FedRAMP

FedRAMP OSCAL Implementers

November 13, 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, responsibilities, and starting points 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)

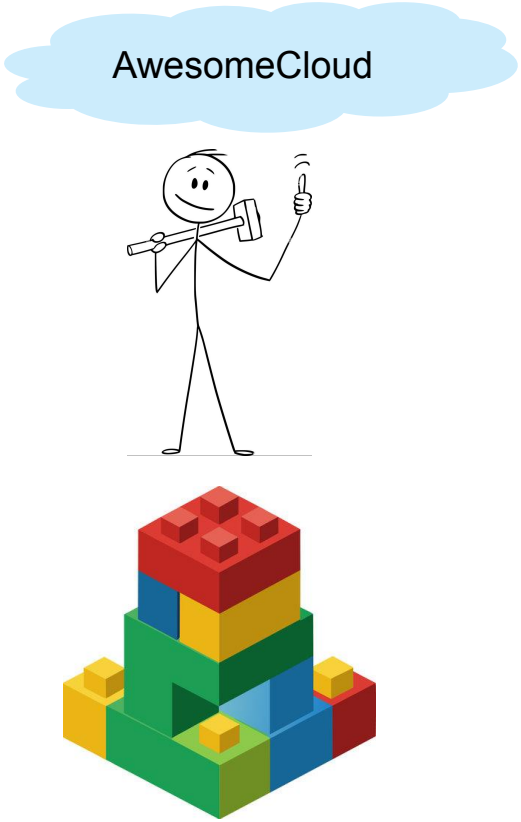
Any questions on status of of items on the board?

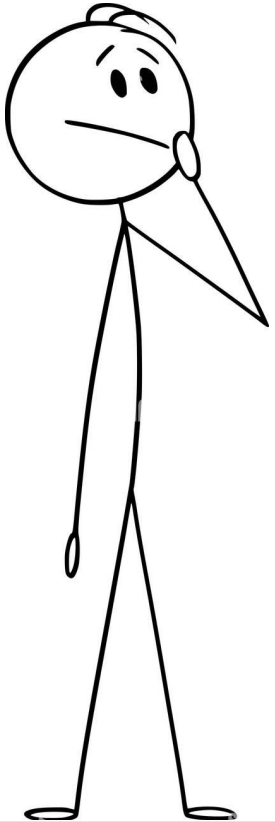
Digital Authorization Packages Pilot

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?

Meet Simon the Security Manager





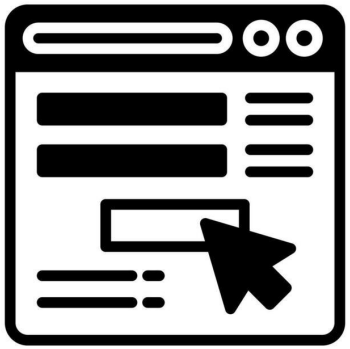
FedRAMP™

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!

Meet Deena the Developer

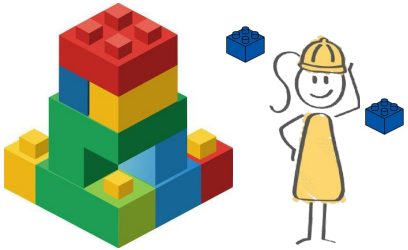
GoodGRC

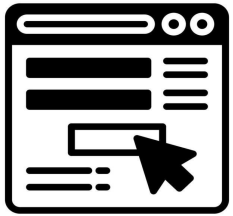


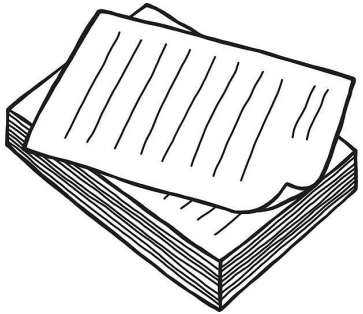
Deena's Dilemma

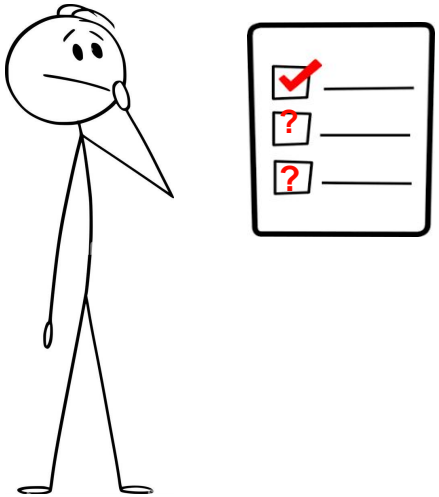
- Deena is in charge of building Simon's GRC platform, GoodGRC.
- Deena wants to use automation to guide Simon through the FedRAMP process, BUT
  - Neither system information nor FedRAMP requirements are easily represented or understood by machines
- She can try to invent her own data format for her 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

