FedRAMP

OSCAL Developer Data Bites

August 31, 2023

GSA

info@fedramp.gov
fedramp.gov

Introduction

Purpose: To create space for dialogue between developers who use OSCAL and the FedRAMP® automation team.

Outcomes:

- Shared understanding of OSCAL artifacts and package requirements for Rev 4&5.
- Productive discussion around OSCAL.

Agenda:

- Welcome
- Pre-Submitted Q&A
- FedRAMP Automation Community Updates
- Managing Document Revisions & Artifacts
- Open Forum
- Next Steps & Closing

Data Bites Guiding Principles

Keep the discussion respectful

Be curious, seek understanding

Speak from your own experience

Challenge through questions

Focus on ideas

Keep it technical

One Year of Data Bites!

Pre-Submitted Questions

Pre-Submitted Questions

Question:

SAR: Do 3PAO's truly submit results without recommending authorizations?

Asking for the attestation requirement to be lifted on account of no authorization recommendation resulting in no attestation. Or, if it can be confirmed that 3PAO's do submit results regardless of the recommendation status, that supports the need for an attestation's recommend authorization even if the value is "no".

Answer:

Escalating to PMO for resolution.

If the PMO office does not recommend authorization, has there ever been an instance where they gave a result that did not recommend authorization? Or did they regularly omit the data, because they cannot provide the desired recommendation. If it's not recommended, what happens?

FedRAMP Automation Community Updates

August 31, 2023

NIST OSCAL version 1.1.1 release (pending)

- FedRAMP will conduct impact analysis and update templates and guidance.

Rev. 4 & Rev 5

- FedRAMP OSCAL Early Adopters Workgroup (OEAW) is progressing and has completed relaxing various validations until Rev 4 / Rev 5 package structure can be fully determined.
- Next Meeting: Starting on availability of REST APIs for OEAW members.
- Starting Phase 2 in mid September to determine package submission process and artifacts.
- Additions to Rev 5 profiles and resolved-profile catalogs in process for core controls and response points.

Issues/Ticket Tags

- **Closed issues/pull requests this cycle**
  - #466- Invalid Links to SAR Guide on github readme.
  - #454 - Remove code related to "automation" and "technical" controls.

Managing Document Revisions & Artifacts

Rev 4 vs. Rev 5 package artifacts

Rev. 4 Document	Rev. 5 Document
3PAO Readiness Assessment Report Guide	3PAO Readiness Assessment Report Guide
FedRAMP Moderate Readiness Assessment Report (RAR) Template	FedRAMP Moderate Readiness Assessment Report (RAR) Template
FedRAMP High Readiness Assessment Report (RAR) Template	FedRAMP High Readiness Assessment Report (RAR) Template
FedRAMP System Security Plan (SSP) Low Baseline Template	FedRAMP High, Moderate, Low, LI-SaaS Baseline System Security Plan (SSP)
FedRAMP System Security Plan (SSP) Moderate Baseline Template	
FedRAMP System Security Plan (SSP) High Baseline Template	

Rev 4 vs. Rev 5 package artifacts

Rev. 4 Document	Rev. 5 Document
· FedRAMP Tailored Security Controls Baseline	SSP Appendix A: LI-SaaS FedRAMP Security Controls
· FedRAMP Tailored Li-SaaS Template	
· FedRAMP Tailored Li-SaaS Ato Letter Template	
· FedRAMP Tailored Li-SaaS Continuous Monitoring Guide	
· FedRAMP Tailored Li- SaaS Self-Attestation Requirements	
ilored Li-SaaS Requirements	

Rev 4 vs. Rev 5 package artifacts

Rev. 4 Document	Rev. 5 Document
N/A- No Rev. 4 version	SSP Appendix A: Low FedRAMP Security Controls
N/A- No Rev. 4 version	SSP Appendix A: Moderate FedRAMP Security Controls
N/A- No Rev. 4 version	SSP Appendix A: High FedRAMP Security Controls
SSP Attachment 5 - FedRAMP Rules of Behavior (RoB) Template	SSP Appendix F: Rules of Behavior (RoB) Template
SSP Attachment 6 - FedRAMP Information System Contingency Plan (ISCP) Template	SSP Appendix G: Information System Contingency Plan (ISCP) Template

