



FedRAMP

# FedRAMP OSCAL Implementers

**October 9, 2024**



[info@fedramp.gov](mailto:info@fedramp.gov)

[fedramp.gov](https://fedramp.gov)

**Purpose:** To engage Cloud Service Providers, 3PAOs, tool vendors and other participants in FedRAMP's OSCAL Implementers activities.

**Outcomes:**

- Shared understanding of current OSCAL issues
- Alignment and clarity around topics covered in #653 up to this point



**Agenda:**

- Welcome
- OSCAL Implementers General Updates
- Digital Authorization Package Topic Discussion
- 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**

# General Updates

---

## Digital Authorization Package Pilot

This week, planned activities include:

### Pilot Participants

- Finish setup local validation tooling in their environments
- Asking for help / reporting problems
- Continue validating their SSPs with the local validation tooling

### FedRAMP OSCAL Automation Team

- Continue building out FedRAMP external constraints for SSP
- Continued updates to documentation
- Continued updates to the [OSCAL-CLI](https://github.com/metaschema-framework/osc-cli/releases) (<https://github.com/metaschema-framework/osc-cli/releases>)

### GitHub Issues

View the [project workboard](https://github.com/orgs/GSA/projects/25/views/3) for more details on ongoing work and upcoming priorities  
<https://github.com/orgs/GSA/projects/25/views/3>)

## Architecture decision records (ADRs)

- [ADR #9](#): Integrate help text and links into constraints directly.
  - Support added in OSCAL-CLI v2.2.0
  - Updating constraints with **help-url** and/or **help-text**
  - Updating documentation site
- New [ADR #10](#) - FedRAMP extensions registry replacement (GH issue [#564](#))
  - Proposes an approach for replacing the prior experimental registry which per [ADR #7](#) was deprecated

## New SSP Validation Constraint(s)

### Constraint

- **SSP constraint:** has-system-id
- **Description:** A FedRAMP SSP must have a FedRAMP system identifier.
- **Help URL:**  
<https://automate.fedramp.gov/documentation/ssp/4-ssp-template-to-oscal-mapping/#system-name-abbreviation-and-fedramp-unique-identifier>
- **Level:** ERROR

### Word SSP Template Screenshot

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
General System Description:	<Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

## SSP Validation Constraints

- address-type
- attachment-type
- authorization-type
- categorization-has-correct-system-attribute
- categorization-has-information-type-id
- cloud-service-model
- component-type
- control-implementation-status
- data-center-US
- data-center-alternate
- data-center-count
- data-center-country-code
- data-center-primary
- deployment-model
- has-authenticator-assurance-level
- has-authorization-boundary-diagram
- has-authorization-boundary-diagram-caption
- has-authorization-boundary-diagram-description
- has-authorization-boundary-diagram-link
- has-authorization-boundary-diagram-link-rel
- has-authorization-boundary-diagram-link-rel-allowed-value
- has-configuration-management-plan
- has-data-flow
- has-data-flow-description
- has-data-flow-diagram
- has-data-flow-diagram-caption
- has-data-flow-diagram-description
- has-data-flow-diagram-link
- has-data-flow-diagram-link-rel
- has-data-flow-diagram-link-rel-allowed-value
- has-data-flow-diagram-uuid
- has-federation-assurance-level
- has-identity-assurance-level
- has-incident-response-plan
- has-information-system-contingency-plan
- has-network-architecture
- has-network-architecture-diagram
- has-network-architecture-diagram-caption
- has-network-architecture-diagram-description
- has-network-architecture-diagram-link
- has-network-architecture-diagram-link-rel
- has-network-architecture-diagram-link-rel-allowed-value
- has-rules-of-behavior
- has-separation-of-duties-matrix
- has-user-guide
- information-type-system
- interconnection-direction
- interconnection-security
- inventory-item-allows-authenticated-scan
- inventory-item-public
- inventory-item-virtual
- missing-response-components
- privilege-level
- prop-response-point-has-cardinality-one
- resource-has-base64-or-rlink
- resource-has-title
- role-defined-authorizing-official-poc
- role-defined-information-system-security-officer
- role-defined-system-owner
- scan-type
- security-level
- system-has-id
- user-type

Highlighted constraints merged to develop branch over the last week - <https://github.com/GSA/fedramp-automation/tree/develop/src/validations/constraints>



