FedRAMP

FedRAMP OSCAL Early Adopters

June 5th, 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 updated 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 (cont'd)
- Separation of Duties: Proposed Changes to OSCAL SSP model
- 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

General Updates

FedRAMP Automation Community Updates

June 5, 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 June 2024

Local Validation Tooling

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

GitHub Issues

Prioritized the following:

- Issue #592 - Refactoring CI to use the OSCAL CLI
- Issue #598 - Setting up test harness and framework to automate testing of OSCAL CLI
- Issue #599 - HTML guides and automation website pre-release updates
- Issue #558 - Mismatch of params (ODPs) / printables guidance
- Issue #534 - Separation of Duties

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

Planned Updates

- Adding a 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)" />
    - Will update PR #574 as these changes are made to the profiles.
- Developing a FedRAMP OSCAL SSP “printable,” open-source reference implementation.
  - Will add guidance into the new HTML guides once the https://automate.fedramp.gov site is launched.

Separation of Duties

Proposed Changes to OSCAL SSP Model

FedRAMP Rev 5 SSP - Separation of Duties Revised Proposal

GitHub Issue #534

Issue:

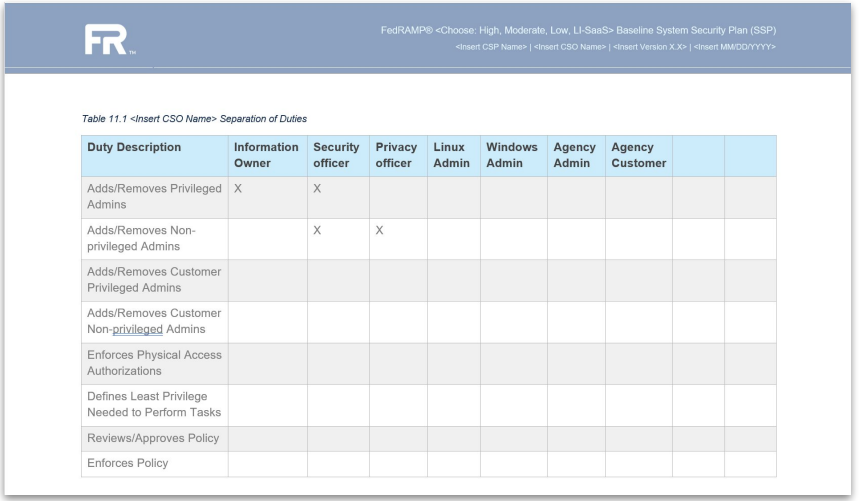
Need an approach for how to represent FedRAMP required separation of duties information in OSCAL

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)*"

Proposed Updates to OSCAL SSP Model:

