



FedRAMP

OSCAL Developer Data Bytes

December 19, 2024



info@fedramp.gov

fedramp.gov

Purpose: To create space for dialogue between developers who use OSCAL and the FedRAMP® automation team.

Outcomes:

- Clarity around responsibilities and benefits of the Digital Authorization Package Pilot
- Productive discussion around OSCAL



Agenda:

- Welcome
- FedRAMP Automation PMO General Updates
- Digital Authorization Package Pilot 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

December 19, 2024

- **FedRAMP Platform**
 - See [changelog](#) for completed and upcoming milestones
- **Developer Hub**
 - New [section with centralized archive](#) of past meeting presentations
 - Ongoing corrections and improvements to SSP guidance sections
- **Other Documentation and Resources**
 - Improving and refining FedRAMP recommended or required approaches for representing data in OSCAL in a variety of SSP areas
 - Updating example FedRAMP SSP
- **Automated Validations**
 - Focus is on [completeness checks](#), first part of the strategy
 - Over 170 added since August 2024
 - Current focus on developing constraints for various areas in SSP front-matter and appendices (e.g., sections 3 - 9, and appendices B-L, N-P)
 - Next SSP areas of focus include:
 - Appendix A - Security Control Implementations
 - Appendix M - Integrated Inventory Workbook
 - User Table

Current Development Priorities & Status

- View the [project workboard](https://github.com/orgs/GSA/projects/25/views/2) for more details on ongoing work and upcoming priorities (<https://github.com/orgs/GSA/projects/25/views/2>)
 - “Ready to Ship” column includes all issues (e.g., constraints) developed to date and slated for future release
 - Digital Authorization Package Pilot participants are evaluating these constraints against their OSCAL SSPs
 - Collaborating with pilot participants, soliciting feedback and resolving identified issues

Important Changes for FedRAMP OSCAL



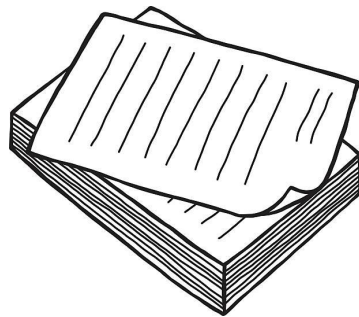
ADR #11 Approved

- Aligning extension property and misc identifier requirements for the official FedRAMP namespace
 - One common URI for FedRAMP **identifier-type**, **system** facet attribute and FedRAMP extension property **namespaces**
 - We reviewed pull requests #[102](#) and #[828](#), they are ready for merge.
 - We will **deploy updated docs and constraints this week**, but first we will:
 - Update these pull requests (you can subscribe to notifications).
 - Send an email to our mailing list oscal-implementer@fedramp.gov.

Reminder to submit questions/topic ideas via <https://forms.gle/M4pT7P2xyE6hRC7DA>

Digital Authorization Packages Pilot

- Let's zoom in on Simon and Deena today.
 - Simon – Security Manager at AwesomeCloud, submitting a digital authorization package for the AwesomeCloud App
 - Deena – Developer working on GoodGRC, Simon's GRC tool
- What does it look like for Simon to prepare a Digital Authorization Package?
- How can Deena help?



- ❖ By July of 2026, Simon will need to submit his digital authorization package using OSCAL
 - His package will need to pass the initial checks of our tooling before submission
- ❖ He has some choices:

Option 1: Simon can learn all about OSCAL, use his brain/ a code editor to produce it, and run our tooling himself to make the necessary corrections



- In situation A, Simon is sad because he has to do a lot of work, and Deena won't make her performance objectives to increase velocity for AwesomeCloud's GRC program.

```
<prop name="asset-id" value="DB-001" ns="http://csrc.nist.gov/ns/oscal"/>
  <prop name="asset-type" value="database"/>
  <prop name="allows-authenticated-scan" value="yes"/>
  <prop name="public" value="no"/>
```



