DRAFT

GUIDE TO OSCAL-BASED FEDRAMP PLAN OF ACTION AND MILESTONES (POA&M)

Version 1.0

June 1, 2020

FedRAMP

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
6/1/2020	Initial Publication	1.0	FedRAMP PMO
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

How to Contact Us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact *info@FedRAMP.gov.*

For more information about FedRAMP, see https://FedRAMP.gov.

TABLE OF CONTENTS

1. OVERVIEW

1.1. Who Should Use This Document?

This document is intended for technical staff and tool developers implementing solutions for importing, exporting, and manipulating Open Security Controls Assessment Language (OSCAL)-based FedRAMP Security Assessment Report (SAR) content.

It provides guidance and examples intended to guide an organization in the production and use of OSCAL-based FedRAMP-compliant SAR files. Our goal is to enable your organization to develop tools that will seamlessly ensure these standards are met so your security practitioners can focus on SAR content and accuracy rather than formatting and presentation.

1.2. Related Documents

This document does not stand along. It provides information specific to developing tools to create and manage OSCAL-based, FedRAMP-compliant Security Assessment Reports.

Refer to the *Guide to OSCAL-based FedRAMP Content* for foundational information and core concepts.

The *Guide to OSCAL-based FedRAMP Content*, contains foundational information and core concepts, which apply to all OSCAL-based FedRAMP guides. This document contains several references to that content guide.

Also, the OSCAL-based FedRAMP POA&M builds on the content expressed in the OSCAL-based System Security Plan (SSP). As a result, this document contains several references to the *Guide to OSCAL-based System Security Plans (SSP)*.

1.3. Basic Terminology

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.

These terms are used by NIST in the creation of OSCAL syntax.

Throughout this document, the following words are used to differentiate between requirements, recommendations, and options.

TERM	MEANING
must	Indicates a required action.
should	Indicates a recommended action, but not necessarily required.
may	Indicates an optional action.

2. FEDRAMP EXTENSIONS, CONFORMITY TAGS, DEFINED IDENTIFIERS, AND ACCEPTED VALUES

NIST designed the core OSCAL syntax to model cybersecurity information that is common to most organization and compliance frameworks; however, NIST also recognized the need to provide flexibility or organizations with unique information needs.

Instead of trying to provide a language that meets each organization's unique needs, NIST provided designed OSCAL with the ability to be extended.

A summary of the FedRAMP extensions, conformity tags, defined identifiers, and accepted values appears in the FedRAMP OSCAL Registry.

As a result, FedRAMP-compliant OSCAL files are a combination of the core OSCAL syntax and extensions defined by FedRAMP. The *Guide to OSCAL-based FedRAMP Content* describes the concepts behind FedRAMP extensions, conformity tags, defined identifiers, and accepted values. The extensions related to the POA&M are cited in this document in context of their use.

FedRAMP extensions, conformity tags, defined identifiers, and accepted values are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

These concepts are described in the Guide to OSCAL-based FedRAMP Content.

3. WORKING WITH OSCAL FILES

This section provides a summary of several important concepts and details that apply to OSCAL-based FedRAMP POA&M files.

The *Guide to OSCAL-based FedRAMP Content* provides important concepts necessary for working with any OSCAL-based FedRAMP file. Familiarization with those concepts is important to understanding this guide.

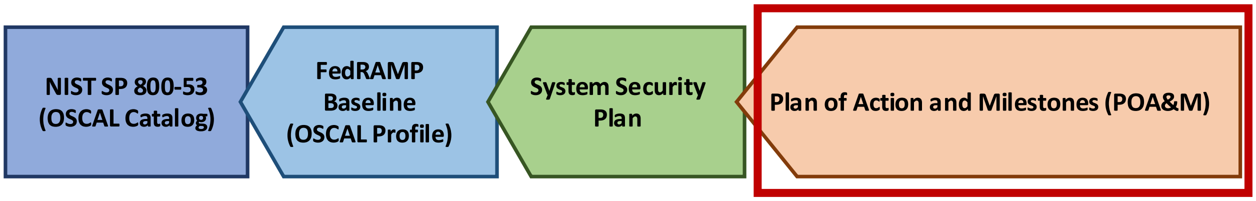
3.1. XML and JSON Formats

The examples provided here are in XML; however, FedRAMP accepts XML or JSON formatted OSCAL-based POA&M files. NIST offers a utility that provides lossless conversion of OSCAL-compliant files between XML and JSON in either direction.

You may submit your POA&M to FedRAMP using either format. If necessary, FedRAMP tools will convert the files for processing.

