FedRAMP

FedRAMP OSCAL Early Adopters

May 8th, 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 the FedRAMP Roadmap and upcoming pilot efforts
- Shared understanding of FedRAMP layout and formatting guidance for generated SSPs
- Alignment around any community issues and an understanding of next steps.

Agenda:

- Welcome
- OEAW General Updates
- FedRAMP Roadmap Update on Digital Authorization Packages
- Guidance on Rendering Printables based on OSCAL
- 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

May 8, 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.

- Newer version of Hugo USWDS theme (PR#581)
- Restructuring of content to provide better integration of general vs model-specific guide content (PR#581)
- Ensure all FedRAMP OSCAL validation rules and constraints are documented
- Diagrams as Code - starting to evaluate use of PlantUML for OSCAL model diagrams in documentation

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 #534 - Separation of Duties
- Issue #555 - Update FedRAMP-SSP-OSCAL-Template.xml based on NIST SP 800-53 rev5.1.1 release
- Issue #558 - Mismatch of params (ODPs) / printables guidance
- 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

FedRAMP Roadmap Update

Digital Authorization Packages

Automation and technology- forward operations

Support machine-readable **“digital authorization packages”**

Our strategy:

- Work collaboratively with OSCAL community on establishing the foundation for creating “digital authorization packages”
- Engage in pilot project(s) initially focused on the OSCAL-based (rev 5) SSP as the essential component of digital authorization package:
  - SSP front-matter
  - Appendix A - FedRAMP Security Controls
  - Appendix E - Digital Identity
  - Appendix J - CIS/CRM
  - Appendix K - FIPS 199
  - Appendix M - Integrated Inventory
  - Appendix Q - Cryptographic Modules
  - Section 11 - Separation of Duties
- Initial focus on most common SSP deficiencies that lead to review delays

Automation and technology- forward operations

Support machine-readable **“digital authorization packages”**

Our goals:

- **Provide Guidance:** Provide accurate, clear, and actionable guidance on producing an OSCAL-based SSP, focusing on common quality problem areas to increase overall quality of SSPs produced by CSPs
- **Provide Richer System Context:** Provide a means to support additional validations and completeness checks by describing the system context in a richer form, using OSCAL SSPs
- **Define Digital Authorization Package Composition:** Gain an understanding of the critical components that need to be supported in digital authorization packages
- **Review Standardization:** Provide a (documented) list of validations that must be checked prior to SSP submission, setting FedRAMP expectations for digital authorization packages
- **Automate Validation Checks:** Reduce review timeframes and improve consistency by automating certain validations, which reduces human effort and detects issues earlier in the process

Automation and technology- forward operations

Support machine-readable **“digital authorization packages”**

Our *tentative* timeline:

- **Pre-Pilot Work (now - August)**
  - Address technical debt
  - Tool bootstrapping
  - Publish pilot details
  - Launch automate.fedramp.gov
- **Pilot Execution Sprints (August)**
  - Each sprint will focus on prioritized 1-2 primary areas of work
- **Initial MVP (September)**
  - Significant guide improvements (SSP focused)
  - Initial validation MVP releases (SSP focused)
  - Website updates
- **Continued Refinement & Additional MVPs (December)**
  - Additional releases

Automation and technology-forward operations

FedRAMP Pilot Experience Form

- FedRAMP is looking for partners (CSPs, tool suppliers, federal agencies, 3PAOs, and others) to participate in **targeted pilot projects** that will advance the program's ability to operationalize its OSCAL-based automation capabilities

- Please stand by if your organization would like to participate in any FedRAMP pilot projects

Parameter Mismatch in SSP Template

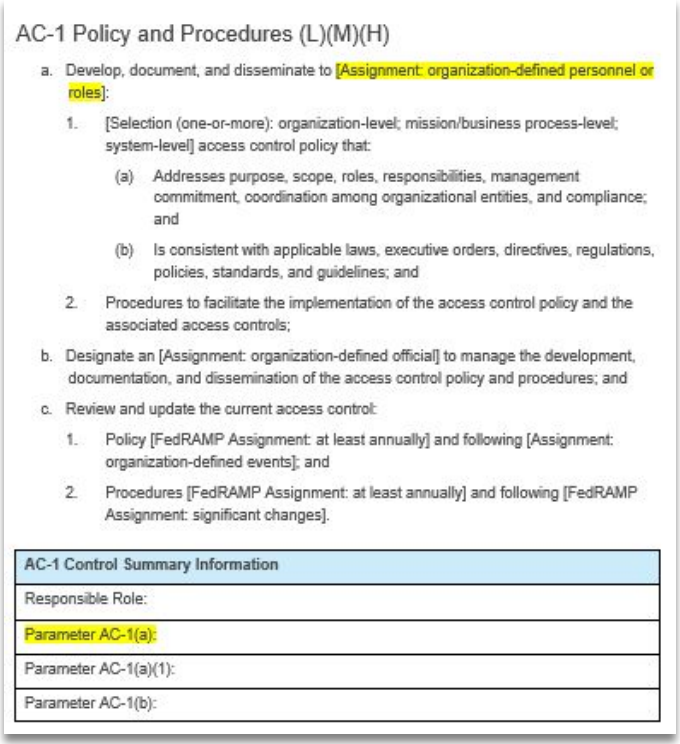
Guidance on Rendering Printables based on OSCAL

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"
  - “ac-01_odp.01” is related to policy and “ac-01_odp.02” is related to procedure.



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].

