FedRAMP

FedRAMP OSCAL Early Adopters

May 22nd, 2024

GSA

info@fedramp.gov

fedramp.gov

Introduction

Purpose: To engage Cloud Service Providers, 3PAOs, tool vendors and other participants in FedRAMP's OSCAL Early Adopters Workgroup (OEAW) activities.

Outcomes:

- Shared understanding of current OSCAL issues.
- Shared understanding of FedRAMP guidance for generated SSPs
- Shared understanding of FedRAMP proposal for Separation of Duties information in OSCAL
- Alignment around any community issues and an understanding of next steps.

Agenda:

- Welcome
- OEAW General Updates
- Guidance on Rendering SSP Printables based on OSCAL
- Proposal for representing Separation of Duties in OSCAL
- Open Forum
- Next Steps & Closing

FedRAMP OEAW Guiding Principles

Keep the discussion respectful

Speak from your own experience

Focus on ideas

Be curious, seek understanding

Challenge through questions

Keep it technical

General Updates

FedRAMP Automation Community Updates

May 22, 2024

Revising OSCAL Guides

FedRAMP automation team is continuing to work towards publishing HTML versions of the OSCAL guides to replace the current PDF versions.

- Guides and related documentation were moved to new repository: https://github.com/GSA/automate.fedramp.gov
- Targeting website launch at the end of June 2024

Local Validation Tooling

FedRAMP automation team is working on adding metaschema validation mechanisms in the OSCAL-CLI tool.

GitHub Issues

Prioritizing issues related to FedRAMP Guides and SP 800-53 Rev 5

- Issue #558 - Mismatch of params (ODPs) / printables guidance
- Issue #534 - Separation of Duties
- Issue #555 - Update FedRAMP-SSP-OSCAL-Template.xml based on NIST SP 800-53 rev5.1.1 release
- Issue #563 - Resolved profile catalog missing props
- Issue #564 - Update FedRAMP Extensions and Values
- Various documentation / guide related issues

View the project workboard for more details on ongoing work and upcoming priorities

Review needed

https://github.com/orgs/GSA/projects/25/views/7

Parameter Mismatch in SSP Template

Guidance on Rendering Printables based on OSCAL

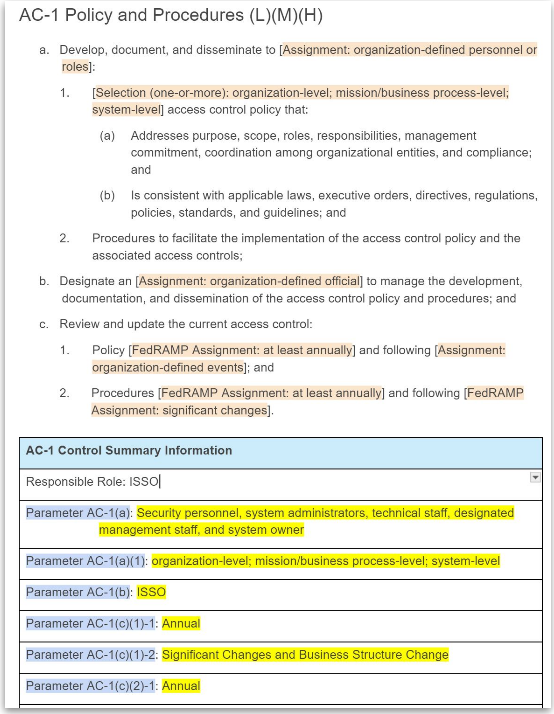
Parameter Mismatch in SSP Template vs OSCAL Baseline

Github Issue #558

Background

- Moved constraints to ODPs (see Draft PR https://github.com/GSA/fedramp-automation/pull/574)
- SSP printable feedback from authorization review team:
  - Reviewers need to see the control description
  - Reviewers need to see parameter description so they have context for provided parameter values
  - Reviewers need to see SSP author’s parameter value
  - Reviewers need a way to correlate the parameter value with the control part (e.g., “Parameter AC-1(a)”)

Current Document Template



AC-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] access control policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

AC-1 Control Summary Information
Responsible Role: ISSO
Parameter AC-1(a): Security personnel, system administrators, technical staff, designated management staff, and system owner
Parameter AC-1(a)(1): organization-level; mission/business process-level; system-level
Parameter AC-1(b): ISSO
Parameter AC-1(c)(1)-1: Annual
Parameter AC-1(c)(1)-2: Significant Changes and Business Structure Change
Parameter AC-1(c)(2)-1: Annual

