FedRAMP OSCAL Early Adopters Workgroup Knowledge Capture

August 23, 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

- 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 demoed/reviewed the Github folder changes. Working through SAR and POAM today, which was just added last week.
- Tom Sr discussed the SAR and small changes made
    - Stephanie: We already opened up a ticket. NIST provides you the opportunity to capture a list of all the methods you used. Instead of leveraging mixed, we were leveraging [breaking up]. We are looking at the mixed only for the historical, but I think it would be useful where they are analyzing the documents and interviewing at the same time. Instead of having 2 separate tests, it may be easier to have 1 result.
    - Dmitri: I am hearing this for the schematron side.
    - Stephanie: This was for the attestation piece for the recommendations. Understanding the use case for that. Because the SAR document for Rev 5 that was published doesn't have a section for recommendations, and I don't know if they would even submit a SAR without a recommendation, and if they do where the 3PAO recommends not moving forward, what is the workflow for that?

- Tom Sr: We have a policy discussion this week we started with the review teams. That did not make the list this week, but I am going to add it to the list for the next biweekly meeting. When we get to Phase II or III, I'm going to ask a member to join the call.
- **Matthew Couglin: I agree with Stephanie. Also, FR has issued guidance for Rev 5 documenting POAM changes. Will this be updated in allowed strings?**
  - **Tom Sr: I'm sure we could do that. If there is a value list, we can update that. Dmitri, can we do that? Is that list in the FR values file? Or in the schematron?**
  - **Dmitri: I will need to double check.**
  - **Stephanie: And that's going to require a NIST ticket too because their NIST schema requires 1 of the following values, not any other. I would recommend adding an additional role: was the test done manual or automated?**
  - **Tom Sr: Good idea. I will talk with the policy review teams.**
- Bryan: You brought up the response points issue. What does this have to do with the substructure in Rev 5 v 4?
- Tom Sr: It's related to getting everybody to agree. There's a lot of CSPs that don't have a GRC tool, so they depend on those templates heavily and we got a lot of feedback on them. Regenerating the Appendix A templates has been challenging.
- Bryan: Are you going to be breaking it out?
  - Tom Sr: SSP validation?
  - Bryan: Yes
  - Tom Sr: I will check
  - Stephanie: For response points, should we have an error or a warning?
  - Tom: That's what he's saying. Should we relax it from an error to a warning. Rev 5 doesn't have it defined yet, or it's defined and we are getting approval. For Rev 4 I'd rather leave it as an error. Anyone object?
  - Matthew: I know we got feedback, breaking it out into the subpart level was helpful and submitting it through OSCAL with a warning would be prudent.
  - Stephanie: Does that mean they are not getting each response point?
  - Matthew: Right now it's at the part level. AC1A instead of AC1A-1, 2 etc.
  - Stephanie: If you look at the Rev 5 profile from FR compared to Rev 4, some controls are answered at different levels. Defined by the response point..
  - Matthew: The error is being thrown because we are doing it as AC1 And not AC1A
  - Stephanie: You need to adjust your responses to meet the requirements. Too granular. I think that's the idea of the response point, what does the government need.
  - Tom Sr: I am not sure. Can we revisit this when the resolved profiles and profiles with response points come out? I think it may address the issue.
  - Greg: There's another perspective for whether it should be an error or warning. The adoption of OSCAL overall. It's a friction point for the adoption of OSCAL when it's an error. I would make the case that the control implementations are going to be

reviewed by a human for now. Maybe we need a different class of warning like we discussed before. I would ask FR considers loosening certain errors like this and classifying them differently to not have CSPs not want to use OSCAL. I would argue that the loosening strategy is around encouraging the adoption of OSCAL.

- Tom Sr: That's what we've been trying to do, but two sides of the coin. I don't have an issue relaxing it to a warning but at some point, we will have to change that.
- Valinder: One more point I want to put in: The response points are not only for statements in SSP but also objectives in SAR and there is a data integrity issue if you do not write it correctly. Tools use these response points to maintain these data sets. To Greg's point I agree, don't want them to have blockers, but I think the error is needed here. Shouldn't be fatal but should be serious enough that it warrants breaking the integrity.
- Greg: It seems to be the case that the more one looks at the data and the way it works, oh I have to generate these each time. If I make a change in the SSP, I don't necessarily need to redo my SAP and SAR, or is that the expectation?
- Tom Sr: Yes, you'd have to regenerate them. But depends on the change.
- Stephanie: A lot of those changes for the SSP hopefully will be part of the annual assessment controls anyways right?
- Tom Sr: Good point. Back to 84H, I think we should leave it as an error for now. We will revisit when we transition to Rev 5.
- Dmitri: Question for clarification about the submitting of attachments from Julien: To clarify, for submitting attachments did we agree on the use of rlinks vs base64? Additionally, for rlinks, can dummy links be provided for security purposes until rlinks get hashed out?
- Tom Sr: Our links. The larger those files get, the processing time on the backend increases exponentially. Took 45min for a POAM.
- Tom Jr: I want to second what Valinder said. When we built the sample package in OSCAL, the idea of response points was at the core of everything we did. Without those, you're going to have issues downstream. When we start doing SCR, there has to be linkage between the SSP and SAR and PAOM. That might generate additional assessments that need to be done, so it needs to be done right.
- Greg: Makes sense, but if that's the vision, the transparency around these need to be generated at the same time. It's always a package.
- Matthew: I don't think it's not not responding to response points but being able to add response points. Grouping multiple test procedures at the wrong control level unless they are more separated.
- Stepahnie: We submitted bugs to identify any misalignments. There are 35 controls that have different response controls than Rev 5. So manual is responding at a different level but this will be fixed.

- **Tom Sr: Maybe having a dedicated session to go over Rev 5 profiles, get them to you guys as a draft form before the final release to get your input, might be a good idea. I'll talk to Rene.** Going to table this one for now. We need to revisit 84H in Rev 5 when we get the profiles out to make sure we've covered our bases.

Participant Questions/Conversation:

- Stephanie Lacy: Do you know when the api documentation will be loaded? The link on the portal doesn't seem to work.
    - Tom Sr. : About 2 weeks
    - Bill: Correct.
    - Stephanie: Perfect! Is the api up and running now? Seems like date structures have changed…
    - Tom Sr: Yes, and they've changed a little. wEre are trying to get the docs out as soon as possible. We just finished week 4, probably going to be closer to 6 weeks

Chat copy:

Stephanie Lacy

12:06 PM

Do you known when the api documentation will be loaded? The link on the portal doesn't seem to work.

Stephanie Lacy

12:10 PM

Perfect! Is the api up and running now?

Stephanie Lacy

12:12 PM

Seems like date structures have changed…

Stephanie Lacy

12:21 PM

1.10 OSCAL nist doesn't like Georgian format

Julien Devlin

12:51 PM

To clarify, for submitting attachments did we agree on the use of rlinks vs base64? Additionally, for rlinks, can dummy links be provided for security purposes until rlinks get hashed out?

Stephanie Lacy

12:54 PM

We are doing rlinks

Stephanie Lacy

12:57 PM

Check bugs 400, 401, 402, 403, and 404 for response point misalignment

Actions

Owner	Action Item
☐	
☐	
☐	
☐	