FedRAMP

FedRAMP OSCAL Early Adopters

February 28th, 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 FedRAMP activities related to OSCAL.
- Shared understanding of current OSCAL issues in the SSP template and how to best handle them.

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

General Updates

FedRAMP Automation Community Updates

February 28, 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.

- Prioritizing SP 800-53 Rev 5 related issues
- Working to make guide development more collaborative

Planned Merges

- PR#540 - Local version of SP 800-53rev5.1.1 (zero padded control IDs)
- PR#557 - Containerized user guides

Other PRs

- PR#541 - Markdown User Guides

Issue #1 Discussion

FedRAMP Rev 5 SSP - Missing Separation of Duties Guidance

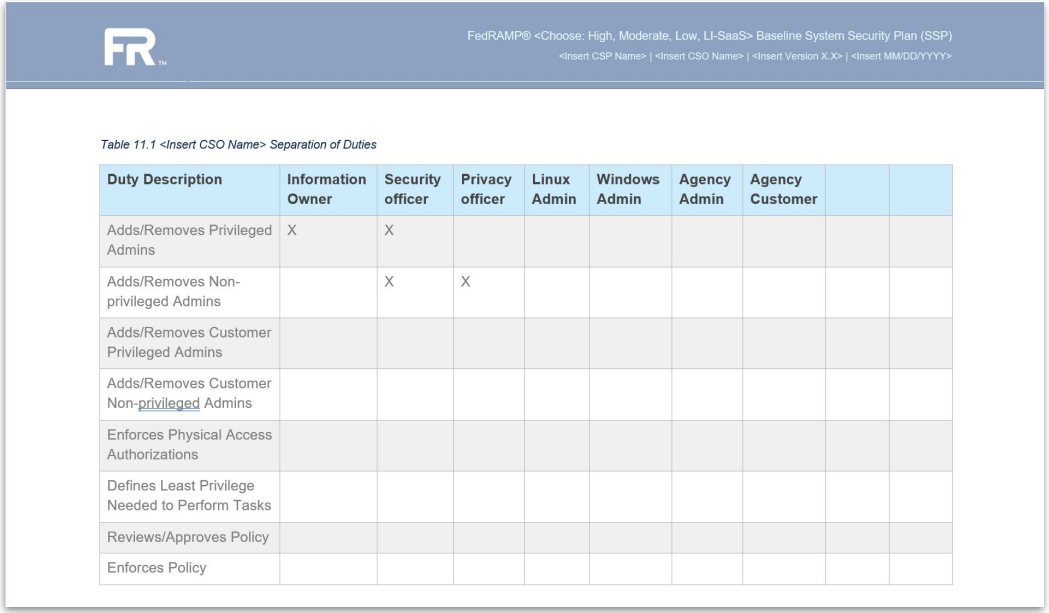
GSA/fedramp-automation#534

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

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.

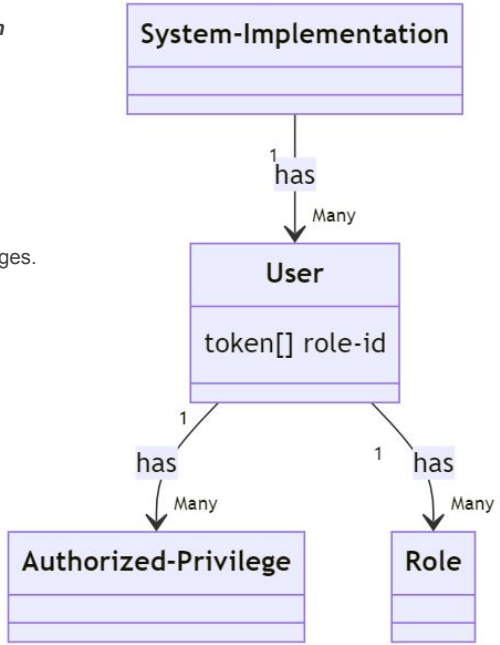
Cons

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

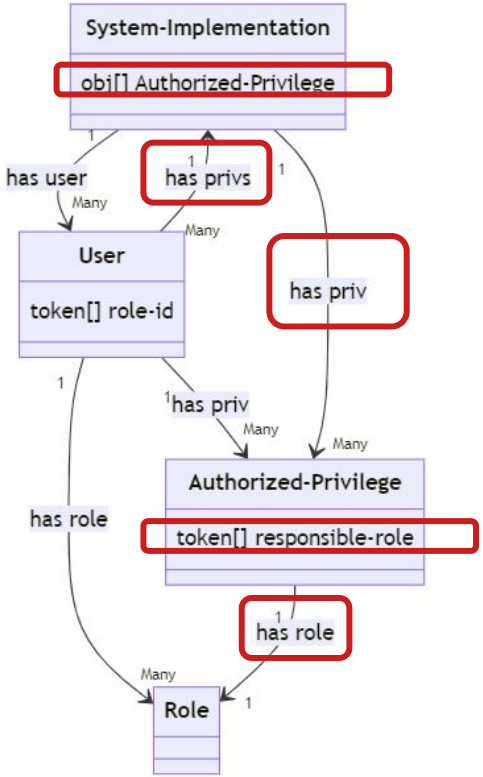
See proposed Metaschema change at
https://github.com/GSA/OSCAL/tree/feature-enhance-roles-option1

