FedRAMP

# OSCAL Developer Data Bites

**September 28, 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 lessons learned from authoring your first OSCAL artifacts for FedRAMP.
- Productive discussion around OSCAL.

**Agenda**:

- Welcome
- Pre-Submitted Q&A
- FedRAMP Automation Community Updates
- Lessons Learned: Authoring your first OSCAL artifacts for FedRAMP
- 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

# Pre-Submitted Questions

# Pre-Submitted Questions

## Question:

**Regarding SA-4 in SSP Appendix A Low FedRAMP Controls.  Under each control, our understanding is that the table entitled "What is the solution and how is it implemented?" contains which control parts are included in the low baseline, and the ones that only have an empty row instead of rows with part names mean that the base control is included.**

**SA-4 is the only control to have a blank row in addition to rows with named parts. Our assumption is that this means both the base control and the parts in the table are included. Is this correct?**

**Answer:**

This issue is being worked with the document template folks at PMO and will be address by them in a forthcoming release.

# Pre-Submitted Questions

## Question:

**When taking a currently authorized FedRAMP CSP's SSP to OSCAL, what is the GSA's expectation on porting over historical revisions? If the Word-based SSP lists several, is the expectation that these would be recreated in OSCAL?**

**Answer:**

There has been no specific guidance from the PMO yet on this.   We have recommend in previous Data Bites and Early Adopters meetings as good practice to convert over the underlying systems first (i.e. IaaS, PaaS) to OSCAL before doing SaaS etc..

I will present this question to the PMO review team and discuss and follow-up once I get an answer.

# FedRAMP Automation Community Updates

## September 28, 2023

### NIST OSCAL version 1.1.1 release (pending)

- FedRAMP automation team is conduct impact analysis and will update templates and guidance accordingly.

### Rev. 4 & Rev 5

- FedRAMP OSCAL Early Adopters Workgroup (OEAW) is progressing and has completed first meeting in Phase 2 (Artifact Management).
- Next Meeting: Comparing compressed artifact formats from PMO standard to proposed OEAW standard.
- Additions to Rev 5 profiles and resolved-profile catalogs in process for core controls and response points to be released shortly.

### Issues/Ticket Tags

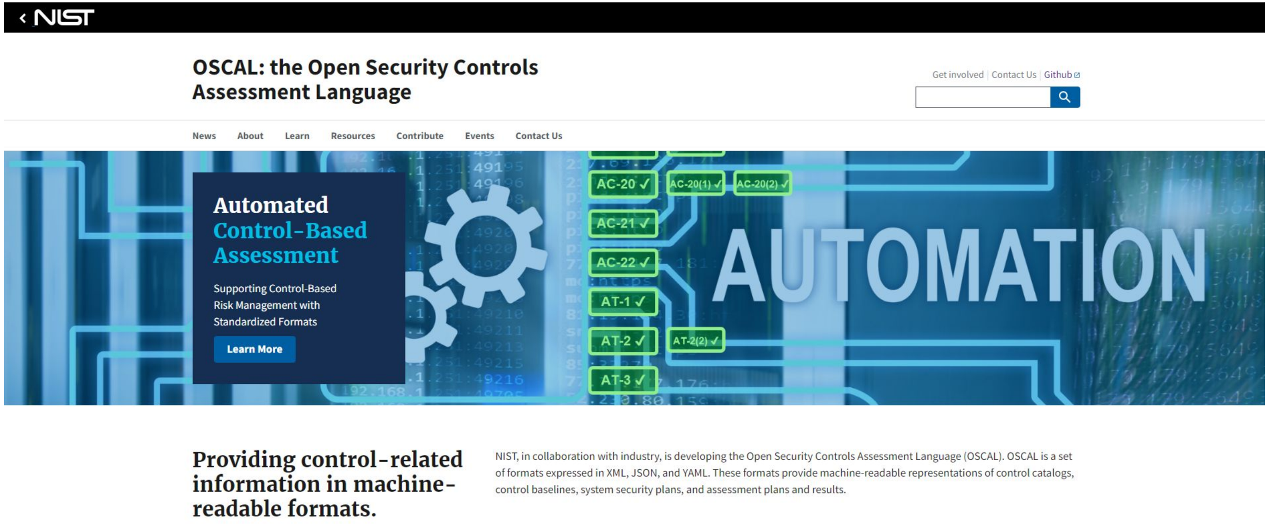
- **Closed issues/pull requests this cycle**
    - #500- SA-4 in SSP Appendix A Low FedRAMP Controls.
    - #497 - Baseline Documents OSCAL Version is 1.0.4 when 1.1.1 is Out
    - #477 - Generating RAR workflow (AS modified SAP, SAR, and POAM)
    - #466 - Invalid Links to SAR Guide
    - #454 - Remove code related to "automation" and "technical" controls

