FedRAMP

FedRAMP OSCAL Early Adopters

December 6th, 2023

GSA

info@fedramp.gov

fedramp.gov

Introduction

Purpose: Recurring meetings to engage Cloud Service Providers, 3PAOs, tool vendors and other participants in FedRAMP's OSCAL Early Adopters Workgroup (OEAW) activities.

Outcomes:

- Shared understanding of Charter and Mission of the Workgroup
- Shared understanding of FedRAMP OSCAL package requirements, and discussion of possible enhancements and solutions.

Agenda:

- Welcome
- Guiding Principles/Mission Review
- OEAW Updates
- Issues Discussion
- Open Forum
- Next Steps & Closing

FedRAMP OEAW Guiding Principles

Keep the discussion respectful

Speak from your own experience

Focus on ideas

Be curious, seek understanding

Challenge through questions

Keep it technical

OEAW Workgroup Charter/Mission - Original

Charter:

To create an engagement space for Cloud Service Providers, 3PAOs, tool developers and others who are adopting OSCAL for the FedRAMP® use case with the goal of refinement of FedRAMP automation technology and processes.

Mission Elements:

- Bring OSCAL early adopters together to foster community engagement for FedRAMP OSCAL use case.
- Provide bi-directional dialogue with participants on engineering process current and future state.
- Refinement of initial technology and processes for the FedRAMP OSCAL automation ecosystem.
- Testing of initial releases of FedRAMP Automation Portal and RESTful API services.

Adjusted Priorities

Our goals remain the same:

- Provide a means for the PMO to accept OSCAL-based FedRAMP packages.
- Provide REST APIs for the submission of OSCAL-based FedRAMP packages and continuous monitoring data.
- Support reuse of FedRAMP authorizations using OSCAL-based FedRAMP packages.
- Provide tooling to support CSPs in the creation of valid OSCAL-based FedRAMP packages.
- Provide tooling to support 3PAOs and agencies in using OSCAL-based FedRAMP packages.

We need to adjust our focus to achieve these goals:

- Local OSCAL validation tooling will allow validation of OSCAL content without the need to prematurely share sensitive data.
- Stabilizing the OSCAL guides is needed to support local validation tooling and the GRC acquisition.
- Need to reduce friction where possible in maintaining OSCAL guides and baselines as well as FedRAMP templates.

OEAW Workgroup Charter/Mission - Adjusted

Charter:

To create an engagement space for Cloud Service Providers, 3PAOs, tool developers and others who are adopting OSCAL for the FedRAMP® use case with the goal of refinement of FedRAMP automation technology and processes.

Mission Elements:

- Bring OSCAL early adopters together to foster community engagement around FedRAMP OSCAL use cases.
- Directly engage with OSCAL early adopter stakeholders to advance technology and processes supporting FedRAMP automation using OSCAL.
- Drive stakeholder feedback on GitHub issues relating to FedRAMP baselines, guides, validation, and other related efforts.
- **On hold:** Standardize RESTful APIs supporting machine-oriented, stakeholder interaction with FedRAMP.

OEAW Going Forward

FedRAMP needs the OSCAL Early Adopters Workgroup to help with:

- Continued identification of issues with the FedRAMP baselines, guides, and validations using GitHub issues.
- Submitting GitHub pull requests to fix defects in baselines, guides, and validations.
- Feedback on changes to FedRAMP baselines, guides, and validations through review of GitHub pull requests.
- Testing and refinement of new tooling supporting FedRAMP stakeholders.

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

General Updates

General Updates

Work on hold due to the GRC tool acquisition:

- Submission portal will be discontinued
  - OSCAL content will be submitted with the traditional package for now.
  - **Moderate impact** systems using MAX.gov / USDA Connect.gov
  - **High** impact systems have their own repositories
- API discussions on hold until GRC tool is acquired
  - API submission is still the mid-term goal.