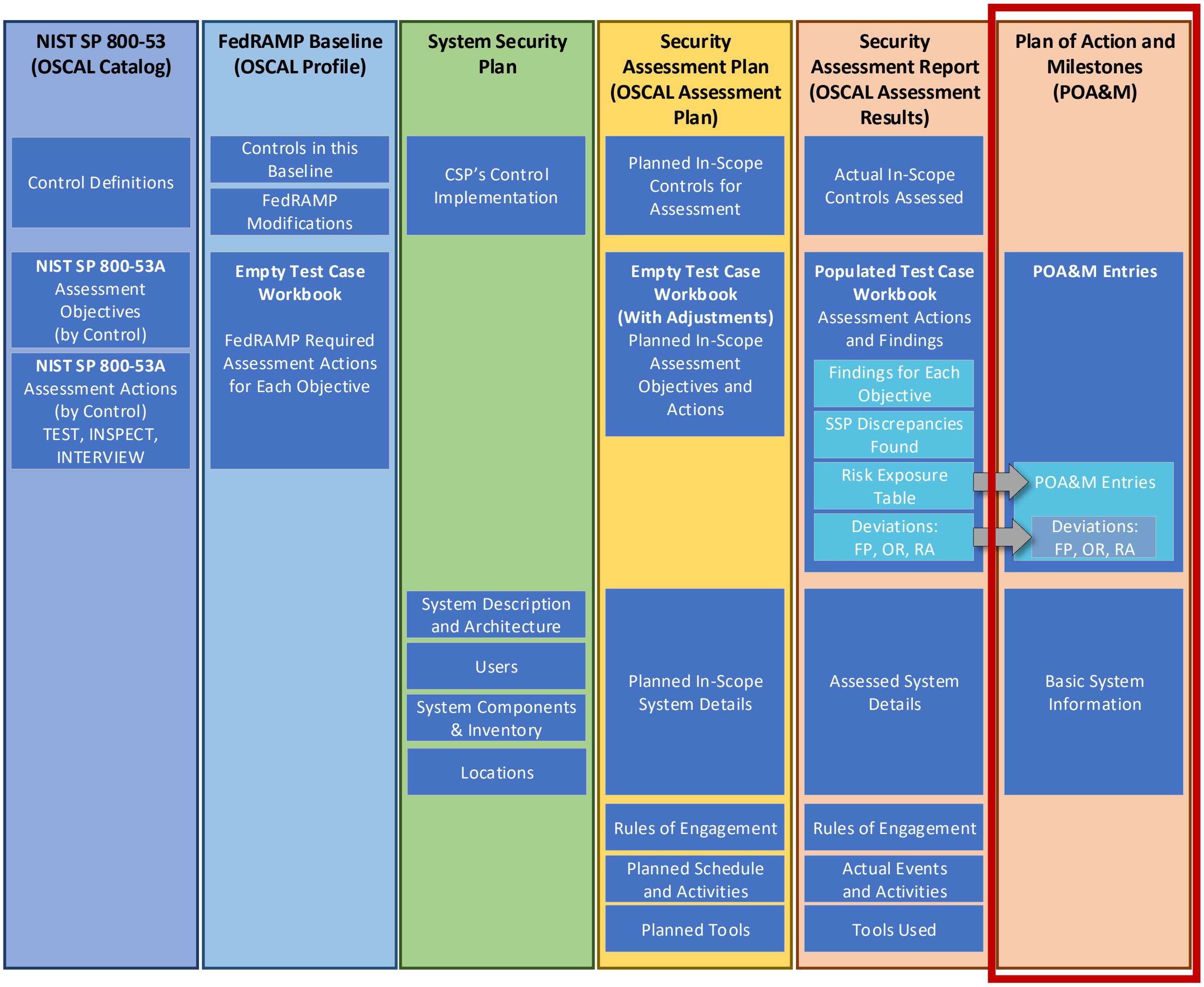
3.2. POA&M File Concepts

Unlike the traditional MS Word-and Excel based SSP and POA&M, the OSCAL-based versions of these files are designed to make information available through linkages, rather than duplicating information. In OSCAL, these linkages are established through `import` commands.



Each OSCAL file imports information from the one before it

For example, the systems impacted by a vulnerability as listed in the POA&M, are defined in the FedRAMP SSP and simply referenced by the POA&M.



Baseline and SSP Information is referenced instead of duplicated.

For this reason, an OSCAL-based POA&M points to the OSCAL-based SSP of the system being assessed. Instead of duplicating system details, the OSCAL-based POA&M simply points to the SSP content (via the SAP) for information such as system description, boundary, users, locations, and inventory items.

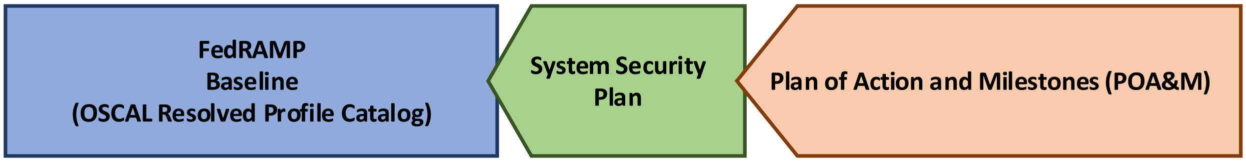
The POA&M also inherits the SSP's pointer to the appropriate OSCAL-based FedRAMP Baseline. Through that linkage, the POA&M references the control baseline definitions for the system's baseline.

3.2.1. Resolved Profile Catalogs

The resolved profile catalog for each FedRAMP baseline is the result of pre-processing the profile and catalog to produce the resulting data. This can reduce overhead for tools by eliminating the need to open and follow references from the profile to the catalog. It also includes only the catalog information relevant to the baseline, reducing the overhead of opening a larger catalog.

Where available, tool developers have the option of following the links from the profile to the catalog as described above, or using the resolved profile catalog. At this time catalogs and profiles remain relatively static. As OSCAL gains wider adoption, there is a risk that profiles and catalogs will become more dynamic, and a resolved profile catalog becomes more likely to be out of date.

Early adopters may wish to start with the resolved profile catalog now, and plan to add functionality later for the separate profile and catalog handling later in their product roadmap.