# Lessons Learned: Authoring your first OSCAL artifacts for FedRAMP.

# Lessons Learned

## Before you begin

**Familiarize yourself with the NIST OSCAL Model: [https://pages.nist.gov/OSCAL](https://pages.nist.gov/OSCAL)**



OSCAL: the Open Security Controls Assessment Language

Automated Control-Based Assessment

Supporting Control-Based Risk Management with Standardized Formats

Providing control-related information in machine-readable formats.

NIST, in collaboration with industry, is developing the Open Security Controls Assessment Language (OSCAL). OSCAL is a set of formats expressed in XML, JSON, and YAML. These formats provide machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results.

# Lessons Learned

## Before you begin

**FedRAMP Automation Repository (Github): [https://github.com/GSA/fedramp-automation](https://github.com/GSA/fedramp-automation)**

- **OSCAL Guides and Templates**
  - □ To ensure our stakeholders can fully express a FedRAMP Security Authorization Package using NIST's OSCAL syntax, the FedRAMP PMO has drafted:
    - ○ FedRAMP-specific **extensions** and guidance
    - ○ OSCAL files in XML and JSON formats to serve as **examples for each deliverable**
- **Schematron Validations**
  - □ The FedRAMP-Automation GitHub repository contains the following schematron validation resources:
    - ○ Complete documentation for each FedRAMP specific validation rule
    - ○ Tools to validate FedRAMP artifacts in browser or install locally
    - ○ Example code applying the validation rules using the compiled-XLST artifact in selected languages

# Lessons Learned

## Authoring Tools

Pre-Requisites:

- Access to a schema aware editing tool (Oxygen XML Editor/Visual Studio)
- Access to a UUID generator (https://uuidgenerator.net)
- Access to FedRAMP Automation Repo (https://github.com/GSA/fedramp-automation)

