



OSCAL Developer Data Bytes

November 21, 2024

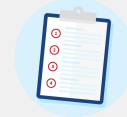


info@fedramp.gov
fedramp.gov

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

Outcomes:

- Clarity around roles and responsibilities during 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

Digital Authorization Package Pilot

This month, planned activities included:

FedRAMP OSCAL Automation Team

- Walking through different key FedRAMP SSP constraints thematically
 - Continued building out external constraints
 - Continued updates to documentation
 - Continued updates to the [OSCAL-CLI](https://github.com/metaschema-framework/oscalschema-framework/releases) (<https://github.com/metaschema-framework/oscalschema-framework/releases>) and other tooling

Pilot Participants

- Collaborating with FedRAMP by testing validation of their OSCAL SSPs using the FedRAMP local validation tooling
- Providing feedback and reporting issues
- Asking for help and scheduling Office Hours

November 21, 2024

- Documentation Updates
 - [Changelog](#) for completed and upcoming milestones for the FedRAMP Platform
 - Many corrections and improvements to example SSP data and guidance
 - Update contact information to include mailing list
 - New section with centralized archive of past meeting presentations
- Constraints Updates
 - Focus is on [completeness checks](#), first part of the strategy
 - Over 100 added since August 2024
 - Current focus areas in SSP:
 - Section 3 System Information
 - Sections 4 and 5 Roles and Responsibilities
 - Section 6 Leveraged Authorizations

November 21, 2024

- Related Efforts
 - Revisions to better align Rev 5 SSP Tables 6.1 and 7.1 modeling in OSCAL
 - Separation of Duty Matrix and User Table
- Applicable Github Issues:
 - Leveraged Authorizations: <https://github.com/GSA/fedramp-automation/issues/807>
 - External Systems and Services Not Having FedRAMP Authorization: <https://github.com/GSA/fedramp-automation/issues/808>
 - Separation of Duties: <https://github.com/GSA/fedramp-automation/issues/534>
 - User Table/OSCAL Assembly: <https://github.com/GSA/fedramp-automation/issues/902>

GitHub Issues

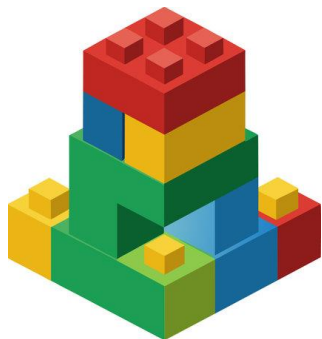
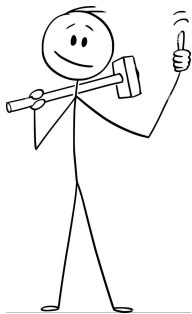
View the [project workboard](https://github.com/orgs/GSA/projects/25/views/3) for more details on ongoing work and upcoming priorities
<https://github.com/orgs/GSA/projects/25/views/3>

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

Digital Authorization Packages Pilot

- Let's tell a story. Today, you're going to meet
 - Simon
 - Deena
 - Riley
- Where do they work?
- What do they do all day at their jobs?
- What will they automate? How? Why will it benefit them?
- How do Simon and Deena get started?

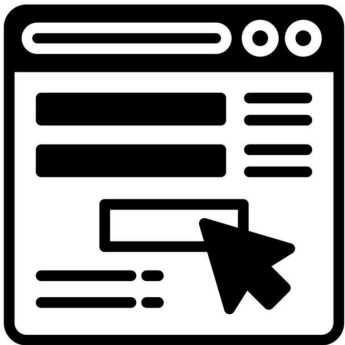
AwesomeCloud



Simon's Dilemma

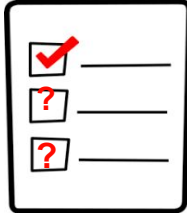
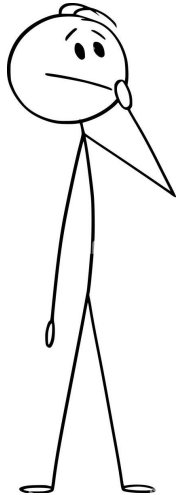
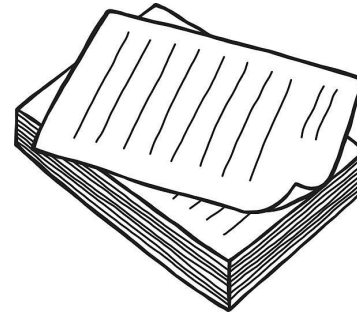
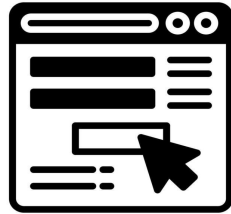
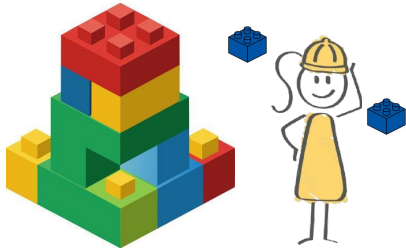
- Company AwesomeCloud finished their system, AwesomeApp– now it's Simon's job to get it FedRAMP authorized!
- He is going to need to produce a System Security Plan that meets FedRAMP requirements
- Simon feels overwhelmed – with so many requirements, resources, and checklists, he doesn't know where to begin – so he goes to Deena for help!

