FedRAMP

FedRAMP OSCAL Implementers

December 18, 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 roles and responsibilities as it relates to OSCAL

Agenda:

- Welcome
- OSCAL Implementers General Updates
- OSCAL Roles & Responsibilities 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

- **SSP Constraints**
  - Significant advancement in various SSP constraint areas
  - Detailed briefings planned for upcoming sessions
- **FedRAMP OSCAL Requirements Refinements**
  - Enhanced tracking of control implementation by component
  - Improving component-based information type and data flow
  - Control Origination
- **Bug Reports**
  - Thanks for bug reports (#977 and #1009)
- **Stay Informed**
  - View the project workboard for more details on ongoing work and upcoming priorities (https://github.com/orgs/GSA/projects/25/views/2)

Important Changes for FedRAMP OSCAL

ADR #11 Approved

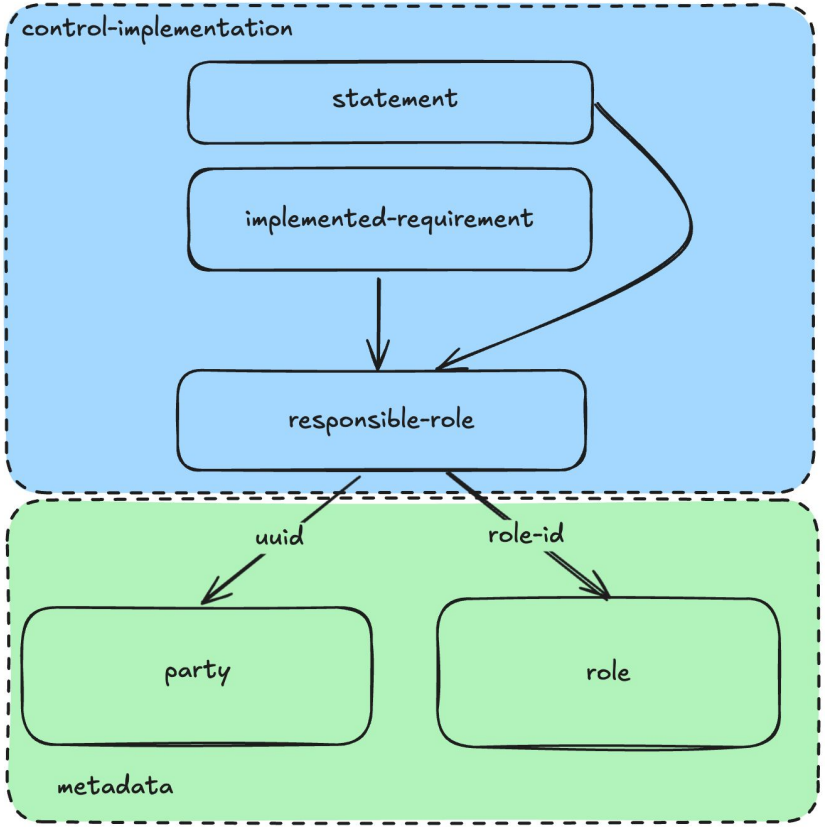
- Aligning extension property and misc identifier requirements for the official FedRAMP namespace
  - One common URI for FedRAMP ***identifier-type***, ***system*** facet attribute and FedRAMP extension property ***namespaces***
  - We reviewed pull requests #102 and #828, they are ready for merge.
  - We will **deploy updated docs and constraints this week,** but first we will:
    - Update these pull requests (you can subscribe to notifications).
    - Send an email to our mailing list oscal-implementer@fedramp.gov.

Deeper Dive into Roles & Responsibilities in OSCAL

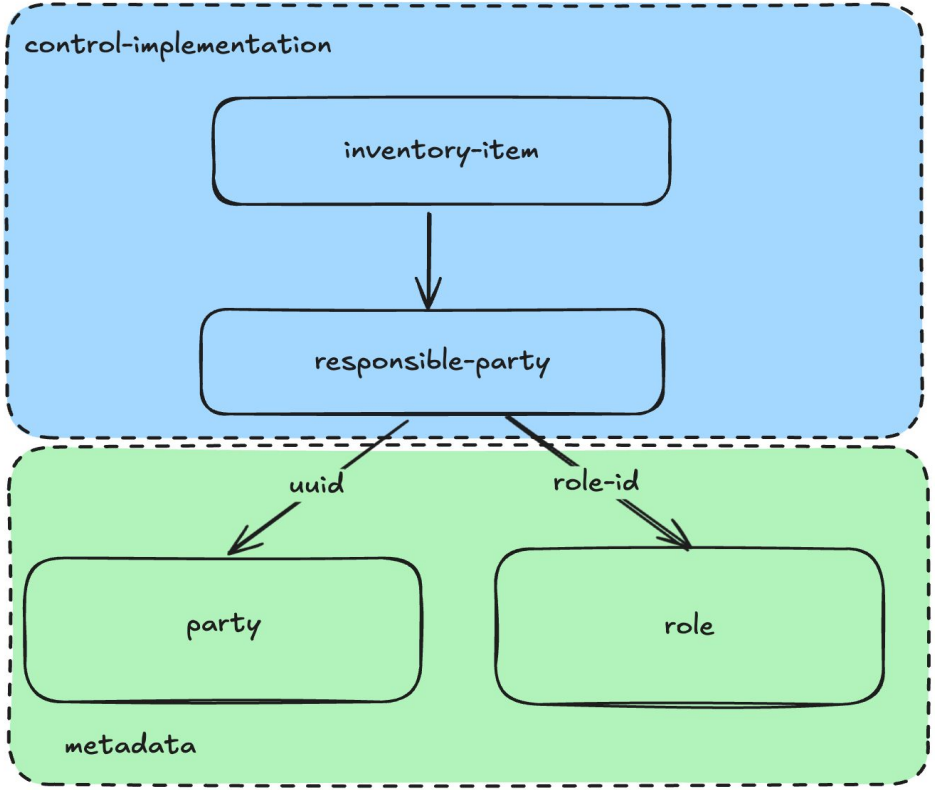
Parties, Roles, and Responsibility in OSCAL

