FedRAMP

Developer Data Bites

September 15, 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 FedRAMP's OSCAL Validations
- Awareness of the validation tools currently available and how to use them

Agenda:

- Welcome
- Pre-Submitted Q&A
- 10x Overview
- FedRAMP Validations & Demo
- 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 1: How is YAML supported? Is there a specific tool recommended for converting YAML to JSON/XML?

FedRAMP supports JSON, XML and YAML. We utilize the NIST OSCAL-CLI tool for converting artifacts between formats available at ***https://github.com/unsistgov/oscal-cli***

Question 2: Are there any validation tools available where an OSCAL file can be uploaded and validated?

*Currently there is an MVP Validation site that OSCAL files can be validated (**https://federalist-2372d2fd-fc94-42fe-bcc7-a8af4f664a51.app.cloud.gov/site/18f/fedramp-automation/#/**). We are demo-ing this tool today.*

Pre-Submitted Questions

Question 3: Will I be able to get OSCAL-based documents for FedRAMP services to import into my GRC? If so, what is the anticipated timeline?

Currently FedRAMP is poised to receive OSCAL-based documents from CSPs and 3PAOs. FedRAMP will store OSCAL security packages for Agency review.

Question 4: Are there details on FedRAMP Excel file to OSCAL mapping?

Would need to know more about your question (i.e. what specific FedRAMP Excel file)? There are OSCAL templates available on the github FedRAMP Automation repository for OSCAL representation of primary artifacts (SSP, SAP, SAR and POA&M).

10x Overview

10x Overview

FedRAMP and 10x together have written over
10,000 lines of code to build automated validation tools.

What is the 10x program?

10x is a crowdsourcing program used to **collect ideas** from federal employees and turn them into **real products** that improve the public's experience with the federal government.

- As 10x explores ideas, they whittle down projects to move through phases, where they continue to research and iterate on it.
- Not every idea moves through all phases of funding. Some graduate from the program at earlier points.
- 10x has funded a total of **268** projects including FedRAMP OSCAL Validations

[1] General Services Administration, *10x Homepage*, August 2022, https://10x.gsa.gov/

FedRAMP Validations

FedRAMP Validations

FedRAMP Validations

FedRAMP will validate all OSCAL artifacts.

What are validations?

Validations are an automated process to help confirm content correctness and fitness for processing.

Which deliverables can be validated?

FedRAMP is able to validate all OSCAL artifacts:

- SSP (System Security Plan)
- SAP (Security Assessment Plan)
- SAR (Security Assessment Results)
- POA&M (Plan of Action & Milestones)

FedRAMP Validations

Users can currently validate basic file conformance, the NIST OSCAL Schema, and FedRAMP’s OSCAL Schematron

FedRAMP Validation Levels

- **Basic File Conformance** - ensure JSON, XML, or YAML is well-formed (e.g. XML all tags have open and closing). Can use any decent XML editor (VS Code, Oxygen).
- **NIST OSCAL Schema Validation** - Validation of OSCAL content (JSON, XML or YAML) by applying the appropriate schema for the respective format (e.g. SSP, SAP, SAR or POAM)
- **FedRAMP OSCAL Schematron Validation** - a framework to take FedRAMP documentation that is properly formatted with NIST OSCAL schemas and check the content for correctness.

***Note:** In order for FedRAMP to validate using Schematron we convert the sourceformat JSON or YAML to XML. We use the OSCAL CLI tool to do this currently.*

FedRAMP Validations

How can you access the validations?

How to access Validations:

- NIST OSCAL CLI Tool (FedRAMP uses for schema validation and document conversion) (https://github.com/usnistgov/oscal-cli)
- FedRAMP Schematron Validations Project (https://github.com/GSA/fedramp-automation)
- 10x Federalist Deployment (https://federalist-2372d2fd-fc94-42fe-bcc7-a8af4f664a51.app.cloud.gov/site/18f/fedramp-automation/)

