FedRAMP

OSCAL Developer Data Bites

October 26, 2023

GSA

info@fedramp.gov
fedramp.gov

Introduction

Purpose: To create space for dialogue between developers who use OSCAL and the FedRAMP® automation team.

Outcomes:

- Shared understanding of Documentation and Validation requirements for Rev 5.
- Productive discussion around OSCAL.

Agenda:

- Welcome
- Pre-Submitted Q&A
- FedRAMP Automation Community Updates
- Documentation and Validation Requirements
- Open Forum
- Next Steps & Closing

Data Bites Guiding Principles

Keep the discussion respectful

Be curious, seek understanding

Speak from your own experience

Challenge through questions

Focus on ideas

Keep it technical

Pre-Submitted Questions

Pre-Submitted Questions

Question:

When converting MS Word based SSP's for pre-existing authorized CSP's to OSCAL SSP files, what is the PMO's guidance on preserving the "Document Revision History?" If this needs to be preserved, what is the guidance on converting legacy MS Word versions to OSCAL?

Answer:

We currently do not have guidance for this, however, OSCAL allows SSP authors to define and specify version numbers for their OSCAL SSPs. That means SSP authors can use the same version numbers for their legacy Word SSPs and the corresponding (converted) OSCAL SSP. but this is not required at the moment.

While FedRAMP currently does not mandate this, there are also several other ways that CSPs can establish a linkage between a converted OSCAL SSP and its source legacy Word SSP, including "prop" or "remark" elements in the OSCAL document revision, and "links" in the OSCAL metadata.

Pre-Submitted Questions

Question: POAM Guide: 4.3 Recommended and Planned Remediation - Lifecycle?

The document explains there must be a response assembly should have a type flag set to "recommendation" or "planned" within the risk assembly. The guide also notes that accepted value of 'type' field within 'remediation issue' are recommendation or planned. However, in the representation example, instead of 'type' field, 'life cycle' field is represented.

Could you clarify if 'life cycle' field is something we should also create/add on top of risk > response > type field? Or should we only define field within the response assembly? It is bit confusing.

Answer:

The field name should be lifecycle. Per @Rene2mt the documentation will be updated for Rev 4 and Rev 5 POAM guides. In NIST JSON outline, there is a type field, whereas in the NIST XML outline there is not. We see the confusion and are going to address with NIST as to why type is in JSON but not in XML (David Waltermire may have some insight).

Pre-Submitted Questions

Question/Issue: Document Templates alignment with OSCAL (Rev 5)

Multiple tickets opened on Github (fedramp-automation) repository related to this subject. Causing confusion among adopters of OSCAL (CSPs, 3PAOs and Tool Vendors)

Answer:

Templates are designed for manual entry and generation of Word/PDF versions is problematic because OSCAL data is broken down at a more detailed level (See example below). Adopters are trying to use the Templates as a guide for mapping OSCAL and to generate Word versions (problematic).

CIS Workbook/SSP Appendix A

FedRAMP-MODERATE Control Implementation Summary (CIS) Worksheet (Rev 5)						
Control ID	Implementation Status					C
	Implemented	Partially Implemented	Planned	Alternative	N/A	S
AC-1 (a)						
AC-1 (b)						
AC-1 (c)						

AC-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

Access Control

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 every 3 years] and following [Assignment: organization-defined events]; and
   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

Pre-Submitted Questions

Document Templates alignment with OSCAL (Rev 5) (Continued)

This issue has been discussed with PMO Documentation Team (10/16/2023). We are looking at a solution for the Rev 5 guides, Templates and resolved-profile-catalogs that will address PMO's concern for ease of use of templates as well as OSCAL requirements. Until then, PMO has agreed to accept documents (SSP Appendix A, CIS Workbook, etc) with the lower level of detail in them (See example below)

AC-1 What is the solution and how is it implemented?
Part a:
Part a1:
Part a1a:
Part a1b:
Part a2:
Part b:
Part c:
Part c1:
Part c2:

FedRAMP Automation Community Updates

October 26, 2023

NIST OSCAL version 1.1.x release

- FedRAMP automation team has completed its impact analysis and will include this schema update in v2.3 release of portal.

Rev. 4 & Rev 5

- FedRAMP OSCAL Early Adopters Workgroup (OEAW) is progressing and has completed Phase 2 (Artifact Management- a.ka. Compressed file submissions).
- Next Meeting: Phase 3 Start (Document and Artifact Management). Focus on package upload, validation and content
- Additions to Rev 5 profiles and resolved-profile catalogs in process for core controls and response points to be released shortly. (See PR #502)

Issues/Ticket Tags

- **Closed issues/pull requests this cycle**
  - Total of 13 issues closed this cycle. (See github.com/GSA/fedramp-automation/issues) for more details.
- **Opened this cycle**
  - 4 new tickets opened this cycle. (See github.com/GSA/fedramp-automation/issues) for more details.

Announcements

- Additions and Transition of resources onto FedRAMP Automation Project.
  - Welcome David Waltermire and Ryan Palmer

Documentation and Validation Requirements Part 1

PMO Required Backmatter Resources and Documents

Rev 5 (System Security Plan)

- SSP Appendix A - FedRAMP Security Controls(implemented-requirements section of OSCAL).
- SSP Appendix C - Security Policies and Procedures (covering all control families)
- SSP Appendix E - Digital Identity Worksheet
- SSP Appendix G - Information System Contingency Plan (ISCP)
- SSP Appendix H - Configuration Management Plan (CMP)
- SSP Appendix I - Incident Response Plan (IRP)
- SSP Appendix J - CIS and CRM Workbook
- SSP Appendix K - FIPS 199 Worksheet (system-information section of OSCAL SSP)
- SSP Appendix M - Integrated Inventory Workbook (inventory/components sections of OSCAL)
- SSP Appendix N - Continuous Monitoring Plan
- SSP Appendix O - POA&M (Separate OSCAL artifact)
- SSP Appendix P - Supply Chain Risk Management Plan (SCRMP)
- SSP Appendix Q - Cryptographic Modules Table (New)

To Be Continued...

Open Forum with Dave

Thank you

Our next Developer Data Bites virtual meeting will be on

Thursday, November 30, 2023 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

OSCAL Resources

NIST:

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

Validations work: https://github.com/18F/fedramp-automation/tree/master/src/validations

Web based validation tool:

https://federalist-2372d2fd-fc94-42fe-bcc7-a8af4f664a51.app.cloud.gov/site/18f/fedramp-automation/#/documents/system-security-plan