Transitioning:

- VITG early adopters GitHub repository transition to GSA - https://github.com/GSA/fedramp-oscal-early adopters

Adjusted priorities:

- Local validation tooling supporting OSCAL validation
- HTML-based guides and guide improvements
- Refocus Early Adopters Workgroup
  - Coordinating OSCAL guide improvement work
  - Early testing of local validation tooling
- Additional tooling
  - Human rendering of OSCAL-based packages
  - Generation of FedRAMP templates based on OSCAL baselines

Fedramp Automation Repository Improvements

The following improvements have been made to the repo:

- Updated issues templates - https://github.com/GSA/fedramp-automation/issues/new/choose
- New project board - https://github.com/orgs/GSA/projects/25

Future improvements:

- Automated broken link checking
- Others?

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

Issues Discussion

Issue/PR Summary

PRs needing stakeholder review:

- (#502) Adding Core Controls and Response Points to Rev5 Baselines
- (#539) Early Review: Markdown/HTML version of FedRAMP Guides for OSCAL-based Content

Issue for discussion today:

- (#461, usnistgov/OSCAL#1956) Discrepancy between NIST OSCAL JSON and XML structure for AR and POAM
- (#535) Discrepancy between baseline XML response-points and SSP Appendix A response-points

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

Discrepancy between OSCAL JSON and XML for AR and POAM

usnistgov/OSCAL#1956, GSA/fedramp-automation#461

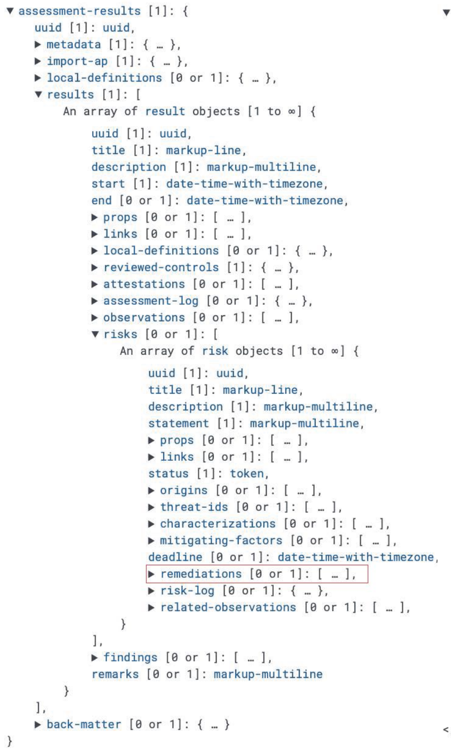
A discrepancy exists between the OSCAL XML and JSON formats for risk responses in AR and POAM models.

- JSON -> remediations
- XML -> response

While the naming is different, the data is the same. For JSON “remediations” should be “responses”.

Recommendation:

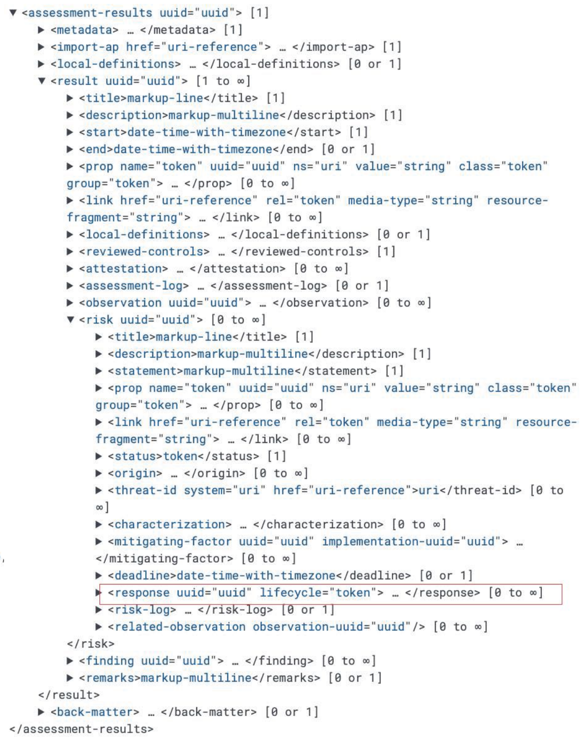
Keep as-is and clarify semantics in documentation, since changing will break backwards compatibility, requiring an OSCAL 2.0.0 release.



```
▼ assessment-results [1]: {
    uuid [1]: uuid,
  ▶ metadata [1]: { … },
  ▶ import-ap [1]: { … },
  ▶ local-definitions [0 or 1]: { … },
  ▼ results [1]: [
      An array of result objects [1 to ∞] {

        uuid [1]: uuid,
        title [1]: markup-line,
        description [1]: markup-multiline,
        start [1]: date-time-with-timezone,
        end [0 or 1]: date-time-with-timezone,
      ▶ props [0 or 1]: [ … ],
      ▶ links [0 or 1]: [ … ],
      ▶ local-definitions [0 or 1]: { … },
      ▶ reviewed-controls [1]: { … },
      ▶ attestations [0 or 1]: [ … ],
      ▶ assessment-log [0 or 1]: { … },
      ▶ observations [0 or 1]: [ … ],
      ▼ risks [0 or 1]: [
          An array of risk objects [1 to ∞] {

            uuid [1]: uuid,
            title [1]: markup-line,
            description [1]: markup-multiline,
            statement [1]: markup-multiline,
          ▶ props [0 or 1]: [ … ],
          ▶ links [0 or 1]: [ … ],
            status [1]: token,
          ▶ origins [0 or 1]: [ … ],
          ▶ threat-ids [0 or 1]: [ … ],
          ▶ characterizations [0 or 1]: [ … ],
          ▶ mitigating-factors [0 or 1]: [ … ],
            deadline [0 or 1]: date-time-with-timezone,
          ▶ remediations [0 or 1]: [ … ],
          ▶ risk-log [0 or 1]: { … },
          ▶ related-observations [0 or 1]: [ … ],
          }
        ],
      ▶ findings [0 or 1]: [ … ],
        remarks [0 or 1]: markup-multiline
      }
    ],
  ▶ back-matter [0 or 1]: { … }
}
```



```
▼ <assessment-results uuid="uuid"> [1]
  ▶ <metadata> … </metadata> [1]
  ▶ <import-ap href="uri-reference"> … </import-ap> [1]
  ▶ <local-definitions> … </local-definitions> [0 or 1]
  ▼ <result uuid="uuid"> [1 to ∞]
    ▶ <title>markup-line</title> [1]
    ▶ <description>markup-multiline</description> [1]
    ▶ <start>date-time-with-timezone</start> [1]
    ▶ <end>date-time-with-timezone</end> [0 or 1]
    ▶ <prop name="token" uuid="uuid" ns="uri" value="string" class="token"
    group="token"> … </prop> [0 to ∞]
    ▶ <link href="uri-reference" rel="token" media-type="string" resource-
    fragment="string"> … </link> [0 to ∞]
    ▶ <local-definitions> … </local-definitions> [0 or 1]
    ▶ <reviewed-controls> … </reviewed-controls> [1]
    ▶ <attestation> … </attestation> [0 to ∞]
    ▶ <assessment-log> … </assessment-log> [0 or 1]
    ▶ <observation uuid="uuid"> … </observation> [0 to ∞]
    ▼ <risk uuid="uuid"> [0 to ∞]
      ▶ <title>markup-line</title> [1]
      ▶ <description>markup-multiline</description> [1]
      ▶ <statement>markup-multiline</statement> [1]
      ▶ <prop name="token" uuid="uuid" ns="uri" value="string" class="token"
      group="token"> … </prop> [0 to ∞]
      ▶ <link href="uri-reference" rel="token" media-type="string" resource-
      fragment="string"> … </link> [0 to ∞]
      ▶ <status>token</status> [1]
      ▶ <origin> … </origin> [0 to ∞]
      ▶ <threat-id system="uri" href="uri-reference">uri</threat-id> [0 to
      ∞]
      ▶ <characterization> … </characterization> [0 to ∞]
      ▶ <mitigating-factor uuid="uuid" implementation-uuid="uuid"> …
      </mitigating-factor> [0 to ∞]
      ▶ <deadline>date-time-with-timezone</deadline> [0 or 1]
      ▶ <response uuid="uuid" lifecycle="token"> … </response> [0 to ∞]
      ▶ <risk-log> … </risk-log> [0 or 1]
      ▶ <related-observation observation-uuid="uuid"/> [0 to ∞]
    </risk>
    ▶ <finding uuid="uuid"> … </finding> [0 to ∞]
    ▶ <remarks>markup-multiline</remarks> [0 or 1]
  </result>
  ▶ <back-matter> … </back-matter> [0 or 1]
</assessment-results>
```

