FedRAMP OSCAL Early Adopters Workgroup Knowledge Capture

August 9, 2023

Meeting Details

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

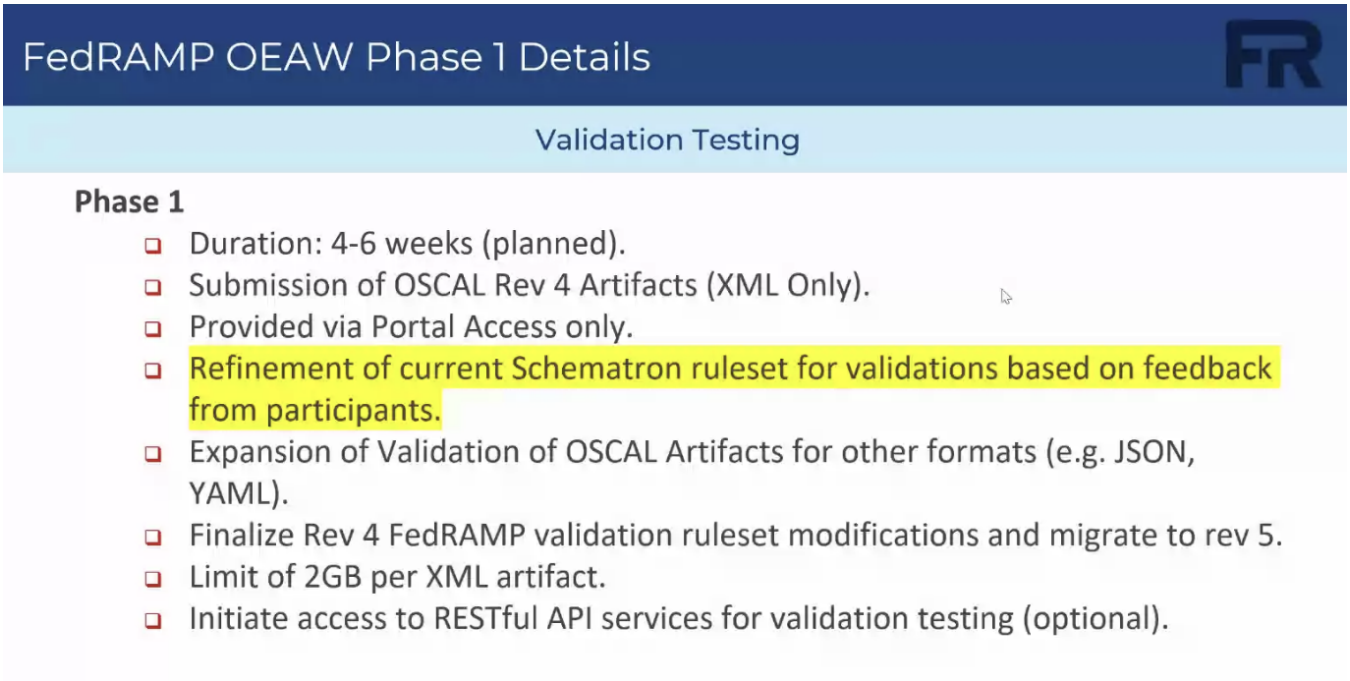
Outcomes

- Shared understanding of Charter and Mission of the workgroup
- Shared understanding of program participation requirements and initial registration process
- Provide an Overview of the phases of the Early Adopters program to the workgroup

Slide Deck

Meeting Notes

- Volpe: Reviewed purpose and outcomes for the workgroup, guiding principles, and introduced the automation development team, and reviewed the workgroup charter/mission, requirements, and registration follow up.

- 

- 2.2 release of the portal next week!

Participant Questions/conversation:

- S Lacy: Confirm, since we can incorporate additional controls, do we still have to include the baseline profile? Where the FR has defined their requirements in their baseline profile from the catalog from NIST. FR has defined them, but I don't think there is a defined baseline profile for the SRG or OSCAL catalog so if we include additional controls outside of the FR, would have to include the baseline profile.
    - I would. But that is a PMO policy question.
- Valinder: If you are going to relax from validation error to warning, is the SAP validated against the baseline or SSP?
    - Tom: The SAP imports the SSP, the SAR, I believe they are going to be validated against the SSP.
    - Valinder: As SAP is going to look for included controls in the SSP and SSP has more controls, that breaks the SAP. the SAP should go against the baseline.
    - S Lacy: How is it going to break the relationship?
        - Valinder: If doing a FR assessment, you shouldn't include other controls outside of FR.
        - Tom: Not getting rid of it, just want it as a warning instead of an error. It can still get through the process. The review team can decide. I did not think of the downstream effects. I don't think it will break the SAP or SAR, but they should be warnings.

