FedRAMP

FedRAMP OSCAL Early Adopters

January 17th, 2024

GSA

info@fedramp.gov
fedramp.gov

Introduction

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

Outcomes:

- Shared understanding of Charter and Mission of the Workgroup
- Shared understanding of FedRAMP OSCAL package requirements, and discussion of possible enhancements and solutions.

Agenda:

- Welcome
- Guiding Principles/Mission Review
- OEAW Updates
- Issues Discussion
- Open Forum
- Next Steps & Closing

FedRAMP OEAW Guiding Principles

Keep the discussion respectful

Be curious, seek understanding

Speak from your own experience

Challenge through questions

Focus on ideas

Keep it technical

Goals and Current Priorities

Our goals:

- Provide a means for the PMO to accept OSCAL-based FedRAMP packages.
- Provide REST APIs for the submission of OSCAL-based FedRAMP packages and continuous monitoring data.
- Support reuse of FedRAMP authorizations using OSCAL-based FedRAMP packages.
- Provide tooling to support CSPs in the creation of valid OSCAL-based FedRAMP packages.
- Provide tooling to support 3PAOs and agencies in using OSCAL-based FedRAMP packages.

We need to focus on the following to achieve these goals:

- Local OSCAL validation tooling will allow validation of OSCAL content without the need to prematurely share sensitive data.
- Stabilizing the OSCAL guides is needed to support local validation tooling and the GRC acquisition.
- Need to reduce friction where possible in maintaining OSCAL guides and baselines as well as FedRAMP templates.

OEAW Workgroup Charter/Mission

Charter:

To create an engagement space for Cloud Service Providers, 3PAOs, tool developers and others who are adopting OSCAL for the FedRAMP® use case with the goal of refinement of FedRAMP automation technology and processes.

Mission Elements:

- Bring OSCAL early adopters together to foster community engagement around FedRAMP OSCAL use cases.
- Directly engage with OSCAL early adopter stakeholders to advance technology and processes supporting FedRAMP automation using OSCAL.
- Drive stakeholder feedback on GitHub issues relating to FedRAMP baselines, guides, validation, and other related efforts.
- **On hold:** Standardize RESTful APIs supporting machine-oriented, stakeholder interaction with FedRAMP.

OEAW Going Forward

FedRAMP needs the OSCAL Early Adopters Workgroup to help with:

- Continued identification of issues with the FedRAMP baselines, guides, and validations using GitHub issues.
- Submitting GitHub pull requests to fix defects in baselines, guides, and validations.
- Feedback on changes to FedRAMP baselines, guides, and validations through review of GitHub pull requests.
- Testing and refinement of new tooling supporting FedRAMP stakeholders.

https://github.com/GSA/fedramp-automation

General Updates

FedRAMP Automation Community Updates

January 17, 2024

NIST OSCAL version 1.1.x release

FedRAMP automation team is continuing to work to update all guidance and validations to align with OSCAL 1.1.1 release.

Revising OSCAL Guides

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

NIST SP 800-53 Revision 5.1.1

The NIST OSCAL content v1.2.1 release included backwards-compatibility breaking changes to the SP 800-53 rev5 catalog.

- Replacement of “labels” with “alt-identifiers”
- Removed non-padded labels
- PRs #542 and #545 adjusted FedRAMP baselines to point to OSCAL content 1.2.0 release

GitHub Issues

- Prioritizing issues related to FedRAMP Guide and SP 800-53 rev 5

Review Needed

github.com/GSA/fedramp-automation/pulls

- #540 Local version of SP 800-53 with zero padded labels
- #541 OSCAL Guides in markdown

