FedRAMP OSCAL Early Adopters Workgroup Knowledge Capture

September 13, 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
- General Artifact Submission – Repository Discussion
  - Tom Sr. reviewed basic repository requirements, current file types supported by RestAPI, checklist differences between Rev 4 and 5, basic ATO package requirements, and current challenges.
  - Tom reviewed package structure ideas submitted by a OEAW member for discussion
    - Valinder: We will need some time to take a look at it. At a high level, do we really need to enforce the packaging structure if we have the basic rule that the SAP SSP POAM and SAR need to be at the top level, and from that point forward they give you a relative path to other documents?
    - Tom: Makes sense.
    - Valinder: Top level documents should be at the top level and the rest at the bottom:
    - Tom: Inclusion of the problems?

    - Valinder: Ambivalent on this as a group. Gone back and forth. I think they're not expecting this profile to be here. The goal from FR is: are you meeting my baseline or not. It's nice to include the profile, but now I'd have to validate it. Great to have, but 2 level hop to figure it out. Introduces complexity. Doesn't hurt to include it, but from a validations perspective, you're always going to check against your baseline.
    - Tom: With profile inclusions, you don't know what you're going to get.
    - Valinder: Exactly. You can open yourself up to a nest.
    - Tom: Agreed. More of a policy question perhaps. For Rev 5, if we do profile updates, that profile will get a new UUID, etc. If we drop the version that they used, that might be the only reason to require it so we know what version someone used.
    - Valinder: Makes sense. SSP is referring to FR baseline, so it can refer to the version that was used. People might be submitting those baselines because they are doing other frameworks as well. No harm in submitting the profiles, but from validations, you can do it all against the FR baselines.
    - Tom: Submit one or more zip files for your package. Now when we upload and process the artifact, we'd have to first decompose the package into our repo, then run validations, then provide a different process to backfeed that. The point of the portal now is to help us work through kinks now with validations and address them, but in a long term view, once you are publishing OSCAL, over time I would see that the validations become less important, excluding a major change to OSCAL.
  - Tom explained ConMon CDM stuff going on right now: In process of taking OSCAL test data and rendering views for DHS for CDM dashboards. How do you feel about single document that includes all the artifacts?
    - Valinder: Imagine putting a SAR into the same document, and it will break everything. Should be UUIDs. I would say we should have reference data about the document itself so you can still package the wrapper project in your zip file. It's a lot of data. Needs to be transported differently. More UUIDs rather than documents.
    - Tom: Just starting down the UUID path. We did a prototype for that, and it kind of works. With the way that tool works, you have to create a specific filter for those comparisons. Tricky.
    - Valinder: I agree**. UUID being a long haul, but a UUID number will get you to an artifact quickly**.
    - Tom: I agree. Here's my takeaways from today. As far as the package artifacts, this structure you are cool with. This makes sense to me for a compressed artifact. Need to work on it a little bit, for example to make sure a SAP isn't missing, we will have to decompress first to check.

Participant Questions/Conversation:

- Greg: I thought there was a performance issue with large embedded files? An FYI - ".DS_Store" happens to be a MacOS hidden file - extra in this case, I'm guessing..
    - Tom: Performance issue is referring to the federalist site. Will take longer with base 64. But we recommend using our links. Gives us a decomposition ability. POAMs that were huge would not get through validations.
- Valinder: Federalist site is really good. Can't put real data in the portal. Run out of simulated data at this point. We are still doing a lot of conversations with real data we want to get validated. Very useful for us.
    - Tom: Not going away anytime soon, talking first of the year maybe.
    - Tom: What are you using for NIST core validations?
        - Valinder: OSCAL CLI with SSD
        - Tom: We put this portal together the way we did because we knew the "garbage in, garbage out" concept. We are going to get aggressive with solving issues between NIST core and schematron. We have been debugging a lot of these issues, so please keep them coming.
- Valinder: Another point: We are getting ready to move to FR 2.0.0 specifications. We need to start talking about versioning slightly differently, from Rev 4 and Rev 5. And how will the validation module work in that sense.
    - Tom: I didn't realize that. Thank you. Rev 4 v 5 issue is one of the reasons we made that a radio button in the file upload. **I could do the 2.0.0. with rev 4 and that could cause issues.** More fun for Dmitri/schematrons! Maybe we could put something in the metadata that would tell us that.

Chat copy:

(N/A)

Actions

Owner	Action Item
	□
	□

	□
	□