FedRAMP

FedRAMP OSCAL Implementers

December 4, 2024

GSA

info@fedramp.gov
fedramp.gov

Introduction

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
- Shared understanding of the applicability of the Digital Authorization Package pilot
- Clarity around roles and responsibilities for different stakeholders

Agenda:

- Welcome
- OSCAL Implementers General Updates
- Digital Authorization Package Topic Discussion
- Open Forum
- Next Steps & Closing

FedRAMP Guiding Principles

Keep the discussion respectful

Be curious, seek understanding

Speak from your own experience

Challenge through questions

Focus on ideas

Keep it technical

General Updates

FedRAMP Automation Community Updates

Current Development Priorities & Status

View the project workboard for more details on ongoing work and upcoming priorities (https://github.com/orgs/GSA/projects/25/views/2)

Any questions on status of of items on the board?

Important changes for FedRAMP OSCAL

ADRs and other important changes

- Replacing spock versions with semantic versions in release strategy (ADR #10)
  - Introducing new "***fedramp-version***" extension property
  - Developing constraints to validate that the ***fedramp-version*** and ***oscal-version*** in the document conform to our release strategy
- Aligning extension property and misc identifier requirements for the official FedRAMP namespace (DRAFT ADR #11)
  - Proposing one common URI for FedRAMP ***identifier-type***, ***system*** facet attribute and FedRAMP extension property ***namespaces***
  - Drafted pull requests #102 and #828 provide a preview of the proposed changes
  - Please provide any feedback by the end of this week

Important changes upstream to NIST OSCAL

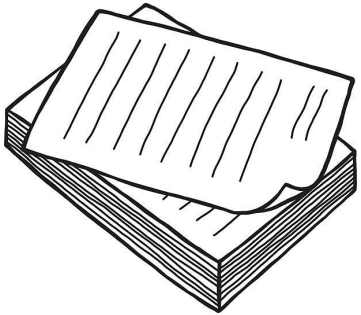
New release for OSCAL models

- NIST released new OSCAL models in v1.1.3
- This patch release has low-risk changes that are backward compatible
  - ✓ Correct digest lengths in #2068
  - ✓ Remove erroneous service/system indices for #2073 in #2075
  - ✓ Clarify protocol port-range docs for #2065 in #2070
  - ✓ Relax component protocol constraint for #1913 in #2063
  - ✓ Do not require a `protocol/@name` for #1772 in #2069
  - ✓ Removed incorrect enforcement of asset-id property at implemented-component in #2064
- NIST, FedRAMP, and community members developed the changes and fixes
- This community's feedback motivated many of these changes!

Digital Authorization Packages Pilot

Storytime

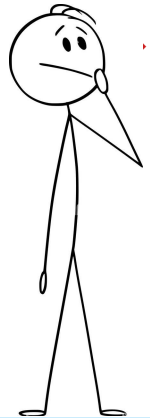
- Let’s zoom in on Simon and Deena today.
  - Simon – Security Manager at AwesomeCloud, submitting a digital authorization package for the AwesomeCloud App
  - Deena – Developer working on GoodGRC, Simon’s GRC tool
- What does it look like for Simon to prepare a Digital Authorization Package?
- How can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



Simon's Options

- 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



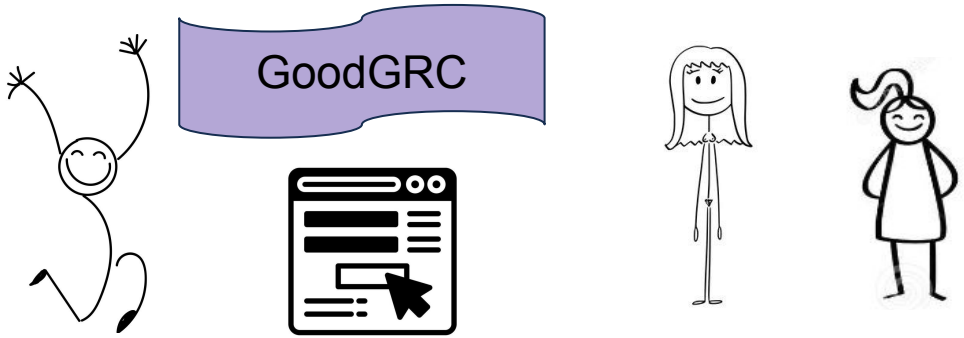
In situation A, Simon is sad because he has to do a lot of work, and Deena won't make her performance objectives to increase velocity for AwesomeCloud's GRC program.

```
<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"/>
```

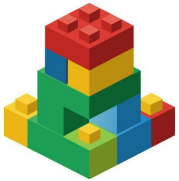
There's another option!

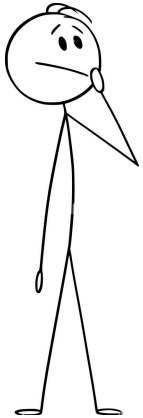
Option 2: Deena adds to the GoodGRC application that is incorporated with FedRAMP tooling, giving Simon a user-friendly interface that produces the OSCAL-based package for him.

- 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





SSP

Control Implementation

System description/ architecture

Users

System components/ inventory

Locations

SAP

Controls to asses

Empty test case workbook

System details

Rules of Engagement

Planned schedule and activities

Planned tools

SAR

Controls assessed

Populated test case workbook

Assessed System Details

Rules of Engagement

Actual Events and Activities

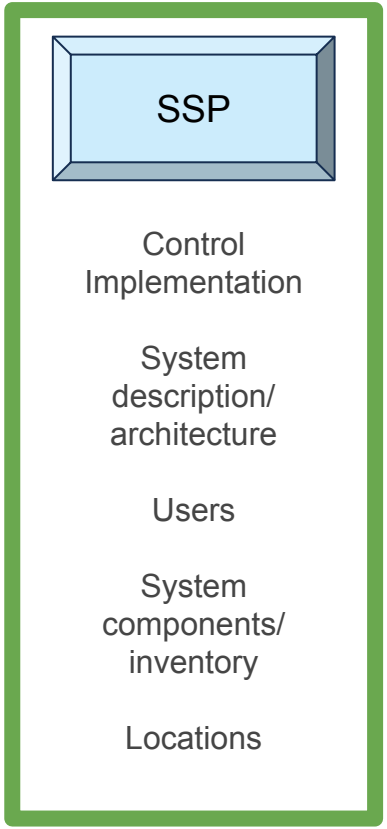
Tools used

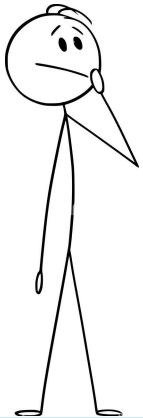
POAM

POAM Entries

Basic System Information

Zooming in on SSPs and our constraint work!





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

Zooming in on System Information Constraints

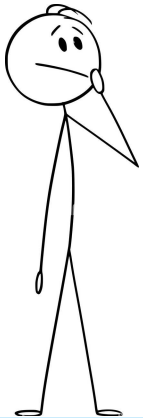
SSP

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

Our next Implementers virtual meeting will be on

Wednesday, December 18, 2024 at 12p ET.

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

Learn more at fedramp.gov

@FEDRAMP

How to Submit Issues with FedRAMP

Ensuring your outstanding issues or questions are received:

Issues can be submitted in several ways:

Preferred	Alternate
Open an issue on fedramp-automation github so that it will benefit the NIST/FedRAMP community. **https://github.com/GSA/fedramp-automation/issues**	Email us at **oscal@fedramp.gov**

Collaboration Resources

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

OSCAL Resources

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