10x ASAP Federalist Demo

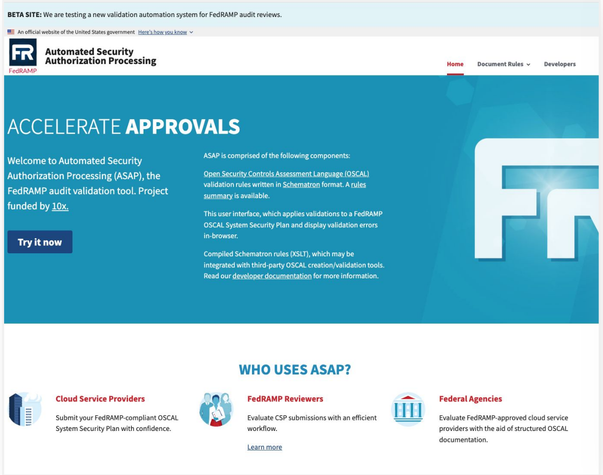
10x ASAP Tool Demo

A tool for users to:

- Browse and filter rules
- Validate SSP documents
- Demonstrate embeddability of rules engine

10x ASAP Tool:
https://federalist-2372d2fd-fc94-42fe-bcc7-a8af4f664a51.app.cloud.gov/site/18f/fedramp-automation/

Intended Users: Tool vendors, drafters, auditors



BETA SITE: We are testing a new validation automation system for FedRAMP audit reviews.

An official website of the United States government Here's how you know

FedRAMP **Automated Security Authorization Processing**

ACCELERATE **APPROVALS**

Welcome to Automated Security Authorization Processing (ASAP), the FedRAMP audit validation tool. Project funded by 10x.

ASAP is comprised of the following components:

Open Security Controls Assessment Language (OSCAL) validation rules written in Schematron format. A rules summary is available.

This user interface, which applies validations to a FedRAMP OSCAL System Security Plan and display validation errors in-browser.

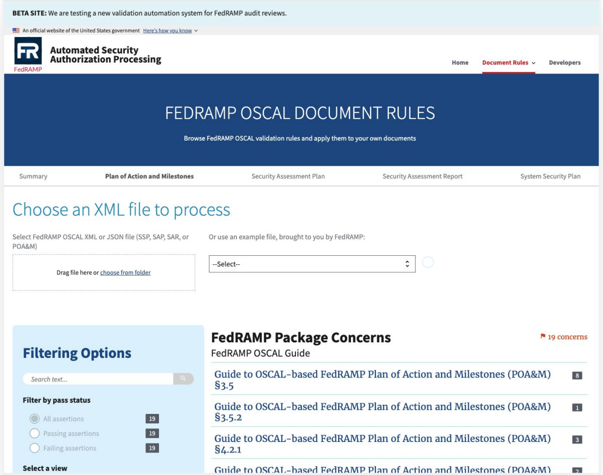
Compiled Schematron rules (XSLT), which may be integrated with third-party OSCAL creation/validation tools. Read our developer documentation for more information.

WHO USES ASAP?

Cloud Service Providers
Submit your FedRAMP-compliant OSCAL System Security Plan with confidence.

FedRAMP Reviewers
Evaluate CSP submissions with an efficient workflow.
Learn more

Federal Agencies
Evaluate FedRAMP-approved cloud service providers with the aid of structured OSCAL documentation.



BETA SITE: We are testing a new validation automation system for FedRAMP audit reviews.

An official website of the United States government Here's how you know

FedRAMP **Automated Security Authorization Processing**

FEDRAMP OSCAL DOCUMENT RULES

Browse FedRAMP OSCAL validation rules and apply them to your own documents

Choose an XML file to process

Select FedRAMP OSCAL XML or JSON file (SSP, SAP, SAR, or POA&M)

Drag file here or choose from folder

Or use an example file, brought to you by FedRAMP:

--Select--

Filtering Options

Search text...

Filter by pass status

● All assertions 19
○ Passing assertions 19
○ Failing assertions 19

Select a view

FedRAMP Package Concerns
FedRAMP OSCAL Guide

19 concerns

Guide to OSCAL-based FedRAMP Plan of Action and Milestones (POA&M) §3.5	8
Guide to OSCAL-based FedRAMP Plan of Action and Milestones (POA&M) §3.5.2	1
Guide to OSCAL-based FedRAMP Plan of Action and Milestones (POA&M) §4.2.1	3
Guide to OSCAL-based FedRAMP Plan of Action and Milestones (POA&M)	2

Try the 10x ASAP Tool Demo here

Open Forum

Thank you

Save the Date! Our next Developer Data Bites virtual meeting will be on **Thursday, September 29, 2022 at 12p EST**.

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:** 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

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