

OSCAL Developer Data Bites

January 11, 2024

info@fedramp.gov fedramp.gov



Introduction

R

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

Outcomes:

- Shared understanding of impacts to FedRAMP's use of NIST OSCAL content due to NIST's 1.2.1 release.
- Shared understanding of updates to HTML-based OSCAL guides.
- Productive discussion around OSCAL.



Agenda:

- Welcome
- General Updates
- FedRAMP Automation

Community Updates

- Pre-Submitted Q&A
- Update on Guides
- NIST 1.2.1 Release
- 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





General Updates



January 11, 2024

NIST OSCAL version 1.1.x release

FedRAMP automation team is continuing to work to update all guidance and validations to align with OSCAL 1.1.1 release.

Revising OSCAL Guides

FedRAMP automation team is continuing to work towards publishing HTML versions of the OSCAL guides to replace the current PDF versions.

GitHub Issues

• Prioritizing issues related to FedRAMP Guide and SP 800-53 rev 5

Review Needed

github.com/GSA/fedramp-automation/pulls

- #502 Adjusted response points
 - Resolves #443, #511, #512, #535
 - Plan to merge on 1/16/2024.
- #540 Local version of SP 800-53 with zero padded labels
- #541 OSCAL Guides in markdown

Pre-Submitted Questions



None received!

Reminder to submit questions/topic ideas via https://forms.gle/M4pT7P2xyE6hRC7DA

Update on Guides



Status Update

Completed "MVP" Markdown versions of:

- Guide to OSCAL-Based FedRAMP Content (rev 5)
- Guide to OSCAL-Based SSP (rev 5)
- Guide to OSCAL-Based SAP (rev 5)
- Guide to OSCAL-Based SAR (rev 5)
- Guide to OSCAL-Based POA&M (rev 5)

Created feature branch for ongoing guides updates

- See <u>README.md</u> for instructions on generating the guides locally
- Please provide feedback on PR<u>#541</u>

In Progress

- Iterative style guide conformance updates
- Address backlog of backlog of <u>documentation / guide related issues</u>
- Identifying a web hosting solution

Collaborating with FedRAMP

What you should expect from FedRAMP

Visibility:

- Work performed through GitHub issues and pull requests
- Discussion of options in GitHub issues and pull requests

Review:

- Changes will be posted as pull requests for review before merging
- Significant changes will be available for review for multiple weeks

What FedRAMP expects from you Collaboration:

- Identify needed changes as issues
- Comment on important issues
 - □ Support the proposed solution
 - □ Identify alternate solutions
- Submit changes through pull requests
- Provide code review of pull requests

Use of GitHub as a collaboration platform will allow for more progress on resolving issues between meetings.

Submitting an Issue

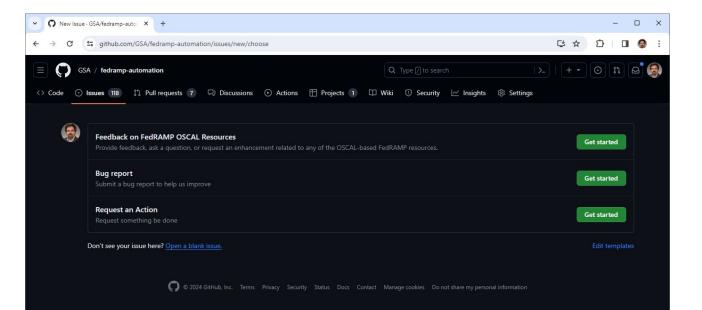
https://github.com/GSA/fedramp-automation/issues/new/choose

Select an appropriate issue template

• Feedback

Bug

• Change request



Identifying issues ready for review

https://github.com/orgs/GSA/projects/25/views/7

FedRAMP maintains a work board providing transparency around active areas of work.

- New Issues/Triage
- Current Work
- Review Needed
- Backlog

▼				
← → C º5 github.com/orgs/GSA/projects/25/views/7		坐 🛯 🎯 :		
GSA / Projects / FedRAMP Automation	t Type [] to search	<u>>_</u> + •	o n 🖻 🛞	
⊕ FedRAMP Automation				
Triage Needed Kanban Kanban Kork Board Review Needed + New view				
😓 status: 👀 In review" 💿 🖸 Discard				
Title	• Assignees •••	Status •••	Linked pull requests	
1 • Response Points missing from Rev-5 Baseline Catalogs #443	😵 Rene2mt 🚽	SS In review	17 #502	
2 • SAP APPENDIX A ASSESSMENT PROCEDURES INCONSISTENT WITH OSCAL #511	😵 Rene2mt 🚽	😌 In review -	11 #502	
3 ③ SAP Appendix A - Test Method (G) does not Align with OSCAL #512	😲 Rene2mt 🚽	00 In review	11 #502	
4 💿 Discrepancy between baseline XML response-points and SSP Appendix A response-points #533	😵 Rene2mt 🚽	(33 In review) -	11 #502	
5 11 Local version of SP800-53 rev5.1.1 that contains the correct labels $\#540$	🧐 david-waltermire 🚽	😌 In review -		
6 🛛 🖁 🖕 Feature markdown guides #541	🛞 david-waltermire a 👻	00 In review		
+ You can use Control + Space to add an item				