Issues Discussion

FedRAMP Rev 5 SSP - Missing Separation of Duties Guidance

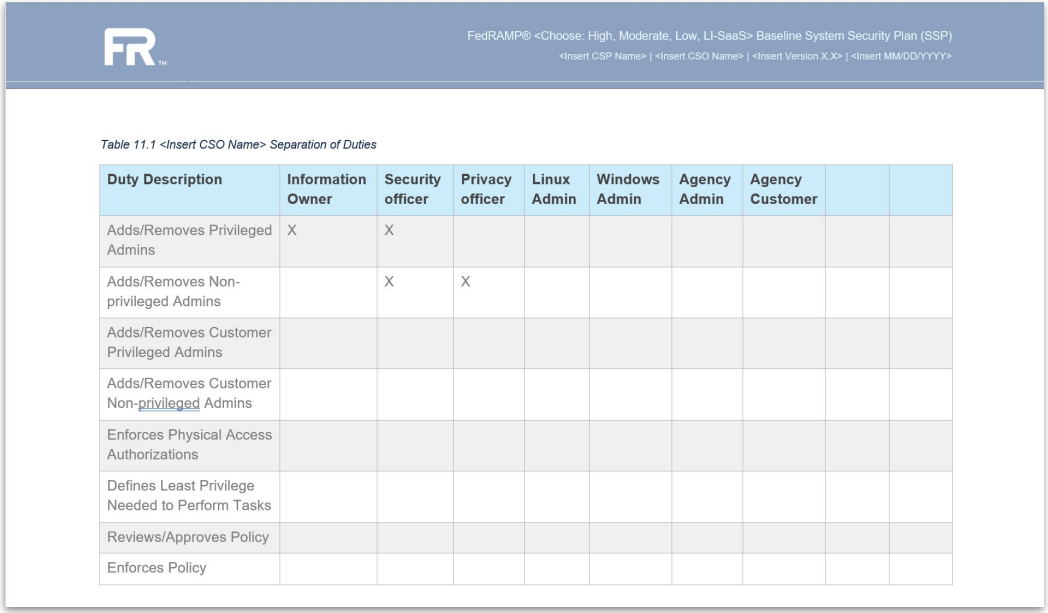
GSA/fedramp-automation#534

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)

GSA/fedramp-automation#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 (cont'd)

GSA/fedramp-automation#534

Example

- No clear / direct way to represent the relationship between authorized privileges and roles in OSCAL models

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

GSA/fedramp-automation#534

Workaround

- Provide separation of duties table as an attached spreadsheet
- In OSCAL:
  - ? ***resource*** in the ***back-matter***
  - ? FedRAMP ***prop***

```
3554          </resource>
3555          <!-- Section 11 - Separation of Duties -->
3556          <resource uuid="49fb4631-1da2-41ca-b0b3-e1b1006d4025">
3557             <title>Separation of Duties Matrix</title>
3558             <description>
3559                <p>Separation of Duties Matrix</p>
3560             </description>
3561             <prop ns="https://fedramp.gov/ns/oscal" name="type" value="separation-of-duties-matrix"/>
3562             <prop name="published" value="2023-01-01T00:00:00Z"/>
3563             <!-- document date -->
3564             <prop name="version" value="Document Version"/>
3565             <rlink href="./documents/Sep_Matrix.docx" media-type="application/msword"/>
3566             <base64 filename="Sep_Matrix.docx" media-type="application/msword">00000000</base64>
3567             <remarks>
3568                <p>May use <code>rlink</code> with a relative path, or embedded as <code>base64</code>.</p>
3569             </remarks>
3570          </resource>
3571       </back-matter>
3572    </system-security-plan>
```

See FedRAMP-SSP-OSCAL-Template.xml for example

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

GSA/fedramp-automation#534

Option 1

- Add ***authorized-privilege*** assembly to ***system-implementation***
- Add ***responsible-role*** construct to ***authorized-privilege***
- Add constraint on ***@role-id***
- In future, consider deprecating ***authorized-privilege*** in ***user*** assembly

Pros

- Define each authorized privilege once and reference
- Privileges follow **role**. Assigning a user a new role, grants privileges.
- A **user** can be directly assigned a privilege.

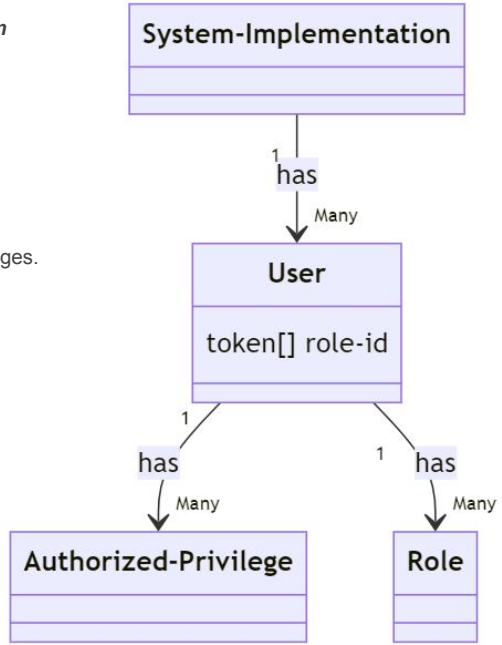
Cons

- Ambiguity (***user*** and ***system-implementation*** both reference ***authorized-privilege***)

