FedRAMP OSCAL Early Adopters

September 13, 2023

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 and discussion or possible solutions.

Agenda:

- Welcome
- Guiding Principles/Mission Review
- Participation Requirements
- OEAW Updates
- ATO Package Requirements
- 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

- **Release 2.2.1** in testing environment addresses several minor github tickets. Will be installed on integration environment this upcoming weekend.

- A word about versions of tools and schemas in REST APIs:

  — NIST Core Validations using OSCAL-CLI 3.4

  — Rev 4 through portal is at OSCAL 1.0.4.

  — Schema pathing on NIST OSCAL site has changed (should be using).

    - https://github.com/usnistgov/OSCAL/releases/download/v1.0.4/oscal_complete_schema.xsd
    - https://github.com/usnistgov/OSCAL/releases/download/v1.0.4/oscal_ssp_schema.xsd

  — Automation Team will be starting to work on transition from OSCAL 1.0.4 to 1.1.0 this coming week.

  — Release 2.3.0 in progress.   Will include consolidated calls for validations (one for NIST and one for FedRAMP schematron. 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.

  —Shooting for Oct 1 release to OEAW of 2.3.0.

FedRAMP OEAW Issue Submission

Current open Issues on Early Adopters GitHub (Portal 2.2.1)

- **(#7) <u>Minified XML behaves differently than "pretty" printed XML</u> (In process)**

- **(#12) One or more responsible parties must be defined for each role. (in process).**

- **(#13) A component must have an allowed type. (in process – types will be added to fedramp_values.xml file)**

- **(#15) Every Asset Identifier must be unique (in process).**

- **(#16) import-profile directive with a URL does not resolve. (in process: will be addressed in phase 2 on file uploads)**

- **(#17) <u>[Feature Request]: A prop in the back matter for the uuid of the imported document</u> (under consideration – more research needed)**

- **(#18) <u>Fatal errors for associated documents in POAM Import</u> (in process).**

- **(#19) <u>SAP Conversion Failure (Status code 400)</u> (in process)**

- **(#20) <u>SAR - Schematron pointed to Assessment Plan</u> (closed – wrong file type selected)**

- **(#21) Swagger sites Failing to load (closed – refer to WebAPI documentation for details)**

FedRAMP OEAW Issue Submission

September 13th, 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.

Initial Phases

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

Repository Discussion

Basic Repository Requirements

- Upload/Download of individual OSCAL artifacts and associated documents.
- Support multiple file formats (see list).
- Support multiple document types (see list)
- Support for compressed files (file structure to be determined)
- Must be able to process and extract base64 encoded documents from OSCAL artifacts
- Must be able to upload individually and in compressed files associated supporting artifacts.
- Must allow quick retrieval of and processing of OSCAL data.
- Must support high speed querying of OSCAL data.
- Must support versioning of all uploaded artifacts.
- Must comply with NARA requirements.
- Must be a HIGH repository.

FedRAMP OEAW Repository Discussion

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
<?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>
```

Current Challenges

- ❑ Verifying package artifact contents.
- ❑ Alignment of artifacts with package submission requirements.
- ❑ Compressed files
  - ○ Which formats to support (gzip, zip, tar, other)
  - ○ Package structure (to be determined)
  - ○ Decompressing and aligning individual files with Document types.
  - ○ File size limitations?

FedRAMP OEAW Repository

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

FedRAMP OEAW Repository

Compressed Package Submission Example (cont.) (zip)

resources 4 items	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

Open Forum

Next Steps

Thank you

Our next OEAW virtual meeting will be on

Weds September 27th, 2023 at 12p ET.

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

Learn more at fedramp.gov

@FEDRAMP

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).

FedRAMP REST API Services

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**
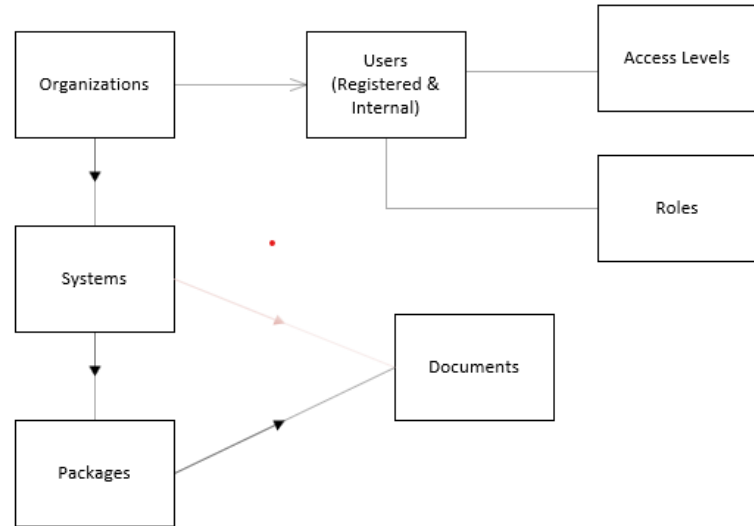

AUTOMATED SECURITY ASSESSMENT PROGRAM LAYERS
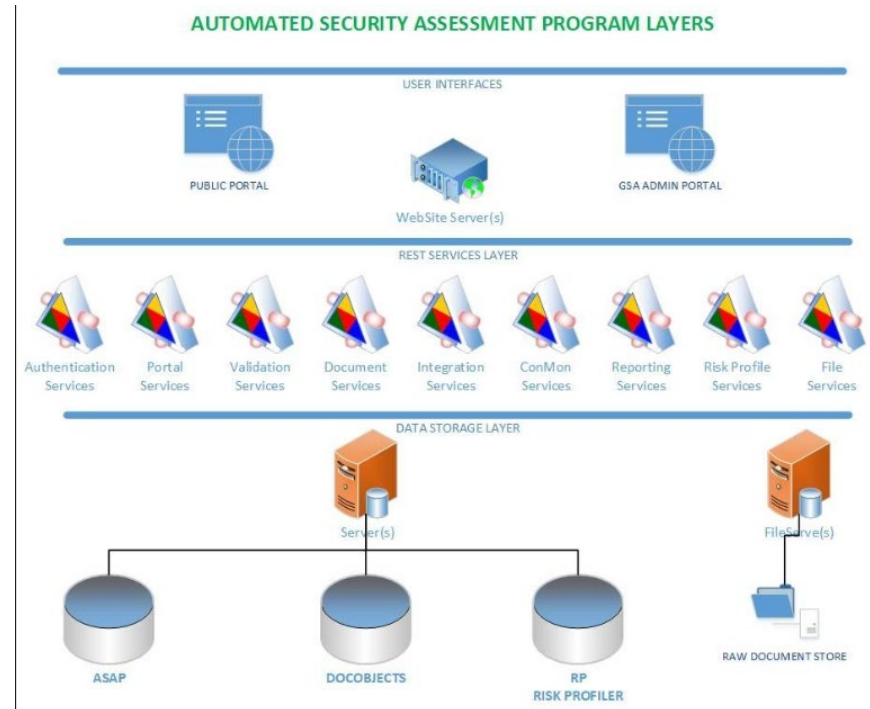
Demo Overview

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

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**

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.

FR

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)

FedRAMP OEAW Phase 4 Details

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.

FedRAMP OEAW Initial Registration Steps

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.**