Discrepancy between baseline XML response-points and SSP Appendix A response-points

GSA/fedramp-automation#535

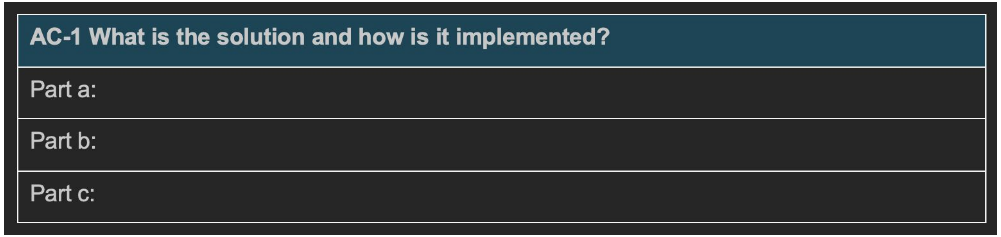
Issue:

A discrepancy exists between the control implementation response points specified in the OSCAL XML profiles versus those implied in the legacy Word SSP Appendix A.

Background:

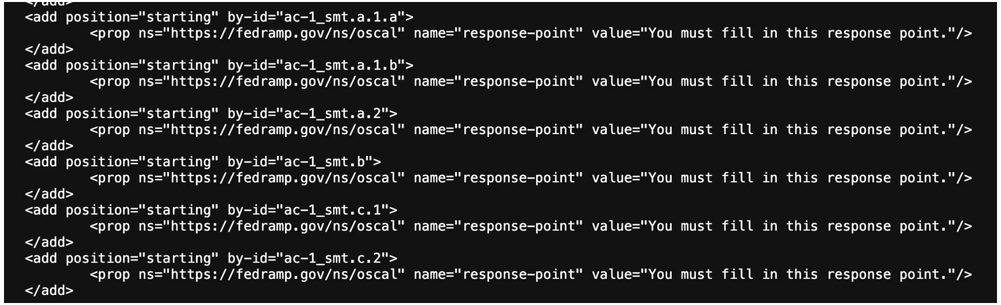
The OSCAL response points were intentionally specified at a more granular level (for -1 controls) to help guide SSP authors in providing more detailed control implementation statements, however, this presumed that more granular responses could be aggregated by rendering tools.