# FedRAMP Roadmap

## *Digital Authorization Packages Pilot*

---



**Review code, data, and documentation before, during, and after release in our GitHub repositories**

---



**Follow official processes to engage us whether participating frequently or ad-hoc**

---



**Full details on the official pilot page:**  
**<https://fedramp.gov/digital-authorization-package-pilot/>**

## Roadmap of Next Steps for Users

### Near-Term

- ✓ Installation of containerized tools
- ✓ Running of tools
- ✓ Reporting problems
- ✓ Writing your own OSCAL documents
- ❑ Using the tooling with OSCAL SSPs
- ❑ Interpreting validation results
- ❑ Configuring the tooling and constraints

Review!

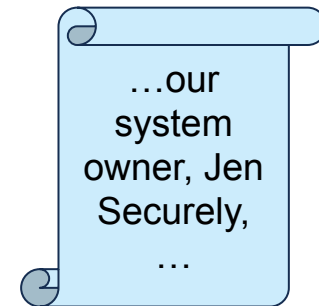
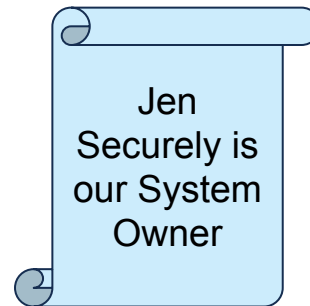
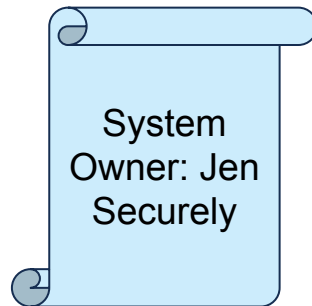
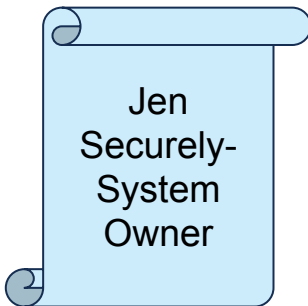
### Longer-Term

- ❑ Using the tooling with POA&Ms
- ❑ Using the tooling with SAP & SAR
- ❑ Advanced features

**See details of planned walkthroughs** - <https://github.com/GSA/fedramp-automation/issues/653>

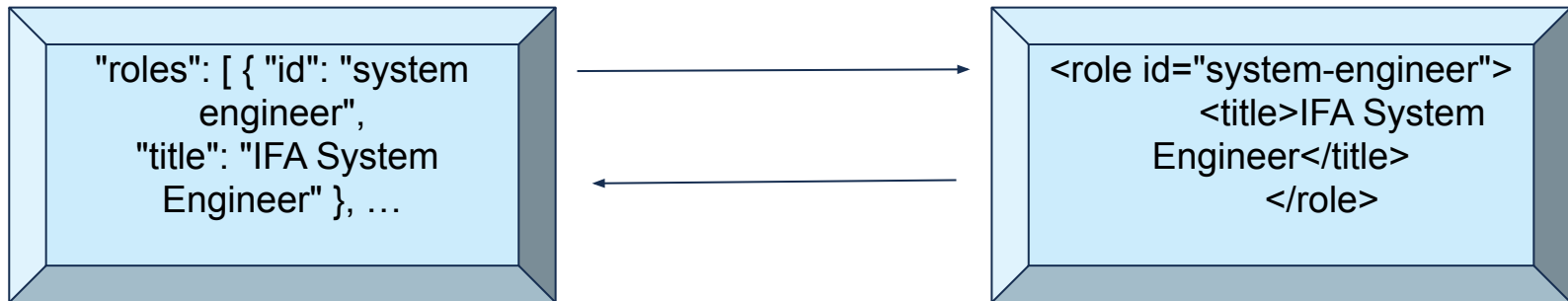
## Why OSCAL?