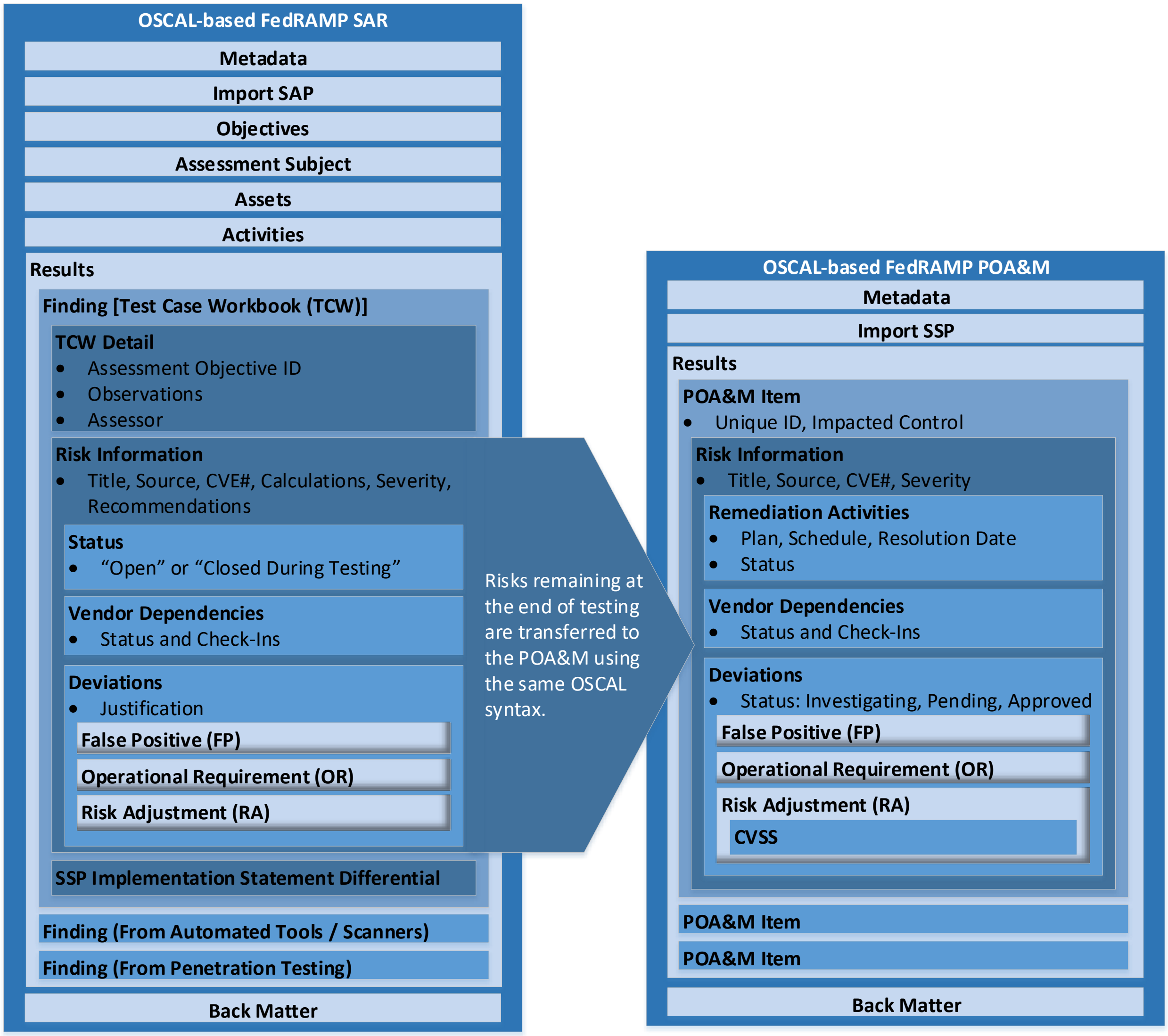

FedRAMP
Baseline
(OSCAL Resolved Profile Catalog)
System Security Plan
Plan of Action and Milestones (POA&M)

The Resolved Profile Catalog for each FedRAMP Baseline reduces tool processing

3.2.2. Residual Risks and SAR/POA&M Syntax Overlap

FedRAMP's requires residual risks from an initial or annual assessment to be reflected in the POA&M. The results portion of an OSCAL-based SAR uses the same syntax as the OSCAL based POA&M to enable easy transfer of residual risk information into the POA&M.

It is important to note that the content of a SAR is the assessor's responsibility, while the content of a POA&M is the system owner's responsibility; however, FedRAMP is aware some assessors will create or update a POA&M for the system owner. Regardless of who updates the POA&M, the common syntax enables easy transfer between a SAR tool and a POA&M tool.


OSCAL-based FedRAMP SAR
Metadata
Import SAP
Objectives
Assessment Subject
Assets
Activities
Results
Finding [Test Case Workbook (TCW)]
TCW Detail
• Assessment Objective ID
• Observations
• Assessor
Risk Information
• Title, Source, CVE#, Calculations, Severity, Recommendations
Status
• “Open” or “Closed During Testing”
Vendor Dependencies
• Status and Check-Ins
Deviations
• Justification
False Positive (FP)
Operational Requirement (OR)
Risk Adjustment (RA)
SSP Implementation Statement Differential
Finding (From Automated Tools / Scanners)
Finding (From Penetration Testing)
Back Matter
Risks remaining at the end of testing are transferred to the POA&M using the same OSCAL syntax.
OSCAL-based FedRAMP POA&M
Metadata
Import SSP
Results
POA&M Item
• Unique ID, Impacted Control
Risk Information
• Title, Source, CVE#, Severity
Remediation Activities
• Plan, Schedule, Resolution Date
• Status
Vendor Dependencies
• Status and Check-Ins
Deviations
• Status: Investigating, Pending, Approved
False Positive (FP)
Operational Requirement (OR)
Risk Adjustment (RA)
CVSS
POA&M Item
POA&M Item
Back Matter

A SAR tool can transfer residual risks to a POA&M using the same OSCAL syntax.

