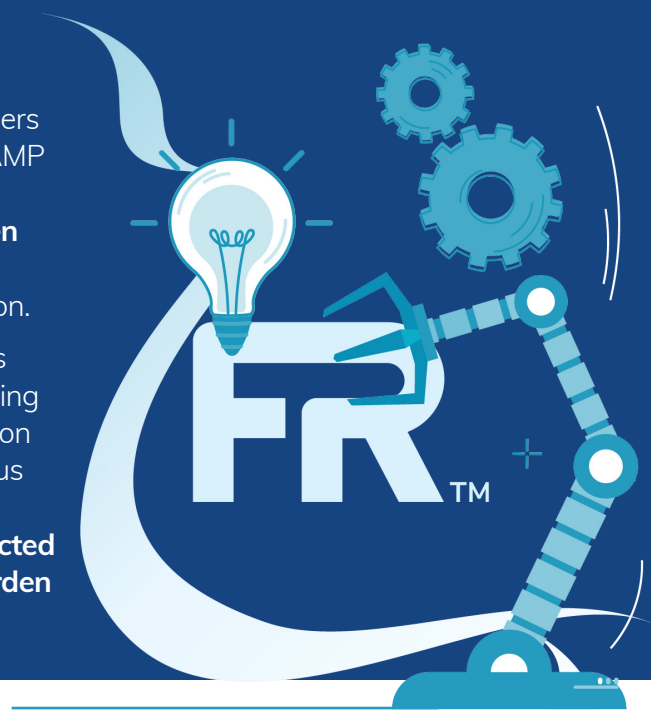
An Automated FedRAMP®

An automated FedRAMP reduces the burden for Cloud Service Providers (CSPs) and Agencies in their endeavor to receive and maintain FedRAMP authorization. An automated FedRAMP means automated processes are needed, which are possible when organizations use the NIST **Open Security Controls Assessment Language (OSCAL)**, a standardized, machine-readable language, to share authorization-related information.

The vision for the FedRAMP Automation Strategy is that stakeholders are creating, submitting, and ingesting assessment documentation using OSCAL-enabled tools. CSPs will submit OSCAL-formatted authorization packages and will have automated channels through which continuous monitoring is performed. An automated FedRAMP will result in **faster identification and resolution for cybersecurity threats, better protected cloud services** for the federal government, and **reduced cost and burden** for all stakeholders.



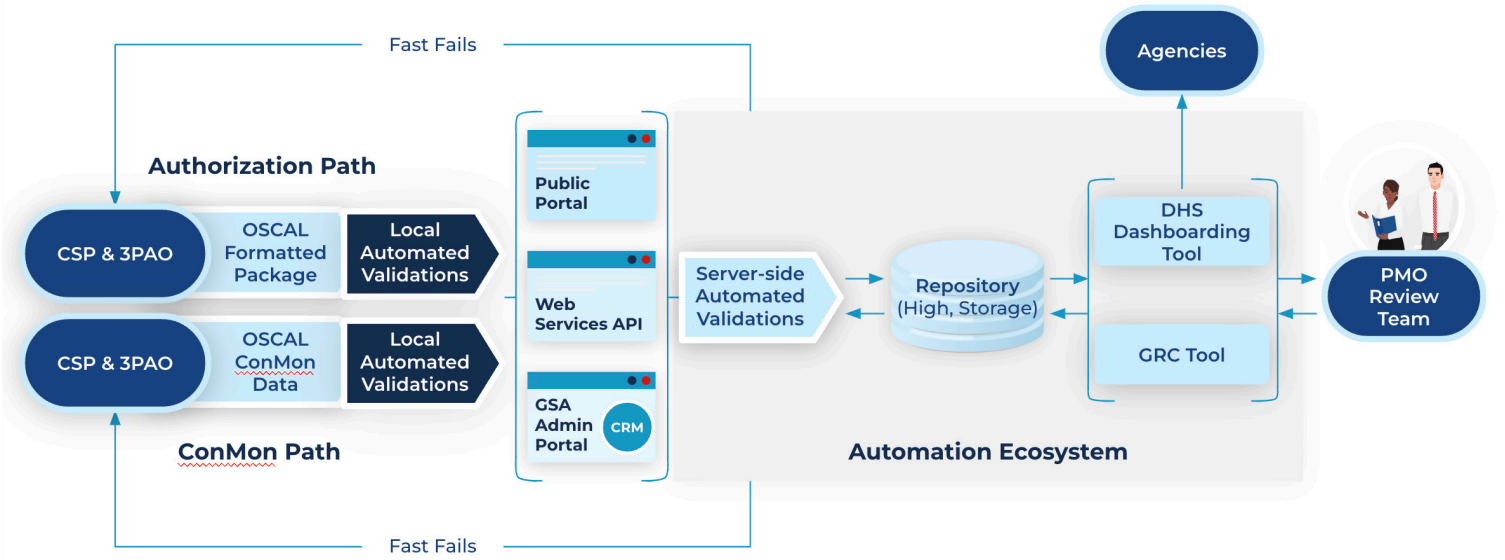
How It Works

An automated ecosystem based on a standardized machine readable format will enable:

Cloud Service Providers (CSPs) and Third Party Assessment Organizations (3PAOs) will have automated mechanisms to self-test, develop, submit, and remediate security packages, reducing the level of effort and timeline for authorizations. Automation will enable a shift from periodic/annual reviews to a continuous approach, reducing both overhead and resource impact associated with these efforts. CSPs will submit Continuous Monitoring data, along with updated package information through a standardized format using an API.

Agencies will have an improved view into risk management, resulting in better informed risk decisions making while authorizing cloud service products. Additionally, improved data freshness will enable agencies to become more agile in threat and risk response.

FedRAMP will receive improved packages at the outset of an authorization lifecycle, allowing reviewers to focus on higher value assessments within the package. Through automated formats, package reviews will be streamlined, less cumbersome on reviewers, and result in faster decision making, allowing higher intake of cloud service products.



Benefits And Outcomes:

A modernized and automated FedRAMP will result in the following benefits and outcomes for both government and industry:

Better Use of Resources

- Reduced Agency and CSP time and cost to develop and submit authorization packages
- Reduced 3PAO and FedRAMP time and cost to review and assess authorization packages
- Reduced level of effort across government and industry due to data standardization

Improved Package Quality

- Reduced passbacks and remediations of documentation shortening authorization timeline
- Greater insight into risk management decisions
- Increased data quality for Continuous Monitoring
- Improved content freshness

Increased Package Throughput

- Increased cloud systems available for federal agencies
- Increased reuse of FedRAMP packages and decreasing duplicative efforts across the federal government

Call To Action

What stakeholders can do to support and reinforce an automated FedRAMP:

CSPs & 3PAOs:

- Deliver security package deliverables in OSCAL.
- Provide ongoing ConMon submissions in OSCAL.
- Support the implementation of ConMon defect checks.

Agencies:

- Acquire new tools or work with existing tools to develop the capability to ingest and produce OSCAL packages.
- Use shared dashboard data to make data-based decisions, which will help determine the appropriate risk level needed to use the Cloud Service Offering in your agency.