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

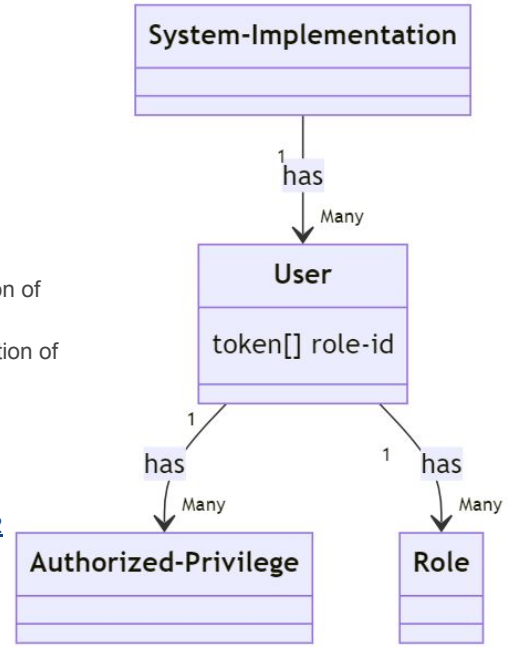
Cons

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

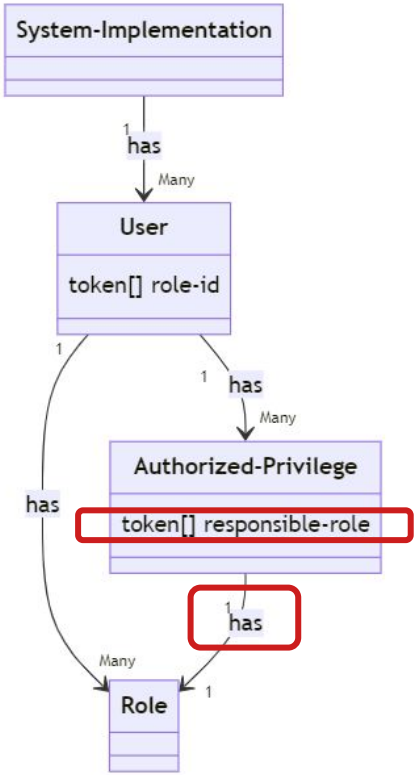
See proposed Metaschema change at
https://github.com/GSA/OSCAL/tree/feature-enhance-roles-option2