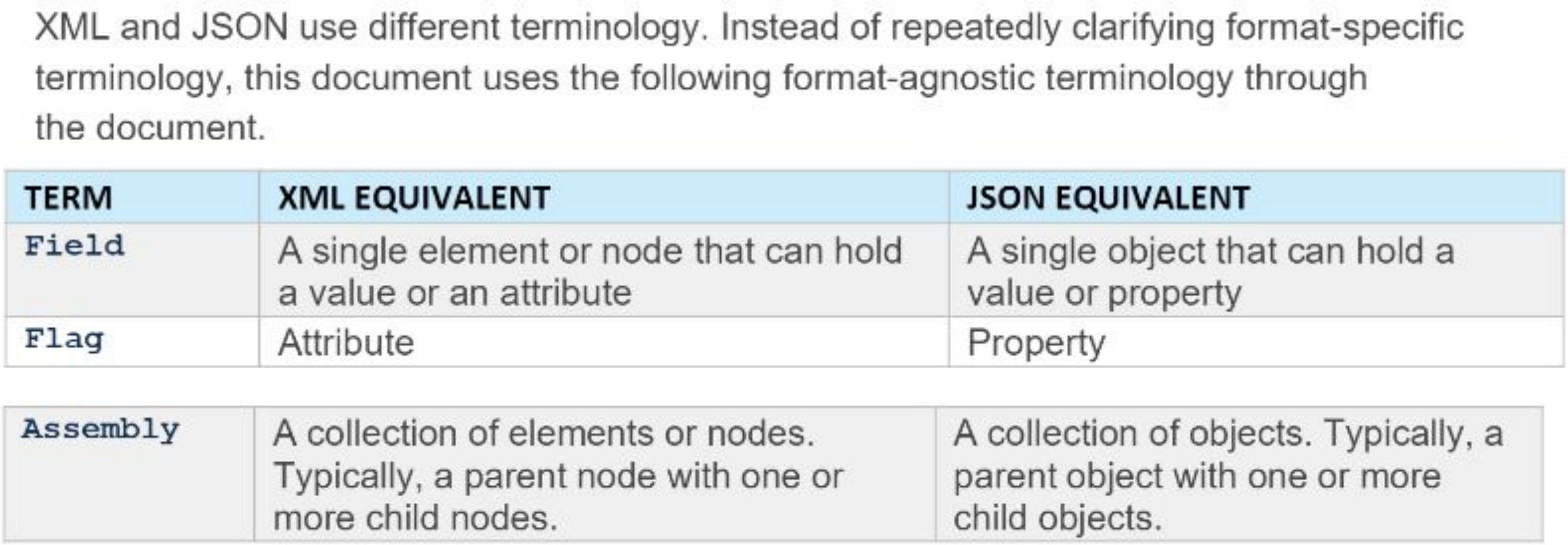
**Decisions:**

- Are you generating for a FedRAMP OSCAL XML, JSON or YAML artifact?
- Decide on which system sensitivity level you are going to use – this decides the schema to use.

# Lessons Learned

## Important things to understand

XML vs. JSON - [Guide to FedRAMP OSCAL Based Content.pdf]



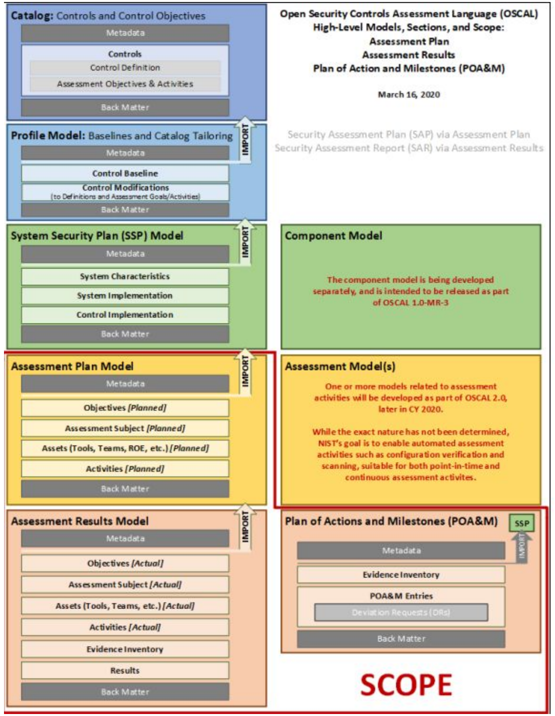
XML and JSON use different terminology. Instead of repeatedly clarifying format-specific terminology, this document uses the following format-agnostic terminology through the document.

| TERM | XML EQUIVALENT | JSON EQUIVALENT |
|---|---|---|
| `Field` | A single element or node that can hold a value or an attribute | A single object that can hold a value or property |
| `Flag` | Attribute | Property |
| `Assembly` | A collection of elements or nodes. Typically, a parent node with one or more child nodes. | A collection of objects. Typically, a parent object with one or more child objects. |

# Lessons Learned

## Model Overview

- OSCAL is a layered Model aligning components within the model with authorization artifacts.
- Each artifact is dependent upon each other.
- SSP imports the profile/resolved-profile-catalog.
- SAP imports the SSP
- SAR imports the SAP
- POA&M imports the SSP (* dependent upon inventory*)
- Start with understanding the profiles and resolved profile catalogs relationship (see [Guide to FedRAMP OSCAL Based System Security Plans.pdf]f)



Open Security Controls Assessment Language (OSCAL)
High-Level Models, Sections, and Scope:
Assessment Plan
Assessment Results
Plan of Action and Milestones (POA&M)