3.3. OSCAL-based FedRAMP POA&M Template

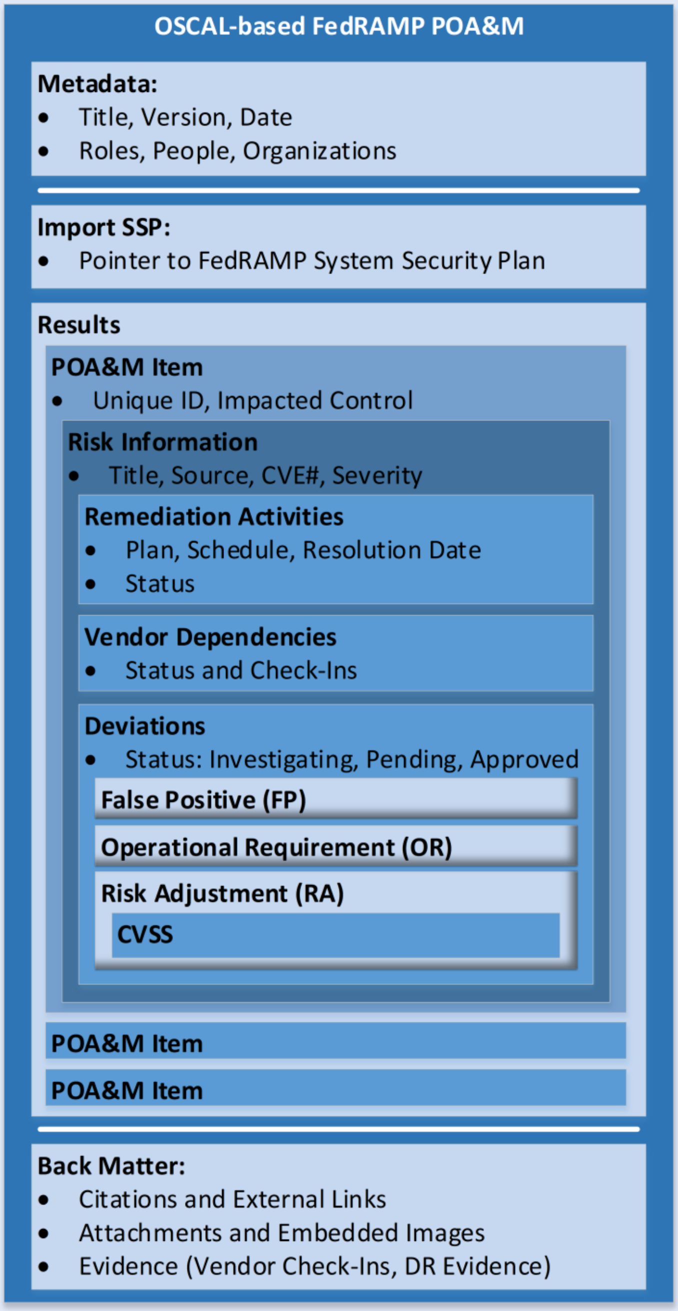
FedRAMP offers an OSCAL-based POA&M shell file in both XML and JSON formats. This shell contains many of the FedRAMP required standards to help get you started. This document is intended to work in concert with that file. The OSCAL-based FedRAMP POA&M Template is available in XML and JSON formats here:

- OSCAL-based FedRAMP POA&M Template (JSON Format): https://github.com/GSA/fedramp-automation/raw/master/templates/poam/json/FedRAMP-POAM-OSCAL-Template.json
- OSCAL-based FedRAMP POA&M Template (XML Format): https://github.com/GSA/fedramp-automation/raw/master/templates/poam/xml/FedRAMP-POAM-OSCAL-Template.xml

3.4. OSCAL's Minimum File Requirements

Every OSCAL-based FedRAMP POA&M file must have a minimum set of required fields/assemblies, and must follow the OSCAL Assessment Results model syntax found here:

https://pages.nist.gov/OSCAL/documentation/schema/assessment-results-layer/poam/


OSCAL-based FedRAMP POA&M
Metadata:
• Title, Version, Date
• Roles, People, Organizations
Import SSP:
• Pointer to FedRAMP System Security Plan
Results
POA&M Item
• Unique ID, Impacted Control
Risk Information
• Title, Source, CVE#, Severity
Remediation Activities
• Plan, Schedule, Resolution Date
• Status
Vendor Dependencies
• Status and Check-Ins
Deviations
• Status: Investigating, Pending, Approved
False Positive (FP)
Operational Requirement (OR)
Risk Adjustment (RA)
CVSS
POA&M Item
POA&M Item
Back Matter:
• Citations and External Links
• Attachments and Embedded Images
• Evidence (Vendor Check-Ins, DR Evidence)

Anatomy of an OSCAL-based FedRAMP POA&M Files

In addition to the core OSCAL syntax, the following FedRAMP-specific implementation applies:

- **Import SSP**: Identifies the OSCAL-based SSP of the system being assessed. Several pieces of information about a system that normally appear in a SAP are now referenced via this import statement.
- **Results**: Enumerates the POA&M entries. Each entry includes the risk information, plan for remediation, and status. Where applicable, deviation information is also included.

3.5. Importing the System Security Plan

OSCAL is designed for traceability. Because of this, the POA&M is designed to be linked to the SSP. Rather than duplicating content from the SSP, the POA&M is intended to reference the SSP content itself.

> ***Unavailable OSCAL-based SSP Content OR Monthly Deliverable Option***
>
> *OSCAL syntax requires the POA&M to import an OSCAL-based SSP, even if no OSCAL-based SSP exists.*
>
> *FedRAMP recognizes some system owners may adopt OSCAL for the POA&M before adopting it for their SSP. Similarly, FedRAMP does not currently require monthly delivery of the SSP with the monthly Continuous Monitoring POA&M delivery.*
>
> *To support these*

Use the `import-ssp` field to specify an existing OSCAL-based SSP. The href flag may include any valid uniform resource identifier (URI), including a relative path, absolute path, or URI fragment.

