject to TX-RAMP requirements provided in Section 3.2.

NOTE: For instances where the contractor is subcontracting to another contracted entity to provide cloud computing services to TxDOT, the contractor must ensure any cloud computing services procured on TxDOT’s behalf meet TX-RAMP requirements.

If a contractor is unable to obtain TX-RAMP Level 1 or Level 2, prior to contract award or renewal, the contractor must obtain a TX-RAMP Provisional Certification through DIR. A TX-RAMP Provisional Certification expires after a set period of time determined by DIR. The contractor is required to obtain TX-RAMP Level 1 or Level 2 certification prior to the expiration of the provisional TX-RAMP certification.

If DIR approves of a Provisional Certification, TxDOT will require additional information from the contractor to further evaluate risks, including:

- Applicable TX-RAMP Evaluation Request form
- TxDOT Security Questionnaire (TSQ)

Other third-party attestations may be accepted in lieu of the TX-RAMP Evaluation Request form by TxDOT at the discretion of the Information Security Office. Contact a TxDOT Procurement Official or Contract Manager for additional information regarding TX-RAMP and Provisional Certification Evaluation.

The TX-RAMP program contains continuous monitoring requirements. Please consult the *TX-RAMP Program Manual* and its accompanying DIR TX-RAMP Program documents to ensure compliance.

3.2 Cloud Services Not Subject to TX-RAMP Certification

This section lists the cloud computing services and systems that may not be subject to the TX-RAMP certification requirements if approved by the TxDOT Chief Information Security Officer, in accordance with *TX--RAMP Program Manual* sections 7.1 or 7.2. All cloud computing services with a high security baseline are subject to TX-RAMP certification requirements and are not included in this section.

Low Security Baseline. If the cloud computing service is a low security baseline and does not store or process Confidential or Regulated TxDOT data, the service may not be subject to TX-RAMP*.*

Moderate Security Baseline. The cloud computing service may not be subject to TX-RAMP if it is a moderate security baseline that does not process or store Confidential or Regulated TxDOT data and that meets one of the following:

- Consumption-Focused Cloud Computing Services: Advisory services, market research, or other resources that are used to gather research or advisory information.
- Graphic Design or Illustration Products: Tools used for design tasks.
- Geographic Information Systems (GIS) or Mapping Products: Applications for geographic mapping and spatial analysis. Geographic Information Systems are computer systems used to capture, store, check, or display data related to positions on Earth's surface.
- Email or Notification Distribution Services: Platforms used for generic communication or notifications.
- Social Media Platforms: Tools for social interaction and public communication.

- Survey Tools: Survey tools not intended to collect confidential or regulated information.
- Collaboration or Productivity Tools: Standard collaboration tools for non-sensitive projects, such as shared document editing or project management.
- Cloud Computing Services for Transmitting Non-Confidential Data to External Governing Bodies: Cloud computing services used to transmit data as required by external governing bodies for purposes of accreditation and compliance.
- General Procurement or eCommerce Services: Services used for purchasing supplies, travel and booking accommodations, reservations, or other general-purpose procurement applications that only access payment information of the agency or agency personnel.
- Public-facing Websites: Hosting static, public-facing websites, or web content that does not process or store confidential state-controlled data.
- Educational or Training Platforms: Cloud platforms that host training materials or educational content, excluding any data regarding sensitive personal information, regulated education records, or proprietary research.
- Marketing and Social Media Analysis: Tools used to gather and analyze public social media data, customer feedback, or market trends.

3.3 TX-RAMP Transitional Grace Period

TxDOT may authorize a transitional grace period to allow for cloud computing services whose existing TX-RAMP certification has expired to continue providing cloud computing services to TxDOT. The grace period must be documented in a Transition Plan that is approved by the TxDOT Chief Information Officer, Chief Information Security Officer, and Information Owner; may not be granted for more than a two-year period; and must be reported to DIR every two years.

Transition Plans must include, at a minimum:

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

3.4 TX-RAMP Exception

TxDOT may authorize a temporary exception to TX-RAMP requirements if necessary to meet statutory or regulatory requirements. Exceptions must be approved by the TxDOT Chief Information Officer, Chief Information Security Officer, the Information Owner, and the Information Owner's Chief. The exception must include a remediation plan for when the agency will become compliant with TX-RAMP.

4. Submitting Documentation

All information security documentation concerning TxDOT data is classified as Confidential. Documentation must be submitted in a manner compliant with SC-08, Transmission of Confidential Data, and SC-28, Protection of Data at Rest, in accordance with the *TxDOT Information Security and Privacy Controls Catalog.* For more guidance about submitting documentation to TxDOT, contact the TxDOT point of contact listed in the solicitation or contract.

5. Reporting Breaches or Potential Incidents

In the event TxDOT data is compromised or potentially compromised, contractors must immediately notify TxDOT via the Report Cybersecurity Incident form on TxDOT.gov.

"Breach" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data, as defined in Texas Business & Commerce. Code §521.053.

"Security Incident" means an event which may result in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources, as defined in Title 1, TAC §202.1(40).

6. Appendix A: Tools, References, and Guidance

See TxDOT Cybersecurity Resources for forms, templates, and guidance applicable to IS-RAMP such as the TxDOT Security Questionnaire, TxDOT Data Classification Policy, and the *TxDOT Information Security and Privacy Controls Standards Catalog*.

See DIR's TX-RAMP website for the TX-RAMP Program Manual and additional guidance and resources, such as the DIR TX-RAMP Assessment Request for vendors.

Revision History

Brief Description of Change

Version	Date	Description of Changes
2022	1/31/2022	Initial release.
2022.1	11/21/2022	Throughout document, changed *third party* to *contractor*. Added new section to separate TSQ requirements from TX-RAMP requirements and added TSQ applicability and contractor receipt of TxDOT data statements. New title for Section 2.3, TSQ Non-Compliance and specified which TSQ sections may have “no” response. New title and section contents for 2.4, Exclusion Requirements. Section 3.1: Updated TX-RAMP Level 1 Effective Date to 1/1/2024. Removed agency provisional sponsorship option and language. Specified accepted attestation reports of SOC 2 type II. Added note for contactor awareness for TX-RAMP continuous monitoring requirements. Section 3.2: Updated TX-RAMP Exclusion criteria statement for list item 1. Added TX-RAMP exclusion determination decision statement.
2023.1	05/11/2023	Section 2.2: Corrected reference in NOTE to reference section 2.4. Changed two instanced of “Exempt” to “Excluded.”
2023.2	12/1/2023	Clarified Exclusion Requirements in Section 2.4 and clarified temporary exception requirements in Section 2.5. Aligned Section 3 contents with the newly released Texas Risk and Authorization Management Program (TX-RAMP) manual issued by Texas Department of Information Resources. Section 3.1 changes include: addressing when contractors providing cloud computer services must be TX-RAMP certified; defining the term renewal; designating that third-party attestations in lieu of TX-RAMP Evaluation Request form may be accepted subject to the discretion of the Information Security Office; and adding a reference to TX-RAMP continuous monitoring requirements. Section 3.2 is now TX-RAMP Certification. Removed the term Exclusions and replaced it with not subject to language to align with TX-RAMP provisions. Added new Section 3.3 1.1 TX-RAMP Transitional Grace Period discussing grace period and transitional plan requirements and approvals. This section also includes the TxDOT exceptions requirements and approvals. Throughout the document, replaced the term vendor with contractors.

Publication Owner

Steven Pryor, TxDOT Chief Information Security Officer, (ITD)
Steven.Pryor@txdot.gov (512) 965-4486