



FedRAMP OSCAL Early Adopters

October 11th, 2023



info@fedramp.gov
fedramp.gov

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 Submissions
- 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

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.

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.

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 an 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.

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)

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

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.

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 contradictory 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

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









Basic ATO Package Requirements

- ❑ Support for multiple access to package artifacts.
- ❑ Must support role based access.
- ❑ Support for grouping of documents and artifacts stored in repository.
- ❑ Support for verifying compliance with required artifacts for FedRAMP authorization processes (i.e. package checklist).
- ❑ Optional submission of OSCAL SSP, SAP, SAR and POAM as single artifact?

```
<?xml version="1.0" encoding="UTF-8"?>
<submission-wrapper>
  <system-security-plan>
    ...
  </system-security-plan>
  <assessment-plan>
    ...
  </assessment-plan>
  <assessment-results>
    ...
  </assessment-results>
  <plan-of-action-and-milestones>
    ..
  </plan-of-action-and-milestones>
</submission-wrapper>
```










Compressed Package Submission Example (zip)

MajorSystemBoundarySubmission 8 items

Name	Last modified	File size
 publishedDocs	-	37 MB
 resources	-	493 KB
 .DS_Store	Jul 28, 2023	6 KB
 FedRAMP - Major System Boundary-FedRAMP_Assessment_Result.jso...	Jul 28, 2023	170 KB
 FedRAMP - Major-System-Boundary_SSP-export_20230724.xml	Jul 26, 2023	722 KB
 FedRAMP - Major_System_Boundary-FedRAMP_Plan_of_Action_and_...	Jul 26, 2023	258 KB
 FedRAMP - Major_System_Boundary-SAP.json	Jul 28, 2023	192 KB
 FedRAMP_rev4_HIGH-baseline_profile.xml	Jul 26, 2023	123 KB





Compressed Package Submission Example (cont.) (zip)

< publishedDocs 33 items

Name	Last modified	File size
 AC Procedures Document.doc	Jul 26, 2023	105 KB
 AT Procedures Document.doc	Jul 26, 2023	1 MB
 AU Procedures Document.doc	Jul 26, 2023	1 MB
 CA Procedures Document.doc	Jul 26, 2023	1 MB
 CM Procedures Document.doc	Jul 26, 2023	1 MB
 CP Procedures Document.doc	Jul 26, 2023	1 MB
 FedRAMP Annual SAP.pdf	Jul 26, 2023	185 KB
 FedRAMP Continuous Monitoring Plan.xlsx	Jul 26, 2023	20 KB
 FedRAMP Initial Authorization Package Checklist.xlsx	Jul 26, 2023	37 KB

Compressed Package Submission Example (cont.) (zip)

< resources 4 items

	Name	Last modified	File size
	AC Procedures Document.doc	Jul 26, 2023	105 KB
	Annotation 2023-07-19 113729.png	Jul 26, 2023	138 KB
	FedRAMP-OSCAL-SSP-Diagram-1024x525.png	Jul 26, 2023	138 KB
	image-5.png	Jul 26, 2023	112 KB

Compressed Package Submissions for HIGH (from PMO)

Agency ATO MAX.gov & High Repository Folder Structure
(*CSP NAME* may be omitted for High repo structures outside of MAX.gov)

"CSP NAME" Archive

"CSP NAME" ATO Letters

"CSP NAME" Continuous Monitoring

- "CSP NAME" Annual Assessments
 - "CSP NAME" AA 20XX
 - "CSP NAME" AA 20XX – POA&M
 - "CSP NAME" AA 20XX - SAP
 - "CSP NAME" AA 20XX - SAR
 - "CSP NAME" AA 20XX - SSP
 - "CSP NAME" AA 20XX – SSP Attachments
- "CSP NAME" Incident Information & Forms
- "CSP NAME" POA&M & Inventory
 - "CSP NAME" Deviation Requests
- "CSP NAME" Significant Changes
- "CSP NAME" Vulnerability Scans
 - "CSP NAME" DB Scans
 - "CSP NAME" OS Scans
 - "CSP NAME" Web Scans

