

# FedRAMP OSCAL Early Adopters Workgroup Kick Off

---

**July 26, 2023**

## Meeting Details

**Purpose:** Kick off meeting for the participants of FedRAMP OSCAL Automation Early Adopters work group (by invitation only).

### 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

### [Slide Deck](#)

## Meeting Notes

- Volpe: Reviewed purpose and outcomes for the workgroup, guiding principles, and introduced the automation development team, and reviewed the workgroup charter/mission, requirements
- Aaron: Provided a demo of the FedRAMP OSCAL Authorization Portal
  - If you registered as part of the workgroup your organization will be listed in the drop down menu; recommend selecting registration type as access to both Portal and API
  - Phase 1 of workgroup will focus on Run Validations under OSCAL utilities
  - If reporting errors and bugs please include screenshots and thorough description of issue
- Participant Questions:
  - Greg Elin: Is a package shared in a particular format (like a zip file) or is a package just serially uploading multiple individual OSCAL files?
    - Volpe: Individual for the purpose of the workgroup. Only xml for phase I. Phase II will get into additional formats.
  - Valinder Mangat: What is the timeline for uploading on portal/rest api? What is the timeline for phase 1 and 2? What is the timeline for JSON via API upload, which is what will be needed for the demo/test
    - Volpe: Will be discussed on the next slides
  - Valinder Mangat: Can we delete files to keep our account tidy?

- Volpe: We don't delete anything, but will talk to the team as a future upgrade.
- Volpe: Reviewed details about Phase I Validation Testing
- Participant Questions:
  - Greg Elin: Will embedding attachments be a requirement or just an option?
    - Volpe: An option right now for phase I
  - Valinder Mangat: What is the timeline for JSON via API upload, which is what will be needed for the demo/test
    - Volpe: 4-5 weeks out based on Phase I.
  - Valinder Mangat: Can the UUID of the reference document be added in the back matter?
    - Volpe: I like this, please open a ticket and include it in the Early Adopter Repository. We can set it up to make it a warning instead of an error when running validations.

## PORTAL SCREENSHOTS

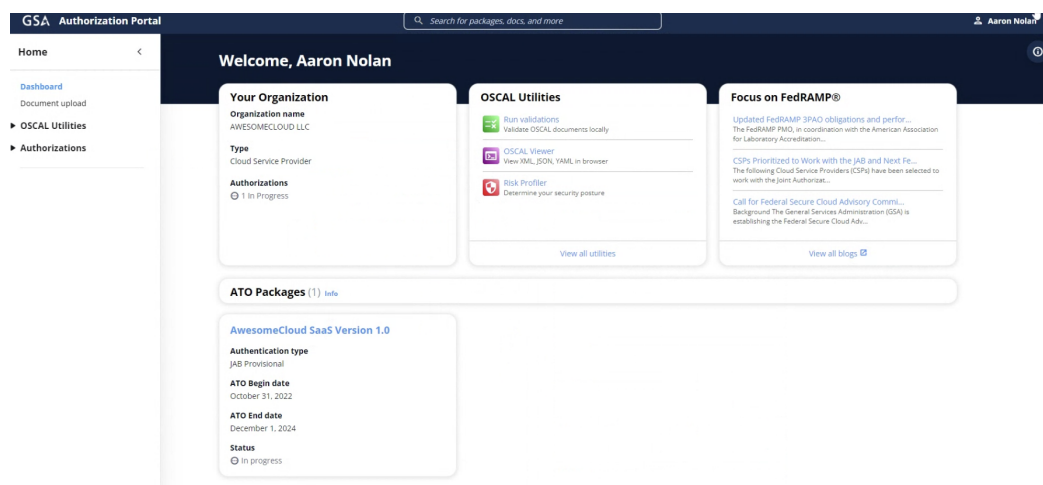


Figure 1: Home Page

The screenshot shows the 'Run Validations' page within the GSA Authorization Portal. The page has a dark blue header with the portal name and a search bar. A left sidebar lists 'OSCAL Utilities' with sub-links for 'Validations', 'OSCAL Viewer', and 'Risk Profiler'. The main content area features a blue banner with a warning about OASD Phase 1 OSCAL Rev 4 Artifact Validation. Below this, the 'Validations' section includes a sub-header and a description. A table for 'Attached files' is currently empty, with 'Remove' and 'Add files' buttons. A 'Validation checks' section lists 'File Schema conformance', 'NIST Core constraints', and 'FedRAMP Schematron constraints'. At the bottom right are 'Clear' and 'Validate' buttons.

GSA Authorization Portal

Search for packages, docs, and more

Aaron Nolan

OSCAL Utilities

Validations

OSCAL Viewer

Risk Profiler

OASD Phase 1 OSCAL Rev 4 Artifact Validation

Please ensure you are selecting OSCAL Rev 4 Artifacts in XML format. Other formats are not supported in Phase 1.