- Greg: Ambiguity here. 4c says required for the applied baseline. I've interpreted the baseline as a recommended set of controls separate from the profile which is the actual set of controls. The applied baseline in that language is ambiguous.
    - Tom: talking about the profile.
    - Greg: I think that if the profile, my understanding of SAP has been that it is a selection of controls that could be evaluated. It could be all or some. Valinder's point is interesting. It's always been a challenge for all content to mix catalogs.
    - Tom: We can leave it as an error and stop the validations.
    - Validner: I think it should be a warning. But should be coupled with downstream also.
    - Tom: I have to go back to PMO review team to set thresholds on the types of errors and warnings and what they're willing to accept. Have to set policy on minimum thresholds.
    - Greg: What if we introduced a critical warning? Error warning then critical warning. As a way to bump something in the warning category but distinguish the important ones from the other ones. A severity threshold. Or critical error v an error.
    - Tom: Good idea, I will pass along. Not all errors are created equal. A severity level would be good.
    - Greg: I like some type of ranking. Distinction between fail and hierarchy of things I need to fix.
    - Dmitri: I can try to create a critical warning. Taking notes.
    - S Lacy: I like the warning idea. When we look at legacy SSP, it's all defined, structured box. Additional info or insight a CSP provides is better. Reciprocity is complex. Gives the PMO an opportunity to see other data.
    - Greg: Agreed.
- Matthew Coughlin: Thinking about on upload. Right now SSP does not store additional control info, just implementation. For OSCAL where would we pull that info from if not in a catalog?
    - Tom: Resolves back to 853 catalog. Who's responsible for providing that additional info. You have to add them to the profile and upload them to the package.
    - S Lacy: If not in NIST catalog, also have to make a new catalog.

- Tom: Same thing with required document. Going to relax to a warning. Same for logo.
- Greg: Returning to my earlier point. If we redefine the text that there shoud not be any controls not in the profile, then that's different from not any controls in a baseline. I'm confused because my assumption is that there is never a control in the SSP that is not in the profile. Are people saying they want to include controls that are not in the referenced profiles?
    - Valinder: Would be an OSCAL violation.

    - Greg: I think warnings are good to start, but I think it makes sense that if you are evaluating the existence of a control in an artifact that does not appear in the profile then that is an error.
    - Tom: **Maybe that is a specific rule in the schematron we should have.**
    - Valinder: Additional info shouldn't be bad, But for all validations should run against FR baselines.
    -
- Tracy Hickman - 12:47 PM - Regarding rlinks with an absolute path, what are expectations on the "shelf life" or durability after we submit a package? Is this what would be hashed out in Phase 3?
    - Tom: Yes. We will have to determine shelf life.

Chat copy:

A Michelle White - QT2F2

12:11 PM

The amendment was posted

Monica Ihli

12:18 PM

No objections. Just want to applaud the direction you are going with it, sounds like a good approach

Greg Elin (RegScale)

12:18 PM

cool

Greg Elin (RegScale)

12:25 PM

Oh, the SAP Bone's connect to the SSP Bone...

Robert Ficcaglia

12:26 PM

in practice (ignoring OSCAL) the SAP should reflect the profile (catalog + agency additions) - not just the baseline catalog

Monica Ihli

12:28 PM

Robert makes a fair point.

But also want to point out: We should ensure the technology reflects the reality of the user's experience. The user's experience shouldn't be dictated by convenience of technology.

Monica Ihli

12:29 PM

If users' need greater flexibility to add controls to the SSP, then we shouldn't deny them the ability to do so because it's inconvenient to enumerate controls downstream rather than say "include everything"

Robert Ficcaglia

12:31 PM

it is a real not theoretical need - agencies have non-NIST controls they add and want them assessed by 3PAO in the SAP. not needed for JAB but will be for Agency sponsors

S Lacy

12:32 PM

Agree Monica. Unless there is a requirement that we exclude all extra non-scoped controls, the additional should be allowed. And this will require 3PAO to do their scoping accurately.

S Lacy

12:34 PM

Robert, the assessment would then fall to the agency for all controls, or only the non-fedRAMP profile controls? Or does that require more in-depth reciprocity.

Robert Ficcaglia

12:36 PM

@SLacy - reciprocity is a good question - as a sponsor I may not want to share my custom control catalog with PMO or others. so then how does that get added to package. and so next sponsor what happens. interesting...

Greg Elin (RegScale)

12:38 PM

Well said, @SLacy

Robert Ficcaglia

12:43 PM

if you are an agency sponsor - you can and do add

Tracy Hickman

12:47 PM

Regarding rlinks with an absolute path, what are expectations on the "shelf life" or durability after we submit a package? Is this what would be hashed out in Phase 3?

Actions

Owner	Action Item
☐	
☐	
☐	
☐	