



OSCAL Developer Data Bites

August 1, 2024

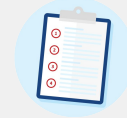


info@fedramp.gov
fedramp.gov

Purpose: To create space for dialogue between developers who use OSCAL and the FedRAMP® automation team.

Outcomes:

- Clarity around the FedRAMP Digital Authorization Package Pilot
- Productive discussion around OSCAL



Agenda:

- Welcome
- FedRAMP Automation PMO General Updates
- Pre-Submitted Q&A
- Digital Authorization Package Pilot Update
- Open Forum
- Next Steps & Closing



Keep the discussion respectful



Be curious, seek understanding



Speak from your own experience



Challenge through questions



Focus on ideas



Keep it technical

General Updates

August 1, 2024

FedRAMP New Automation Website

FedRAMP has released a new hub for technical documentation and guidance on digital authorization packages

- See the [FedRAMP Announcement \(7/11\)](#)
- See the site at <https://automate.fedramp.gov>

Local Validation Tooling

FedRAMP automation team is working on enhancing metaschema validation mechanisms in the OSCAL-CLI tool.

GitHub Issues

Prioritized the following:

- Issue #599 - completed HTML guides and automation website pre-release updates
- Issue #592 - Refactoring CI to use the OSCAL CLI
- Issue #598 - Setting up test harness and framework to automate testing of OSCAL CLI
- Issue #564 - Review of FedRAMP OSCAL extensions and values
- Issue #563 - Resolved profile catalogs are missing props

View the [project workboard](#) for more details on ongoing work and upcoming priorities

Review needed

<https://github.com/orgs/GSA/projects/25/views/7>

Pre-Submitted Questions

None received!

Reminder to submit questions/topic ideas via <https://forms.gle/M4pT7P2xyE6hRC7DA>

FedRAMP Roadmap

Digital Authorization Packages Pilot Update

Support machine-readable “**digital authorization packages**”

Our goals:

- **Provide Guidance:** Provide accurate, clear, and actionable guidance on producing an OSCAL-based SSP, focusing on common quality problem areas to increase overall quality of SSPs produced by CSPs
- **Provide Richer System Context:** Provide a means to support additional validations and completeness checks by describing the system context in a richer form, using OSCAL SSPs
- **Define Digital Authorization Package Composition:** Gain an understanding of the critical components that need to be supported in digital authorization packages
- **Review Standardization:** Provide a (documented) list of validations that must be checked prior to SSP submission, setting FedRAMP expectations for digital authorization packages
- **Automate Validation Checks:** Reduce review timeframes and improve consistency by automating certain validations, which reduces human effort and detects issues earlier in the process

What is the scope of the pilot?



The pilot will focus on maturing guidance and validations to establish a baseline of requirements for FedRAMP SP 800-53 rev5 based system security plans

FedRAMP Automation OSCAL Team

- Implement SSP-related constraints and validations
- Develop automated unit tests for each constraint
- Update [documentation](#) as-needed for each constraint
- Auto-generated constraints documentation (e.g., all allowed-values)

Pilot Partners (CSPs and Agencies)

- Use FedRAMP's external constraints to validate OSCAL SSPs
- Provide feedback on automated validations
- Provide input on opportunities for new validations

Note: The pilot will not focus on agency use of cloud services. This will be covered in future pilots.

Work collaboratively with OSCAL community on establishing the foundation for creating
“digital authorization packages”

Our strategy:

- Focus on the OSCAL-based (rev 5) SSP as the essential component of digital authorization package:
 - SSP front-matter
 - Appendix A - FedRAMP Security Controls
 - Appendix E - Digital Identity
 - Appendix J - CIS/CRM
 - Appendix K - FIPS 199
 - Appendix M - Integrated Inventory
 - Appendix Q - Cryptographic Modules
 - Section 11 - Separation of Duties
- Initial focus on most common SSP deficiencies that lead to review delays

The pilot will work through SSP validations in a **phased, iterative** approach.