Reviewing a pull request

https://github.com/GSA/fedramp-automation/pulls

- Provide an overall review
- Comment on individual changes
- Propose adjustments

- O Feature markdown guides by d	× +	- 🗆 X
← → C (25 github.com/G	SA/fedramp-automation/pull/541/files	다 🖈 🖸 🛯 🔕 :
Feature markdown g Feature markdown g Changes from	guides #541 all commits ▼ File filter ▼ Conversations ▼ 🔞 ▼	0 / 168 files viewed Review in codespace Review changes -
Q Filter changed files	🛉 🗸 💠 🛈 4 💶 .gitmodules 🖓	Viewed 📮 …
🕒 .gitmodules		20 + url = <u>https://github.com/usnistgov/hugo-uswds.git</u>
✓ ■ docs ■ README.md	← ⑦ 86 ■■■■■ docs/README.md □	Viewed D ····
archetypes		
🗋 default.md		 2 + 3 + This subdirectory contains source code for the FedRAMP OSCAL GitHub Page (URL TBD). Below are instructions for building the base of the subdiverse structure of the
content		site for local development if making any contributions to the documentation.
🗋 _index.md	\pm	<pre>4 + 5 + The website is built using the [Hugo](https://gohugo.io/)</pre>
🗸 🖿 about		static site generator and the [United States Web Design
🗋 _index.md		System](<u>https://designsystem.digital.gov/</u>) (USMDS).
🗋 faq.md	\pm	<pre>b + 7 + ## Prerequisites</pre>
🗋 release.md		8 + 9 + If using Docker:
contact		9 + 11 USING DOCKEP: 10 +
🗋 _index.md	• ·	11 + - [Docker 20.10+](<u>https://docs.docker.com/install/</u>) 12 +

Collaboration Resources

FedRAMP Automation GitHub: <u>https://github.com/GSA/fedramp-automation</u>

- Open Issues: <u>https://github.com/GSA/fedramp-automation/issues</u>
- Open Pull Requests: <u>https://github.com/GSA/fedramp-automation/pulls</u>
- Active Work: <u>https://github.com/orgs/GSA/projects/25/views/3</u>
- Community Review Needed: <u>https://github.com/orgs/GSA/projects/25/views/7</u>

GitHub Resources:

- Issues: <u>https://docs.github.com/en/issues</u>
- Pull Requests: <u>https://docs.github.com/en/pull-requests</u>

NIST 1.2.1 Release

NIST OSCAL Content v1.2.1 Release



Background

The NIST OSCAL content v1.2.1 release included backwards-compatibility breaking changes to the SP 800-53 rev5 catalog.

- Replacement of "labels" with "alt-identifiers"
- Removed non-padded labels

FedRAMP adjustments

FedRAMP adjustments to address the compatibility-breaking changes:

- PR #542 reverted catalog to the previous NIST v1.2.0 release
- PR #540 makes similar changes using new "labels"
- Provides zero-padded and non-padded labels

</param>

<prop name="alt-identifier" class="sp800-53" value="AC-01"/> <prop name="alt-identifier" class="sp800-53a" value="AC-01"/> <prop name="sort-id" value="ac-01"/>

<prop ns="http://csrc.nist.gov/ns/rmf" name="implementation-level"

<prop name="label" value="AC-1"/> <prop name="label" class="sp800-53-zero-padded" value="AC-01"/> <prop name="label" class="sp800-53a" value="AC-01"/> <prop name="sort-id" value="ac-01"/> <prop ns="http://csrc.nist.gov/ns/rmf" name="implementation-leve

Lessons Learned



Challenge

- 1. Review was insufficient.
- 2. Rationale for changes was not clear.
- 3. PR 228 changed way too many things, making it impossible to diff using GitHub's web UI.
- 4. Changes occurred in related PRs 2 days before merging, while many were on leave for the holidays.
- 5. Due to the rate of changes to PRs, it was not clear if/when the work was ready for review.
- 6. Changes were backwards-compatibility breaking and inconsistent with expectations.

Lesson Learned

- Use a project board to provide summary issue/PR status. Widely advertise the need for reviews.
- 2. Explain the "what", "why", and "how" in issues/PRs.
- Break up multiple changes into multiple PRs. To maximize review, diffs should be viewable in the GitHub UI, if possible.
- Provide more time for review after a significant change is made. Allow more time during holiday periods.
- Mark PRs in development as "draft". Remove "draft" status when ready for review.
- 6. Develop SP 800-53 catalog style guide to ensure consistency. Enforce with external constraints.

Open Forum

Thank you

Our next Developer Data Bites virtual meeting will be on

Thursday, February 8, 2024 at 12p ET.

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





Ensuring your outstanding issues or questions are received:

Issues can be submitted in several ways:



Open an issue on fedramp-automation github so that it will benefit the NIST/FedRAMP community.

https://github.com/GSA/fedramp-automa tion/issues

Alternate

Email us at oscal@fedramp.gov



NIST:

https://pages.nist.gov/OSCAL/

Learning Resources: <u>https://pages.nist.gov/OSCAL/learn/</u>

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-automa tion/#/documents/system-security-plan