OSCAL Developer Data Bytes

September 26, 2024

info@fedramp.gov

fedramp.gov

Introduction

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

Outcomes:

- Shared understanding of how the FedRAMP Automation team plans to use future Data Bytes meetings and topics we plan to cover

- Clarity around the roadmap for the digital authorization package pilot

- Productive discussion around OSCAL

Agenda:
- Welcome
- FedRAMP Automation PMO General Updates
- Pre-Submitted Q&A
- Survey Results Analysis and Discussion
- Digital Authorization Package Pilot Update
- Open Forum
- Next Steps & Closing

Data Bytes Guiding Principles

Keep the discussion respectful

Be curious, seek understanding

Speak from your own experience

Challenge through questions

Focus on ideas

Keep it technical

General Updates

FedRAMP Automation Community Updates

Digital Authorization Package Pilot

Ongoing and planned activities include:

Pilot Participants

- Finish setup local validation tooling in their environments
- Begin validating their SSPs with the local validation tooling
- Asking for help / reporting problems
- Schedule Office Hours

FedRAMP OSCAL Automation Team

- Continue building out FedRAMP external constraints
- Continued updates to documentation
- Continued updates to the OSCAL-CLI (https://github.com/metaschema-framework/oscal-cli/releases)

GitHub Issues

Ongoing:

- Issue #653 - Technical walkthroughs of FedRAMP Automation Tools (epic)
- Issue #657 - SSP Metadata constraints (epic)
- Issue #658 - SSP Back-Matter constraints (epic)
- Issue #661 - SSP System Characteristics constraints (epic)
- Issues #57, 44, 55 - documentation updates on automate.fedramp.gov
- Issue #603 - OSCAL CLI and External Constraints Improvements

View the project workboard for more details on ongoing work and upcoming priorities (https://github.com/orgs/GSA/projects/25/views/3)

Pre-Submitted Questions

Pre-Submitted Questions

Question 1 - Can we cover updates / deadlines for the various OSCAL-related activities from M-24-15, Modernizing the Federal Risk and Authorization Management Program?

We have discussed the FedRAMP roadmap and strategic goals for 2024-2025 in prior Data Bytes sessions, but we will provide periodic updates about ongoing and planned OSCAL related activities aligned to M-24-15.

Community members are encouraged to review M-24-15 - https://www.whitehouse.gov/wp-content/uploads/2024/07/M-24-15-Modernizing-the-Federal-Risk-and-Authorization-Management-Program.pdf

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

Topic Survey Results

Community Topics of Interest - Survey Results

Category	Topic	Timeframe	% Requested
Authorization	NIST OSCAL vs FedRAMP Namespace collisions	Near-term	31%
Authorization	Release and Versioning Strategy	Near-term	14%
Authorization	Guidance on printable documents for CSPs that have migrated to OSCAL	Mid-term	34%
Authorization	Workflows for OSCAL to Word SSPs (and other documents)	Mid-term	55%
ConMon	OSCAL in Continuous Monitoring	Long-term	72%
ConMon	POA&M Management	Long-term	59%
ConMon	SBOM & Vulnerability sharing with upstream/downstream managers	Long-term	38%

Plans for Future Data Bytes

- Provide FedRAMP automation roadmap updates periodically:

  - ☐ Digital Authorization Package pilot outcomes

  - ☐ Upcoming features and improvements

  - ☐ Planned milestones and releases

- Stakeholder input and feedback on releases

- Address topics of interest as we progress from authorization to continuous monitoring

Digital Authorization Package Pilot Update

FR

Pilot Participant Expectations

- Must be able to manually or automatically produce OSCAL SSP(s) based on real-world data
- Must 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.), including posting issues and contributing to discussions on GitHub

**See details on how to participate at** https://www.fedramp.gov/digital-authorization-package-pilot/

Digital Authorization Package Pilot

FR

Validation Tooling

- FedRAMP is prioritizing development of automated validation tooling in a phased / iterative manner:
  - ☐   Prepare your system
  - ☐   Implement and document your system
  - ☐   Contextualize your system

Digital Authorization Package Pilot

FedRAMP is prioritizing development of automated validation tooling in a phased / iterative manner

PHASE 1

Prepare Your System

PHASE 2

Implement and Document Your System

PHASE 3

Contextualize Your System

Digital Authorization Package Pilot

FR
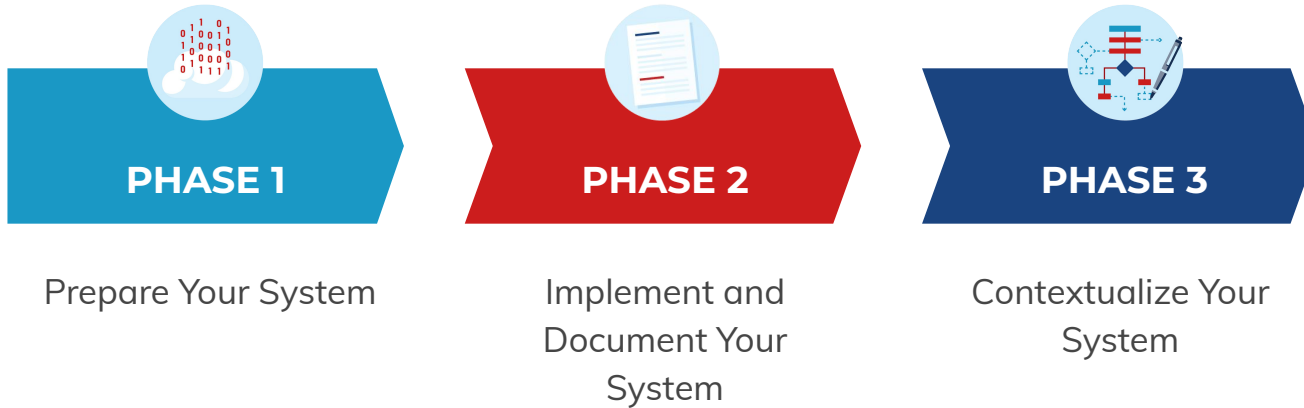
Near-Term

- ✓ Containerized tools
- ✓ Installation of tools
- ✓ **Asking for help / reporting problems**
- ❏ Writing your own OSCAL documents
- ❏ Using the tooling with OSCAL SSPs
- ❏ Interpreting validation results
- ❏ Configuring the tooling and constraints

Longer-Term

- ❏ Using the tooling with POA&Ms
- ❏ Using the tooling with SAP & SAR
- ❏ Advanced features

See details of planned walkthroughs - https://github.com/GSA/fedramp-automation/issues/653

Open Forum

Thank you

Our next Developer Data Bytes virtual meeting will be on

Thursday, October 24, 2024 at 12p ET.

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

Learn more at **fedramp.gov**

@FEDRAMP

Collaborating with FedRAMP

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

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**

OSCAL Resources

FR

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