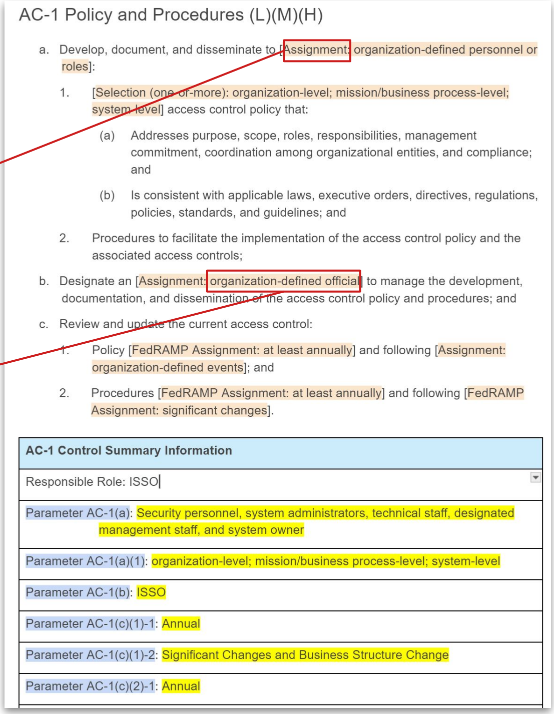
Parameter Mismatch in SSP Template vs OSCAL Baseline

Github Issue #558

Control Information

- Control information must be pulled from catalog or resolve profile catalog imported in the OSCAL SSP.
  - If the OSCAL SSP imports a profile, the profile resolution will be required.
- Control information must include
  - Control Title
  - Control Description
  - Parameter Assignment
    - “Assignment” vs “FedRAMP Assignment”
  - Parameter Description
    - Get value from parameter <label> field
    - Use OSCAL in-line param insertions (e.g., <insert type="param" id-ref="ac-1_prm_1"/>)

Current Document Template



AC-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] access control policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

AC-1 Control Summary Information
Responsible Role: ISSO
Parameter AC-1(a): Security personnel, system administrators, technical staff, designated management staff, and system owner
Parameter AC-1(a)(1): organization-level; mission/business process-level; system-level
Parameter AC-1(b): ISSO
Parameter AC-1(c)(1)-1: Annual
Parameter AC-1(c)(1)-2: Significant Changes and Business Structure Change
Parameter AC-1(c)(2)-1: Annual

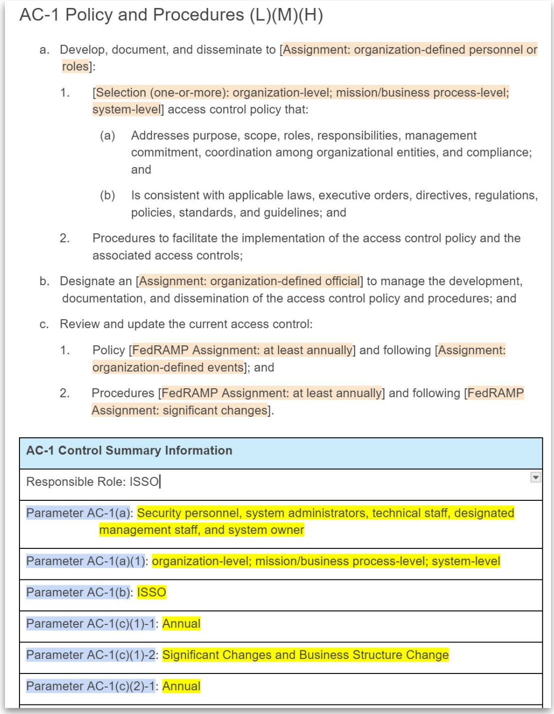
Parameter Mismatch in SSP Template vs OSCAL Baseline

Github Issue #558

Control Information (cont'd)

- Issues
  - Parameters with option selection in catalog do not have "label" or "guideline" fields to use for "parameter description" (e.g., Parameter AC-1(a)(1) -> ac-01_odp.03)
  - OSCAL catalog "label" field data differs slightly from the template (e.g., OSCAL ODP has "*official*" whereas template states "*organization-defined official*")
  - "FedRAMP Assignment" is implicit based on constraint specified in FedRAMP profile; all other parameters should be preceded with "Assignment: organization-defined "

Current Document Template



AC-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] access control policy that:

   (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

AC-1 Control Summary Information
Responsible Role: ISSO
Parameter AC-1(a): Security personnel, system administrators, technical staff, designated management staff, and system owner
Parameter AC-1(a)(1): organization-level; mission/business process-level; system-level
Parameter AC-1(b): ISSO
Parameter AC-1(c)(1)-1: Annual
Parameter AC-1(c)(1)-2: Significant Changes and Business Structure Change
Parameter AC-1(c)(2)-1: Annual

