FedRAMP

FedRAMP OSCAL Implementers

August 14, 2024

GSA

info@fedramp.gov
fedramp.gov

Introduction

Purpose: To engage Cloud Service Providers, 3PAOs, tool vendors and other participants in FedRAMP's OSCAL Implementers activities.

Outcomes:

- Shared understanding of current OSCAL issues
- Alignment on progress toward digital authorization pilot

Agenda:

- Welcome
- OSCAL Implementers General Updates
- Digital Authorization Package Pilot Review & Updates
- Open Forum
- Next Steps & Closing

FedRAMP Guiding Principles

Keep the discussion respectful

Be curious, seek understanding

Speak from your own experience

Challenge through questions

Focus on ideas

Keep it technical

OSCAL Implementers Changes

Purpose

- To align the structure and cadence of the OSCAL Implementers meetings to support our digital authorization package pilot

Changes Made

- Increase the frequency of these meetings from biweekly to weekly
- Change the meeting name to OSCAL Implementers

Coming Changes

- Expand the audience of OSCAL Implementers through the use of a public sign-up form

Outcomes

- Increased engagement with the OSCAL community while we launch the pilot
- Clarity on actions, responsibilities, progress, and achievements as we work through the pilot

General Updates

FedRAMP Automation Community Updates

August 14, 2024

Local Validation Tooling

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

- New version available
- Building out FedRAMP external constraints and unit tests for OSCAL CLI
  - Track latest progress in PR#622

GitHub Issues

Prioritized the following:

- 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

FedRAMP Roadmap

Digital Authorization Packages Pilot Update

Automation and technology- forward operations

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

Our goals:

- **Define Digital Authorization Package Composition:** Gain an understanding of the critical components that need to be supported in digital authorization packages.
- **Provide Guidance:** Provide accurate, clear, and actionable guidance on producing an OSCAL-based SSP. Increase increase overall quality of SSPs produced by CSPs and OSCAL tools by addressing common issues.
- **Provide Richer System Context:** Ensure richer system context through additional validations and completeness checks over OSCAL SSPs.
- **Stabilize Validations:** 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, Tool Providers, 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.

Establishing machine-readable “digital authorization packages”

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

How will the pilot be executed? (cont'd)

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

How will the pilot be executed?

Voluntary participation by any CSP, Tool Provider, 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.

Automation and technology- forward operations

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

Our *tentative* timeline:

- **Pre-Pilot Work (August)**
  - Launch automate.fedramp.gov (completed)
  - Tool bootstrapping (in progress)
  - Address technical debt (in progress)
  - Publish pilot details (in progress)
- **Pilot Execution Sprints**
  - 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 (Ongoing)**
  - Additional releases

Monitoring Progress

- 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 and tool providers 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 Implementers virtual meeting will be on

Wednesday, August 21, 2024 at 12p ET.

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

Learn more at fedramp.gov

@FEDRAMP

How to Submit Issues with FedRAMP

Ensuring your outstanding issues or questions are received:

Issues can be submitted in several ways:

Preferred	Alternate
Open an issue on fedramp-automation github so that it will benefit the NIST/FedRAMP community. **https://github.com/GSA/fedramp-automation/issues**	Email us at **oscal@fedramp.gov**

Collaboration Resources

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

OSCAL Resources

NIST:

OSCAL repo: 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
Early Adopter repo: https://github.com/GSA/fedramp-oscal-earlyadopters