FedRAMP

Developer Data Bites

September 1, 2022

GSA

info@fedramp.gov
fedramp.gov

Introduction

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

Outcomes:

- Understanding of the Data Bites session structure and goals
- Awareness of the current state of FedRAMP's OSCAL use

Agenda:

- Welcome
- FedRAMP Automation Vision
- Data Bites Overview
- OSCAL Current State
- Open Forum *(time permitting)*
- Next Steps & Closing

Automation Vision

Automation Vision: OSCAL

FedRAMP's automation vision is based on the Open Security Controls Assessment Language (OSCAL)

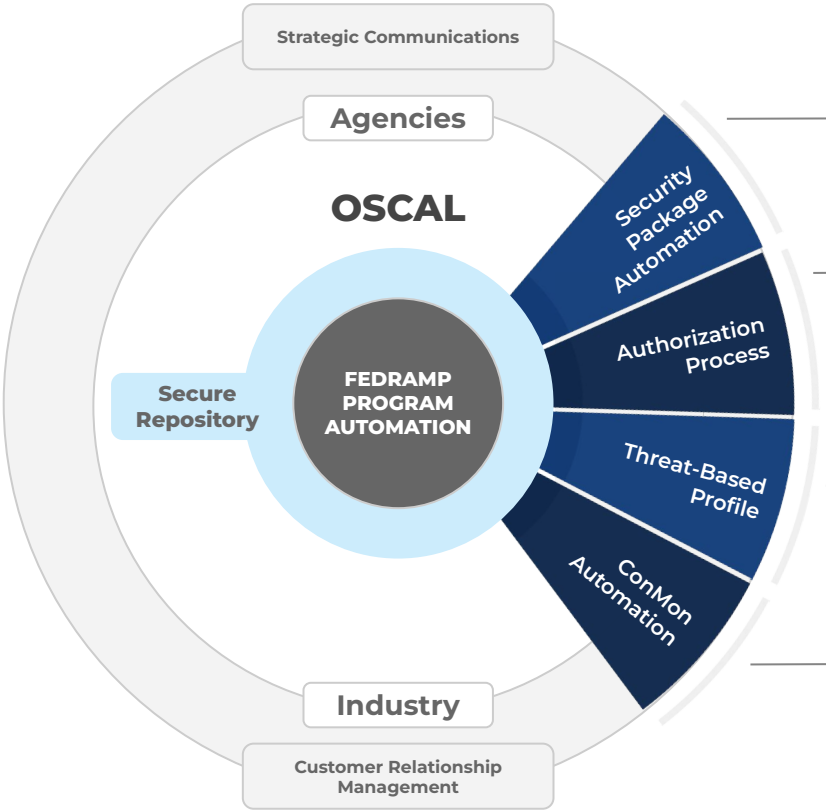
What is OSCAL?

The National Institute of Standards and Technology (NIST) is developing OSCAL to address security control documentation and assessment challenges by:

- Developing a standard approach to security control assessment
- Easing assessments across multiple components
- Simplifying simultaneous support of multiple regulatory frameworks
- Automating reviews and assessments[1]

[1] National Institute of Standards and Technology, *Learn more about* OSCAL, August 22, 2022, https://pages.nist.gov/OSCAL/about/

FedRAMP Automation via OSCAL



FedRAMP OSCAL Baselines and Security Package Materials

The development of the FedRAMP baseline and security package materials in OSCAL. (Rev 5)

Authorization Process

Modernize the authorization process by leveraging OSCAL standard machine-readable format to expedite and automate the review process. This includes an initial automated validation of packages.

Threat Based Profile

Conducted control scoring (Rev 5) with DHS CISA .govCAR. Evaluating methodology for application to FedRAMP annual assessment requirements.

Continuous Monitoring

In initial planning to utilize OSCAL to collect and automate continuous monitoring, shifting to an ongoing authorization model.

Data Bites Series

Data Bites Series

What can you expect from these sessions?