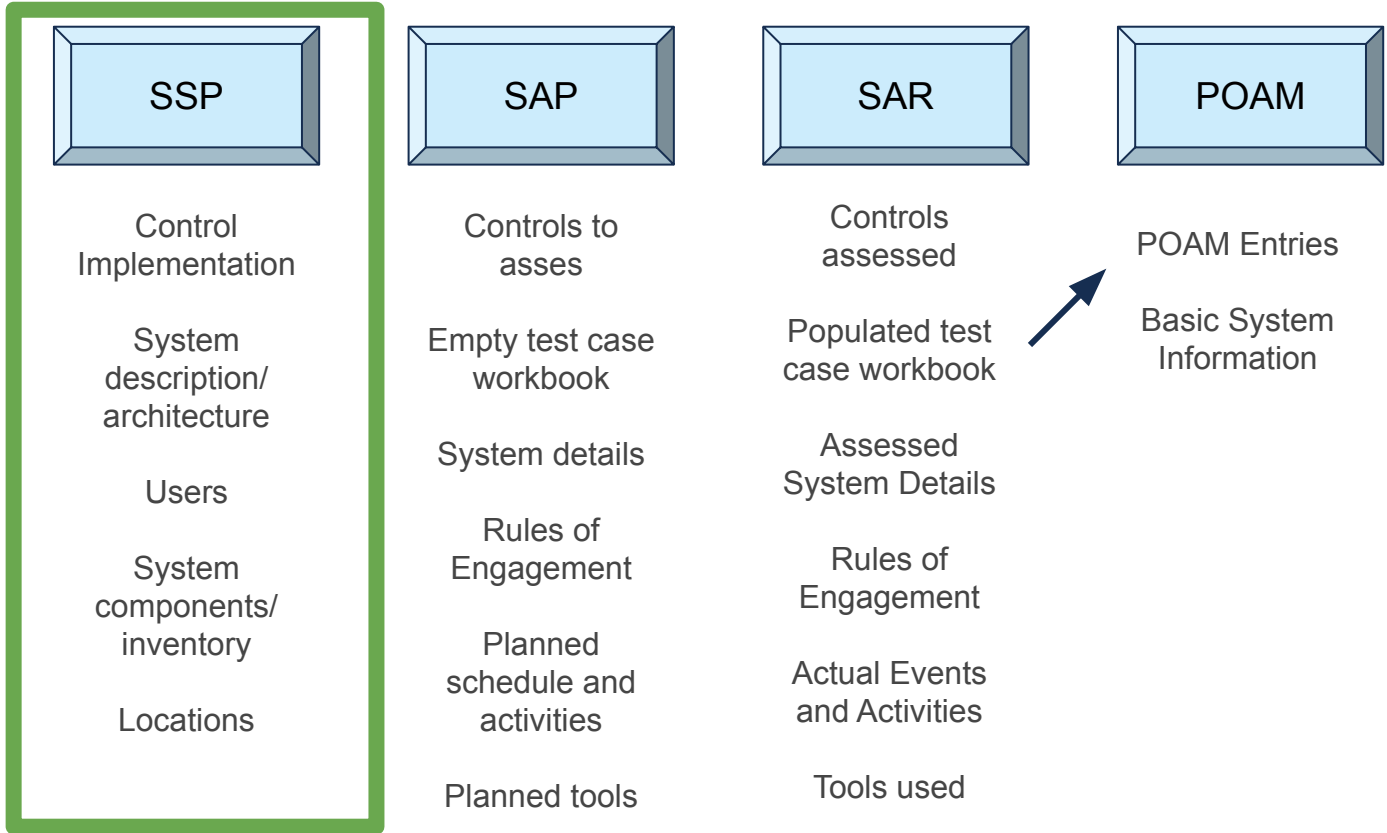
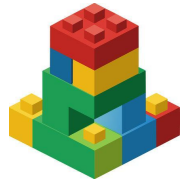
There's another option!

Option 2: Deena adds to the GoodGRC application that is incorporated with FedRAMP tooling, giving Simon a user-friendly interface that produces the OSCAL-based package for him.

- ❖ In situation 2, everyone is happy — Simon has a clean user interface that guides him on how to fill things out correctly
- ❖ Deena has a happy customer and meets her performance objectives.
- ❖ Either way, Riley is happy because automation is handling the more tedious parts of her job.



The Digital Authorization Package





Control
Implementation

System
description/
architecture

Users

System
components/
inventory

Locations

Constraint Categories

System information and overview

Who, where, what (roles, parties, locations, users)

Architecture, diagrams, and narratives

Leveraged services (FedRAMP-authorized)

External services (not FedRAMP-authorized)

Digital identity information

FIPS-199 categorization

Related laws and regulations

Inventory and PPSM information

Policy, procedure, and guide attachments

Control requirement documentation





System
description/
architecture

Locations &
Users

System
components/
inventory

Control
Implementation

System information and overview

[Who, where, what \(roles, parties, locations, users\)](#)

[Architecture, diagrams, and narratives](#)

[Leveraged services \(FedRAMP-authorized\)](#)

[External services \(not FedRAMP-authorized\)](#)

[Digital identity information](#)

[FIPS-199 categorization](#)

[Related laws and regulations](#)

[Inventory and PPSM information](#)

[Policy, procedure, and guide attachments](#)

[Control requirement documentation](#)



Let's look at the "Word-based Template"



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.)].

How do GoodGRC fields relate to FedRAMP OSCAL



CSP Name:	OSCAL required field
CSO Name:	OSCAL required field
FedRAMP Package ID:	Under Construction
Service Model:	FedRAMP constraint has-cloud-service-model
Digital Identity Level (DIL) Determination (SSP Appendix E):	FedRAMP constraint has-identity-assurance-level

FIPS PUB 199 Level (SSP Appendix K):	FedRAMP constraint has-security-sensitivity-level
Fully Operational as of:	FedRAMP constraint fully-operational-date
Deployment Model:	FedRAMP constraint has-cloud-deployment-model
Authorization Path:	FedRAMP constraint authorization-type
General System Description:	OSCAL required field

Open Forum

Thank you

Please be on the lookout for new calendar invites in 2025

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

Learn more at fedramp.gov



[@FEDRAMP](https://twitter.com/FEDRAMP)

Collaborating with FedRAMP

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>

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>