SAP Import Representation

```
   <import-ssp href="../sap/FedRAMP-SSP-OSCAL-File.xml" />

- OR -

   <import-ssp href="#attached-ssp" />
```

XPath Queries

```
(SAR) URI to SSP:
  /*/import-ssp/@href
```

If the value is a URI fragment, such as `#attached-ssp`, the name to the right of the hashtag (#) is the ID value of a resource in the SSP file's `back-matter`. Refer to the *Guide to OSCAL-based FedRAMP Content, Section 2.6, Citations, Attachments and Embedded Content in OSCAL Files*, for guidance on handling.

SAP Back Matter Representation

```
<back-matter>
   <resource id="attached-ssp">
      <title>[System Name] [FIPS-199 Level] SAP</title>
      <prop name="type" ns="https://fedramp.gov/ns/oscal">sap</prop>
      <!-- Specify the XML or JSON file location. Only one required. -->
      <rlink media-type="application/xml" href="./CSP_System_SSP.xml" />
      <rlink media-type="application/json" href="./CSP_System_SSP.json" />
   </resource>
</back-matter>
```

Do Not Embed the SSP in the POA&M

While OSCAL provides the ability to embed the SSP in the POA&M, this approach does not align with FedRAMP's current delivery process and is discouraged.

XPath Queries

```
(SAP) Referenced OSCAL-based SSP
XML:
  /*/back-matter/resource[@id='ssp-ref']/rlink[@media-
  type='application/xml']/@href
OR JSON:
  /*/back-matter/resource[@id='ssp-ref']/rlink[@media-
  type='application/json']/@href
```

FedRAMP SSPs are delivered by the Cloud Service Provider (CSP), while FedRAMP SAPs are delivered by the assessor. For this reason, FedRAMP strongly encourages the use of relative paths from the OSCAL-based FedRAMP SAP to the OSCAL-based FedRAMP SSP.

Where the provided path is invalid, tool developers should ensure the tool prompts the user for the updated path to the OSCAL-based SSP.

3.5.1. If No OSCAL-based SSP Exists (General)

The OSCAL-based POA&M must always have an `import-ssp` field, even if no OSCAL-based SSP is available. To compensate for this, use a URI fragment that points to a `resource` in the `back-matter`. The resource must have a FedRAMP conformity tag with the value:

- `no-oscal-ssp`

POA&M Representation

```
<import-ssp href="#ssp-information" />

<back-matter>
   <resource id="ssp-information">
      <title>System's Full Name</title>
      <prop name='conformity'
            ns='https://fedramp.gov/ns/oscal'>no-oscal-ssp</prop>
         <prop name="title-short"
            ns="https://fedramp.gov/ns/oscal">SFN</prop>
         <prop name="system-id"
            ns="https://fedramp.gov/ns/oscal">FR00000000</prop>
         <prop name="import-profile" ns="https://fedramp.gov/ns/oscal">
                                    #fedramp-moderate-baseline</prop>
   </resource>
</back-matter>
```

XPath Queries

```
(POA&M) Resource representing system details when no OSCAL-based SSP exists:
  /*/back-matter/resource/prop[@name='conformity']
  [@ns='https://fedramp.gov/ns/oscal'][string()='no-oscal-ssp']/..
```

3.6. Importing the FedRAMP Baseline

Once the content of the OSCAL-based SSP is accessible as a result of the actions in the previous section, the tool must then determine which FedRAMP baseline (profile) to open. Use the following query within the imported OSCAL-based SSP:

SSP XPath Queries

```
(SSP) Query the SSP for the Applicable Profile:
  /*/import-profile/@href
```

As with the `import-ssp` field in the previous section, this is any URI, including an absolute path, relative path, or URI fragment. If the value is a URI fragment, refer to the SSP's back-matter resource with that ID.

3.6.1. If No OSCAL-based SSP Exists (FedRAMP Baseline)

If no OSCAL-based SSP exists, as described in *Section 3.5.1, If No OSCAL-based SSP Exists (General),* the resource with the `no-oscal-ssp` conformity tag must designate the applicable FedRAMP baseline using the FedRAMP OSCAL Extension `baseline-resource-id`, which contains the ID of another resource containing a link to the appropriate FedRAMP baseline.

SAP Representation

```
<import-ssp href="#ssp" />

<back-matter>
   <resource id="ssp-information">
      <title>System's Full Name</title>
      <prop name='conformity'
            ns='https://fedramp.gov/ns/oscal'>no-oscal-ssp-available</prop>
            ns="https://fedramp.gov/ns/oscal">FR00000000</prop>
      <prop name="import-profile" ns="https://fedramp.gov/ns/oscal">
                                          #fedramp-moderate-baseline</prop>
   </resource>
</back-matter>
```

XPath Queries

```
(SAP) Path to Appropriate FedRAMP Baseline When No OSCAL-based SSP
  Exists:
  /*/back-matter/resource/prop [@name='conformity']
  [@ns='https://fedramp.gov/ns/oscal'] [string()='no-oscal-
  ssp']/../prop[@name='import-profile']
  [@ns='https://fedramp.gov/ns/oscal']

NOTE if URI fragment (starts with '#'), strip the '#' and use the
  following"
  /*/back-matter/resource[@id='fedramp-moderate-baseline']
  /rlink[@media-type='application/xml']/@href

NOTE: Replace 'application/xml' with 'application/json' for JSON version of
  baseline.
```

The OSCAL-based FedRAMP SAP Template includes pre-loaded resources for the FedRAMP High, Moderate, and Low baselines. Their Resource IDs are `fedramp-high-baseline`, `fedramp-moderate-baseline` and `fedramp-low-baseline`. This enables the import-profile field to simply use a URI reference, such as `#fedramp-moderate-baseline`.

4. POA&M TEMPLATE TO OSCAL MAPPING

The OSCAL POA&M Model is used to represent the FedRAMP POA&M. This model includes:

- Metadata and back-matter syntax, which is common to all OSCAL models
- ; and
- Results syntax, which is common to the SAR and POA&M.