March 16, 2020

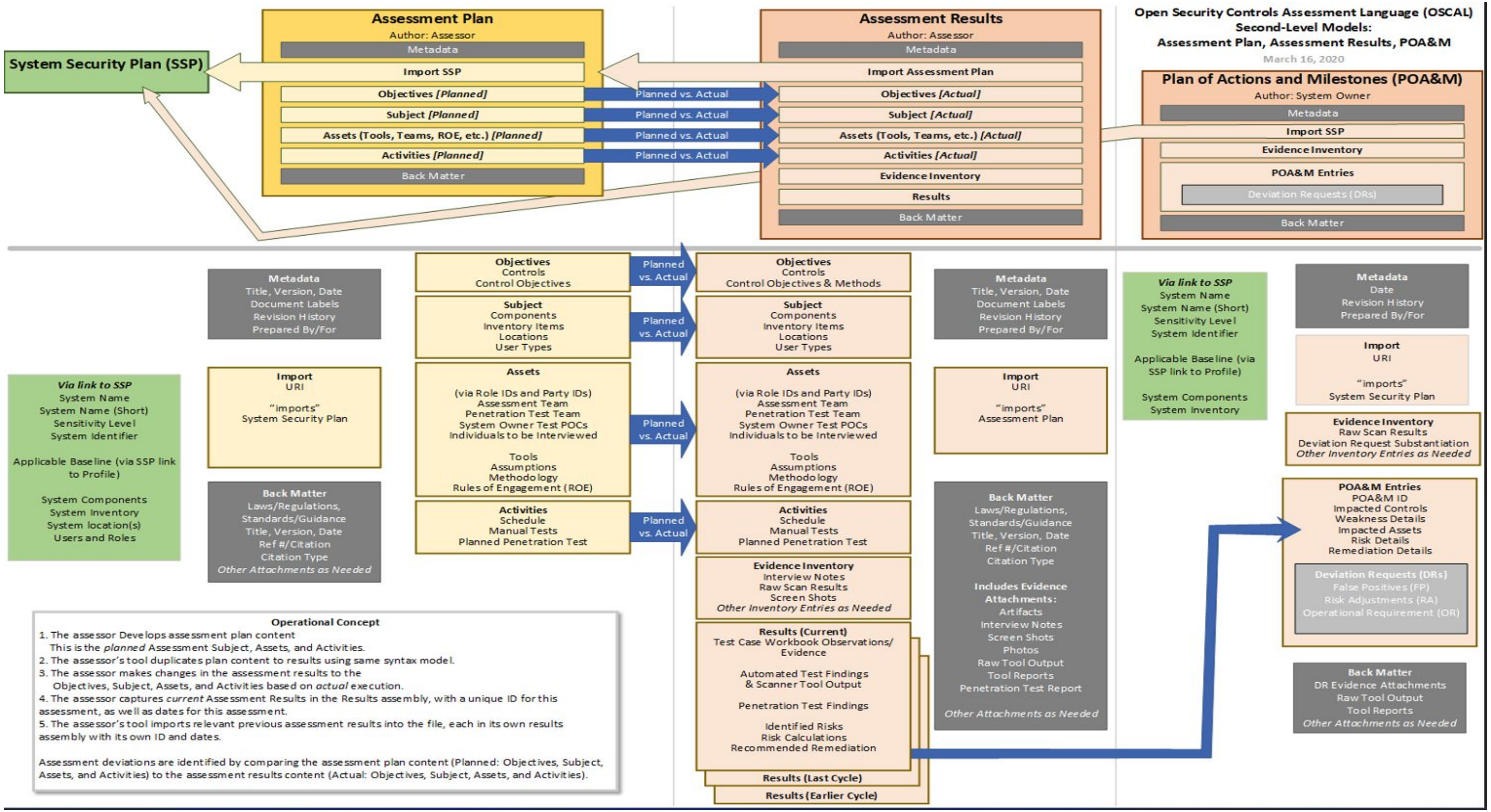
Security Assessment Plan (SAP) via Assessment Plan
Security Assessment Report (SAR) via Assessment Results

The component model is being developed separately, and is intended to be released as part of OSCAL 1.0-MR-3

One or more models related to assessment activities will be developed as part of OSCAL 2.0, later in CY 2020.

While the exact nature has not been determined, NIST's goal is to enable automated assessment activities such as configuration verification and scanning, suitable for both point-in-time and continuous assessment activites.