- Parties: Can be people or organizations & can be linked together
  - I.e. “Simon” is his own party, and can be a member of party “AwesomeCloud”
- Roles: Think job title - one party can have multiple roles
  - I.e. Simon could be ”system owner,” “authorizing official,” and “privacy point of contact”
- Responsibilities: Every control needs to have either a responsible party or a responsible role
  - I.e. AC-3, access enforcement, must have either a party or role that is accountable for it
  - Responsible party could be Simon, or AwesomeContractor
  - Responsible role could be “information system security officer”

An Illustration



An Illustration (cont.)



Why Does FedRAMP Care About This?

- Accountability:
  - Clear ownership ensures tasks are completed, prevents delays or gaps in addressing security issues
- Risk Management:
  - Reduces risk of overlooked vulnerabilities, insider threats
- Security Principles:
  - Aligns with separation of duties, least privilege, and shared responsibility principles
- Incident Response:
  - Enables swift containment and prevents delays caused by unclear responsibilities

What Were Old Responsibility Parties Like?

AC-2 Control Summary Information
Responsible Role:
Parameter AC-2(c):
Parameter AC-2(d)(3):
Parameter AC-2(e):
Parameter AC-2(f):
Parameter AC-2(h):
Parameter AC-2(h)(1):
Parameter AC-2(h)(2):
Parameter AC-2(h)(3):
Parameter AC-2(i)(3):
Parameter AC-2(j):
Implementation Status (check all that apply):

What Were Old Responsibility Parties Like?

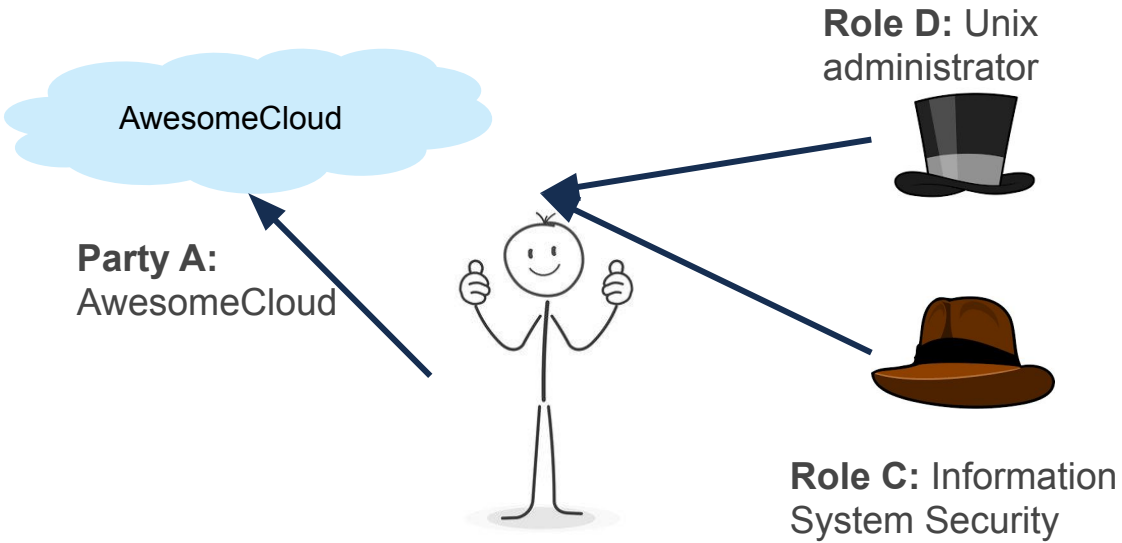
Duty Description	Information Owner	Security officer	Privacy officer	Linux Admin	Windows Admin	Agency Admin	Agency Customer		
Adds/Removes Privileged Admins	X	X							
Adds/Removes Non-privileged Admins		X	X						

How is OSCAL an Improvement?

- ➔ Allows for explicit definitions of roles and parties
- ➔ Allows for tight linkage between a person, the org they are a part of, their role, and the controls they are responsible for
  - ◆ No more flipping back and forth in spreadsheets
- ➔ OSCAL creates a graph that can represent the complexity of today's systems
- ➔ If that graph doesn't link up in an appropriate way (i.e. no party assigned to a role), we throw an error

Example Scenario

➔ Look, it's Simon in the metadata!



Implemented Requirement
AC-3: Access Enforcement

- **Responsible Party:** B

~or~

- **Responsible Role:** C

Let’s Have a Responsibility Party with Code!

NIST OSCAL models have their own internal constraints for party, responsible-party, role, and responsible-role.

- `index-metadata-role-id` (in SSP metadata; implemented-requirement; inventory-item)
- `index-metadata-party-uuid` (in SSP metadata; implemented-requirement; inventory-item)

FedRAMP builds on top of these constraints, analyzing party, role, and responsible-party relations.

- `role-defined-prepared-for`
- `responsible-party-prepared-for`
- `responsible-party-is-person`
- `role-defined-information-system-security-officer`

Open Forum

Thank you

Please be on the lookout for new calendar invites in the coming year

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