This guide assumes tool developers are already familiar with the *Guide to OSCAL-based FedRAMP Content* .

Instead of duplicating content from those guides, this document refers to them and only add details that are unique to the POA&M.

The TCW is addressed first because several of the individual SAR pages are generated from OSCAL-based TCW content

4.1. Test Case Workbook (TCW) Findings

Understanding how to represent the test case workbook content in OSCAL's `results` assembly is a foundational concept, and is addressed first. The page-by-page SAR representation is built on this representation, typically by defining a "view" of the data.

4.2. Representing the POA&M

This is based on the Excel-based FedRAMP POA&M Template.

Content that is common across OSCAL file types is described in the *Guide to OSCAL-based FedRAMP Content*. This includes the following:

TOPIC	LOCATION
Title Page	*Guide to OSCAL-based FedRAMP Content, Section 4.1*
Prepared By/For	*Guide to OSCAL-based FedRAMP Content, Section 4.2 - 4.4*
Record of Template Changes	Not Applicable. Instead follow *Guide to OSCAL-based FedRAMP Content, Section 2.3.2, OSCAL Syntax Version*
Revision History	*Guide to OSCAL-based FedRAMP Content, Section 4.5*
How to Contact Us	*Guide to OSCAL-based FedRAMP Content, Section 4.5*
Laws, Regulations, Standards and Guidance	*Guide to OSCAL-based FedRAMP Content, Section 4.7 and 4.8*
Acronyms and Glossary	*Guide to OSCAL-based FedRAMP Content, Section 4.7*

The following pages are intended to be printed landscape on tabloid (11" x 17") paper.

[Image intentionally left blank.]

4.3. Automated Tools

Automated scanning tool output is simply another finding; however, the objective-status is typically not present.

FedRAMP requires exactly one finding assembly for each unique vulnerability identified by the scanning tool. Within this finding assembly, there must be exactly one observation assembly.

The date-time-stamp field must be set to the automation tool's discovery timestamp.

Within the observation assembly, the observation-method field must be set to "TEST", and the observation-type field must be set to "finding".

The uuid flag of the origin field must identify the automated tool's UUID, and the type flag must be set to "tool". The scanning tool should have been previously defined in the SAP's assets assembly and copied to the SAR. If not, the scanning tool should be added to the SAR assets assembly as described in the *Guide to OSCAL-based Security Assessment Plans (SAP)*, *Section 4.14, SAP Test Plan: Testing Performed Using Automated Tools*.

The href flag in the relevant-evidence field must contain a URI fragment that points to the resource containing the raw tool output attached in the back-matter.

At the end of the findings assembly, the UUID for the tool operator must be listed as the party-uuid for the finding. There may be more than one.

Representation

```
<results id="results-2">
   <!-- title, description, start, end -->
   <finding uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
      <title>Discovery Scan Results</title>
      <description><p>The results of the discovery scan.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <observation uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d">
         <description>
            <p>Sample description.</p>
         </description>
         <observation-method>TEST</observation-method>
         <observation-type>finding</observation-type>

         <!-- subject-reference -->
         <!-- subject-reference -->

         <origin uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" type="tool" />

         <relevant-evidence href="#19a07333-4e87-46dc-abab-adad60e706b9">
            <description>
               <p>Raw scanner tool output - discovery scan.</p>
            </description>
         </relevant-evidence>

      </observation>
      <party-uuid>f4568fda-c6d2-4640-adec-0012015af7d0</party-uuid>
      <party-uuid>e934d8b5-13e5-4f77-b55e-871e6f2df2fe</party-uuid>
   </finding>
</results>
```

[Image intentionally left blank.]

The `description` assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.3.1. Automated Tools: Discovery Scans

Any undocumented devices identified by the discovery scans must be added to the SAR's `local-definitions` assembly within the `assessment-subjects` assembly as either inventory-items or components, as described in the *Guide to OSCAL-based Security Assessment Plans (SAP)*, *Section 4.5, SAP IP Addresses Slated for Testing*.

This should include information such as IP address, host name, and OS, as well as any other details typically reported for an undocumented host. All component and inventory-item syntax from the SSP is available here. Each undocumented device should then be listed as an individual subject-reference.

If the assessor believes any of the undocumented devices represent a risk, the risk assembly may be added with the appropriate information; however, it is not automatically required for discovery scans..

Representation

```
<results id="results-2">
   <!-- title, description, start, end -->
   <finding uuid="d6316907-a5e5-4ad5-871d-f2f29938360e">
      <title>Discovery Scan Results</title>
      <description><p>The results of the discovery scan.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <observation uuid="6841d8eb-a72c-4672-acc2-2fd265d9617d">
         <description>
            <p>Undocumented devices found on network.</p>
         </description>
         <observation-method>TEST</observation-method>
         <observation-type>finding</observation-type>
         <subject-reference type="inventory-item"
                              uuid-ref="f61f4408-2cb8-444a-a312-bc88412e7c61" />
         <subject-reference type="inventory-item"
                              uuid-ref="02075556-3660-4112-8982-02fc7d6fac00" />
         <subject-reference type="inventory-item"
                              uuid-ref="5efe2c07-9fdf-453a-8457-6471046082fb" />
         <subject-reference type="component"
                              uuid-ref="75b059f2-a9ba-40b1-a1e0-881196ca1ead" />

         <origin uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" type="tool" />

         <relevant-evidence href="#19a07333-4e87-46dc-abab-adad60e706b9">
            <description>
               <p>Raw scanner tool output - discovery scan.</p>
            </description>
         </relevant-evidence>

      </observation>
      <!-- risk -->
      <party-uuid>f4568fda-c6d2-4640-adec-0012015af7d0</party-uuid>
      <party-uuid>e934d8b5-13e5-4f77-b55e-871e6f2df2fe</party-uuid>
   </finding>
</results>
```

[Image intentionally left blank.]