Meet Simon the Security Manager





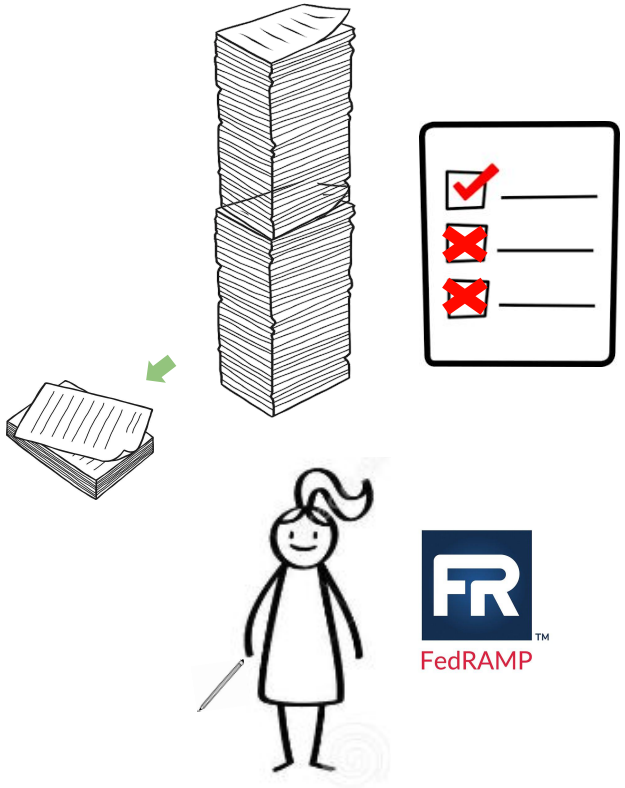


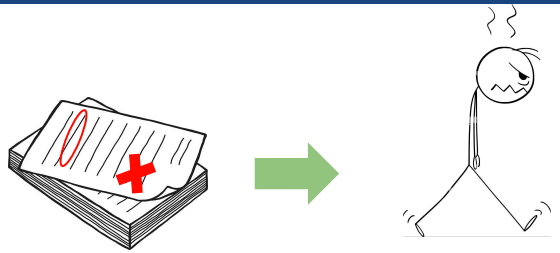


The Process

- 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.