Need to ensure proposed updates are backwards compatible



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

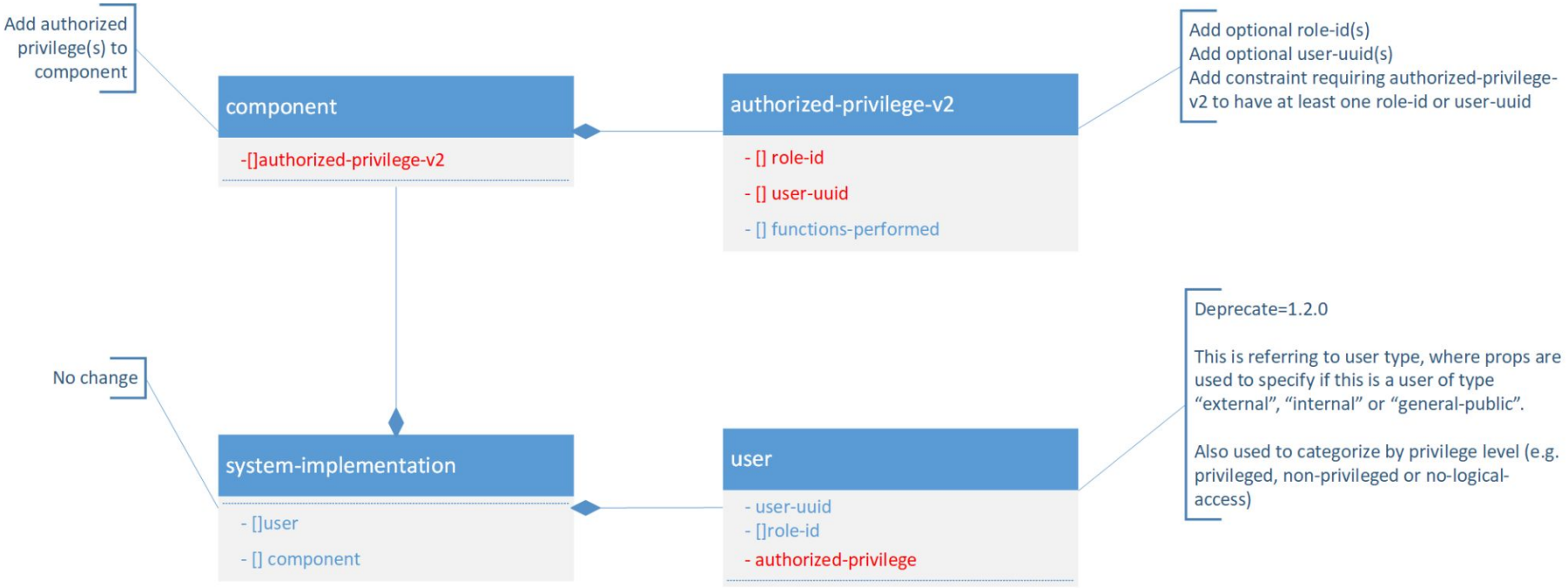
<Insert CSP Name> | <Insert CSO Name> | <Insert Version X.X> | <Insert MM/DD/YYYY>

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									

FedRAMP Rev 5 SSP - Separation of Duties Revised Proposal

GitHub Issue #534



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 - Separation of Duties Revised Proposal

GitHub Issue #534

```
<!-- SEPARATION OF DUTIES EXAMPLE-->
<!-- Components -->
<!-- OSCAL requires existance of a "this-system" component -->
<component uuid="60f92bcf-f353-4236-9803-2a5d417555f4" type="this-system">
   <title>This System</title>
   <description>
      <p>The entire system as depicted in the system authorization boundary</p>
      <p>Email is employed</p>
   </description>
   <status state="operational"/>
   <authorized-privilege-v2>
      <title>Request New Training - for self</title>
      <function-performed>Authorizes access to request training (for self) from the catalog.</function-performed>
      <role-id>"employee"</role-id>
   </authorized-privilege-v2>
   <authorized-privilege-v2>···
   </authorized-privilege-v2>
   <authorized-privilege-v2>
      <title>Approve Employee Training Request</title>
      <function-performed>Authorizes access to approve employee training requests</function-performed>
      <role-id>"manager"</role-id>
      <role-id>"director"</role-id>
      <!-- alternatively, can associate with director user instead of role -->
      <user-uuid>ba7708c1-4041-48ab-9b7b-1ddb5e175fe0</user-uuid>
   </authorized-privilege-v2>
   <authorized-privilege-v2>
      <title>Approve Manager Training Request</title>
      <function-performed>Authorizes access to approve manager training requests</function-performed>
      <role-id>"director"</role-id>
      <!-- alternatively, can associate with director user instead of role -->
      <user-uuid>ba7708c1-4041-48ab-9b7b-1ddb5e175fe0</user-uuid>
   </authorized-privilege-v2>
   <authorized-privilege-v2>
      <title>Procure Training</title>
      <function-performed>Authorizes access to set billing information</function-performed>
      <function-performed>Authorizes access to execute purchase of training modules</function-performed>
      <role-id>"accounting"</role-id>
```

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 - Separation of Duties Revised Proposal

GitHub Issue #534

Updates to Proposal #4

- Ensure backwards compatibility.
  - Created a new **authorized-privilege-v2** assembly.
  - Added constraint on **authorized-privilege-v2** assemblies to either have a **role-id** or **user-uuid**.
  - Rolled back addition of **uuid** flag in the **authorized-privilege** assembly.
  - Updated the **authorized-privilege** assembly with a **deprecated** flag (version 1.2.0).
- Supports both *user-centric* and *component-centric* definition of authorized-privileges.
- Allows association of association of authorized privileges with role, users, or both.

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

Open Forum

Thank you

Our next OEAW virtual meeting will be on

Wednesday, June 19th, 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