The description assemblies are *Markup multiline*, which enables the text to be formatted.
See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.3.2. Automated Tools: Identified Vulnerabilities

There must be one `finding` assembly for each unique vulnerability. All devices identified as having that unique vulnerability must be itemized with `subject-reference` fields in the `observations` assembly.

The individual components and inventory-items on which the scans are performed should already be marked as to whether authenticated scanning is possible.

All components and inventory-items found to have the vulnerability must be cited using their UUID in the subject-reference field. One subject-reference for each item.

The `uuid` flag of the `origin` field must be set to the tool's UUID, and the `type` flag must be set to "`tool`".

Representation

```
<results id="results-2">
   <!-- title, description, start, end -->
   <finding uuid="170dd310-1a92-4fcf-a12b-ebfa03d9e6d8">
      <title>[EXAMPLE]Infrastructure Scan Unique Vulnerability</title>
      <description><p>Example infrastructure scan finding.</p></description>
      <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
      <observation uuid="63fd3d97-26c9-4d4c-8d24-9fbc482b7f52">
         <description>
            <p>[EXAMPLE]Scanner Output.</p>
         </description>
         <observation-method>TEST</observation-method>
         <observation-type>finding</observation-type>
         <!-- subject-reference -->
         <!-- subject-reference -->

         <origin uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" type="tool" />

         <relevant-evidence href="#171b44a2-9b52-4c46-b912-54bd274b2761">
            <description>
               <p>Raw scanner tool output - Infrastructure and OS Scan.</p>
            </description>
         </relevant-evidence>
      </observation>
      <!-- risk - Exactly one. See next page. -->
 </results>
```

See next page for risk assembly

[Image intentionally left blank.]

The `description` assemblies are *Markup multiline*, which enables the text to be formatted. See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

The `risk` assembly uses `risk-metric` fields to capture relevant tool output details. The `system` flag allows `risk-metric` fields from different tools and different security frameworks to co-exist in the same file.

FedRAMP required risk-metric fields, such as likelihood and impact, have a system flag with a value of "https://fedramp.gov". FedRAMP required risk metrics must also have the class flag set to either "initial" or "residual". There must always be an intimal risk metric. If adjusted, there may be a residual risk metric as well.

The `uuid` flag of the `origin` field must be set to the tool's UUID, and the `type` flag must be set to "`tool`".

Representation

```
    <results id="results-2">
       <!-- title, description, start, end -->
       <finding uuid="170dd310-1a92-4fcf-a12b-ebfa03d9e6d8">
          <title>[EXAMPLE]Infrastructure Scan Unique Vulnerability</title>
          <description><p>Example infrastructure scan finding.</p></description>
          <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
          <!-- observation: impacted hosts, tool used, link to raw scans -->
          <risk uuid="ae628cc5-b64c-4030-af30-57e6b24a6ae7">
             <title>Vulnerability Title</title>
             <description>
                <p>This is a description of the vulnerability provided by the tool.</p>
             </description>

             <risk-metric name="vulnerability-id"
                                   system="scanner-name">VulID-001</risk-metric>
             <risk-metric name="plugin-id"
                                   system="scanner-name">Plugin-ID</risk-metric>
             <risk-metric name="iavm-severity"
                                   system="scanner-name"></risk-metric>
             <risk-metric name="AV"
                                   system="CVSSv3.1">network</risk-metric>

             <risk-metric name="vulnerability-id"
                                   system="CVE">CVE-2020-00000</risk-metric>

             <risk-metric name="impact"     class="initial"
                             system="scanner-name">tool-provided-severity</risk-metric>
             <risk-metric name="impact"     class='initial'
                             system="https://fedramp.gov">high</risk-metric>
             <risk-metric name="likelihood" class='initial'
                             system="https://fedramp.gov">high</risk-metric>
             <risk-metric name="priority"
                             system="https://fedramp.gov">1</risk-metric>

             <risk-statement>
                <p>This is the tool-provided statement about the identified risk.</p>
                <p>This field must be present.</p>
                <p>If no risk statement from tool, set to 'No Risk Statement'.</p>
             </risk-statement>

             <!-- remediation: recommendation -->

             <risk-status>open</risk-status>
          </risk>
     </results>
```

For information about the remediation assembly, see *Section* ***Error! Reference source not found., Error! Reference source not found.***.

[Image intentionally left blank.]

Accepted Values

- The type flag on the remediation field:
    - **recommendation**
    - **planned**
    - **final**
- The type flag on the recommendation-origin field :
    - **party**
    - **tool**

The description fields are *Markup multiline*, which enables the text to be formatted. See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.3.3. Recommended and Planned Remediation

For the risk assembly, there must be a remediation assembly containing the tool's recommended mitigation. The type flag must be set to "recommendation".

There must also be a remediation assembly containing the CSP's intended mitigation plan. The type flag must be set to "planned".

When the risk is closed, there must be a third remediation-assembly with a type value of "final".

For the tool recommended remediation, the recommendation-origin field's type flag should be set to "tool", and the uuid-ref should contain the UUID of the tool that generated the recommendation.

For the CSP's planned and final remediation, the recommendation-origin field's type flag should be set to "party", and the uuid-ref should contain the UUID of either the CSP itself or the ISSO overseeing the activities.