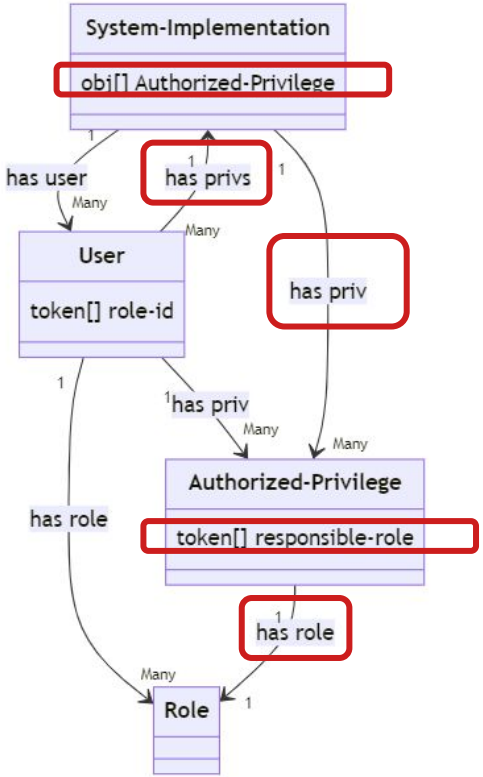
See proposed Metaschema change at
https://github.com/GSA/OSCAL/tree/feature-enhance-roles-option1

See sample OSCAL in Draft PR at
https://github.com/GSA/fedramp-automation/pull/548

BEFORE



AFTER



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

GSA/fedramp-automation#534

Option 2

- Add ***responsible-role*** construct to ***authorized-privilege***
- Add constraint on ***@role-id***

Pros

- Relatively minor change

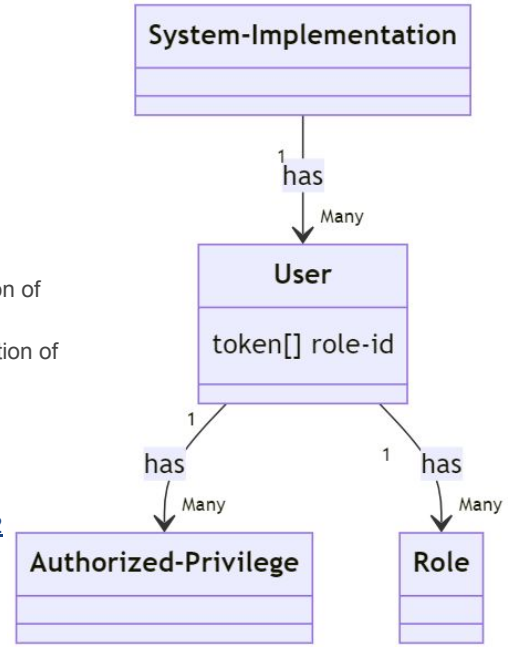
Cons

- Requires ***user***, which may not be necessary for separation of duty
- Privileges are bound to the **user**. Likely results in duplication of privileges.

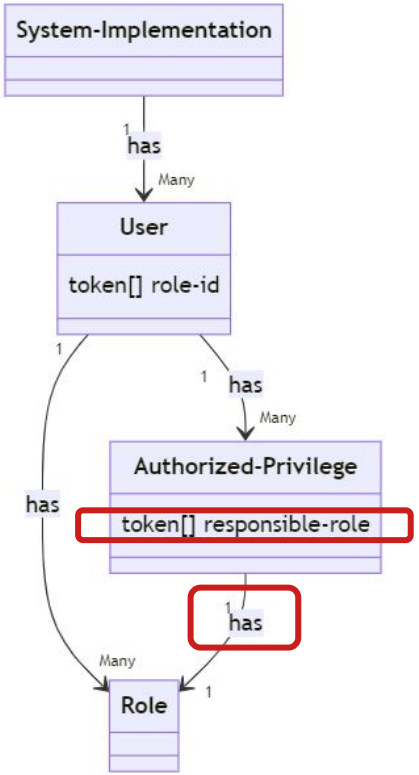
See proposed Metaschema change at
https://github.com/GSA/OSCAL/tree/feature-enhance-roles-option2

See sample OSCAL in draft PR at
https://github.com/GSA/fedramp-automation/pull/549

BEFORE



AFTER



Open Forum

Next Steps

Thank you

Our next OEAW virtual meeting will be on

Wednesday, January 31st, 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