Dashboard > OSCAL Utilities > Validations

### Validations

Run OSCAL document validations against File Schema, NIST, and FedRAMP standards

Attached files

Remove Add files

<input type="checkbox"/>	Name	Type	Size	Document type
No attached files				
No attached files to be validated				

Validation checks

File Schema conformance

NIST Core constraints

FedRAMP Schematron constraints

Clear Validate

Figure 2: Run Validations Page

The screenshot shows the 'Risk Profiler' page within the GSA Authorization Portal. The page has a dark blue header with the portal name and a search bar. A left sidebar lists 'OSCAL Utilities' with sub-links for 'Validations', 'OSCAL Viewer', and 'Risk Profiler'. The main content area features a sub-header and a description. Below this, there are two dropdown menus for selecting a System Security Plan (SSP). The 'Threat Based Risk Profile' section shows 'No Risk Profile' and a 'Generate Risk Profile' button. The 'Capability summary' section shows 'No capability summary'.

GSA Authorization Portal

Search for packages, docs, and more

Aaron Nolan

OSCAL Utilities

Validations

OSCAL Viewer

Risk Profiler

Dashboard > OSCAL Utilities > Risk profiler

### Risk Profiler

Generate a comprehensive risk profile. This enables you to proactively address concerns and maintain a robust security posture in line with FedRAMP requirements

Select a System Security Plan (SSP)

AwesomeCloud SaaS Version 1.0

AwesomeCloudSSP1.xml

Threat Based Risk Profile

Reset

No Risk Profile

No Risk Profile to display

Generate Risk Profile

Capability summary

No capability summary

No capability summary to display

Figure 3: Risk Profiler Page

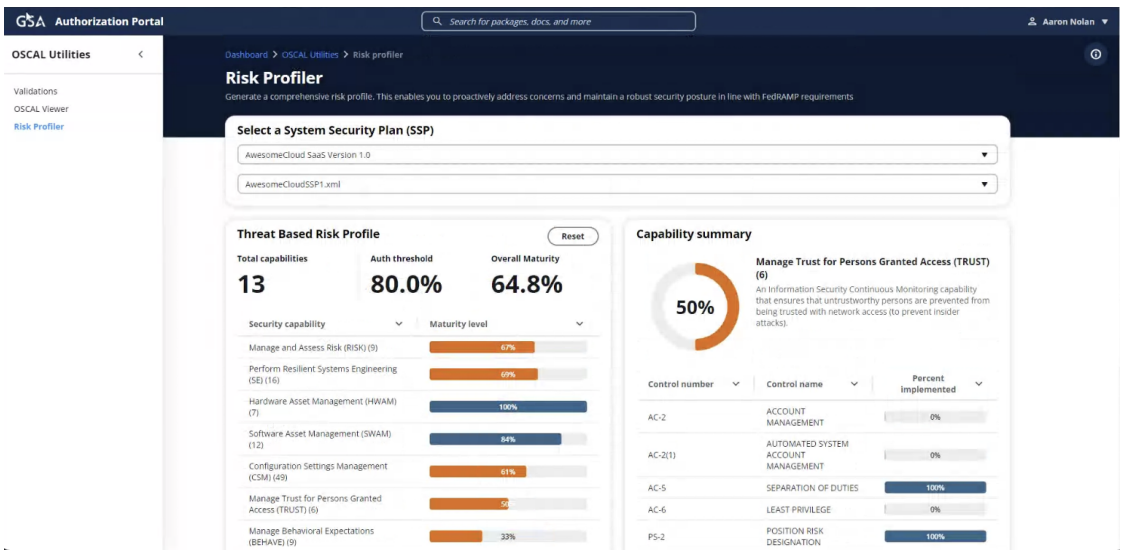


Figure 4: Example of Risk Profile Output

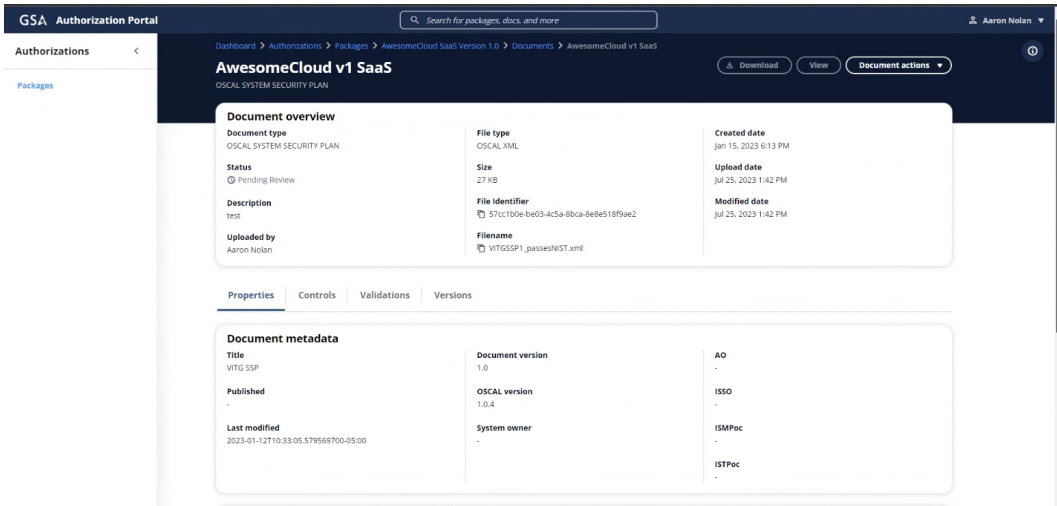


Figure 5: Submitted Artifact Overview (Will be focus of Phase II)

Actions

Owner		Action Item	
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		