Representation

```
   <results id="results-2">
      <!-- title, description, start, end -->
      <finding id="finding-1">
         <title>TCW Objective</title>
         <description><p>May be empty.</p></description>
         <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
         <!-- objective-status -->
         <!-- observation -->
         <!-- . -->
         <risk uuid="1689ec06-100a-4fed-9df9-e69f07d3f3c9">
            <!-- title, description, likelihood, impact, risk-statement -->

            <remediation uuid="fde4758d-6417-4f35-ba71-278af4f008f8"
                                                               type="recommendation">
               <title>Assessor's Recommendation</title>
               <description>
                  <p>A description of the Recommendation for Remediation.</p>
               </description>
               <recommendation-origin type="party"
                                  uuid-ref="49f73135-efab-4275-9a79-003656ad890a" />
            </remediation>

            <remediation uuid="9c3be116-9be2-4e34-b9ce-4f2b49975133"
                                                               type="recommendation">
               <title>Tool-Provided Recommendation</title>
               <description>
                  <p>A description of the Recommendation for Remediation.</p>
               </description>
               <recommendation-origin type="tool"
                                  uuid-ref="9d194268-a9d1-4c38-839f-9c4aa57bf71e" />
            </remediation>


            <!-- risk-status -->
         </risk>
      </finding>
   </results>
```

See the next page for XPath Queries.

[Image intentionally left blank.]

4.3.4. Evidence and Artifacts

All artifacts reviewed and all evidence collected must be attached (by link or embedded Base64) as a resource in the back-matter. See the *Guide to OSCAL-based FedRAMP Content*, *Section 2.6, Citations, Attachments, and Embedded Content in OSCAL Files* for more information.

Evidence must have the FedRAMP extension "`type`" with the value set to "`evidence`".

Reviewed Artifacts must have the FedRAMP extension "`type`" with the value set to "`artifact`".

Additional type fields may also be add with values such as plan, policy, or image. This adds clarity and can ensure specific tables are generated properly.

Artifacts may be cited from an `observation` as an `observation-source`.

Evidence may be cited from an `observation` as `relative-evidence`.

A SAR tool could use either an `rlink` or `base64` field here, and may use both. If both are present, FedRAMP tools will give preference to the `base64` content. If an `rlink` is used, its href should have a relative path to ensure the path remains valid when the OSCAL content is delivered to FedRAMP.

Tools may include multiple `rlink` fields for the same resource. This may be useful if an assessor wanted to maintain an absolute link to the file's authoritative source location as well as a relative link suitable for delivery to FedRAMP.

Representation

```
<!-- results -->
<back-matter>
   <resource uuid="65fb91b1-f7dc-46bf-8b99-bd98f1a5293d">
      <title>[EXAMPLE]Interview Notes</title>
      <prop name="type" ns="https://fedramp.gov/ns/oscal">evidence</prop>
      <rlink media-type="application/msword" href="./interview-notes.docx"></rlink>
      <base64 media-type="application/msword"
                                  filename="interview-notes.docx">00000000</base64>
   </resource>

   <resource uuid="f32b7ab1-baf1-451a-b3a1-1dfdadbe8dc7">
      <title>[EXAMPLE]AC Policy</title>
      <prop name="type" ns="https://fedramp.gov/ns/oscal">artifact</prop>
      <prop name="type" ns="https://fedramp.gov/ns/oscal">policy</prop>
      <prop name="version">2.1</prop>
      <prop name="publication">2018-11-11T00:00:00Z</prop>
      <rlink media-type="application/pdf" href="./artifacts/AC_Policy.pdf"></rlink>
      <base64 media-type="application/pdf" filename="AC_Policy.pdf">00000000</base64>
   </resource>

   <resource uuid="53af7193-b25d-4ed2-a82f-5954d2d0df61">
      <title>[EXAMPLE]Screen Shot</title>
      <prop name="type" ns="https://fedramp.gov/ns/oscal">evidence</prop>
      <rlink media-type="image/jpeg" href="./evidence/screen-shot.jpg"></rlink>
      <base64 media-type="image/jepg" filename="screen-shot.jpg">00000000</base64>
   </resource>
</back-matter>
```

APPENDICIES

APPENDIX A. CVSS SCORING

Common Vulnerability Scoring System (CVSS) metrics may be added to any risk-assembly using `prop` fields.

The FedRAMP OSCAL Registry includes a tab with the specific `name` and `class` flag values to use for CVSS versions 2, 3 and 3.1. An OSCAL file may use either the all upper-case abbreviation, or the all lower-case name for each CVSS metric.

Representation

```
   <results id="results-2">
      <!-- title, description, start, end -->
      <finding id="finding-1">
         <title>TCW Objective</title>
         <description><p>May be empty.</p></description>
         <date-time-stamp>2020-03-01T10:11:12Z</date-time-stamp>
         <!-- objective-status -->
         <!-- observation -->
         <risk id="risk-3-1">
            <title>Vulnerability Title</title>
            <description />

            <!-- CVSS Metrics using V3.1 abbreviations -->
            <risk-metric name="AV" system="CVSSv3.1"
                  ns="https://fedramp.gov/ns/oscal">network</risk-metric>

            <risk-metric name="AC" system="CVSSv3.1"
                  ns="https://fedramp.gov/ns/oscal">high</risk-metric>

            <risk-metric name="PR" system="CVSSv3.1"
                  ns="https://fedramp.gov/ns/oscal">low</risk-metric>

            <!-- CVSS Metrics using V3.1 names -->
            <risk-metric name="access-vector"       class="CVSSv3.1"
                  ns="https://fedramp.gov/ns/oscal">network</risk-metric>

            <risk-metric name="access-complexity"   class="CVSSv3.1"
                  ns="https://fedramp.gov/ns/oscal">high</risk-metric>

            <risk-metric name="privileges-required" class="CVSSv3.1"
                  ns="https://fedramp.gov/ns/oscal">low</risk-metric>

         <!-- risk-statement -->
         <!-- risk-status -->
         </risk>
         <!-- party-id -->
      </finding>
```

At this time, CVSS metrics in OSCAL has not been formally coordinated with NIST nor the Forum of Incident Response and Security Teams (FIRST), and must be treated as a FedRAMP Extension.