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

BEFORE

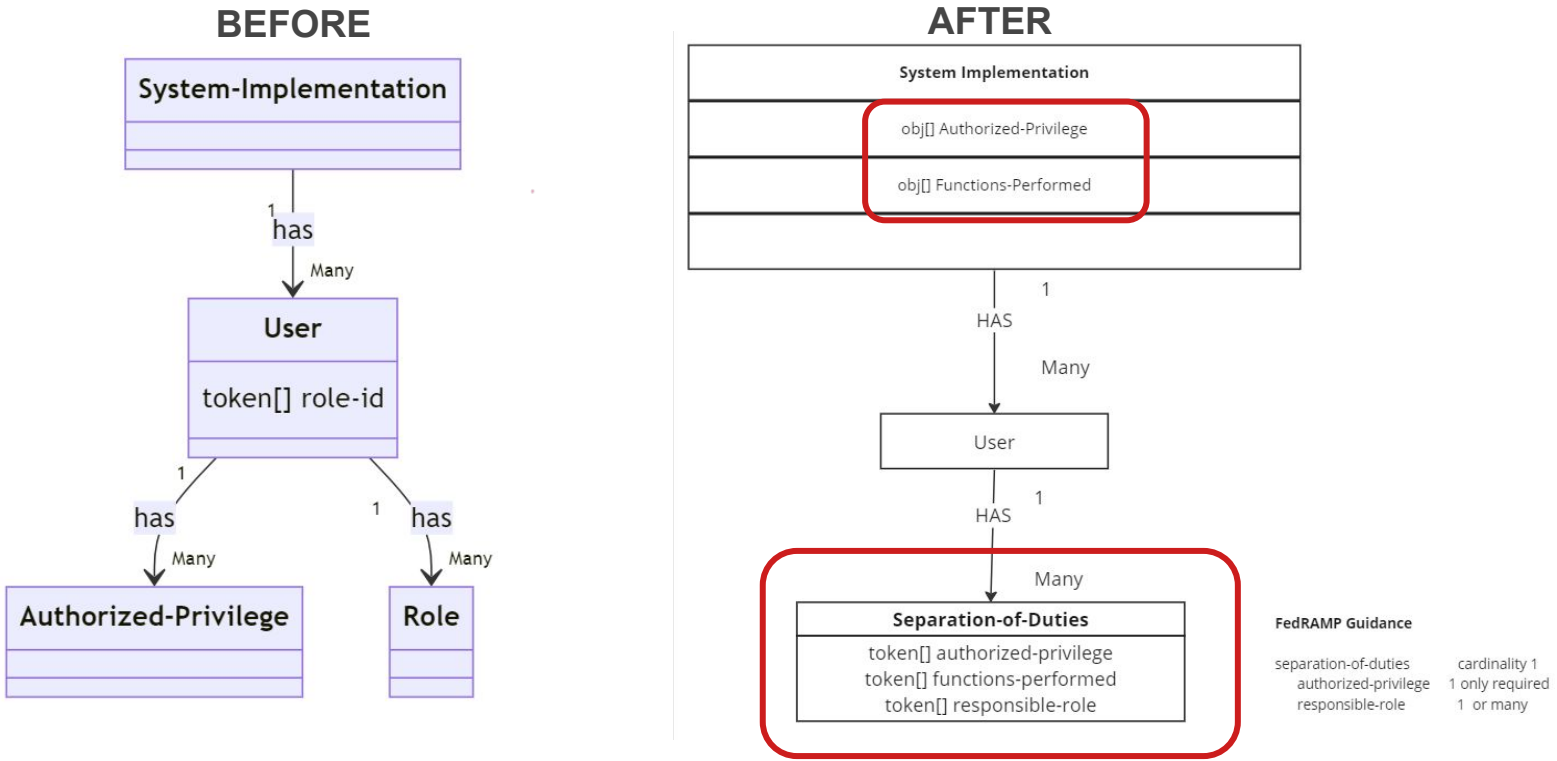


AFTER



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

Community Proposed Solution #3



Issue #2 Discussion

FedRAMP SSP Appendix Content

FedRAMP Rev 5 SSP Appendices

- ***Appendix A: FedRAMP Security Controls ****
- Appendix B: Related Acronyms
- Appendix C: Security Policies and Procedures
- Appendix D: User Guide
- ***Appendix E: Digital Identity Worksheet ****
- Appendix F: Rules of Behavior
- Appendix G: Information System Contingency Plan (ISCP)
- Appendix H: Configuration Management Plan (CMP)
- Appendix I: Incident Response Plan (IRP)
- ***Appendix J: CIS and CRM Workbook ****
- ***Appendix K: FIPS 199 Worksheet ****
- Appendix L: CSO-Specific Required Laws and Regulations
- ***Appendix M: Integrated Inventory Workbook ****
- Appendix N: Continuous Monitoring Plan
- ***Appendix O: POA&M ****
- Appendix P: Supply Chain Risk Management Plan (SCRMP)
- ***Appendix Q: Cryptographic Module Table ****

FedRAMP SSP Appendix Content

FedRAMP Rev 5 SSP Appendices - Planned Updates

- **Markdown SSP User Guide**
  - Ensure clear examples are provided for all appendices (A - Q)
  - Add page indexes & hard links for enhanced reference to examples
- **OSCAL SSP Template**
  - Ensure clear examples are provided for all appendices (A - Q)

Issue #3 Discussion

Parameter Mismatch in SSP Template vs OSCAL Baseline

Github Issue #558

- **SSP Word Template**
  - For dash-1 controls (e.g. AC-1), the first parameter (e.g. "Parameter AC-1(a)") maps to the aggregate parameter id "ac-1_prm_1".
    - In the OSCAL catalog, “ac-1_prm_1” aggregates "ac-01_odp.01 and ac-01_odp.02"
- **OSCAL to Human-Readable Conversions**
  - The current structure makes it possible to convert from the more granular OSCAL parameters to the aggregate (e.g. when rendering into human-readable formats)
- **SSP (Word) Template to OSCAL Conversions**
  - The current structure makes it challenging to automatically convert human readable SSP (parameters) into OSCAL

Parameter Mismatch in SSP Template vs OSCAL Baseline (Cont'd)

Github Issue #558

- **FedRAMP Defined and Constrained Parameters**
  - Of the controls with aggregated parameters, only SA-15 has a FedRAMP constraint
- **Recommendation / Guidance**
  - FedRAMP OSCAL SSPs must provide the granular "ODP" level parameters. This will be clarified in the User Guides and sample OSCAL SSP template
  - Development of guidelines around generating the SSP Word Template

Open Forum

Thank you

Our next OEAW virtual meeting will be on

Wednesday, March 13th, 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