GoodGRC



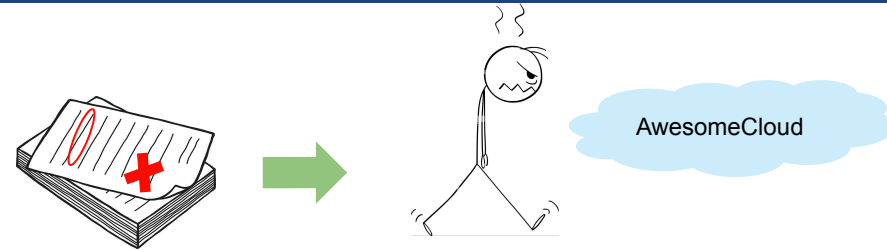
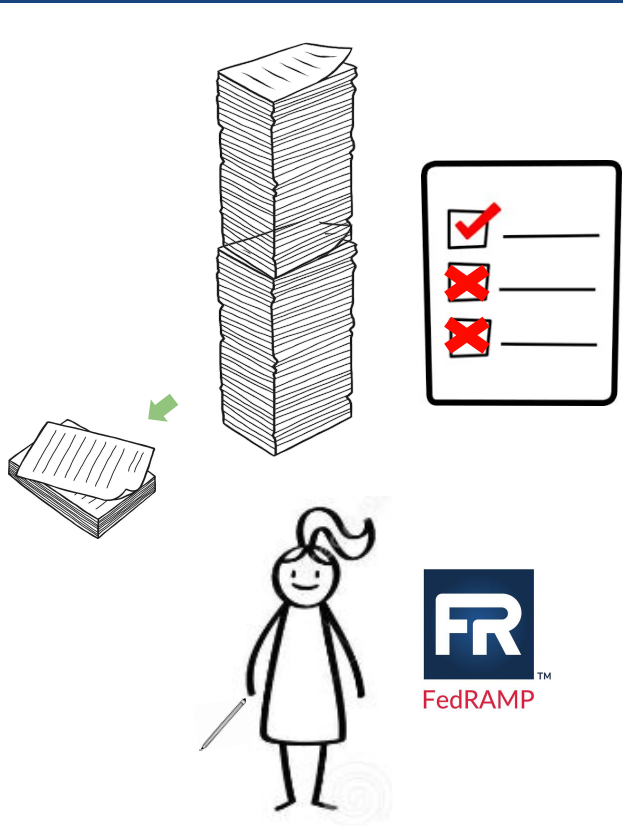
Deena's Dilemma

- Deena is in charge of building Simon's GRC platform, GoodGRC.
- Deena wants to use automation to guide Simon through the FedRAMP process, BUT
 - Neither system information nor FedRAMP requirements are easily represented or understood by machines
- She can try to invent her own data format for her data model– very hard to do
 - Proprietary formats aren't easily understood or translated between parties
- Or... she can use her data model and convert to word documents which makes it even worse



The Process

- Over the next several months, Simon and AwesomeCloud engineers inspect the system, hire a 3PAO, and use GoodGRC to get their new service, AwesomeApp, authorized by FedRAMP
- They review checklists and FedRAMP guidance, but they have trouble knowing how to apply it to this system
- Finally, Simon produces a 100 page SSP document that he **thinks** is good enough to submit.



Riley's Dilemma

- Riley has A LOT of packages to review – it will take months to get to AwesomeCloud's package
- She manually checks and cross-references hundreds of controls
- Simple mistakes, insufficient information, and system vulnerabilities means that she needs to meet with AwesomeCloud several times
- Then, she needs to **pass back** the package for AwesomeCloud to correct



Validation Tooling: The FedRAMP automation team is currently building the tooling that checks digital packages, starting with SSPs