Session Structure:

1. Welcome
2. Information Briefing
3. Q&A

Within each session we hope to achieve the following:

- Technical Discussions around OSCAL
- Access to FedRAMP Automation Team through pre-submitted questions and live Q&A
- Shared Understanding of FedRAMP's OSCAL Plans

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

OSCAL Current State

Differences Between NIST and FedRAMP

NIST

- Catalog/Profile Model for 800-53 Rev 4 and Rev 5.
- Working at OSCAL version 1.0.5
- Published LOW, MOD, HIGH catalogs/baselines for 800-53 Rev 4 and Rev 5
- OSCAL Tools are evolving and open source.
- Support for XML, JSON and YAML

FedRAMP

- Assumes schema compliance with NIST OSCAL core syntax.
- Extends NIST OSCAL with extended namespace and properties (ns=”https://fedramp.gov/ns/oscal”).
- Resolved FedRAMP Profiles - Rev 5 to be released soon.
- Publishing updates to Rev. 4 to address issues that have been identified to date
- Specific Schematron validation requirements - checks for FR specific values and properties
- Support for XML, JSON and YAML.

How to Submit Issues with FedRAMP

Ensuring your outstanding issues or questions are received:

Issues can be submitted in several ways:

- **Preferred:** Open an issue on fedramp-automation github so that it will benefit the NIST/FedRAMP community. https://github.com/GSA/fedramp-automation/issues

- **Alternate:** Email us at oscal@fedramp.gov

Updates to 800-53 Rev 4 and Rev 5

- Current support for SSP, SAP, SAR and POAM.
- Current updates and ongoing work available at (https://github.com/18F/fedramp-automation/tree/master/src/validations)
- Working 2 week sprints releasing updates where changes are pushed to primary FedRAMP automation repo (https://github.com/GSA/fedramp-automation/tree/master/src/validations)
- When fully implemented, the GSA ecosystem will support APIs for validation.

Updates to 800-53 Rev 4 and Rev 5 initial release

- 800-53 Rev 4 - Updates to Guides (SSP, SAP, SAR and POAM) and templates to resolve currently identified documentation and template inconsistencies.
  - Will be released on GitHub
- 800-53 Rev 5 - Updated Guides, (word and OSCAL)templates for Rev 5 scheduled for October 1, 2022.
  - Generating word templates using OSCAL

Open Forum

Pre-Submitted Questions

Question 1: What is a good starting point for an organization that wants to use OSCAL for security and compliance efforts?

A good place to start is the NIST OSCAL site - https://pages.nist.gov/OSCAL/

Question 2: Which language (xml, json, yaml) has the most support and documentation from NIST and GSA?

All formats are supported by GSA. We are using the NIST OSCAL-CLI to convert between formats. In most cases to date, we have been converting received content to xml.

Pre-Submitted Questions

Question 3: What is the best recommended approach to include attachments for an SSP or SAR?

We are still evolving with OSCAL. At this point, we prefer embedded links to accessible attachments until our automation ecosystem is in place. However, if you send artifacts as base64 you must conform to the accepted types specified in the guides so that they pass schematron validations.

Question 4: How can an agency start to build a minimally viable product to prepare for automated consumption of an OSCAL SSP? Are tools being recommended to process and scan for such data?

There are viable products on the market, but we can't recommend or endorse specific tools. FedRAMP recently released an RFI for an OSCAL GRC and there was as robust response.

Pre-Submitted Questions: OSCAL Tools

Question 5: How many packages with OSCAL, where the OSCAL use was successful, have been reviewed and or submitted?

Two so far with more en route.

Question 6: How is OSCAL, as shown in the FedRAMP Guide to OSCAL SSP PDF, rendered into a Word document?

Currently there are Minimal Viable Product (MVP) tools available on the FedRAMP Github Repository that will render a limited version of the SSP, SAP and SAR in Rev 4.. However, not all data fields are output to Word in the MVPs. It is open source and can be downloaded and enhanced from https://github.com/GSA/oscal-ssp-to-word. Updates to these tools are slated post FedRAMP Rev 5 release.

What would you like to see covered in future sessions?

Thank you

Save the Date! Our next Developer Data Bites virtual meeting will be on **Thursday, September 15, 2022 at 12p EST**.

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

Learn more at fedramp.gov

@FEDRAMP

OSCAL Resources

NIST:
https://pages.nist.gov/OSCAL/
https://pages.nist.gov/OSCAL/learn/
https://github.com/usnistgov/OSCAL/releases (current release)
https://github.com/usnistgov/OSCAL/tree/develop (development version)
https://github.com/usnistgov/oscal-content (content repo)

FedRAMP:
https://github.com/GSA/fedramp-automation (current repo)
https://github.com/GSA/fedramp-automation/issues (current issues)
https://github.com/18F/fedramp-automation/tree/master/src/validations (validations work)
https://federalist-2372d2fd-fc94-42fe-bcc7-a8af4f664a51.app.cloud.gov/site/18f/fedramp-automation/#/documents/system-security-plan (web based validation tool)