# Lessons Learned (Relationships)



Open Security Controls Assessment Language (OSCAL)
Second-Level Models:
Assessment Plan, Assessment Results, POA&M
March 16, 2020

System Security Plan (SSP)

**Assessment Plan**
Author: Assessor
Metadata
Import SSP
Objectives *[Planned]*
Subject *[Planned]*
Assets (Tools, Teams, ROE, etc.) *[Planned]*
Activities *[Planned]*
Back Matter

Planned vs. Actual
Planned vs. Actual
Planned vs. Actual
Planned vs. Actual

**Assessment Results**
Author: Assessor
Metadata
Import Assessment Plan
Objectives *[Actual]*
Subject *[Actual]*
Assets (Tools, Teams, etc.) *[Actual]*
Activities *[Actual]*
Evidence Inventory
Results
Back Matter

**Plan of Actions and Milestones (POA&M)**
Author: System Owner
Metadata
Import SSP
Evidence Inventory
POA&M Entries
Deviation Requests (DRs)
Back Matter

*Via link to SSP*
System Name
System Name (Short)
Sensitivity Level
System Identifier

Applicable Baseline (via SSP link to Profile)

System Components
System Inventory
System location(s)
Users and Roles

**Metadata**
Title, Version, Date
Document Labels
Revision History
Prepared By/For

**Import**
URI

"imports"
System Security Plan

**Back Matter**
Laws/Regulations,
Standards/Guidance
Title, Version, Date
Ref #/Citation
Citation Type
*Other Attachments as Needed*

**Objectives**
Controls
Control Objectives

**Subject**
Components
Inventory Items
Locations
User Types

**Assets**

(via Role IDs and Party IDs)
Assessment Team
Penetration Test Team
System Owner Test POCs
Individuals to be Interviewed

Tools
Assumptions
Methodology
Rules of Engagement (ROE)

**Activities**
Schedule
Manual Tests
Planned Penetration Test

Planned vs. Actual
Planned vs. Actual
Planned vs. Actual
Planned vs. Actual

**Objectives**
Controls
Control Objectives & Methods

**Subject**
Components
Inventory Items
Locations
User Types

**Assets**

(via Role IDs and Party IDs)
Assessment Team
Penetration Test Team
System Owner Test POCs
Individuals to be Interviewed

Tools
Assumptions
Methodology
Rules of Engagement (ROE)

**Activities**
Schedule
Manual Tests
Planned Penetration Test

**Evidence Inventory**
Interview Notes
Raw Scan Results
Screen Shots
*Other Inventory Entries as Needed*

**Results (Current)**
Test Case Workbook Observations/ Evidence

Automated Test Findings
& Scanner Tool Output

Penetration Test Findings

Identified Risks
Risk Calculations
Recommended Remediation

**Results (Last Cycle)**

**Results (Earlier Cycle)**

**Metadata**
Title, Version, Date
Document Labels
Revision History
Prepared By/For

**Import**
URI

"imports"
Assessment Plan

**Back Matter**
Laws/Regulations,
Standards/Guidance
Title, Version, Date
Ref #/Citation
Citation Type

**Includes Evidence Attachments:**
Artifacts
Interview Notes
Screen Shots
Photos
Raw Tool Output
Tool Reports
Penetration Test Report

*Other Attachments as Needed*

*Via link to SSP*
System Name
System Name (Short)
Sensitivity Level
System Identifier

Applicable Baseline (via SSP link to Profile)

