Data Classification Tool

Table of Contents

1. Document Revision History

Date	Description	Version	Governance Body
December 2020	Original Publication	1.0	StateRAMP Steering Committee
October 2021	Security status updates	1.1	StateRAMP Staff
April 2022	Updates	1.2	StateRAMP Standards and Technical Committee and Board
August 2024	Updates to instructions and formatting.	1.3	StateRAMP Staff

2. Introduction and Purpose

This document is intended to be used by state and local governments and procurement officials as a tool for determining the appropriate StateRAMP security requirements in procurements with the intent of procuring a service provider using or offering Infrastructure as a Service (IaaS), Software as a Service (SaaS), and/or Platform as a Service (PaaS) solutions that process, store, and/or transmit government data and any related information as defined by NIST 800-53. These include Personally Identifiable Information (PII), Personal Health Information (PHI), Payment Card Industry (PCI), and Criminal Justice Information (CJI). Identifying the data classification aids the Member Organization (Organization) in maintaining the security, confidentiality and integrity of their data in alliance with its governing body.

According to the Federal Information Security Management Act (FISMA) requirements, there are three distinct security objectives for information and information systems: confidentiality, integrity, and availability. These standards are used as the foundation to ensure vendors are providing solutions that meet the minimum-security requirements to process, store, and transmit certain types of government data and any related information.

It is necessary for the Organization, as defined by the StateRAMP Bylaws, to accurately determine their required security baseline prior to publishing a procurement so that the Organization can select a vendor that meets the government's needs and provides the appropriate security controls to protect the government data. The determination to which procurements this process should apply should be based on the Organization's policies and/or standards. Procurement should partner with the information security team, Chief Information Officer, and Chief Information Security Officer and/or the Risk Management team to ensure the appropriate standards are included in the procurement.

This data classification self-assessment is based on the NIST 800-53 Revision 5 (or current) requirements and designed to help state and local governments easily identify the appropriate StateRAMP security category to include a solicitation. Definitions of StateRAMP Ready, StateRAMP Provisionally Authorized, and StateRAMP Authorized, as well as Low Impact, Moderate Impact, and High Impact, can be found in the StateRAMP Security Assessment Framework located here, with further information available on StateRAMP's Templates and Resources page.

3. Instructions

Answer the questions in the survey section to determine what StateRAMP security category requirements you need to include in your solicitation to ensure your data is protected.

4. Survey Questions

1. Will the vendor process, transmit, and/or store non-sensitive State data, metadata, and/or data that may be released to the public that requires no additional levels of protection?
    a. If yes, StateRAMP Low is recommended.
2. Will the vendor process, transmit, and/or store personally identifiable information (PII) as defined by the U.S. Department of Labor (DOL)?
    a. If yes, StateRAMP Moderate is recommended.
3. Will the vendor process, transmit, and/or store protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA)?
    a. If yes, StateRAMP Moderate is recommended.
4. Will the vendor process, transmit, and/or store payment card industry (PCI) data as defined by the PCI Security Standards Council (PCI SSC)?
    a. If yes, StateRAMP Moderate is recommended.
5. Will the vendor process, transmit, and/or store criminal justice information (CJI) data as defined by FBI CJIS division?
    a. If yes, StateRAMP Moderate is recommended.
    b. Note: States may add additional controls to StateRAMP Moderate to comply with the CJIS requirements.
6. Will the loss or unavailability of the data processed, transmitted, and/or stored by the service provider disrupt government operations?
    a. If yes, StateRAMP Moderate is recommended.
7. Will the loss or unavailability of the data that is processed, transmitted, and/or stored by the service provider result in a loss of confidence or trust in the government?
    a. If yes, StateRAMP Moderate is recommended.

5. Next Steps

Data processed, transmitted, and/or stored by the vendor includes information shared inside and outside of the provider's cloud service application. Similarly, if state or local laws have identified any other data type not included in the survey above as confidential, a StateRAMP Moderate is recommended. Once a procurement has been completed partner with the information security team, Chief Information Officer, Chief Information Security Officer, and/or Risk Management team to ensure the appropriate standards have been met.