Overview

Achieving a StateRAMP status—Ready, Provisionally Authorized, or Authorized—requires an independent audit conducted by Third Party Assessing Organizations (3PAOs). After the 3PAO audit for Ready or Authorized status, the provider and 3PAO must submit a final package to the StateRAMP PMO for security review.

Key Components of the Final Packages:

- Assessors must provide a package that includes:
  - Assessor Matrix: Incorporates the StateRAMP Readiness Assessment Review (RAR), StateRAMP Security Assessment Review (SAR), test case procedures, risk exposure template, and system overview.
  - Security Assessment Plan
- Service Providers must provide a security package that includes:
  - Operational Controls Matrix: Formerly known as the System Security Plan (SSP).
  - Continuous Monitoring Matrix: Now combined with a Plan of Action & Milestones (POA&M).

Products achieving any of the three statuses will be listed on the [StateRAMP Authorized Product List (APL)](#).

GET STARTED WITH STATERAMP TEMPLATES

Download compiled packages, templates, and sample policies for both Service Providers and Assessors below:

- [Service Provider Package for Low Impact (Last Published: Jan 8, 2024)](#)
- [Service Provider Package for Moderate Impact (Last Published: Jan 10, 2024)](#)
- [3PAO Package for Low Impact (Last Published: Jan 8, 2024)](#)
- [3PAO Package for Moderate Impact (Last Published: December 12, 2024)](#)

These packages include required templates and sample policies for every NIST 800-53 control family, along with templates for Rules of Behavior, Incident Response Plan, Configuration Management Plan, Information System Contingency Plan, and Supply Chain Risk Management.

For archived Rev. 4 templates, please contact pmo@stateramp.org.