System Components
System Inventory

**Metadata**
Date
Revision History
Prepared By/For

**Import**
URI

"imports"
System Security Plan

**Evidence Inventory**
Raw Scan Results
Deviation Request Substantiation
*Other Inventory Entries as Needed*

**POA&M Entries**
POA&M ID
Impacted Controls
Weakness Details
Impacted Assets
Risk Details
Remediation Details

**Deviation Requests (DRs)**
False Positives (FP)
Risk Adjustments (RA)
Operational Requirement (OR)

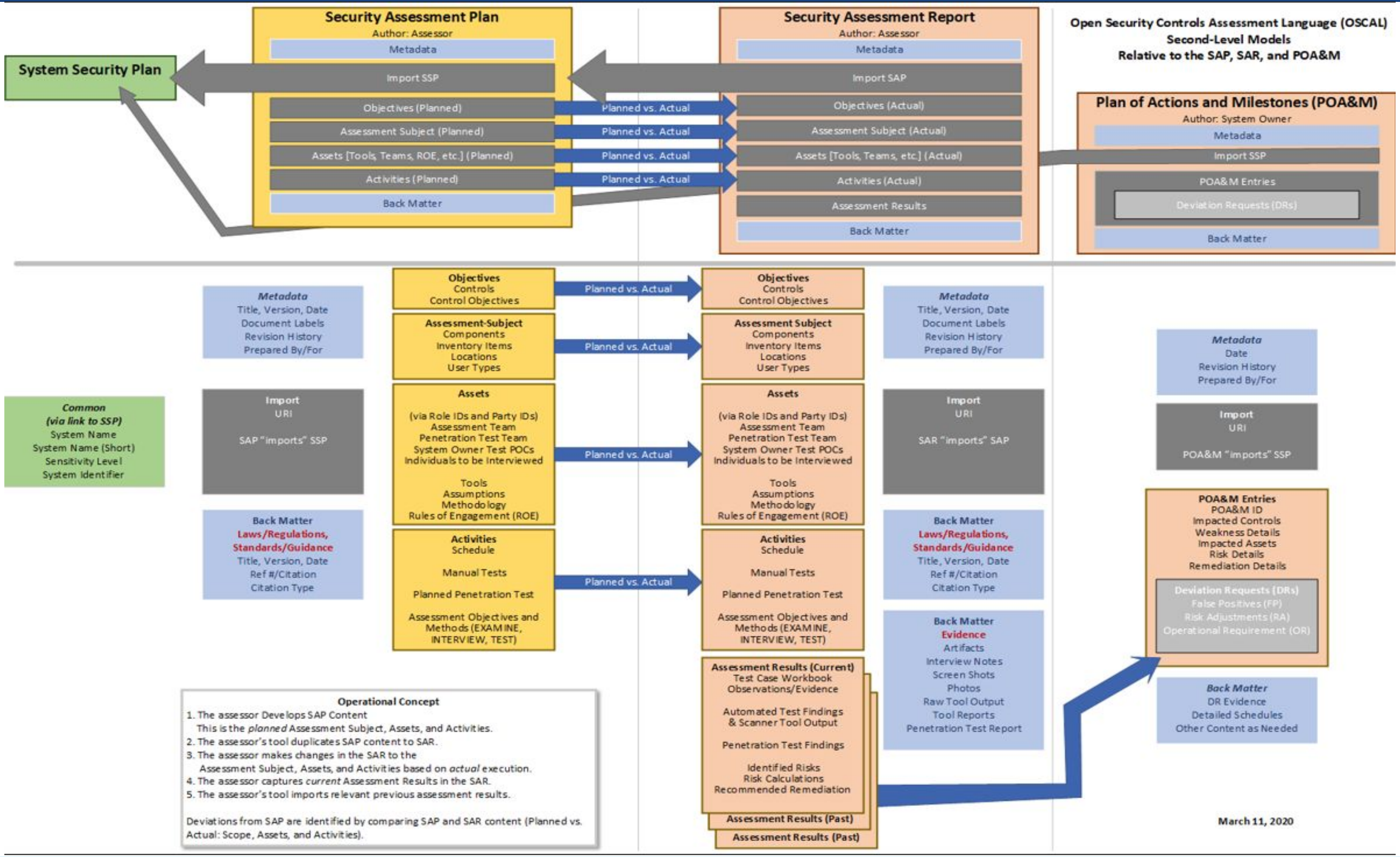
**Back Matter**
DR Evidence Attachments
Raw Tool Output
Tool Reports
*Other Attachments as Needed*

**Operational Concept**

1. The assessor Develops assessment plan content
   This is the *planned* Assessment Subject, Assets, and Activities.
2. The assessor's tool duplicates plan content to results using same syntax model.
3. The assessor makes changes in the assessment results to the Objectives, Subject, Assets, and Activities based on *actual* execution.
4. The assessor captures *current* Assessment Results in the Results assembly, with a unique ID for this assessment, as well as dates for this assessment.
5. The assessor's tool imports relevant previous assessment results into the file, each in its own results assembly with its own ID and dates.

Assessment deviations are identified by comparing the assessment plan content (Planned: Objectives, Subject, Assets, and Activities) to the assessment results content (Actual: Objectives, Subject, Assets, and Activities).