Rev 4 vs. Rev 5 package artifacts

Rev. 4 Document	Rev. 5 Document
SSP Attachment 9 - FedRAMP Low or Moderate Control Implementation Summary (CIS) Workbook Template	SSP Appendix J: CIS and CRM Workbook *(updated 7/13/2023)*
SSP Attachment 9 - FedRAMP High Control Implementation Summary (CIS) Workbook Template	
SSP Attachment 13 - FedRAMP Integrated Inventory Workbook Template	SSP Appendix M: Integrated Inventory Workbook Template
N/A- No Rev. 4 version	SSP Appendix Q: Cryptographic Modules Table
FedRAMP Security Assessment Report (SAR) Template	FedRAMP Security Assessment Report (SAR) Template
FedRAMP Annual Security Assessment Report (SAR) Template	
SAR Appendix A - FedRAMP Risk Exposure Table Template	SAR Appendix A: FedRAMP Risk Exposure Table (RET) Template

Rev 4 vs. Rev 5 package artifacts

Rev. 4 Document	Rev. 5 Document
FedRAMP Security Assessment Plan (SAP) Template	FedRAMP Security Assessment Plan (SAP) Template
FedRAMP Annual Security Assessment Plan (SAP) Template	
SAP Appendix A - FedRAMP Low Security Test Case Procedures Template	SAP Appendix A: FedRAMP Low Security Test Case Procedures Template
SAP Appendix A - FedRAMP Moderate Security Test Case Procedures Template	SAP Appendix A: FedRAMP Moderate Security Test Case Procedures Template
SAP Appendix A - FedRAMP High Security Test Case Procedures Template	SAP Appendix A: FedRAMP High Security Test Case Procedures Template
FedRAMP Security Controls Baseline	FedRAMP Security Controls Baseline
N/A- No Rev. 4 version	FedRAMP Rev. 4 to Rev. 5 Assessment Controls Selection Template *(updated 8/10/2023)*

Rev 4 vs. Rev 5 package artifacts

Rev. 4 Document	Rev. 5 Document
FedRAMP Initial Authorization Package Checklist	FedRAMP Initial Authorization Package Checklist
SSP Attachment 12 - FedRAMP Laws and Regulations Template	FedRAMP Laws, Regulations, Standards and Guidance Reference
SSP Attachment 4 - FedRAMP Privacy Impact Assessment (PIA) Template	Retired
FedRAMP Master Acronym & Glossary	Retired
FedRAMP Low Authorization Toolkit	Retired
FedRAMP Tailored Authorization Toolkit	Retired
FedRAMP Moderate Authorization Toolkit	Retired
FedRAMP High Authorization Toolkit	Retired

Rev 4 vs. Rev 5 package artifacts

OSCAL

- System Security Plan (SSP) attachments are now called **Appendices**.
  - FedRAMP validation output mapping and references will change.
- SSP document alignment changes
  - Single template for front matter.
  - Separated controls section into Appendix A by baseline in legacy templates.
  - OSCAL Impacts:
    - Appendix A is included in control-implementation assembly.
    - No separate document (needed for OSCAL submission).
    - FedRAMP automation team considering displaying front matter in Portal/GRC tool vs. generating.

Rev 4 vs. Rev 5 package artifacts

OSCAL

- SSP Attachment 9 migrated to individual CIS/CRM Workbook **(Appendix J).**
  - OSCAL Impacts:
    - Able to generate implementation summary and control origination worksheet summaries from OSCAL.
    - Annotation of responsibility matrix (Low, Moderate, High, LI-SaaS) Worksheet (in progress).
    - Automation team is looking at adding to FedRAMP OSCAL use case for responsibility matrices.
- SSP Attachment 4 - FedRAMP Privacy Impact Assessment - **retired**.
  - OSCAL validations now have this as optional.
    - Relaxed in FedRAMP validations to warning.

Rev 4 vs. Rev 5 package artifacts

OSCAL

- **(Added for Rev 5)** SSP Appendix Q SSP Appendix Q: Cryptographic Modules Table.
  - OSCAL Impacts:
    - Not currently represented in OSCAL.
    - FedRAMP automation team is looking at specifically extending FR namespace for support.
- SSP Attachment 12 - FedRAMP Laws and Regulations no longer required in Rev 5 OSCAL **(separate legacy document)**.
  - Also relaxed Rev 4 validation check.

Open Forum

Thank you

Our next Developer Data Bites virtual meeting will be on

Thursday, September 28, 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:

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

Validations work: https://github.com/18F/fedramp-automation/tree/master/src/validations

Web based validation tool:

https://federalist-2372d2fd-fc94-42fe-bcc7-a8af4f664a51.app.cloud.gov/site/18f/fedramp-automation/#/documents/system-security-plan