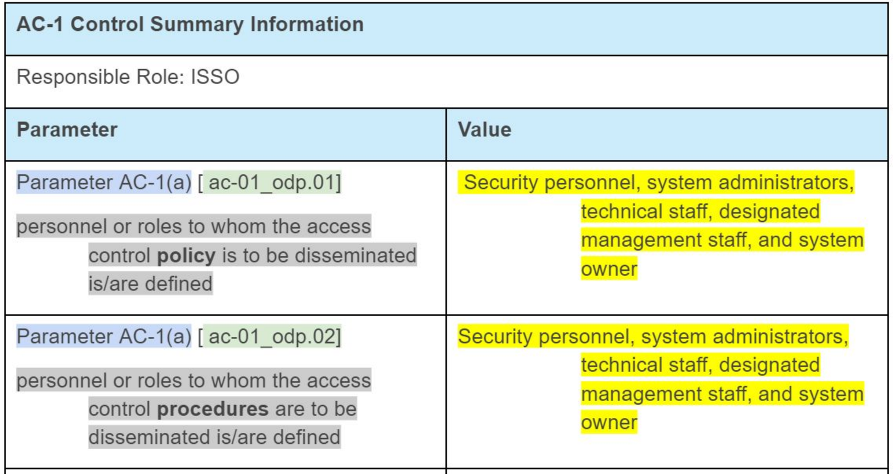
Parameter Mismatch in SSP Template vs OSCAL Baseline

Github Issue #558

Control Response

- Must provide the granular “ODP” level parameters.
- Must provide the SSP author’s specified parameter value(s).
- Must provide correlation between the ODP and the control part (e.g., “Parameter AC-1(a)”).
- Optional - should provide parameter “label” or “guideline” from source catalog

Sample Generated SSP Control Implementation



AC-1 Control Summary Information	
Responsible Role: ISSO	
Parameter	**Value**
Parameter AC-1(a) [ac-01_odp.01] personnel or roles to whom the access control **policy** is to be disseminated is/are defined	Security personnel, system administrators, technical staff, designated management staff, and system owner
Parameter AC-1(a) [ac-01_odp.02] personnel or roles to whom the access control **procedures** are to be disseminated is/are defined	Security personnel, system administrators, technical staff, designated management staff, and system owner

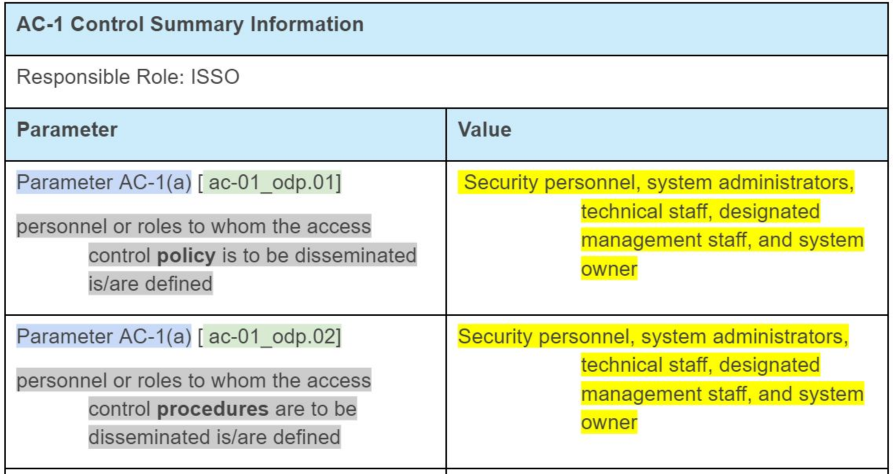
Parameter Mismatch in SSP Template vs OSCAL Baseline

Github Issue #558

Next Steps

- FedRAMP to create new FedRAMP extension to support mapping between the ODP and the control part
  - e.g., <prop name="label" ns="https://fedramp.gov/ns/oscal" value="AC-1(a)" />
  - e.g., <prop name="param-label" ns="https://fedramp.gov/ns/oscal" value="AC-1(a)" />
- FedRAMP to provide an open-source reference implementation

Sample Generated SSP Control Implementation



AC-1 Control Summary Information	
Responsible Role: ISSO	
Parameter	**Value**
Parameter AC-1(a) [ac-01_odp.01] personnel or roles to whom the access control **policy** is to be disseminated is/are defined	Security personnel, system administrators, technical staff, designated management staff, and system owner
Parameter AC-1(a) [ac-01_odp.02] personnel or roles to whom the access control **procedures** are to be disseminated is/are defined	Security personnel, system administrators, technical staff, designated management staff, and system owner