AwesomeCloud

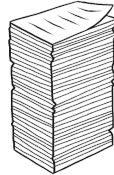
OSCAL SSP



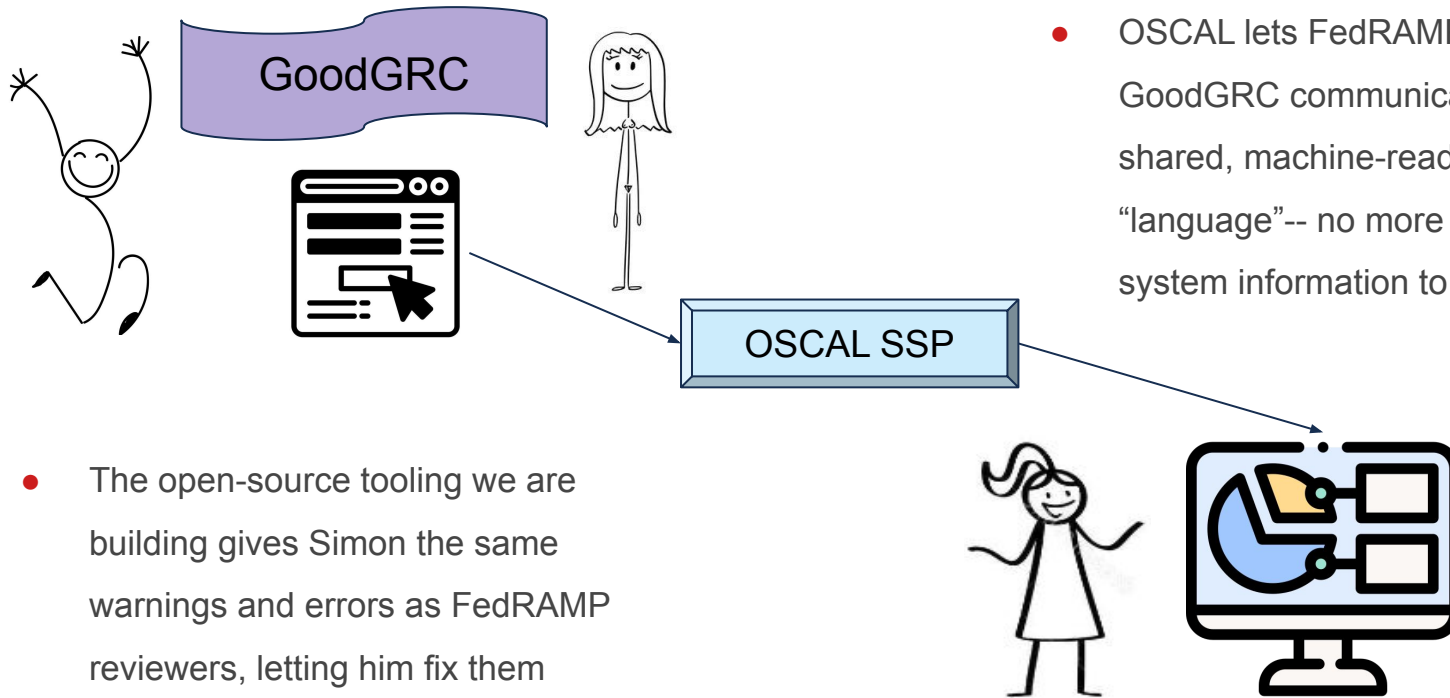
C:\WARNING...
Valid?



OSCAL SSP



**We are helping companies
submit better packages
faster- thereby reducing
passbacks and speeding up
reviews**



- The open-source tooling we are building gives Simon the same warnings and errors as FedRAMP reviewers, letting him fix them pre-submission

- OSCAL lets FedRAMP and GoodGRC communicate directly in a shared, machine-readable “language”-- no more translating system information to .docx

Starting at the beginning– what does this look like?



FedRAMP® (High, Moderate, Low, LI-SaaS) Baseline System Security Plan (SSP)

<test> | <Insert CSO Name> | <Insert Version X.X> | <Insert MM/DD/YYYY>



Document tabs



Tab 1

FedRAMP® (High, Moder...

Introduction

Purpose

System Information

System Owner

Assignment of Security R...

Leveraged FedRAMP-Aut...

External Systems and Ser...

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>

- A very rough outline of what GoodGRC could look like to Simon, starting with the most important
- Highlighted box represents the only “critical” level constraints so far– importing the profile/catalog

How do they start?



Document tabs +

Tab 1

FedRAMP® (High, Moder...

Introduction

Purpose

System Information

System Owner

Assignment of Security R...

Leveraged FedRAMP-Aut...

External Systems and Ser...

Illustrated Architecture a...



FedRAMP® (High, Moderate, Low, LI-SaaS) Baseline System Security Plan (SSP)

<test> | <Insert CSO Name> | <Insert Version X.X> | <Insert MM/DD/YYYY>

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):	Moderate

Open Forum

Thank you

Our next Developer Data Bytes virtual meeting will be on

Thursday, December 19, 2024 at 12p ET.

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

Learn more at fedramp.gov



@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>