FedRAMP

OSCAL Developer Data Bytes

October 24, 2024

GSA

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 our OSCAL Validation Development Priorities & Roadmap
- Productive discussion around OSCAL

Agenda:

- Welcome
- FedRAMP Automation PMO General Updates
- Pre-Submitted Q&A
- FedRAMP OSCAL Validation Development Priorities & Roadmap
- 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

Digital Authorization Package Pilot

This week, 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)

FedRAMP Automation Community Updates

October 24, 2024

- Documentation Site Updates
  - PR #91- Security sensitivity level
  - PR #85 - Primary / alternate processing locations
  - Issue #82 - Fix namespaces for system identifier type and other namespace values
  - Issue #57 - Responsible party is person
  - PR #56 - System characteristics

- Constraints Updates
  - PR #800 - FedRAMP extension “fedramp-version” prop
  - PR #796 - Fix by-component implemented-requirement checks
  - PR #795 - Updates to “data-center” constraint unit test
  - PR #792 - Add “help-url” to all constraints

GitHub Issues

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 - Are there any authorized tools CSPs could use to manage the conversion of Word/text based documents to OSCAL/XML format?

There are many commercial and open-source tools that can help CSPs create OSCAL documents. FedRAMP cannot attest to whether these tools can "convert" Word/text-based documents to OSCAL.   CSPs must determine which solutions are viable for their particular situation.

Pre-Submitted Questions

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

FedRAMP OSCAL Validation Development Priorities & Roadmap

FedRAMP OSCAL Validation Goals

Provide a means to **validate FedRAMP OSCAL packages before submission** to FedRAMP for **completeness**, **accuracy**, and to ensure the package is **free of errors**.

Our goals:

- Define fully how to use OSCAL to represent a FedRAMP package.
- Help creators of OSCAL packages ensure all OSCAL and FedRAMP specific requirements are met.
  - **Completeness:** Ensure that required content is provided.
  - **Consistency:** Normalize package data to **enable machine analysis**.
  - **Free from Error:** Find common data errors (e.g., broken cross-references, invalid/nonsensical values) before submission.
- Increase consumer confidence in FedRAMP OSCAL packages to improve the consumer experience and reduce review times.

Digital Authorization Package Pilot

The pilot focuses on maturing guidance and automation by establishing an initial set of validation checks for FedRAMP SP 800-53 rev5 based packages, starting with the SSP

FedRAMP Automation Team

- Plan, develop and publish:
  - □ validation mechanisms (constraints)
  - □ example OSCAL content
  - □ automated unit tests
  - □ documentation https://automate.fedramp.gov/documentation/

Pilot Partners (CSPs, Tool Developers, and Agencies)

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

Note: The pilot focuses on CSP-developed artifacts. Agency use of cloud services will be covered in future pilots.

Our Prioritization Philosophy

Prioritization Principles:

- Simple constraints over complex
- Prioritizing higher value, lower effort constraints first
- Focus on items that apply to all impact levels (H/M/L)

Deliver Incremental Value via Themed Collections of Constraints:

- Theme 1: Completeness Checks
- Theme 2: Data and Referential Integrity Checks
- Theme 3: Reviewer Automation

High-Level Development Roadmap

Now

Next

Later

Completeness Checks

Ensure the presence of required content and attachments within the package submission.

Focus on fields that are optional in the OSCAL core syntax, but required for FedRAMP submissions.

Enforcement of FedRAMP allowed values where applicable.

Integrity Checks

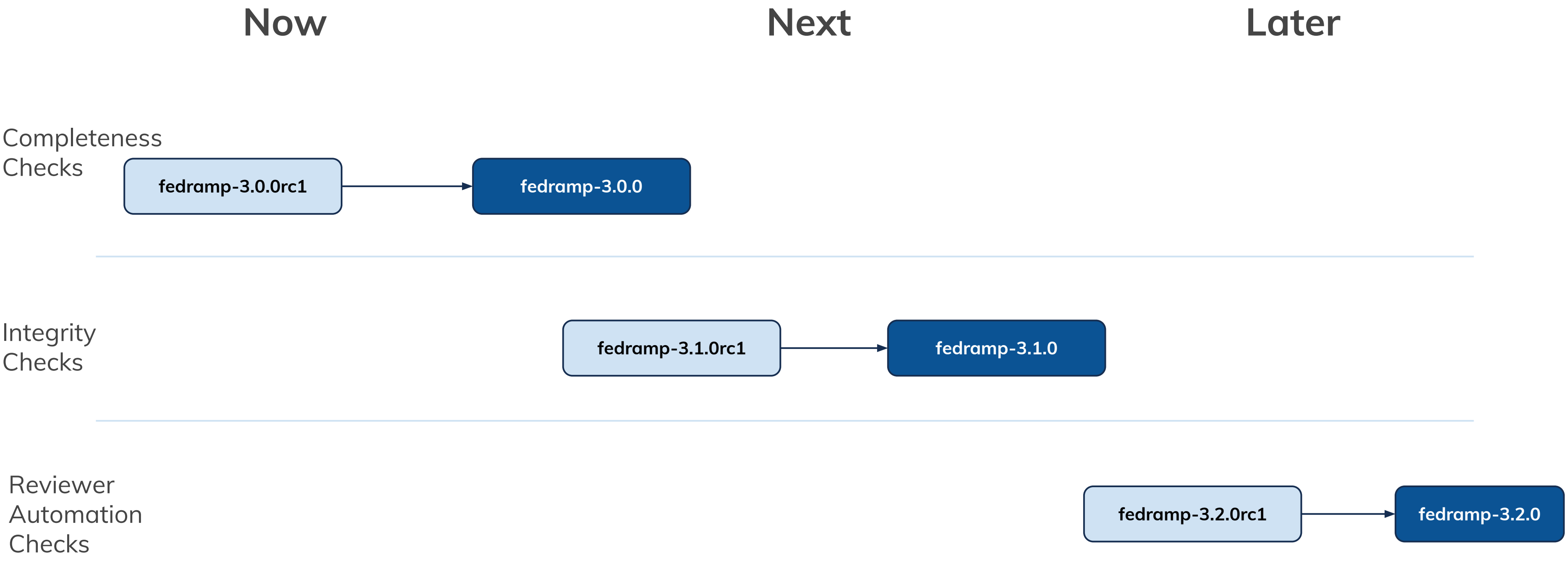
Focus on data correlation and consistency checks within the OSCAL content, similar to database referential integrity checks.

This includes both inter- and intra-document cross-references.

Reviewer Automation

Advanced and complex digital package quality checks to that support decision-makers in understanding the CSO’s risk posture.

Release Plan



Now

Next

Later

Completeness Checks

fedramp-3.0.0rc1

fedramp-3.0.0

Integrity Checks

fedramp-3.1.0rc1

fedramp-3.1.0

Reviewer Automation Checks

fedramp-3.2.0rc1

fedramp-3.2.0

Open Forum

Thank you

Our next Developer Data Bytes virtual meeting will be on

Thursday, November 21, 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

How to Submit Issues with FedRAMP

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

OSCAL Resources

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