FedRAMP OSCAL Early Adopters Workgroup Knowledge Capture

October 11, 2023

Meeting Details

Purpose: Weekly working session for the participants of FedRAMP OSCAL Automation Early Adopters work group (by invitation only).

Outcomes

- Shared understanding of Charter and Mission of the Workgroup
- Shared understanding of SAR Schematron Rules and rule levels.

Slide Deck

Meeting Notes

- Introduction
    - Tom Sr. reviewed purpose and outcomes for the workgroup, guiding principles, workgroup's charter/mission, provided some OEAW updates, current issues on the early adopters github
- Tom Sr: In between two phases: Phase 2 ending General artifact submission, Phase 3 beginning document and artifact management.
- Tom Sr discussed resolutions on compressed files.

Participant Questions/Conversation:

- Dave W: Is the point to sync the OSCAL points with the spreadsheet?
    - Tom Sr: Originally yes.
    - Dave: Do we want the same response points for both?
    - Tom Sr: I wanted to align, but the review team/PMO didn't want to do that and wanted to keep it the way it was.
- Valinder: Schematron seems to fail. Validates the URL but not really.

        - Tom Sr: Current checks for a resolved profile catalog. We have a meeting with 10x folks. The way the rules are written is why they are failing.
        - Tom Sr: What are your thoughts on what we should validate from a schematron perspective?
        - Valinder: SSP is pointing back to a FR baseline so you have a list of FR published baselines, with UUIDs. You should be looking that it points back to one of those UUIDs.
        - Tom Sr: Whose UUIDs get updated is the question.
        - Valindar: Your implications don't change whether its a URL or UUID. I could still point to an older version and it should be accepted. Can't just point to a current one, will need previously published ones.
        - Dave: **Tom, if you could invite me to those meetings I'd love to join.** I'm concerned about using UUIDs here for the long term. EVerytime there is a new version of the profile we'll have to update the schematron rules. It might be better to be more predictable to use the URL of the resource.
        - Valinder: Agreed. From our tooling perspective, we have all these files imported and we look them up by UUID. We do not go out dynamically to resolve them. We would still like to see the UUIDs.
        - Dave: The URI/L could be used as an identifier too.
        - Tom: The process takes so long for authorization now. The update to OSCAL throughout that process. **Do you have them submit their profile w/ the package, or do you say you'll always go against the latest, or set up github to have versioning?**
        - **Dave W: I think the latter.** It's important that each increment of change be versioned and it's clear what the submitted is using. Regardless of which solution we pick, that should be an outcome.
    - Greg Elin: Well, how long is a back matter links suppose to last? 6 months? 6 years?
        - Tom Sr: That's the golden question. Right now the current transition plan. The package should be submitted w/ back matter resource as part of the package that you submit. You submit updated docs as they request them. With OSCAL you'll have to submit all four documents plus the back matter resource references may change which means you'll have to resubmit.
        - Greg: If an ATO package is sent in everything should be available for three years or until the next ATO package.
        - Tom: The PMO says we delete nothing
        - Greg: Great. Does that mean then that the reference links have to stay up?
        - Tom: If it's named the same.
        - Dave: For things that aren't updated, how should those persist over time?
        - Tom: It will persist over the authorization of course. Right now there is a target of Jan to get a full package in.

        - Dave: Michelle mentioned there are fed regulations on records retention. If you think about links being informative links instead of normative links, there's probably a difference in retention as it relates to those. So we should think through that.
        - Greg: Here's the use case. It's 2 years after an ATO package has been submitted. And there are links to artifacts. Those other artifacts happen to be hosted on some service provider, like a GRC Saas. It's possible that something changes with that GRC Saas. **Is there an obligation for that GRC Saas, if an artifact is published, is there an obligation for that R-link to continue to be valid bc maybe the Saas does some refactoring and that link is no longer there? Or are there links right now that are to OMB Max?**
        - **Dave: Valid question. PMO will discuss.**
        - Greg: If you pick that link, you've got to support that link.
        - Dave: Exactly. Not just an OSCAL problem either.
        - Tom: I know OMB Max, there's so much hand holding between the submitters and PMO review teams that documents get uploaded and reloaded all the time. I don't know what checks and balances are in place for it. My guess is none until someone figures it out in the review. Automation can resolve this.
        - Dave: There's more characterization around the link there is in OSCAL, so it would be helpful to drive feedback to a CSP if the link goes dead. I think we need to think about link management.
    - Valinder: We are able to generate those files successfully. 100MB is plenty for us.
        - Tom Sr: Any submitted through portal?
        - Valinder: No, these are real packages.
        - Tom: I'd love to test it if you have the test data. I'm more concerned about the technical side, time outs, etc. How big was the one we got Aaron?
        - Aaron: It was just the SSP, 22MB. Can talk more offline about it.

Chat copy:

12:02:10 From Darcy Steiner to United Solutions(Direct Message):

Hi! Can you confirm your name please?

12:07:41 From United Solutions to Darcy Steiner(Direct Message):

Matthew Coughlin

12:11:06 From Darcy Steiner to United Solutions(Direct Message):

ty!

12:18:27 From Greg Elin to Darcy Steiner(Direct Message):

Yes, pls show an example of issue...

12:18:49 From Darcy Steiner to Everyone:

Greg Elin asked, “Yes, pls show an example of issue...”

12:19:19 From Greg Elin to Darcy Steiner(Direct Message):

Thanks. I meant to post to everyone...

12:19:39 From Darcy Steiner to Greg Elin(Direct Message):

No problem! Had to update the setting

12:32:20 From Greg Elin to Everyone:

Well, how long is a back matter links suppose to last? 6 months? 6 years?

12:42:39 From A. Michelle White to Everyone:

See the General Records Schedule for file retention.

12:42:40 From A. Michelle White to Everyone:

https://www.archives.gov/records-mgmt/grs

12:50:59 From Greg Elin to Everyone:

+1 for delete

Actions

Owner	Action Item
Tom Sr.	☐ Invite Dave W to 10x meetings? (unclear on meeting request)
	☐
	☐
	☐