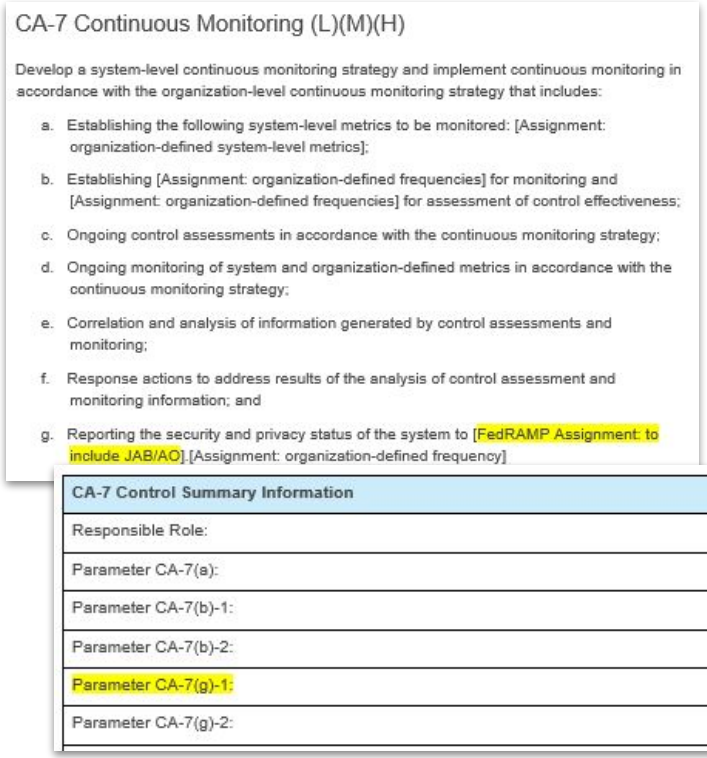
AC-1 Control Summary Information
Responsible Role:
Parameter AC-1(a):
Parameter AC-1(a)(1):
Parameter AC-1(b):

Parameter Mismatch in SSP Template vs OSCAL Baseline

Github Issue #558

SSP Word Template

- Several other instances, such as CA-7 where parameter ca-7_prm_4 is an aggregates “ca-07_odp.04” which is related to security and “ca-07_odp.06” which is related to privacy.



CA-7 Continuous Monitoring (L)(M)(H)

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];

b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to [FedRAMP Assignment: to include JAB/AO].[Assignment: organization-defined frequency]

CA-7 Control Summary Information
Responsible Role:
Parameter CA-7(a):
Parameter CA-7(b)-1:
Parameter CA-7(b)-2:
Parameter CA-7(g)-1:
Parameter CA-7(g)-2:

Parameter Mismatch in SSP Template vs OSCAL Baseline

Github Issue #558

OSCAL to Human-Readable Conversions

- Additionally, the community needed guidelines around generating SSP Word Templates
  - How should parameters be displayed in printables? Aggregated or as individual ODPs?
  - What parameter identifiers should be displayed in printables (e.g., sp800-53a label such as AC-01_ODP[01])?

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

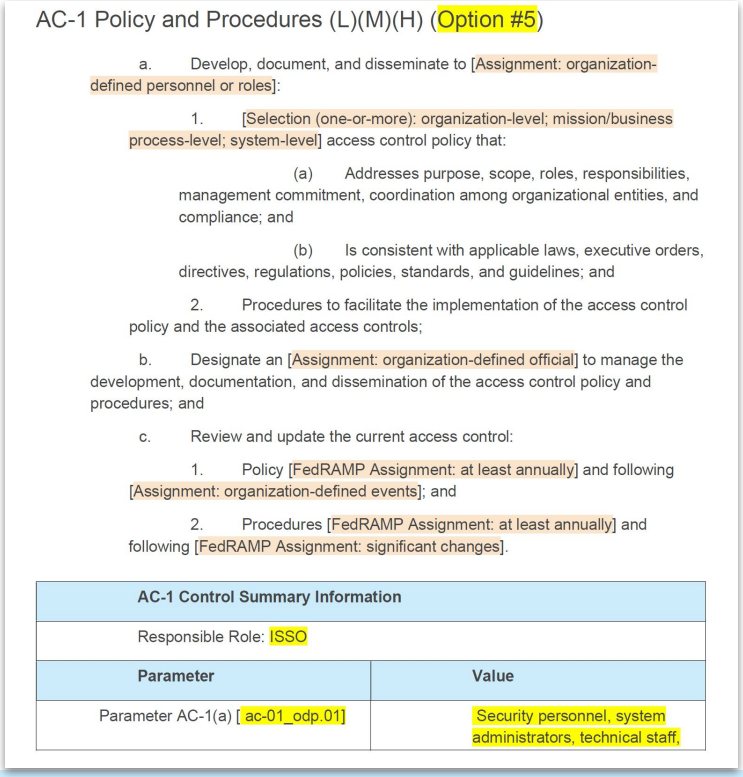
Github Issue #558

FedRAMP OSCAL Profile Update

- Realigned parameter constraints with corresponding ODPs
  - Draft PR #574 pending review - https://github.com/GSA/fedramp-automation/pull/574

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



AC-1 Policy and Procedures (L)(M)(H) (Option #5)

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	**Value**
Parameter AC-1(a) [ac-01_odp.01]	Security personnel, system administrators, technical staff,

Open Forum

Thank you

Our next OEAW virtual meeting will be on

Wednesday, May 22nd, 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