FedRAMP

OSCAL Developer Data Bites

May 30, 2024

GSA

info@fedramp.gov

fedramp.gov

Introduction

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

Outcomes:

- Introduction of new OSCAL FedRAMP staff
- Shared understanding of current team issues and recent updates
- Productive discussion around OSCAL

Agenda:

- Welcome
- FedRAMP Automation PMO General Updates
- Pre-Submitted Q&A
- 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

General Updates

Meet the Team

FedRAMP Automation & OSCAL Federal Team

David Waltermire - Data Strategy & Standards Lead

Rene-Claude Tshiteya - Technical SME, OSCAL Automation Developer

Paul Wand - Technical SME, OSCAL Automation Developer

Dimitri Zhurkin - Technical SME, OSCAL Automation Developer

Karen Scarfone - Technical SME, OSCAL Automation Writer

Jake Ahearn - Process SME

The Teams Focus for FY24

- Launch and further development of the automate.fedramp.gov website
  - Guide improvements
  - Frequently Asked Questions (FAQs)
- Addressing github.com/GSA/fedramp-automation issues
  - Focus on OSCAL SSPs issues
- FedRAMP validation rules using OSCAL-CLI
- Supporting OSCAL-related pilots
  - Digital authorization package
  - Continuous Monitoring data
- Supporting data platform implementation

FedRAMP Automation Community Updates

May 30, 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.

- Guides and related documentation were moved to new repository: https://github.com/GSA/automate.fedramp.gov
- Targeting website launch at the end of June 2024

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

Pre-Submitted Questions

Pre-Submitted Questions

Question (Issue #595):

Q: How can CSPs identify **ports and protocols** that are in a **disallow list** within their accreditation boundary, instead of only identifying the protocols and ports that are in an **allow list**?

A: OSCAL SSP components may be products, services, application programming interface (APIs), policies, processes, plans, guidance, standards, or other tangible items that enable security and/or privacy. When applicable, components can use the protocol assembly to provide information about the communication protocols used by the service, but this is not intended to serve as ACLs.

For FedRAMP SSPs, the organizational-defined parameter(s) for control CM-7 is where prohibited or restricted functions, system ports, protocols, software, and/or services should be specified. FedRAMP also recommends referencing some configuration resource (e.g., from firewall, etc.) via links to provide additional information about disallow listed ports and protocols.

Pre-Submitted Questions

Question (Issue #596):

Q: When creating back-matter, what is the recommendation for all appendices that are associated with the SSP? Specifically Appendix B, L, E (content that is defined as included in the legacy SSP but NOT included in OSCAL). For example:

- For Appendix B (Acronyms), should each should each acronym be included as a resource in the back-matter, or the appendix?
- For Appendix L (Laws & Regulations), should a record of each law be a created resource in the back-matter?

A: In OSCAL:

- Appendix B should be represented as a single back-matter resource that has a collection of CSP provided acronyms. Alternatively, see proposed machine-readable approach using **parts**.
- Appendix L should be provided as a single back-matter resource that has a collection of CSO-Specific Required Laws and Regulations.
- Appendix E (Digital Identity Level) should be represented in the **system-characteristics** via the "*identity-assurance-level*", "*authenticator-assurance-level*", and "*federation-assurance-level*" properties.

Pre-Submitted Questions

Question (Issue #596):

Q: For systems with complex appendices (Q - Cryptographic Modules Table, M - Integrated Inventory Workbook). What is the guidance for attaching instead of integrating into the SSP?

A: In OSCAL, inventory and cryptographic modules should not be provided as attachments but instead as inventory items and components. See inventory-item and component examples.

Pre-Submitted Questions

Question:

Q: In OSCAL, if Appendix C (Policies and Procedures) is a *.zip, CSP needs to define it as a policy or procedure (which is different than the legacy document SSP where policies and procedures may be combined into a single document). How should Appendix C contents be represented in OSCAL?

A: FedRAMP OSCAL SSPs must provide both policy and procedure back-matter resources for each control family in the baseline (see example).

- Each back-matter resource must specify a “type”
- If the CSPs policies and procedures are in a combined single document, each back-matter resource can reference the same “combined” policy and procedure document
- If the CSPs policies and procedures are a collection of individual documents, combined into a single *.zip, each resource must ensure its links are relative to the referenced items in the bundled zip.
- We need to work out specific guidelines for packaging, so use of a ZIP is only notional right now.

Open Forum

Thank you

Our next Developer Data Bites virtual meeting will be on

Thursday, June 27, 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