"CSP NAME" Initial ATO Assessment

- "CSP NAME" POA&M
- "CSP NAME" SAP
- "CSP NAME" SAR
- "CSP NAME" SSP
- "CSP NAME" SSP Attachments

Validation Testing

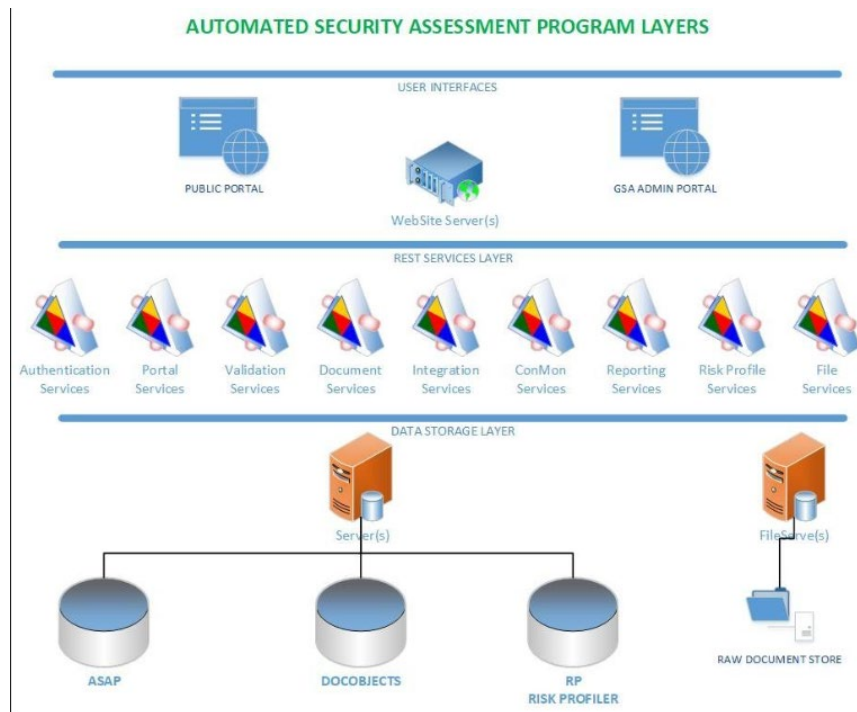
Phase 1

- ❑ Duration: 4-6 weeks (planned).
- ❑ Submission of OSCAL Rev 4 Artifacts (XML Only).
- ❑ Provided via Portal Access only.
- ❑ Refinement of current Schematron ruleset for validations based on feedback from participants.
- ❑ Expansion of Validation of OSCAL Artifacts for other formats (e.g. JSON, YAML).
- ❑ Finalize Rev 4 FedRAMP validation ruleset modifications and migrate to rev 5.
- ❑ Limit of 2GB per XML artifact.
- ❑ Initiate access to RESTful API services for validation testing (optional).

OVERVIEW

REST API Service Ports

- **Authentication Services: port 8080**
- Portal Services: port 8081
- **Validation Services: port 8082**
- Document Services: port 8083
- Integration Services: port 8084
- ConMon Services: port 8085
- Reporting Services: port 8086
- Risk Profile Services: port 8087
- **File Services: port 8088**

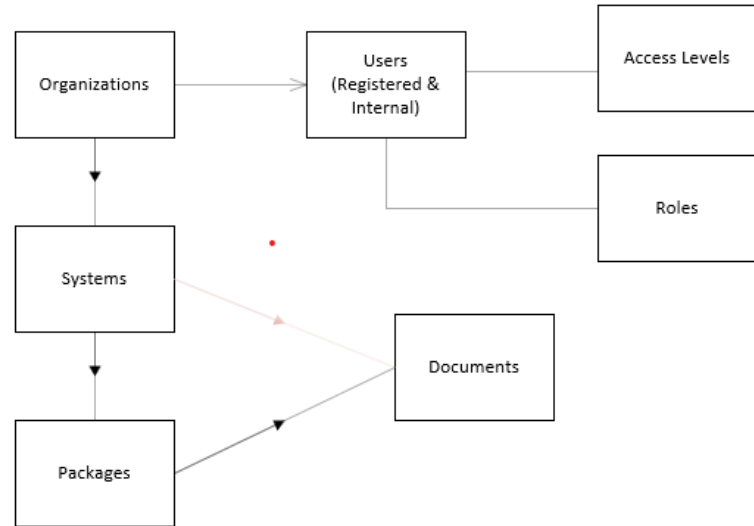


Demo Overview

Authentication
Services

File Upload
Services

Validation Services



Resources

<https://github.com/vitg-gsa-automation/earlyadopters/blob/main/presentations/materials/FR-REST-API-Type-Lists.xlsx>

<https://github.com/vitg-gsa-automation/earlyadopters/blob/main/presentations/materials/WebAPI%20Documentation.pdf>

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>

OEAW Phases



General Artifact Submission

Phase 2:

- ❑ Duration: 4-5 weeks (planned)
- ❑ Submission of non-OSCAL legacy package artifacts.
- ❑ Provided via Portal Access only.
- ❑ Refinement of Authorization Package submission process.
- ❑ Initial design of intra-artifact submission processes (e.g. leveraged authorizations)
- ❑ Access to RESTful API services for validation testing (optional)
- ❑ Review and update of RESTful API services documentation.

Document and Artifact Management

Phase 3:

- ❑ Duration: 2-4 weeks (planned)
- ❑ Organization, System and Package structure.
- ❑ Provided via portal access only.
- ❑ Versioning and ATO package relationships
 - ❑ Legacy
 - ❑ Leveraged Authorizations
 - ❑ UUID management
- ❑ Access to RESTful API services for validation testing (optional)

Process Improvement and New Functionality

Phase 4:

- ❑ Duration: TBD (ongoing)
- ❑ Adoption Challenges and Solutions for FedRAMP use case.
- ❑ Challenges with NIST OSCAL Core and potential future updates and model changes.
- ❑ Authorization vs. Automation.
- ❑ Re-visit FedRAMP validations.

July 26, 2023

1. Whitelisting of IPs to gain access to portal and RESTful API services.
 - Send email to oscal@fedramp.gov with IPs to be whitelisted for access.
 - Limit of 2 per organization or an IP address range.
 - MFA is being utilized via SMS only. Provide a valid cell # for each organizational registrant.
 - Provide company/organization logo for portal (optional).
2. Once confirmed, a link to the FedRAMP Portal will be automatically sent to registrant for site access for Phase 1.
 - Register within 5 days of receiving invitation email.
 - Login to Portal to confirm organizational details and verify access.
 - Each participating organization will be provided with its own workspace in the portal. Documents will not be shared between participants unless otherwise agreed to
 - Each participating organization will be provided with a sample Authorization Package for testing validation and uploading of OSCAL artifacts.
3. **THIS IS A BETA TEST SITE – NO SENSITIVE DATA.**