Separation of Duties

Proposed OSCAL Changes

FedRAMP Rev 5 SSP - Missing Separation of Duties Guidance

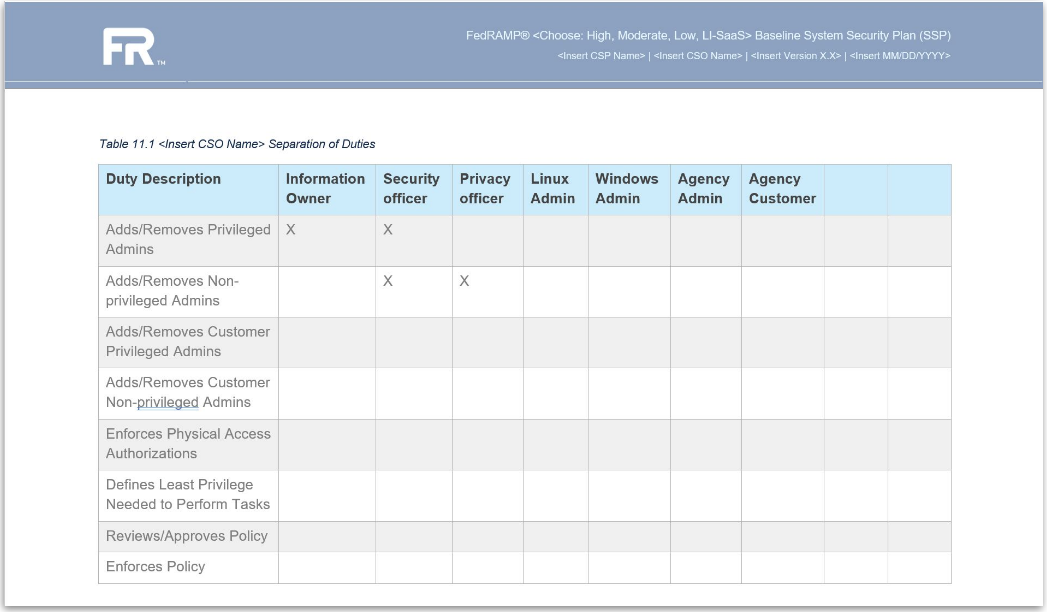
GitHub Issue #534

Issue:

Need an approach for how to represent FedRAMP required separation of duties information in OSCAL

Background:

New table (11.1) in the FedRAMP SSP template *“captures the roles and access privileges for all individuals or roles that access the cloud service offering (CSO)”*



FedRAMP® <Choose: High, Moderate, Low, LI-SaaS> Baseline System Security Plan (SSP)
<Insert CSP Name> | <Insert CSO Name> | <Insert Version X.X> | <Insert MM/DD/YYYY>

Table 11.1 <Insert CSO Name> Separation of Duties

Duty Description	Information Owner	Security officer	Privacy officer	Linux Admin	Windows Admin	Agency Admin	Agency Customer		
Adds/Removes Privileged Admins	X	X							
Adds/Removes Non-privileged Admins		X	X						
Adds/Removes Customer Privileged Admins									
Adds/Removes Customer Non-privileged Admins									
Enforces Physical Access Authorizations									
Defines Least Privilege Needed to Perform Tasks									
Reviews/Approves Policy									
Enforces Policy									

Template Instruction - *“If the CSO has many more duties and roles than what can fit within a table of this size, you may use an Excel spreadsheet and reference it as an appendix within the SSP and this section.”*

FedRAMP Rev 5 SSP - Missing Separation of Duties (cont'd)

GitHub Issue #534

Example

- Roles across the top
- Privileges down the left column
- Many-to-Many association between "roles" and "duties" (privileges)

Duty Description	HR	Accounting	Director	Manager	Employee
Request New Training - for Self					x
Request New Training - for Employee	x		x	x	
Approve Employe Training Requests			x	x	
Approve Manager Training Requests			x		
Procure Training		x			
Configure New Training Courses / Events	x				
Register for Approved Training				x	x
View Employee Training Records	x		x	x	

