



FedRAMP OSCAL Early Adopters

July 26, 2023

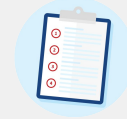


info@fedramp.gov
fedramp.gov

Purpose: Initial Kick Off 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.
- Provide an Overview of the phases of the Early Adopters program to the workgroup.



Agenda:

- Welcome
- Charter and Mission
- Team Introductions
- Participation Requirements
- Portal Demo
- Overview of Phases
- 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

Meet the FedRAMP Automation Development Team



William Krupinsky (Development Team Lead, “Magician”):

- Sr. Engineer/Architect, Full Stack Developer, Splunk Admin

Aaron Nolan (User Interface, “Hipster”):

- Sr. Software Engineer

Thomas Penna (REST API developer, Validations, “Lovable Bear”):

- Sr. Software Engineer, Full Stack Developer

Dimitri Zhurkin (Schematron Validations, “sch Master”):

- Sr. Software Engineer

Thomas Volpe Sr (FedRAMP Automation SME)

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 Participation Requirements



July 26, 2023

- Participants must show a willingness to share information, experiences and expertise among peers and potential competitors for the goal of improving and resolving current challenges. (Elephant in the room!)
- Participants must be willing to dedicate resources and time for the refinement of the FedRAMP automation ecosystem.
- Participants must adhere to the FedRAMP OEAW Guiding Principles.
- Participants must be willing to submit bug reports and help in the process improvement activities of the working group in a timely fashion.
- Participants must be willing to work with the FedRAMP automation ecosystem development team in a professional and expeditious manner to resolve identified issues.
- Participants agree to only upload non-sensitive data. (Must agree on portal each time they log in).
- Participants agree to participate in weekly meetings every Weds for the duration.

July 26, 2023

- ❖ We are beta testing the software of the FedRAMP automation ecosystem.
- ❖ Development of FedRAMP automation ecosystem ongoing.
- ❖ Current state of OSCAL and FedRAMP's OSCAL use case.
 - Rev 4 to Rev 5 transition
- ❖ Portal will only support XML submission during Phase 1 activities.
 - Expansion to other formats post Phase 1.
 - Required to use OSCAL CLI or Java base XSLT (from NIST) to convert other formats to XML prior to upload.

FedRAMP OEAW Initial Registration Steps



July 26, 2023

- ❖ 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 IPs per organization or an IP address range.
 - MFA is being utilized via SMS only. Provide a valid cell # for each registrant.
- ❖ 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.**
 - Optionally each participating organization can be provided with a sample Authorization Package (SSP, SAR, SAP, POAM) for testing validation and uploading of OSCAL artifacts but we prefer you use your own.
- ❖ **THIS IS A BETA TEST SITE – NO SENSITIVE DATA.**

July 26, 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.
 - **Whitelist volpegroup.com** domain on your spamwall or add to safe senders list.

Portal Demo



OEAW Phases

Initial Phases

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

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).

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 artifact submission (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.

Open Forum

Thank you

Our next OEAW virtual meeting will be on

Weds August 2nd, 2023 at 12p ET.

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

Learn more at **fedramp.gov**



@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>