FedRAMP

OSCAL Developer Data Bites

May 2, 2024

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 the short-term strategy and goals for certain milestone in the FedRAMP roadmap
- Alignment around how OSCAL and automation fit into the future landscape of the PMO
- Productive discussion around OSCAL

Agenda:

- Welcome
- General Updates
- FedRAMP Automation Community Updates
- Pre-Submitted Q&A
- Deep Dive into FedRAMP Future Roadmap
- Open Forum
- Next Steps & Closing

Data Bites Guiding Principles

Keep the discussion respectful

Speak from your own experience

Focus on ideas

Be curious, seek understanding

Challenge through questions

Keep it technical

General Updates

FedRAMP Automation Community Updates

May 2, 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.

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
  - Issues #555, #558, #563, #534, and #556

Current Work:

https://github.com/orgs/GSA/projects/25/views/3

Pre-Submitted Questions

Pre-Submitted Questions

Question (Issue #588):

Q: I could not find any mapping details or context for incorporating the Original Risk Rating, Comments, and Auto Approve attributes into an OSCAL based POA&M submission.

A: The POA&M user guide will need to be updated with more details.

- **POA&M Original Risk Rating - The original risk is captured in the risk assembly (plan-of-action-and-milestones\risk\characterization\facet["risk"]) with a child assembly state="initial". Then, the poam-item just references the risk assembly.**
- **POA&M Comments - FedRAMP currently does not have specific assembly/object where this content must go, however the plan-of-action-and-milestones\poam-item\remarks can be used for that purpose. Alternatively, a custom namespace prop could be added to the poam-item to capture POA&M comments.**
- **POA&M Auto-Approve - Not formally operationalized yet by FedRAMP. OSCAL guidance is pending based on a finalized determination of scope and requirements.**

Pre-Submitted Questions

Question (Issue #550):

Q: Does the FedRAMP PMO prioritize OSCAL-submitted packages (i.e. do they get to jump to the front of the review queue) and save 3-4 months of sitting in a queue?

A: No. The anticipated time savings from OSCAL-submitted packages is due to 1) ability to (partially) validate package content earlier in the process thus reducing issue discovery during PMO review and 2) reduction in the time and scope of human review (by Agencies, PMO, etc.) with automated validations.

Q: If it is still a first-in-first-out queue for all packages (OSCAL included), are you able to estimate the time-savings? For example how long would it typically take a reviewer to validate the completeness of a package?

A: FedRAMP is planning to collect such metrics in some upcoming pilot projects. More details will be coming soon.

Pre-Submitted Questions

Question (Issue #550) (cont.):

Q: What is the FedRAMP PMO's take on how OSCAL is received by Agencies in lieu of a traditional package?

A: FedRAMP intends to make digital authorization packages available to agencies in OSCAL but also intends to make the package information available in human readable format ("printables") via its automation platform.

Q: Can an OSCAL SSP be submitted, but the resulting SAP/SAR/POA&M be in the traditional format if preferred or required by Agencies and 3PAO?

A: The long-term goal is for digital authorization packages, inclusive of the SSP, SAP, SAR, and POA&M, and use of the automation platform conversion capabilities to provide traditional ("printables") documents for stakeholders that prefer or require those formats.

Pre-Submitted Questions

Question (Issue #589):

Q: According to the Guide to OSCAL-based FedRAMP System Security Plans (SSP), an inherited control implementation description is optional, however according to NIST a description property is required on an 'inherited' object. Furthermore, the FedRAMP validations requires that an inherited control implementation description must contain at least 32 words.

A: The SSP user guide needs to be updated with more details. We may need to split the current validation into two separate validations:

- **A description field must exist on any inherited control implementation AND must be non-empty. A failure of either condition would result in an "error".**
- **The content length in the description field should be greater than or equal to 32 characters. A failure of this condition would result in a "warning".**

OSCAL SSP validations and the OSCAL SSP template also need to be updated.

Pre-Submitted Questions

Question (Issue #569):

Q: For the Digital Identity Level (DIL) Determination there is a discrepancy between the document templates and OSCAL with the values it accepts. In the document templates it accepts the following values: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL 1/FAL1/AAL1, but in OSCAL it needs an integer: 1, 2, or 3. Is there a reason for having this difference between the documents and OSCAL? Could we instead use only one of the value option types (string vs integer)?

A: The document templates followed the nomenclature in NIST 800-63. OSCAL has named properties that align (there is an implicit mapping). For example:

- **OSCAL <prop name="identity-assurance-level" value="1" /> is the equivalent of IAL1 in the documented template**
- **OSCAL <prop name="authenticator-assurance-level" value="2" /> is the equivalent of AAL2 in the documented template**
- **OSCAL <prop name="federation-assurance-level" value="3" /> is the equivalent of FAL3 in the documented template**

Removing these props from core NIST OSCAL would be a backwards breaking/non-compatible change and adding new props would be duplicative, so we do not foresee a change in the near-term.

FedRAMP Roadmap Deep Dive

Orient FedRAMP around the customer experience

Incentivize CSPs to provide **secure configuration profiles**

Our strategy:

- Partner with CISA to ensure that CSPs provide secure configuration profiles to harden cloud services

Our goals:

- Provide guidance and capabilities to secure agencies' cloud business application environments
- Protect federal information that is created, accessed, shared, and stored in these environments
- Build on CISA's Secure Cloud Business Applications (SCuBA) Project

FedRAMP as a leader in cybersecurity and risk management

Bring more **technical capacity** and **expertise** into the FedRAMP program

Our strategy:

- Position the program as a **leader in cybersecurity** and risk management

Our goals:

- Increase the cybersecurity expertise in FedRAMP
- Improve the FedRAMP guidance and training
    - Implement public facing FedRAMP knowledge base
    - Develop customer-informed training strategy

Scale the size and scope of a trusted FedRAMP marketplace

Centralize and **automate** continuous monitoring

Our strategy:

- Scale the capacity to provide continuous monitoring for all cloud services in the FedRAMP Marketplace

Our goals:

- Form pilots that will be used to understand what resources and capabilities are needed to fully centralize continuous monitoring across the entire FedRAMP marketplace on an ongoing basis
- The PMO and agencies will have visibility into the key information they need to make continued authorization decisions

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

Open Forum

Thank you

Our next Developer Data Bites virtual meeting will be on

Thursday, May 30, 2024 at 12p ET.

Submit questions and future discussion topics to OSCAL@fedramp.gov

Learn more at fedramp.gov

@FEDRAMP

Collaborating with FedRAMP

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

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