FedRAMP Rev 5 SSP - Missing Separation of Duties Guidance

GitHub Issue #534

Prior Proposals

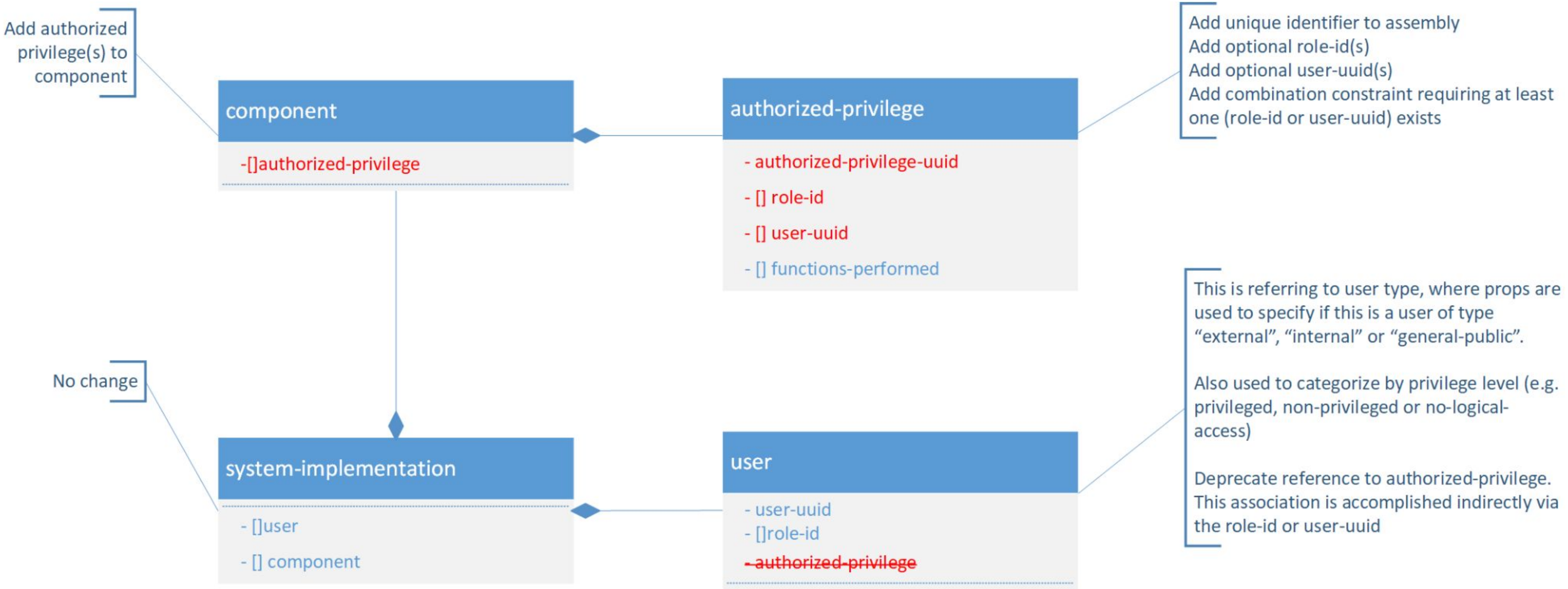
- Option #1 - See https://github.com/GSA/fedramp-automation/pull/548
- Option #2 - See https://github.com/GSA/fedramp-automation/pull/549
- Option #3 - See https://github.com/GSA/fedramp-automation/issues/534#issuecomment-1919916609

However, we realized that support for contextualizing separation of duties around components would be very useful.

FedRAMP Rev 5 SSP - Missing Separation of Duties Guidance

GitHub Issue #534

New Proposal



Add authorized privilege(s) to component

Add unique identifier to assembly
Add optional role-id(s)
Add optional user-uuid(s)
Add combination constraint requiring at least one (role-id or user-uuid) exists

No change

This is referring to user type, where props are used to specify if this is a user of type "external", "internal" or "general-public".

Also used to categorize by privilege level (e.g. privileged, non-privileged or no-logical-access)

Deprecate reference to authorized-privilege. This association is accomplished indirectly via the role-id or user-uuid

See sample OSCAL in draft PRs at https://github.com/GSA/fedramp-automation/pull/594 and https://github.com/GSA/OSCAL/pull/3

FedRAMP Rev 5 SSP - Missing Separation of Duties Guidance

GitHub Issue #534

Next Steps

- Community Review and Comment on DRAFT PRs ahead of next EAWG Meeting (June 5th, 2024)
    - See proposed Metaschema Changes - https://github.com/GSA/OSCAL/pull/3
    - See example implementation - https://github.com/GSA/fedramp-automation/pull/594
- FedRAMP automation team updates / finalizes proposal
- FedRAMP automation team to submit PR for consideration by NIST OSCAL team

Open Forum

Thank you

Our next OEAW virtual meeting will be on

Wednesday, June 5th, 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