# Lessons Learned



Open Security Controls Assessment Language (OSCAL)
Second-Level Models
Relative to the SAP, SAR, and POA&M

*Common (via link to SSP)*
System Name
System Name (Short)
Sensitivity Level
System Identifier

*Metadata*
Title, Version, Date
Document Labels
Revision History
Prepared By/For

Import
URI
SAP "imports" SSP

Back Matter
Laws/Regulations, Standards/Guidance
Title, Version, Date
Ref #/Citation
Citation Type

Objectives
Controls
Control Objectives

Assessment-Subject
Components
Inventory Items
Locations
User Types

Assets
(via Role IDs and Party IDs)
Assessment Team
Penetration Test Team
System Owner Test POCs
Individuals to be Interviewed

Tools
Assumptions
Methodology
Rules of Engagement (ROE)

Activities
Schedule

Manual Tests

Planned Penetration Test

Assessment Objectives and Methods (EXAMINE, INTERVIEW, TEST)

Objectives
Controls
Control Objectives

Assessment Subject
Components
Inventory Items
Locations
User Types

Assets
(via Role IDs and Party IDs)
Assessment Team
Penetration Test Team
System Owner Test POCs
Individuals to be Interviewed

Tools
Assumptions
Methodology
Rules of Engagement (ROE)

Activities
Schedule

Manual Tests

Planned Penetration Test

Assessment Objectives and Methods (EXAMINE, INTERVIEW, TEST)

Assessment Results (Current)
Test Case Workbook
Observations/Evidence

Automated Test Findings
& Scanner Tool Output

Penetration Test Findings

Identified Risks
Risk Calculations
Recommended Remediation

Assessment Results (Past)
Assessment Results (Past)

*Metadata*
Title, Version, Date
Document Labels
Revision History
Prepared By/For

Import
URI
SAR "imports" SAP

Back Matter
Laws/Regulations, Standards/Guidance
Title, Version, Date
Ref #/Citation
Citation Type

Back Matter
Evidence
Artifacts
Interview Notes
Screen Shots
Photos
Raw Tool Output
Tool Reports
Penetration Test Report

*Metadata*
Date
Revision History
Prepared By/For

Import
URI
POA&M "imports" SSP

POA&M Entries
POA&M ID
Impacted Controls
Weakness Details
Impacted Assets
Risk Details
Remediation Details

Deviation Requests (DRs)
False Positives (FP)
Risk Adjustments (RA)
Operational Requirement (OR)

*Back Matter*
DR Evidence
Detailed Schedules
Other Content as Needed

Operational Concept
1. The assessor Develops SAP Content
   This is the *planned* Assessment Subject, Assets, and Activities.
2. The assessor's tool duplicates SAP content to SAR.
3. The assessor makes changes in the SAR to the
   Assessment Subject, Assets, and Activities based on *actual* execution.
4. The assessor captures *current* Assessment Results in the SAR.
5. The assessor's tool imports relevant previous assessment results.

Deviations from SAP are identified by comparing SAP and SAR content (Planned vs. Actual: Scope, Assets, and Activities).

March 11, 2020

# Lessons Learned

- Always use the NIST schemas and metaschemas to determine values and check against NIST schema and metaschema for each document type and details. Your best friend to do this:

  https://github.com/usnistgov/OSCAL/tree/main/src/metaschema

- Other links you will find useful:

  src/metaschema/oscal_ssp_metaschema.xml
  xml/schema/oscal_ssp_schema.xsd
  src/metaschema/oscal_assessment-plan_metaschema.xml
  xml/schema/oscal_assessment-plan_schema.xsd
  src/metaschema/oscal_assessment-results_metaschema.xml
  xml/schema/oscal_assessment-results_schema.xsd
  src/metaschema/oscal_poam_metaschema.xml
  xml/schema/oscal_poam_schema.xsd

- Start with authoring XML if doing by hand.

# Lessons Learned Discussion

**Based on your experience with OSCAL thus far…**

What additional things have you come across?

What challenges have you had to overcome with the Model specific to your implementation?

# Open Forum

# Thank you

Our next Developer Data Bites virtual meeting will be on

**Thursday, October 26, 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