Meet Riley the Reviewer



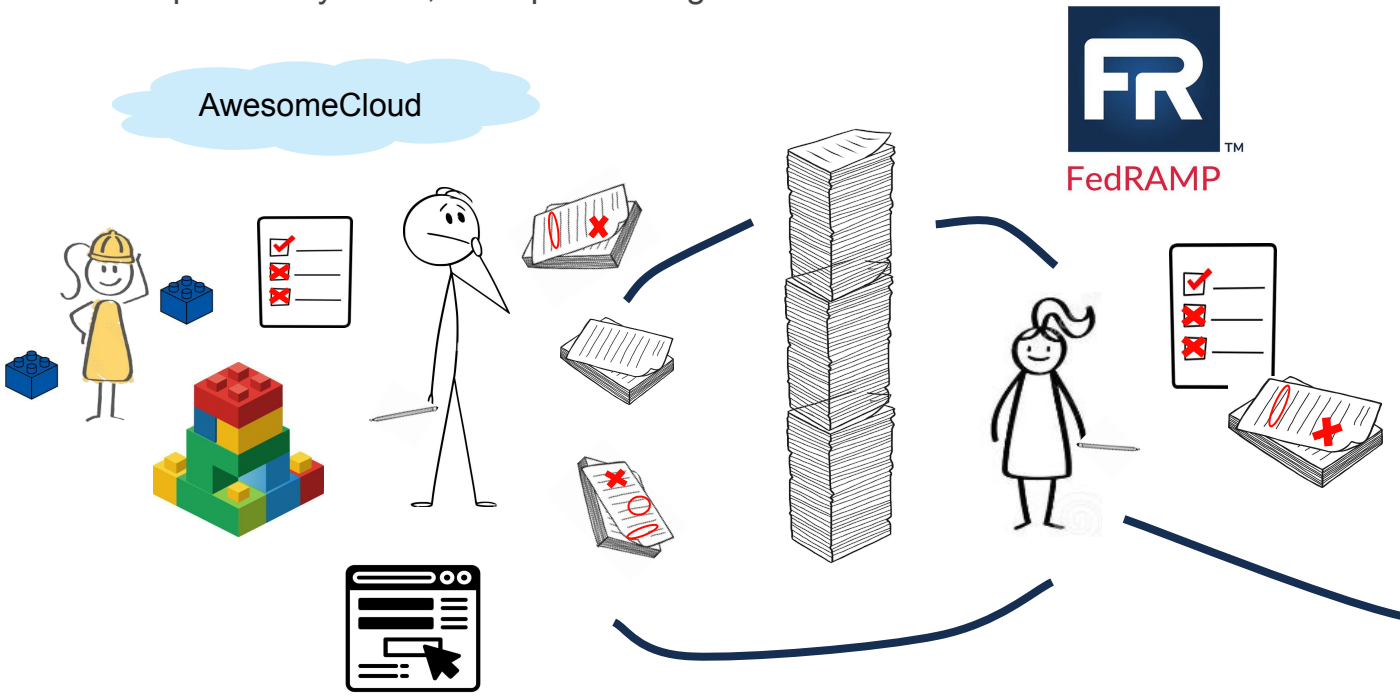


Riley's Dilemma

- 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

Welcome to the FedRAMP review loop

- This correction, resubmission, re-review cycle can repeat many times, each pass taking months

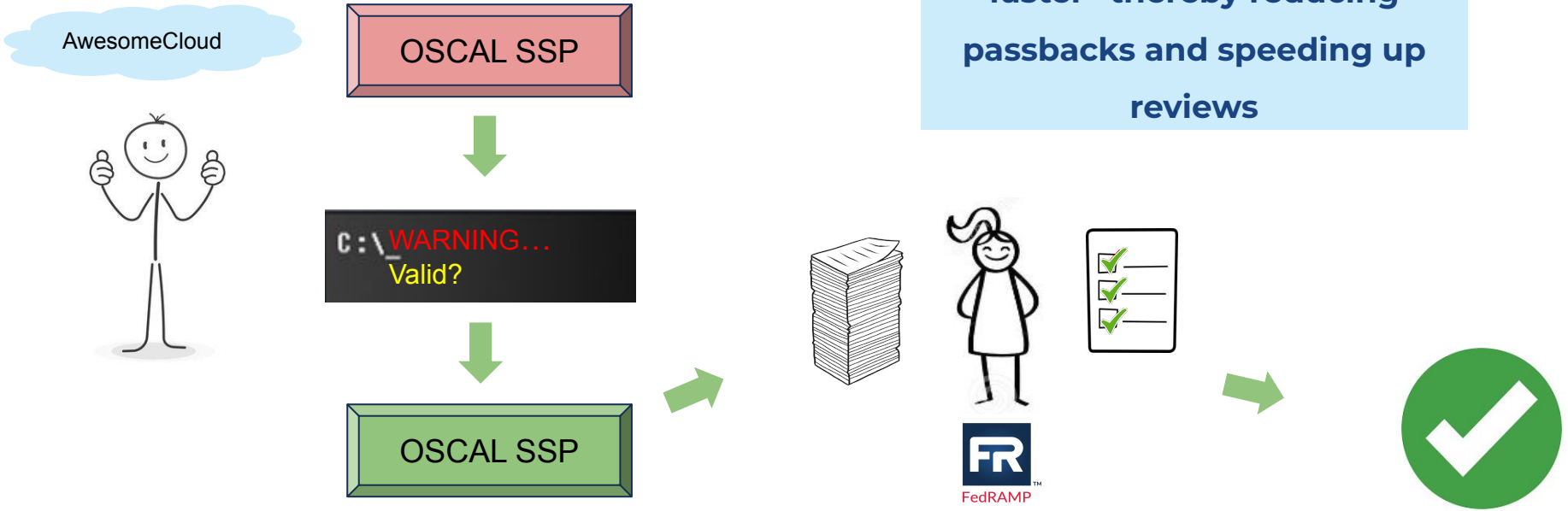


Companies do break free eventually– but it takes a long time and is very manual and costly for all involved.