Response Points in Word SSP Appendix A



AC-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

Response Points in OSCAL Baselines



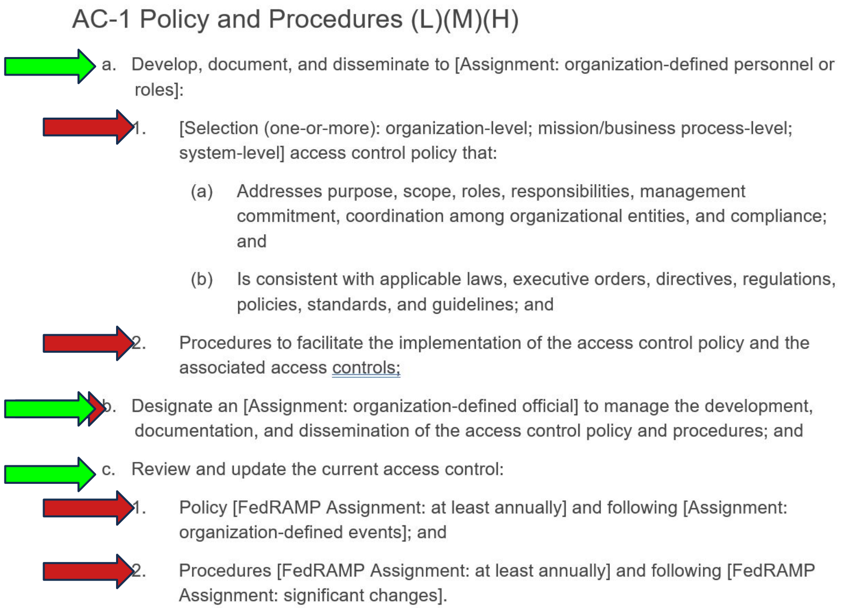
```
</add>
<add position="starting" by-id="ac-1_smt.a.1.a">
        <prop ns="https://fedramp.gov/ns/oscal" name="response-point" value="You must fill in this response point."/>
</add>
<add position="starting" by-id="ac-1_smt.a.1.b">
        <prop ns="https://fedramp.gov/ns/oscal" name="response-point" value="You must fill in this response point."/>
</add>
<add position="starting" by-id="ac-1_smt.a.2">
        <prop ns="https://fedramp.gov/ns/oscal" name="response-point" value="You must fill in this response point."/>
</add>
<add position="starting" by-id="ac-1_smt.b">
        <prop ns="https://fedramp.gov/ns/oscal" name="response-point" value="You must fill in this response point."/>
</add>
<add position="starting" by-id="ac-1_smt.c.1">
        <prop ns="https://fedramp.gov/ns/oscal" name="response-point" value="You must fill in this response point."/>
</add>
<add position="starting" by-id="ac-1_smt.c.2">
        <prop ns="https://fedramp.gov/ns/oscal" name="response-point" value="You must fill in this response point."/>
</add>
```

Discrepancy between baseline XML response-points and SSP Appendix A response-points (Continued)

GSA/fedramp-automation#535

Should FedRAMP align the response points as follows:

- For "-1" controls (e.g., AC-1, AT-1, AU-1, etc.):
  - Require a response at the letter sub-part of the requirement (e.g., AC-1(a), AC-1(b), AC-1(c))
- For controls that do not have multiple parts (e.g., AC-2(1), AC-2(2), AC-2(4), etc.):
  - require a response at the control level
- For controls that have multiple parts (e.g., AC-2(a) through AC-2(l)), and perhaps sub parts (e.g., AC-2(d)(1), AC-2(d)(2), etc.):
  - Only require response at the letter sub-part level (e.g. AC-2(d)) but not at the sub-part (e.g., AC-2(d)(1)



AC-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] access control policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

1. Policy [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

Discrepancy between baseline XML response-points and SSP Appendix A response-points (Continued)

GSA/fedramp-automation#535

Impacted Controls:

- AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PS-1, RA-1, SA-1, SC-1, SI-1, SR-1
- For controls that do not have multiple parts (e.g., AC-2(1), AC-2(2), AC-2(4), etc.):
  - require a response at the control level
- For controls that have multiple parts (e.g., AC-2(a) through AC-2(l)), and perhaps sub parts (e.g., AC-2(d)(1), AC-2(d)(2), etc.):
  - Only require response at the part level (e.g. AC-2(d)) but not at the sub-part (e.g., AC-2(d)(1)

Open Forum

Next Steps

Thank you

Our next OEAW virtual meeting will be on

Wednesday, December 20th, 2023 at 12p ET.

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

Learn more at fedramp.gov

@FEDRAMP

How to Submit Issues with FedRAMP

Ensuring your outstanding issues or questions are received:

Issues can be submitted in several ways:

✓ **Preferred**	**Alternate**
Open an issue on fedramp-automation github so that it will benefit the NIST/FedRAMP community. **https://github.com/GSA/fedramp-automation/issues**	Email us at **oscal@fedramp.gov**

OSCAL Resources

NIST:

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

Learning Resources: https://pages.nist.gov/OSCAL/learn/

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

Early Adopter repo: https://github.com/GSA/fedramp-oscal-earlyadopters