- Handwritten System Security Plans (and other artifacts) **do not have consistent formats**
- Machines can't evaluate word doc SSPs consistently– so humans have to :(



## Why OSCAL?

- OSCAL is a consistent, machine-readable format for security artifacts
  - Representable interchangeably in JSON and XML



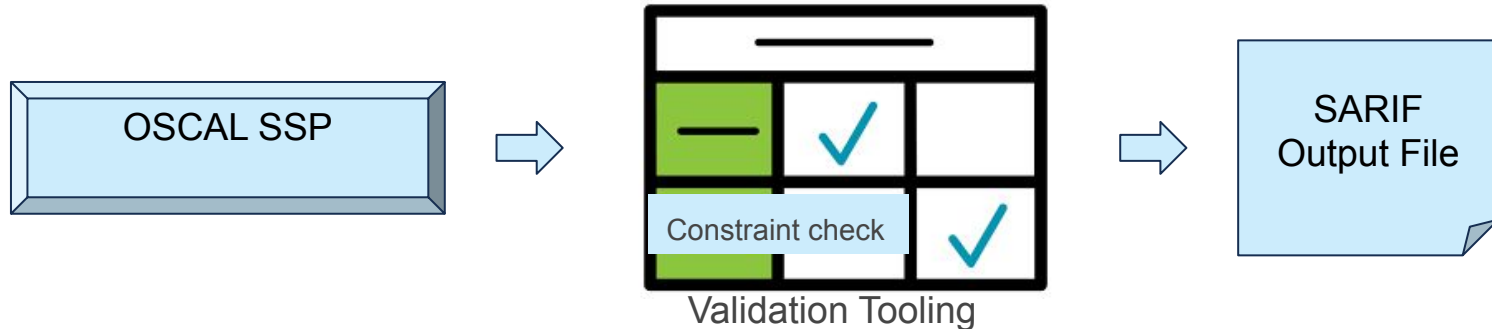
**Note:** We do not expect people to manually produce OSCAL. There are tools that will help with this, but we are not involved in building them

## Validation Tooling and Constraints 101

- At this point, we are trying to refine FedRAMP’s validation tooling
- **WE NEED YOUR FEEDBACK:** You get to have a say in the future of FedRAMP—and the industry
  - Validation Tooling = (automated) FedRAMP rubrics for SSPs
  - Constraint = a single line-item on a rubric
  - SARIF output file = your grade, and how to improve

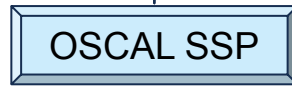
Two “rubrics”:

- External-allowed-values
- External-constraints

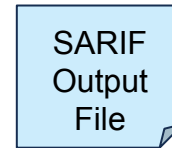


## Command Structure

```
oscal-cli validate <oscal-artifact> -c <fedramp-external-constraints> -o <sarif-output>
```



Validation Tooling



A “container” takes all dependencies and git files and bundles them into one neat install

## Container Prefix

```
docker run -it --rm -v $(pwd):/data ghcr.io/gsa/fedramp-automation/validation-tools:latest
```


Mount current  
directory

Load our fedramp-automation github


## Today's Plan

### What we will do today!

- Setting up VSCode
  - Add SARIF and XML extension
- Installing the containerized version of the tooling
- Running the tooling on some example SSP files
- Interpreting the results
- Submitting an issue



Please interrupt me whenever!!



Please ask questions!!

### What you will need to follow along

- VSCode installed
- Docker Desktop or alternative installed
- A github account
- Some example SSP files downloaded (your own or ours)



# Open Forum

---

# Thank you

Our next Implementers virtual meeting will be on  
**Wednesday, October 16, 2024 at 12p ET.**

**Submit questions and future discussion topics to [OSCAL@fedramp.gov](mailto:OSCAL@fedramp.gov)**

**Learn more at [fedramp.gov](https://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](mailto:oscal@fedramp.gov)

## FedRAMP Automation GitHub: <https://github.com/GSA/fedramp-automation>

- Open Issues: <https://github.com/GSA/fedramp-automation/issues>
- Open Pull Requests: <https://github.com/GSA/fedramp-automation/pulls>
- Active Work: <https://github.com/orgs/GSA/projects/25/views/3>
- Community Review Needed: <https://github.com/orgs/GSA/projects/25/views/7>

## GitHub Resources:

- Issues: <https://docs.github.com/en/issues>
- Pull Requests: <https://docs.github.com/en/pull-requests>

## **NIST:**

**OSCAL repo:** <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>

**Early Adopter repo:** <https://github.com/GSA/fedramp-oscal-earlyadopters>