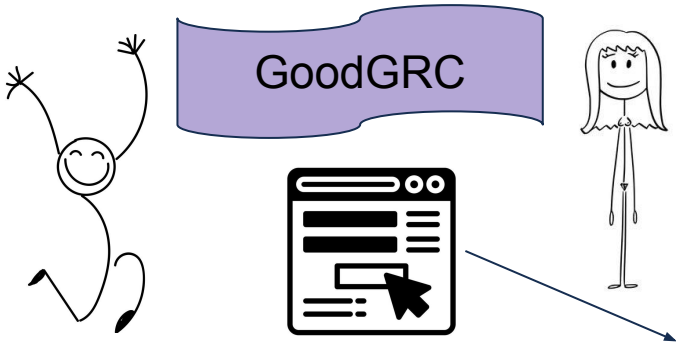
Simon's new journey

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

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



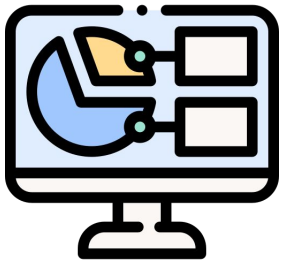
Closing the loop



OSCAL SSP

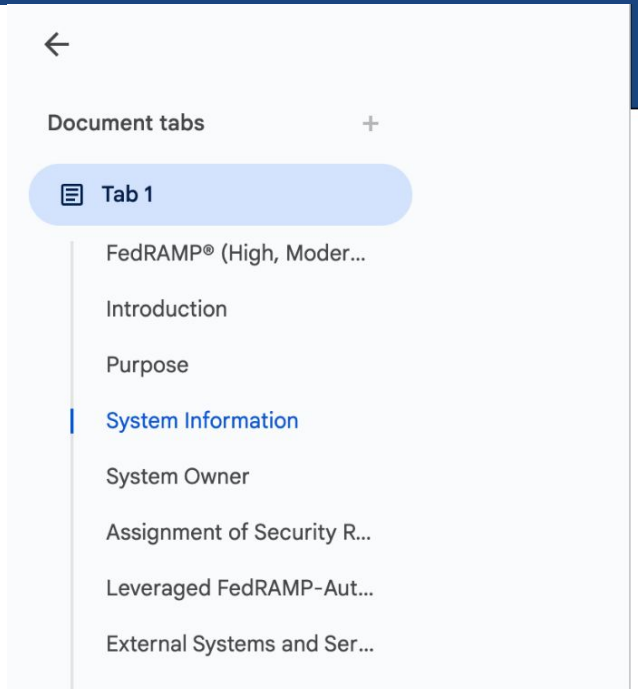
- OSCAL lets FedRAMP and GoodGRC communicate directly in a shared, machine-readable “language”-- no more translating system information to .docx

