FedRAMP

Developer Data Bites

February 16, 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 how to create a minimal OSCAL artifact using 3rd party tools that pass basic schema validation
- Productive Discussion around OSCAL for FedRAMP

Agenda:

- Welcome
- Pre-Submitted Q&A
- Demo – Creation of Minimal OSCAL Artifacts that Pass NIST Validations
- 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

Pre-Submitted Questions

Pre-Submitted Questions

Question 1: How are you going to handle OSCAL documents that referenced in leveraged authorizations specified in the OSCAL SSP?

There are 3 possible scenarios:

1. OSCAL SSP with Access: The SSP of leveraging system can "see" the leveraged system's SSP
2. OSCAL SSP - No Access: The SSP of the leveraging system is NOT permitted to "see" the full leveraged system's SSP.
3. Legacy SSP or CRM: The leveraged system's SSP is not expressed in OSCAL, or its CRM is not.

References: https://pages.nist.gov/OSCAL/presentations/oscal-leveraged-authorizations-v2.pdf

FedRAMP Automation GitHub Updates

Update on FedRAMP automation repository

10x Flexion Transition

- 10x/Flexion team has transitioning the majority of Schematron validations support but is still available for consultation to FedRAMP team for limited period of time.
- Tom Penna and Tom Volpe Sr

Issues/Ticket Tags

- **Newly opened issues this cycle**
    - #385: Add rev 5 ruleset to web documentation and template release (pending finalization of FedRAMP Rev 5 baselines)
    - #384: Rules for managing UUID creation and updates (See comment on GH Issue)
    - #383: Risk Log Requirements (documentation updates in progress)
    - #382: Cloud Service Model error (schematron bug - fix in progress)
- **Closed issues this cycle related to Schematron Validations**
    - No tickets closed this cycle.

Demo –
Creation of Minimal OSCAL Artifacts that Pass NIST Validations using 3rd Party Tool

DEMO STUFF

Pre-Requisites

- Access to a schema aware editing tool (Oxygen XML Editor/Visual Studio)
- Access to a UUID generator (https://uuidgenerator.net)
- Access to FedRAMP Automation Repo (https://github.com/GSA/fedramp-automation)

Decisions:

- Are you generating for a FedRAMP OSCAL artifact?
- Decide on which system sensitivity level you are going to use - this decides the schema to use.

Demonstration Information

Useful Links

3rd Party Tools

- https://www.oxygenxml.com/xml_editor/download_oxygenxml_editor.html (Oxygen XML Editor)
- https://github.com/usnistgov/OSCAL/tree/main/xml/schema (NIST xsd schemas)
- https://github.com/usnistgov/oscal-content/tree/main/nist.gov/SP800-53/rev4/xml (NIST profiles)
- https://github.com/GSA/fedramp-automation/tree/master/dist/content/rev4/baselines/xml (FedRAMP profiles)
- https://code.visualstudio.com/download (Visual Studio Code)
- https://marketplace.visualstudio.com/items?itemName=qub.qub-xml-vscode
- https://marketplace.visualstudio.com/items?itemName=redhat.vscode-xml

Open Forum

What topics do you want to see in the future?

Quick Poll

What to you want to see?

1. Demo of NIST Deepdiff tool
2. Demo of GSA Public portal prototype
3. Referencing leveraged authorizations in OSCAL

Would you be interested in participating in a formal working group for early adopters of OSCAL with FedRAMP (CSPs, GRC Tool Vendors, etc.)?

→ *Please note this would include sharing information, challenges, and solutions among peers.*

Thank you

****NEW ZOOM LINK for Next Meeting****

Our next Developer Data Bites virtual meeting will be on **Thursday, March 16, 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

Rev 5 Update

Rev 5 Timeline

Estimated Release Date of XXXXXXX

- Phase 1 Release: XXXXXXX
  - Rev 5 Baselines
  - CSP Transition Plan
- Phase 2 Release: XXXXXXX
  - Templates
  - OSCAL Docs
- Phrase 3 Release: XXXXXXX
  - Everything else (+45 documents)

Notes:

- Hand jamming is not the desired way to generate artifacts. But this demo will show how to do it.
- Demo will help you understand the NIST + FedRAMP schema requirements.

Demo Instructions:

1. Open Oxygen
2. Open up fedramp template on https://github.com/GSA/fedramp-automation/dist/content/rev4
3. Open up UUID Generator (https://www.uuidgenerator.net)
4. Open up NIST reference page for SSP Schema Outline (https://pages.nist.gov/OSCAL/reference/latest/system-security-plan/xml-outline/)
5. Create NEW project in Oxygen
6. Tools -> Generate Sample XML)
   - select schema (oscal-ssp_schema.xsd)
   - select default namespace (http://csrc.nist.gov/ns/oscal/1.0)
7. Generate UUID for SSP and put into top <system-security-plan> element.
8. Generate UTC compliant date time (use current-dateTime()) in xpath Window and open message and copy and paste into SSP.
9. Modify import-profile (use FedRAMP profile located at https://github.com/GSA/fedramp-automation/dist/content/rev4/templates/ssp (moderate)
10. Add remarks copied from fedramp rev 4 template
11. Enter systemID with FedRAMP ns specification (copy from rev 4 template)
    - speak to NIST template and show location. Google NIST 800-53 OSCAL profile and show moderate)
    - explain namespace specificity.
12. Enter secondary SystemID (users own SystemIdentifier if applicable- not required)
13. Add system shortname
14. Add system description
15. Add additional FedRAMP properties (copied from template)
16. Update sensitivity level to "fips-199-moderate"

*** Note revalidate at steps 6-16 to show compliance.

USEFUL LINKS NOT SHOWN IN PRESENTATION SLIDES:

Links to baseline profiles used during demo:

NIST: https://raw.githubusercontent.com/usnistgov/oscal-content/main/nist.gov/SP800-53/rev4/xml/NIST_SP-800-53_rev4_MODERATE-baseline_profile.xml
FedRAMP: https://raw.githubusercontent.com/GSA/fedramp-automation/release/fedramp1.0.0-oscal1.0.0/baselines/rev4/xml/FedRAMP_rev4_MODERATE-baseline_profile.xml