Phase I - Foundational Data

- Metadata
- Back-Matter (including non-machine readable SSP attachments)
- Import-Profile
- System Characteristics
- System Implementation

Phase II - Control Implementation Data

- Single Component Responses (e.g., “This System”)
- Multi-Component Responses

Phase III - Leveraged Authorization Data

- Implementation Reuse
- Responsibilities

Voluntary participation by any CSP and Agency

- Must have / be able to produce OSCAL SSP(s) based on real-world data
- Must attempt to use available documentation at <https://automate.fedramp.gov/documentation> to guide OSCAL SSP development efforts
- Must use OSCAL-CLI to exercise FedRAMP external constraints on OSCAL SSPs
- Must be willing to run validation tool and provide feedback (e.g., identified issues, unclear documentation, desired enhancements, etc.)
- Must be willing to post issues and contribute to discussions on GitHub

FedRAMP will collaborate with pilot partners

- Validation Tooling - Provide builds based on oscal-cli that will include FedRAMP validations.
- GitHub Issues - Issue discussion and resolution will be managed through GitHub for the benefit of the community.
- Office Hours - FedRAMP will host office hour sign-ups, for direct “one-on-one” discussions, troubleshooting, etc., with pilot partners. Office hour time-blocks will be available weekly beginning in mid-August 2024.

Support machine-readable “**digital authorization packages**”

Our tentative timeline:

- **Pre-Pilot Work (August)**
 - Launch automate.fedramp.gov
 - Tool bootstrapping
 - Address technical debt
 - Publish pilot details
- **Pilot Execution Sprints (August)**
 - Each sprint will focus on prioritized 1-2 primary areas of work
- **Initial MVP (September)**
 - Significant guide improvements (SSP focused)
 - Initial validation MVP releases (SSP focused)
 - Website updates
- **Continued Refinement (December)**
 - Additional releases

- FedRAMP OSCAL automation team will track:
 - The burn-down rate on its issue backlog of SSP related validations
 - The burn-down rate on its issue backlog of SSP related documentation issues
- Obtain feedback from CSPs on their ability to produce OSCAL-based FedRAMP SSPs that pass validation
- Obtain feedback from Agencies on their ability to validate received OSCAL-based FedRAMP SSPs

Open Forum

Thank you

Our next Developer Data Bites virtual meeting will be on

Thursday, August 22, 2024 at 12p ET.

Submit questions and future discussion topics to OSCAL@fedramp.gov

Learn more at fedramp.gov



@FEDRAMP

Collaborating with FedRAMP

FedRAMP Automation GitHub: <https://github.com/GSA/fedramp-automation>

- Open Issues: <https://github.com/GSA/fedramp-automation/issues>
- Open Pull Requests: <https://github.com/GSA/fedramp-automation/pulls>
- Active Work: <https://github.com/orgs/GSA/projects/25/views/3>
- Community Review Needed: <https://github.com/orgs/GSA/projects/25/views/7>

GitHub Resources:

- Issues: <https://docs.github.com/en/issues>
- Pull Requests: <https://docs.github.com/en/pull-requests>

Ensuring your outstanding issues or questions are received:

Issues can be submitted in several ways:



Preferred

Open an issue on fedramp-automation github so that it will benefit the NIST/FedRAMP community.

<https://github.com/GSA/fedramp-automation/issues>

Alternate

Email us at oscal@fedramp.gov

NIST:

<https://pages.nist.gov/OSCAL/>

Learning Resources: <https://pages.nist.gov/OSCAL/learn/>

Current release: <https://github.com/usnistgov/OSCAL/releases>

Development version: <https://github.com/usnistgov/OSCAL/tree/develop>

Content repo: <https://github.com/usnistgov/oscal-content>

FedRAMP:

Current repo: <https://github.com/GSA/fedramp-automation>

Current issues: <https://github.com/GSA/fedramp-automation/issues>

Validations work: <https://github.com/18F/fedramp-automation/tree/master/src/validations>

Web based validation tool:

<https://federalist-2372d2fd-fc94-42fe-bcc7-a8af4f664a51.app.cloud.gov/site/18f/fedramp-automation/#/documents/system-security-plan>