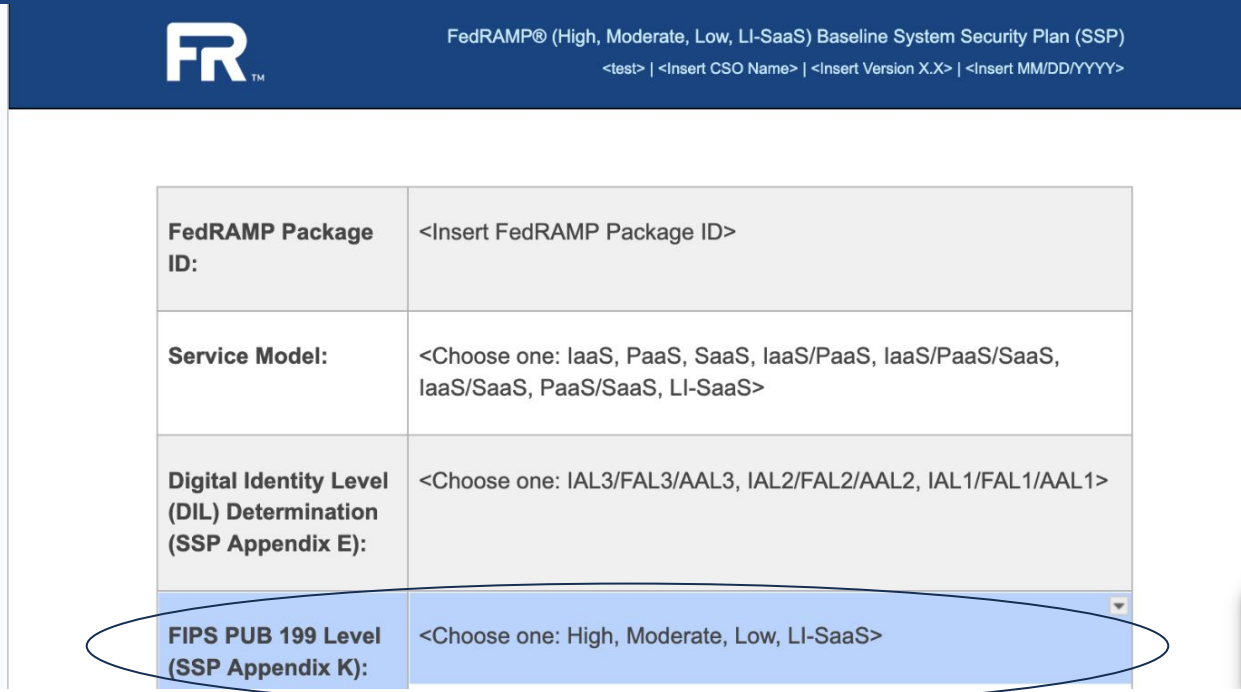
- The open-source tooling we are building gives Simon the same warnings and errors as FedRAMP reviewers, letting him fix them pre-submission



FedRAMP

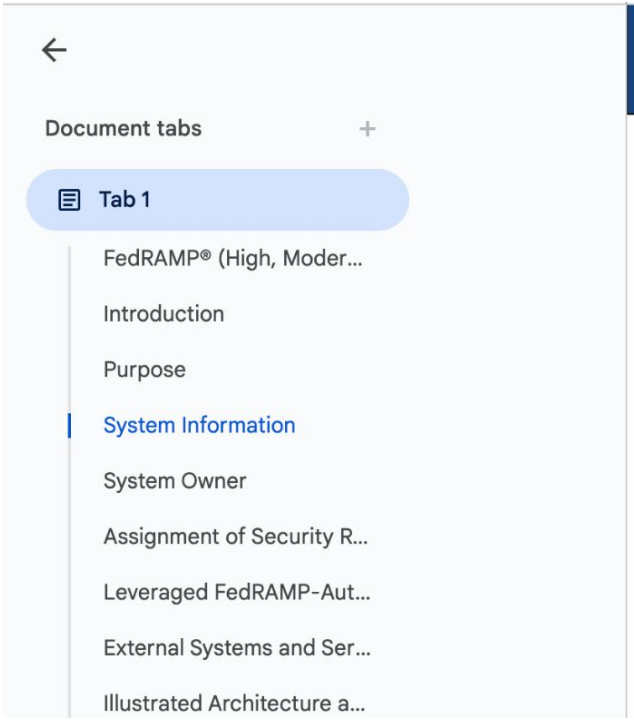
Starting at the beginning– what does this look like?





- 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?



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**

Under of the hood (of where they start)


```
{
 "system-security-plan": {
   "import-profile": {
     "href": "#e82e9b95-5b88-4dfb-93fa-fd26137429a0"
   },
   "back-matter": {
     "resources": [
       {
         "uuid": "e82e9b95-5b88-4dfb-93fa-fd26137429a0",
         "rlinks": [
           {
             "href": "FedRAMP_rev5_HIGH-baseline_profile.json",
             "media-type": "application/json"
           }
         ]
...
```

How do I start?

- Where can I find documentation about this requirement?
- Where and how do constraints check this requirement?
  - import-profile-has-available-document
    - Did the OSCAL SSP import an actual profile document?
      - If yes, continue
      - If no, CRITICAL ERROR
  - import-profile-resolves-to-fedramp-content
    - Is the profile document a fedramp document?
      - If yes, continue
      - If no, CRITICAL ERROR

Open Forum

Thank you

Our next Implementers virtual meeting will be on

Wednesday, December 4, 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