FedRAMP

FedRAMP OSCAL Early Adopters

October 11th, 2023

GSA

info@fedramp.gov
fedramp.gov

Introduction

Purpose: Ongoing weekly meeting to engage Cloud Service Providers, 3PAOs, tool vendors and other participants in FedRAMP's OSCAL Early Adopters Work Group (OEAW) activities.

Outcomes:

- Shared understanding of Charter and Mission of the Workgroup
- Shared understanding of program participation requirements and initial registration process.
- Shared understanding of repository package requirements (compressed files) and discussion or possible enhancements and solutions.

Agenda:

- Welcome
- Guiding Principles/Mission Review
- Participation Requirements
- OEAW Updates
- Issues Discussion
- Compressed File Submisisons
- Open Forum
- Next Steps & Closing

FedRAMP OEAW Guiding Principles

Keep the discussion respectful

Be curious, seek understanding

Speak from your own experience

Challenge through questions

Focus on ideas

Keep it technical

OEAW Workgroup Charter/Mission

Charter:

To create an engagement space for Cloud Service Providers, 3PAOs, tool developers and others who are adopting OSCAL for the FedRAMP® use case with the goal of refinement of FedRAMP automation technology and processes.

Mission Elements:

- Bring OSCAL early adopters together to foster community engagement for FedRAMP OSCAL use case.
- Provide bi-directional dialogue with participants on engineering process current and future state.
- Refinement of initial technology and processes for the FedRAMP OSCAL automation ecosystem.
- Testing of initial releases of FedRAMP Automation Portal and RESTful API services.

FedRAMP OEAW Updates

October 11th, 2023

- **Release 2.3** in testing environment will close multiple github tickets. Delay in rolling out due to some enhancements and issues identified during testing.
- A word about versions of tools and schemas in REST APIs:
  - NIST Core Validations using OSCAL-CLI 3.4
  - Rev 4/Rev 5 through portal is at OSCAL 1.1.1 will be part of this 2.3 release
  - Schema pathing on NIST OSCAL site will change with 2.3 (should be using).
    - https://github.com/usnistgov/OSCAL/releases
    - Automation Team will continue to work on transition from OSCAL 1.0.4 to 1.1.1 this coming week.
  - Release 2.3.0 will include consolidated calls for validations (one for NIST and one for FedRAMP schematron (See Demo). Will also include fixes for OSCAL NIST vs. FedRAMP use case issues with Schematron validations (See github tickets for more detail). Also will include swagger documentation inclusion into REST API calls for OEAW review.

FedRAMP OEAW Issue Submission

October 11th, 2023

The working group will have the following options when identifying and submitting issues related to the Portal and RESTful API services:

- Submission of general questions will be done via sending and email to oscal@fedramp.gov.
- Submission of suggestions for process and software improvement can be done via submission form built into the portal or by sending an email to oscal@fedramp.gov.
- Submission of bug reports will be done through the issue to the FedRAMP OSCAL Early Adopters repository (https://github.com/vitg-gsa-automation/earlyadopters) or sending an email with screen snapshots to devops@volpegroup.com
  - ? Once the developers review the bug report they will initiate next steps with submitter.
  - ? All bug reports will be tagged as FedRAMP automation Portal or REST API issues in the early adopters repository.

FedRAMP OEAW Issue Submission

October 11th, 2023

Current open Issues on Early Adopters GitHub (Portal 2.2.1)

- **(#7) Minified XML behaves differently than “pretty” printed XML (in process)**
- **(#12) Rule 55b. One or more responsible parties must be defined for each role (in process)**
- **(#16) import-profile directive with a URL does not resolve. (for discussion)**
- **(#17) [Feature Request]: A prop in the back matter for the uuid of the imported document (need to consider long term implications)**
- **(#18) [Feature Request]: Enable deletion of uploaded documents via the portal (for discussion)**

FedRAMP OEAW Phases Overview

Initial Phases

- Phase 1 Validation Testing
- Phase 2 General Artifact Submission
- Phase 3 Document and Artifact Management
- Phase 4 Process Improvement and New Functionality

Issues Discussion

FedRAMP-Automation Issue Submission

October 11th, 2023

Some important issues opened on fedramp-automation

- **(#511) SAP Appendix A Assessment procedures inconsistent with OSCAL**

  ? The assessment procedure naming convention does not align with the FedRAMP baseline profile, or the OSCAL NIST catalog. We are aware of the issue. The TCW was created by a 3PAO for the Rev 4 and Rev 5 release and there are discrepancies. On next update to profiles and resolved-profile-catalogs for response points and Core controls we will get this resolved.

- **(#512) SAP Appendix A Test Method (G) does not align with OSCAL**

  ? OSCAL resolved baseline catalog does not identify the specific methods required per objective. However, these are defined in the SAP Appendix A, and do not align with the overall assignments of the test methods allocated by NIST. Similar to #511 above, will be resolved in next profile and resolved-profile and templates push to github fedramp-automation.

FedRAMP OEAW Validations/Enhancement Discussions

October 11th, 2023

Current open Issues on Early Adopters GitHub (Portal 2.2.1)

- **(#16) import-profile directive with a URL does not resolve. (for discussion)**

  - ? **Known documentation issue:** Per Guide to OSCAL-based FedRAMP System Security Plans (Section 3.2.1) the import-profile must reference a resolved-profile-catalog document in FedRAMP. We recognize that the language in section 3.5 of same document is contradictatory and will be addressed in a subsequent document update.

  - ? Current Schematron ruleset checks for resolved-profile-catalog specifically.

- **(#17) [Feature Request]: A prop in the back matter for the uuid of the imported document (need to consider long term implications)**

  - ? The automation team has reviewed this request and we will be willing to accepting the props as optional in the backmatter resource. We would be targeting release 2.4 of REST API to implement note: Pending discussion with OEAW workgroup on 10/11 meeting to delve into side effects and potential downstream implications of these props. Also will need to discuss the Schematron rules associated with the props as optional.

- **(#18) [Feature Request]: Enable deletion of uploaded documents via the portal (for discussion)**

  - ? Per original PMO discussions, there would be no actual document deletions once an artifact has been uploaded to the ecosystem. However, we can implement a “delete” option that simply hides the artifacts from view? Would this be sufficient?

Repository Discussion

FedRAMP OEAW Repository Discussion

Resolutions on compressed files

- Upload/Download of individual OSCAL artifacts and associated documents supported in compressed files. OSCAL documents will be uploaded to the root of the compressed file.
- Upload/Download of compressed packages and artifacts will be supported with the following assumptions:
  1. All rlinks included in the OSCAL documents will need to resolve to the directory structure as represented in the document. i.e. if subfolders are used, then the extracted artifact must exist in that subfolder.
  2. File size limit will still be 100 MB (as is with OMB Max) for upload through the REST APIs.
  3. Interim transition for PMO package review is moving to USDA service until FedRAMP can fully stand up the automation ecosystem.
- Submission of OSCAL SSP, SAP, SAR and POAM as single combined artifact will not be supported for the foreseeable future.

Open Forum

Next Steps

Thank you

Our next OEAW virtual meeting will be on

Weds October 25th, 2023 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**

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